GUÍA GENERAL PARA LA ELABORACIÓN DE PLANES DE RECUPERACIÓN DE DESASTRES DESDE EL PMI EN LAS ÁREAS DE TECNOLOGÍA INFORMÁTICA DE LAS EMPRESAS PEQUEÑAS Y MEDIANAS EN BOGOTA D.C.

YISEL ADRIANA ROMERO ROMERO

UNIVERSIDAD DE LA SALLE

FACULTAD DE INGENIERÍA

POSGRADOS EN INGENIERÍA

MAESTRÍA EN INGENIERÍA

BOGOTÁ D.C.

2014

GUÍA GENERAL PARA LA ELABORACIÓN DE PLANES DE RECUPERACIÓN DE DESASTRES DESDE EL PMI EN LAS ÁREAS DE TECNOLOGÍA INFORMÁTICA DE LAS EMPRESAS PEQUEÑAS Y MEDIANAS EN BOGOTA D.C.

YISEL ADRIANA ROMERO ROMERO

Trabajo de grado para optar el título de

Magíster en Ingeniería con Énfasis en Gestión de Proyectos

Director

MSc. DIANA JANETH LANCHEROS CUESTA

UNIVERSIDAD DE LA SALLE

VICERRECTORÍA ACADÉMICA

FACULTAD DE INGENIERÍA

MAESTRÍA EN INGENIERÍA

BOGOTÁ D.C.

2014

Nota de aceptación:

_____

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Bogotá D.C., 26 de noviembre de 2014

DEDICATORIA

Este trabajo de grado está dedicado a Dios quien me da la sabiduría y los recursos para estudiar y crecer profesionalmente, a las personas más importantes en mi vida, mi familia y mi amado esposo, quienes siempre están a mi lado, para brindarme su amor y apoyo en cada instante de mi vida. Finalmente uno de los motivos qué me han llevado a soñar y esforzarme para brindarle lo mejor de los años de mi vida y antes de su nacimiento; a mi hijo(a).

Gisell Adriana Romero Romero

AGRADECIMIENTOS

Quiero agradecer a las personas que aportaron en el desarrollo de la tesis de grado, con sus sugerencias, correcciones, seguimiento y motivación.

A mis asesores, Ingeniero Hernando Peña, Ingeniera Diana Lancheros, por su dedicación y compromiso durante la ejecución de este proyecto.

A la Ingeniera María Lucía Muñoz quien me aportó, grandes conocimientos como experta en el tema de Plan de Recuperación de Desastres.

A la ingeniera Sonia Camargo que con su seguimiento me aportó a tener siempre presente el compromiso de terminar la tesis

Finalmente a mis compañeros de la maestría que con sus sugerencias y motivaciones fueron un significativo apoyo en momentos de desmotivación.

TABLA DE CONTENIDO

LISTA DE CUADROS

pág.

LISTA DE ILUSTRACIONES

Pág.

LISTA DE ANEXOS

RESUMEN

La guía para la elaboración de planes de recuperación de desastres está basada en los estándares del PMI “Instituto de Gestión de Proyectos” aplicando los conceptos de gerencia de proyectos enfocada en las áreas de tecnología informática de las empresas medianas y pequeñas en Bogotá D.C., presentando un modelo de referencia en el cual se describe por medio de un conjunto de acciones gerenciales cómo implementar el DRP “Plan de Recuperación de Desastres” en las empresas, diseñando un metodología para realizar un análisis de impacto del negocio y su relación con las situaciones posibles de riesgos.. Además se realiza un análisis acerca de la importancia de un DRP en las áreas de tecnología informática para las empresas medianas y pequeñas en Bogotá D.C.; Finalmente con la evaluación de un experto y auditores de sistemas informáticos se valida la viabilidad de la guía propuesta.

ABSTRACT

The guide to elaborate disaster recovery plans is based on PMI (Project Management institute) standards, applying concepts of management project and it is focused in technology departments in medium and small enterprises in Bogota D.C, it shows a reference model that describes through a group of management actions how to implement a DRP in these enterprises, it designing a methodology to perform a business impact analysis and its relation with possible risks, additionally is performed an analysis about the importance of an DRP implementation in technology department in medium and small companies in Bogota D.C. Finally, with the evaluation of an expert and system information auditors is validated the viability of proposed guide.

INTRODUCCIÓN

El presente trabajo de investigación ha sido fundamentado en la necesidad de implementar planes de recuperación de desastres (DRP) en las empresas pequeñas y medianas en Bogotá D.C., con el propósito de preservar el activo más preciado, como lo es la información, proveniente del hardware y software de las áreas de tecnología informática, ya que al no disponer de normas, políticas, procedimientos y metodologías al momento de restaurar los servicios de las aplicaciones y equipos se producen cuantiosas pérdidas económicas.

En la actualidad para las empresas pequeñas y medianas en Bogotá D.C, no existe un ente regulador que les exija tener planes de recuperación de desastres, pero lo más alarmante es que este grupo de empresas no está dando la importancia necesaria a la seguridad y protección de la información, al no tener en sus organizaciones planes que garanticen la confiabilidad, disponibilidad e integridad de la misma.

Es evidente que las empresas no están cuantificando las pérdidas financieras que pueden llegar a experimentar ante la no implementación de un DRP. Incluso es muy probable que en su mayoría, este grupo de empresas no haya identificado los riesgos a los cuales se encuentran expuestos, al no disponer medidas de seguridad que eviten estas amenazas, tanto que en situaciones extremas pueden hasta llegar, con un cierre definitivo, por causa del desconocimiento y falta de planeación en este ámbito.

Los planes de recuperación de desastres ayudan a garantizar, −para cualquier evento de desastre inesperado− el conocer y disponer de un plan para responder durante y después del incidente,

logrando que los procesos del área de tecnología informática no interfieran con los servicios, tanto internos como externos de la empresa.

La presente tesis pretende diseñar una guía para la elaboración de planes de recuperación de desastres desde el PMI en las áreas de tecnología informática de las empresas pequeñas y medianas en Bogotá D.C., con el propósito de que las empresas puedan tener una visión general para desarrollar e implementar el DRP, garantizando la continuidad y la protección de la información por medio de un conjunto de acciones gerenciales.

Por lo tanto dentro del desarrollo de la guía se tiene en primera instancia realizar un diagnóstico de implementación del DRP por medio de una muestra para empresas pequeñas y medianas en Bogotá D.C., con el propósito de tener una conclusión general de cómo se encuentran las empresas actualmente frente a los planes de recuperación de desastres, aportando al desarrollo de la guía general para la elaboración de planes de recuperación de desastres, descritos por medio de etapas, actividades, entregables y propuestas en forma de ejemplo para en el momento realizar un análisis de impacto y la identificación de los riesgos que pueden presentarse en el área tecnología informática, con el propósito de ser evaluada finalmente por expertos.

1. GENERALIDADES

En este capítulo se presentan los temas relacionados con la investigación y el caso de estudio para su desarrollo. Asimismo, se expone el planteamiento del problema, los objetivos del estudio, el alcance, la delimitación, la justificación, y finalmente los antecedentes.

1.1 PLANTEAMIENTO DEL PROBLEMA

En esta sección se expone el problema que se ha venido presentando y presentan las empresas por la falta de planes de recuperación de desastres, iniciando con la descripción o contextualización y posteriormente con la formulación del problema.

1.1.1 Descripción del problema

Actualmente en las organizaciones existe una dependencia de los datos o la información, convirtiéndose ésta, en un activo valioso, el cual no puede estar significativamente expuesto a ningún peligro o amenaza. Es por ello que la seguridad informática se ha convertido en una prioridad, que ayuda a garantizar la confidencialidad, integridad y disponibilidad de la información debido a que hoy en día también existen diferentes tipos de riesgos, como por ejemplo; los problemas de hardware y software, virus informáticos y catástrofes naturales, los cuales ocasionan interrupciones en un servicio o pérdida de información, impactando de forma crítica en las finanzas corporativas.

Por los motivos expuestos anteriormente es necesario evaluar ¿Qué tan preparadas se encuentran las organizaciones para afrontar este tipo de impactos teniendo en cuenta los factores tecnológicos, talento humano, planes, políticas o procedimientos, recursos y viabilidad de la empresa para continuar sin algunos de sus procesos fundamentales? ¿Las empresas poseen planes de continuidad del negocio que les permitan identificar los impactos que pueden afectarlas?

De esta forma es preciso identificar que el plan de continuidad del negocio (BCP), es: *un conjunto de procedimientos y estrategias definidos para asegurar la reanudación oportuna y ordenada de los procesos del negocio generando un impacto mínimo o nulo ante una contingencia, es una metodología que abarca a toda la organización y el objetivo es identificar los impactos resultado de interrupciones en la operación y escenarios de desastre que puedan afectar la operación de una empresa así como las técnicas para cuantificar y calificar dichos impacto.* (Plan de Recuperación de Desastres DRP, 2013) Por lo tanto las empresas deberían contemplar e identificar los impactos que pueden afectar a toda la organización y de esta manera mitigar cualquier impacto de desastre, por medio de los planes de continuidad.

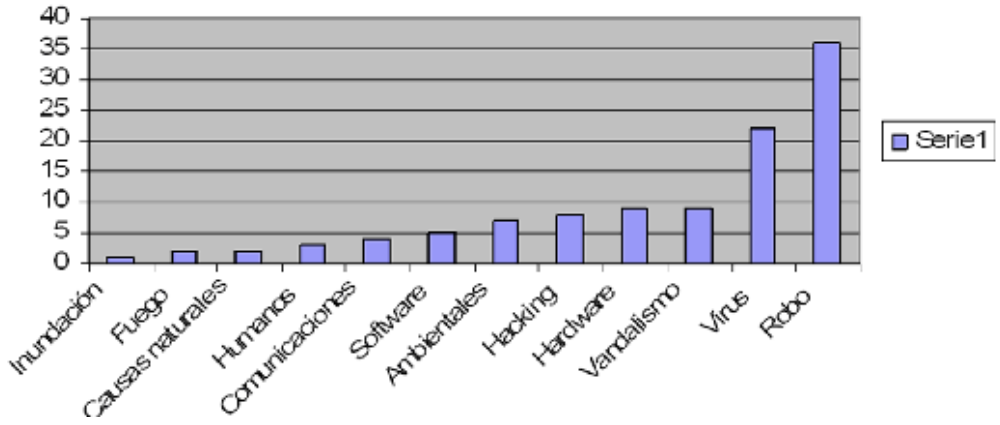
Ahora para el caso en que se requiera iniciar con un plan enfocado únicamente para las áreas de tecnología informática, surge entonces el plan de recuperación de desastres (Disaster Recovery Plan) plan por medio del cual y sirviéndose de procesos de recuperación, se ayudará a preservar el hardware y el software de un negocio.

Entonces, cuando una empresa desee comenzar de nuevo con sus operaciones en caso de un desastre natural o causado por humanos, el DRP al ser un proceso ejecutable y auto-sostenible de

recuperación, asegurará la reintegración de los procedimientos, aplicaciones, operaciones, sistemas, redes e instalaciones, que son críticos para la continuidad de negocio, por lo tanto este plan permitirá contar con la capacidad para restablecer la infraestructura tecnológica de la organización en caso de una disrupción severa.

Las preguntas para describir la problemática de la tesis están planteadas para conocer en primera instancia ¿Qué tan conscientes están las empresas ante un desastre? Como lo muestra la ilustración 1, acerca de una estadística de las frecuencias de las amenazas que se pueden presentar en una empresa.

Ilustración 1. Frecuencia de las amenazas.



Fuente: (Latam, 2008) Risk Management for your business

En una segunda instancia, la siguiente pregunta que surge para describir la problemática, es para el caso en que las empresas sean conscientes de los desastres a los cuales se encuentran expuestos, ¿Por qué las empresas no implementan o no poseen un DRP? si el plan de recuperación de desastres es una alternativa en el momento de mitigar los riesgos asociados a las empresas.

1.1.2 Formulación del problema

Lo anterior conduce a la siguiente pregunta: ¿Existe una guía general para la elaboración de planes de recuperación de desastres o un proceso que diseñe cómo se debe de implementar, para las empresas pequeñas y medianas en Bogotá D.C.?

1.2 OBJETIVOS DEL ESTUDIO

En el estudio se plantearon los siguientes objetivos:

1.2.1 Objetivo general

Diseñar una guía general para la elaboración de planes de recuperación de desastres, por medio de una muestra de 7 (siete) empresas pequeñas y medianas en Bogotá D.C. en las áreas de tecnología informática desde el Project Management Institute (PMI)

1.2.2 Objetivos específicos

- ✓ Realizar un diagnóstico del conocimiento y grado de implementación de un plan de recuperación de desastres en el segmento de empresas medianas y pequeñas en Bogotá D.C., a partir de una muestra por sectores no regulados.

- ✓ Proponer el conjunto de acciones gerenciales desde el PMI, que se use como la guía general para la elaboración de planes de recuperación de desastres en las empresas pequeñas y medianas no reguladas en Bogotá D.C.

- ✓ Validación de la guía general para la elaboración de planes de recuperación de desastres por un experto en DRP y al menos 2 auditores de sistemas informáticos.

1.3 ALCANCE Y DELIMITACIÓN

En esta sección se establece hasta dónde llega la investigación, fijando límites y el alcance de la misma, pero al mismo tiempo dejando planteada la posibilidad de otras investigaciones.

1.3.1 Alcance

Este trabajo de investigación propone una guía general para elaborar un plan de recuperación de desastres en las empresas pequeñas y medianas en Bogotá D.C. que se utilice para ayudar a garantizar la continuidad del negocio, aplicando el marco de referencia establecido por el PMI® Finalmente, el diseño de la guía será validado por medio de un experto de DRP y mínimo 2 auditores de sistemas.

1.3.2 Delimitación

Se presenta una guía general para la elaboración de planes de recuperación de desastres desde el PMI en las áreas de Tecnología Informática para las empresas pequeñas y medianas en Bogotá D.C., describiendo por medio de acciones gerenciales, las etapas y las actividades propuestas, cómo se debe implementar, junto con los entregables necesarios que se deben documentar.

1.4 JUSTIFICACIÓN

El siguiente trabajo proyecta dar a conocer a las personas y a las organizaciones que la aplicación e implementación de un Plan de recuperación de desastres, permite disminuir la posibilidad de

ocurrencia de un incidente disruptivo o ayuda a las organizaciones a estar preparadas cuando algún incidente ocurra.

De la misma forma, es importante resaltar que actualmente la recuperación de desastres ha cobrado real importancia en la informática empresarial, pues es gracias a este recurso que las organizaciones pueden tener un plan de acción que les permita mantenerse firmes ante una adversidad y así prolongar su vida útil por un largo periodo de tiempo. Hoy en día, las organizaciones deben garantizar a sus aliados, clientes y demás involucrados, la capacidad de responder de forma madura y eficiente a cualquier situación de incidencia que ponga en riesgo la estabilidad de la empresa.

En la misma línea de lo expuesto previamente, los planes de recuperación de desastres han cobrado real importancia en la informática empresarial, pues es gracias a este recurso, que las organizaciones pueden tener un plan de acción, que les permita mantenerse firmes ante una adversidad y así prolongar su vida útil por un largo periodo de tiempo.

La guía se desarrolla con el propósito de aportar a la elaboración e implementación de planes de recuperación de desastres, específicamente en las áreas de tecnología informática para las empresas pequeñas y medianas en Bogotá D.C., especificando que el segmento de las 7 (siete) empresas entrevistadas, con las cuales se realizó el diagnóstico para la investigación, son empresas no reguladas, es decir son aquellas que actualmente no poseen un ente regulador que les demande implementar un DRP, por ello, esta guía asimismo pretende generar conciencia de la necesidad de garantizar la protección de la información y estar preparados cuando algún

evento no esperado ocurra, sin tener una norma que regule a las empresas acerca de los planes de recuperación de desastres.

1.5 ANTECEDENTES

Dentro de la información encontrada para la investigación referente al trabajo del Plan de recuperación de desastres, se identificó que en las bases de datos por ejemplo como Science Direct y Scopus entre otras, que gran parte de los estudios, guías, normas y libros son de nivel internacional y reflejan la gran importancia de implementar el DRP en las organizaciones. A continuación se relacionan algunos antecedentes;

El primero de ellos a mencionar es la guía para crear un plan de recuperación en caso de desastre en el sistema informático del centro de datos de un grupo financiero, por Jorge Salazar Villalobos, realizado en el año 2008, en esta investigación el autor presenta una guía que permite crear un procedimiento de recuperación ante desastres, para el sistema informático de tarjeta de crédito ubicado en el centro de datos de un grupo financiero. Otro documento que habla acerca de la continuidad del negocio y planificación de recuperación de desastres realizada por Marcos Eric Conrad, Seth Misenar, Josué Feldman en el año 2010, se resume como el plan de continuidad del negocio y recuperación de desastres de Planificación (BCP / DRP) que se ha convertido en un dominio crítico en el cuerpo común de conocimientos. Finalmente se relaciona un documento, denominado el Plan de Recuperación de Desastres, base fundamental en la Continuidad del Negocio de Pacific Rubiales Energy, realizado por Villamil Granada, Leoncio Felipe en el año 2014, en este artículo se presenta un análisis sobre los componentes que deberá tener un plan de recuperación de desastres informático en Pacific Rubiales Energy, alineado con

las mejores prácticas de continuidad del negocio así como los objetivos estratégicos del negocio para la toma de decisiones de la alta Gerencia que le permitan mantener la operación en condiciones de emergencia, mitigando el riesgo de pérdida de producción y en consecuencia una correspondiente pérdida de valor de la acción en las bolsas de valores.

2. MARCO DE REFERENCIA

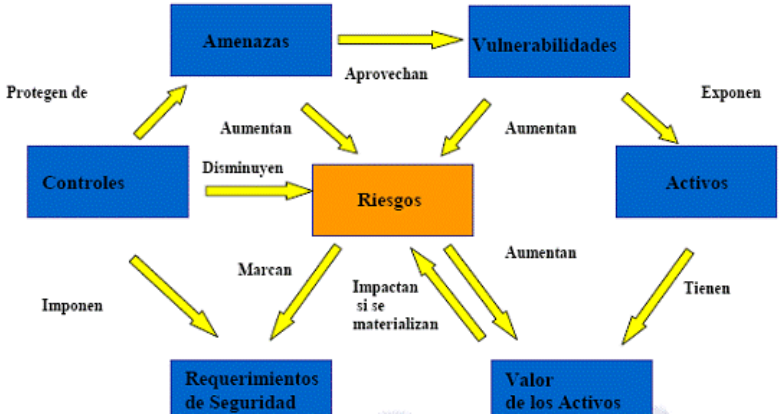
En este capítulo se tratan los temas que permiten al lector ubicarse espacial y temporalmente de tal forma que logre una comprensión del proyecto de investigación y para ello se desarrolla el marco teórico, el marco conceptual, el marco legal, el marco geográfico y finalmente el marco metodológico.

2.1 MARCO TEÓRICO

2.1.1 Seguridad informática

Es el área, que se enfoca en la protección del software y hardware de una empresa, *"además de todo lo que la organización valore como activo y signifique un riesgo, para el caso en que, esta información confidencial, llegue a manos de otras personas, convirtiéndose, en información privilegiada"*. (Arcos, 2011), es por ello que las empresas deben garantizar que toda la información que poseen, tanto propia como la de las empresas donde prestan sus servicios, se encuentren aseguradas con medidas que reduzcan o eliminen todos los riesgos asociados a este activo, cómo lo muestra la ilustración 2.

Ilustración 2. Gestión de la seguridad de la información



Fuente: (Duque, 2012) Gestión Calidad Consulting

Estas amenazas o vulnerabilidades que pueden presentarse en una organización, cómo la negación del servicio, virus informáticos, divulgación no autorizada de información, usos indebidos, interrupción, destrucción no autorizada de la información, causados voluntariamente o involuntariamente desde la propia empresa, fraude, espionaje, sabotaje, vandalismo, riesgos provocados por accidente o los riesgos ocasionados por catástrofes naturales, son riesgos que afectan directamente a los activos de una empresa, en el momento que existan formas de acceso o brechas que no controlen o mitiguen estos riesgos, ya que ocasionan en la mayoría de las veces, pérdidas de recursos que nunca habían sido contemplados ni cuantificados.

Señalando de esta manera que toda organización, está expuesta a cualquier tipo de amenazas, y las áreas de tecnología informática tienen como responsabilidad frente a la información contenida y circulante, garantizar la confidencialidad, integridad y disponibilidad, como lo expone la ISO2007: *La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización. La confidencialidad, integridad y disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad,*

conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos (ISO 27000, 2012).

Por lo tanto a las organizaciones, les corresponde validar las herramientas de protección que más se les adecúen, con el propósito de implementar mecanismos de seguridad que sean renovados contantemente, con el propósito que marchen de la mano con los avances tecnológicos y de esta forma tener un nivel parejo de seguridad, logrando garantizar la seguridad informática.

2.1.2 Plan de continuidad de negocio

El Plan de Continuidad del Negocio (BCP), es un proceso que se implementa en las organizaciones para prevenir interrupciones que afecten el desempeño o servicios de las actividades de una organización, permite además, evitar o minimizar su impacto (económico y duración), ante un evento de riesgo. Pero existe un antes y un después en el mundo de la continuidad de negocio, por ello es importante mencionar cómo se inicia la necesidad de generar planes de continuidad del negocio.

> *"Hasta los tristes acontecimientos del 11 de septiembre del 2001 existía cierta conciencia de la necesidad de establecer planes de recuperación ante desastres, la mayoría de veces circunscrita a determinados entornos (como el militar, "padre" de la continuidad, o el sector financiero) y, muy especial, a sus entornos de tecnologías de la información"* (Hervías, Gestionando la Continuidad del nuestro negocio, 2010).

Después de este suceso, se inicia una nueva etapa dentro las organizaciones con el Plan de Continuidad del Negocio (BCP), como un proceso vital a desarrollar, considerado parte integral de la estrategia del negocio.

En noviembre del 2006, se publica la norma BS25999, como un estándar internacional, la cual se convierte en una norma certificable, seguida de más de 50 normas, regulaciones, estándares y guías relacionadas con la gestión de riesgos y la continuidad del negocio.

De esta forma surgen diferentes enfoques e investigaciones acerca del plan de continuidad del negocio, por ejemplo el instituto Británico, *BCI (Business Continuity Institute), recoge las dos metodologías más extendidas para la gestión de la continuidad* y el instituto Estadounidense, *DRII (Disaster Recovery Internacional Institute), define la Gestión de la Continuidad del Negocio (BCP) como el "proceso de desarrollar acuerdos previos y procedimientos que permitan a una organización responder un evento de modo que las funciones críticas del negocio continúen con los niveles de interrupción o cambios esenciales planificados* (Hervías, Gestionando la Continuidad de nuestro negocio, 2010), Logrando de esta manera generar nuevos cambios en las organizaciones al momento de pensar en la continuidad de su negocio.

2.1.3 Importancia del plan de continuidad del negocio

El Plan de Continuidad de Negocio debe ser considerado como un proceso fundamental dentro de una organización, ya que de éste depende su supervivencia o continuidad, puesto que determina cuáles son los puntos bajo los cuales la organización no puede dejar de operar para

que siga en pie, permitiendo que la empresa continúe brindando sus servicios cuando ocurra un desastre o una interrupción de las actividades.

Ignorar el Plan de continuidad del negocio, traería consigo grandes pérdidas al negocio ya que sin su implementación no les permitirá conocer factores relevantes como su operación, tiempo estimado de entrega, entrega de materia prima, programación de producción, entre otros factores. Por lo tanto la viabilidad y continuidad del negocio es una de las mayores intranquilidades de los gerentes de las empresas; por esta razón, suelen invertir en estudios de mercado que les permitan incrementar sus ventas y determinar acciones de mejora que le permitan a la organización adaptarse de mejor manera a los cambios del entorno.

Es así como la necesidad de implementación de un Plan de continuidad de negocio se hace evidente, pues de éste depende directamente la vida útil de la organización y su mantenimiento en una línea del tiempo larga y a la vez estable.

2.1.4 Plan de recuperación de desastres (DRP)

El DRP, es un proceso que se realiza en las áreas de tecnología informática de las empresas, el cual por medio de un documentado establece estrategias y procedimientos para recuperar y proteger la infraestructura tecnológica en caso de un desastre, lo anterior lo podemos confirmar con la siguiente definición; *El plan de recuperación ante desastres (del inglés Disaster Recovery Plan) es un proceso de recuperación que cubre los datos, el hardware y el software crítico, para que un negocio pueda comenzar de nuevo sus operaciones en caso de un desastre natural o causado por humanos.* (wikipedia, 2014)

En el DRP, se describen los procedimientos esenciales que debe ejecutar la organización para proteger la infraestructura tecnológica antes o en caso de un desastre (que afecten datos, hardware o software) ya sea natural, intencional o involuntario, e impida la continuidad del negocio, además define unas estrategias con una combinación de medidas preventivas, detectivas y correctivas.

Para el caso de las medidas preventivas, la función principal es identificar anticipadamente los eventos no deseados antes de suceder; las medidas detectivas identifican los eventos antes del momento de presentarse y las medidas correctivas aseguran la toma de acciones para restituir un evento no deseado; lo anterior implica contemplar todas las medidas para cuando se produzca una contingencia que afecte al negocio y ejecutar continuamente frente a un riesgo el siguiente proceso:

1. *Eliminar la amenaza completamente*
2. *Minimizar la probabilidad de que ocurra*
3. *Minimizar el efecto*. (ISO27001, 2014)

De esta forma, pueden verse estas medidas como directrices para los servicios de recuperación de desastres de las tecnologías de información y comunicaciones.

Pero, cuando llega el momento de implementar un DRP en las empresas, a menudo no se conoce cómo se debe desarrollar, para esto es transcendental tener en cuenta unos aspectos importantes

para su desarrollo, como los mencionan algunos autores, que han escrito acerca de los planes de recuperación de desastres.

En la primera etapa del DRP, se debe pensar inicialmente en el desastre. Aquí es necesario imaginar la posibilidad de ocurrencia de toda clase de riesgos, que se pueden presentar en la empresa, por ejemplo se podría hacer la siguiente pregunta ¿Qué pasaría si dentro de la empresa se presenta un incendio? ¿Cómo sería el escenario de recuperación? Para una segunda etapa se debe tener presente la gestión humana del riesgo, siendo esto, un punto vital dentro la implementación de un DRP, es donde se escogerá el personal idóneo para asumir los roles para controlar las crisis.

Dentro de la implementación del DRP se debe realizar un inventario de las aplicaciones, se debe evaluar cada módulo para determinar su criticidad en caso de crisis y el trato que debe dársele, permitiéndonos conocer la necesidad del respaldo y restauración de datos e información, además, se debe llegar a considerar, a continuación, la falta de disponibilidad en función del grado de criticidad de los datos, de las actividades y los procesos técnicos o tecnológicos.

Algunos DRP prevén la construcción de instalaciones en un lugar distante, el cual será el que tomará control en caso de desastre en las instalaciones principales, para cuando inicie la situación en crisis en las organizaciones.

A partir de esta toma de conciencia, se podrá calcular y negociar un valor de la implementación, definiendo las prioridades y las técnicas, por ejemplo, si el respaldo de los datos y la

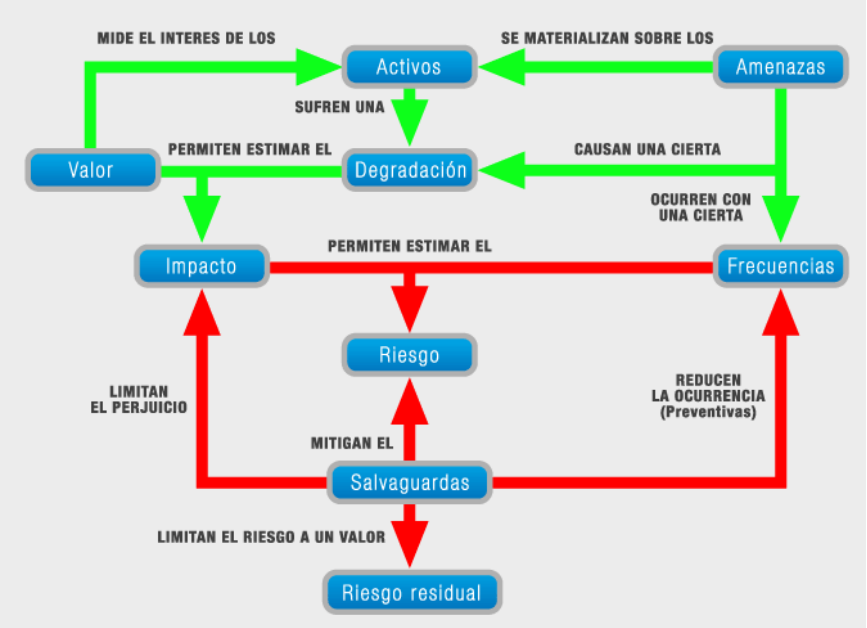
recuperación de las actividades deben efectuarse en menos de un minuto, se deben implementar entornos síncronos y el coste de la infraestructura se elevará.

2.1.5 Análisis del impacto al negocio (BIA)

El propósito fundamental del Análisis de Impacto sobre el negocio, conocido más comúnmente como BIA, (Business Impact Análisis) pretende identificar los diferentes sucesos que podrían impactar en la continuidad de las operaciones, sus finanzas, el talento humano, la legalidad y la reputación de la organización.

Para llevar a cabo este procedimiento con éxito, es necesario diseñar una metodología de análisis y gestión de riesgos, ver ilustración 3, donde se puedan identificar los procesos claves de la organización y se puedan tener presentes tres aspectos para el análisis de los riesgos *: La criticidad de los recursos de información relacionados con los procesos críticos del negocio, El período de recuperación crítico antes de incurrir en pérdidas significativas* y finalmente el *Sistema de clasificación de riesgos"* (Sánchez N. , 2013),

Ilustración 3. Metodología de análisis y gestión de riesgos de los sistemas de información.



Fuente: (Camelo, 2010) MAGERIT

Asimismo, se pueden establecer los recursos de información que se encuentran en mayor estado crítico como aplicaciones, datos, redes, software de sistema, instalaciones o centros de procesamiento, etc. Es una de las formas como se realiza un plan de gestión de riesgo en el momento de realizar el análisis de impacto.

El BIA está conformado por una serie de componentes claves que son necesarios para continuar con la operatividad del negocio transcurrido un incidente; entre estos cabe resaltar:

- Personal requerido
- Áreas de trabajo
- Registros vitales- *Backups* de información
- Aplicativos Críticos
- Dependencias de otras áreas

- Dependencias con Terceras partes
- Criticidad de los recursos de información
- Participación del personal de Seguridad Informática y los usuarios finales
- Análisis de todos los tipos de recursos de información

2.1.6 Diseño de un DRP

A continuación se describen los pasos o la metodología que comúnmente se ha venido planteando, para la ejecución del Plan de Recuperación de Desastres, este conjunto de prácticas abarca áreas como:

• **Iniciación y Gestión del proyecto**

En el comienzo del proyecto, se delimitan los objetivos, el alcance, estimación de tiempos, costos, recursos humanos, materiales y financieros del proyecto, además se realiza una evaluación de los riesgos para iniciar con su previa gestión.

• **Evaluación y control de riesgo**

La evaluación es el proceso mediante el cual se identifica el peligro o se estima el riesgo, valorando la probabilidad y las consecuencias de que se materialice el peligro, para así adoptar medidas preventivas para eliminar o reducir el riesgo.

• Análisis de impacto del negocio

Es una parte clave del proceso de continuidad del negocio, que analiza funciones de negocio de gestión crítica, e identifica y cuantifica el impacto que podría tener en la organización.

• Estrategias de la Gestión de Continuidad del Negocio

La gestión de la continuidad del negocio deberá incluir al proceso de evaluación, controles para la identificación y reducción de riesgos, limitar las consecuencias de incidencias dañinas y asegurar la reanudación a tiempo de las operaciones esenciales.

• Respuesta a emergencias y operaciones

Una respuesta eficaz ante una emergencia debe estar liderada por un departamento dentro de la organización, quienes serán los encargados del análisis y seguridad de la información, de conducir la planificación para casos de emergencia y hacer las veces de servicio de alerta temprana. También emprender evaluaciones rápidas de las necesidades y prestar asistencia en el desarrollo de un marco estratégico de respuesta. Asimismo, proponer políticas y estrategias que aseguren a toda la organización en todos sus ámbitos. Además debe ofrecer orientación con relación a la función que ha de desempeñar en la preparación y mitigación de crisis. Este Departamento establece las normas institucionales y se encarga de la supervisión operativa de las respuestas ante desastres naturales.

2.1.7 Metodología PMI

Con el propósito de aplicar los conocimientos adquiridos durante la maestría en ingeniería con énfasis en gestión de proyectos, se estableció diseñar la guía general para la elaboración de planes de recuperación de desastres desde el PMI, Es por esto, que en el momento de seleccionar, cómo gestionar un proyecto para la elaboración del DRP por medio de una guía, se selecciona la metodología del PMI, basada en las mejores prácticas existentes para la administración de proyectos, recogidas en el PMBOK, la cual, ofrece unos lineamientos que aportan a la ejecución de proyectos exitosos, aplicando los conocimientos, habilidades, herramientas y técnicas que contribuyen a las etapas y actividades requeridas para este proyecto.

2.2 MARCO CONCEPTUAL

Para los efectos de la presente investigación, una vez desarrollado el proceso de búsqueda, interpretación y clasificación, se definieron los siguientes conceptos, pertinentes para su aplicación.

2.2.1 Plan de Continuidad de Negocio (BCP):

Es un proceso que se implementa en la organizaciones para prevenir interrupciones que afecten el desempeño o servicios de las actividades de una organización, permite además, evitar o minimizar su impacto (económico y duración), en un evento de riesgo.

2.2.2 Desastres:

"Es un evento calamitoso, repentino o previsible, que trastorna seriamente el funcionamiento de una comunidad o sociedad y causa unas pérdidas humanas, materiales, económicas o ambientales que desbordan la capacidad de la comunidad o sociedad afectada para hacer frente a la situación a través de sus propios recursos." (Roja, 2014)

2.2.3 Plan de Recuperación de Desastres (DRP):

Es un proceso que se realiza en las áreas de tecnología informática de las empresas, el cual por medio de un documentado establece estrategias y procedimientos para recuperar y proteger la infraestructura tecnológica en caso de un desastre.

2.2.4 Riesgo:

En términos del Riesgo Tecnológico, existe consenso generalizado en definirlo como: la posibilidad de pérdidas derivadas de un evento relacionado con el acceso o uso de la tecnología, que afecta el desarrollo de los procesos del negocio y la gestión de riesgos de la organización, al comprometer o degradar las dimensiones críticas de la información (Ej. confidencialidad, integridad, disponibilidad) (Franco, 2013).

2.2.5 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" (CIIFE, 2014).

2.2.6 Vulnerabilidad:

"Son las características y las circunstancias de una comunidad, sistema o bien que los hacen susceptibles a los efectos dañinos de una amenaza" (CIIFE, 2014).

2.2.7 Análisis de impacto del negocio:

Es una actividad que se realiza durante la implementación de un DRP y pretende identificar los diferentes sucesos que podrían impactar en la continuidad de las operaciones, sus finanzas, el talento humano, la legalidad y la reputación de la organización.

2.2.8 Gestión de Proyectos:

Es la disciplina, que guía e integra, los procesos donde se planifica, dirige y controla el desarrollo de un proyecto, con el propósito de garantizar la ejecución del mismo, cumpliendo de esta forma, con el alcance a un valor mínimo y dentro de un período de tiempo específico.

2.2.9 Proyecto:

Es un conjunto de actividades, las cuales se encuentran interrelacionadas y desarrolladas de manera coordinada, que busca alcanzar un determinado objetivo, dentro de restricciones de tiempo, costos y recursos.

2.2.11 Pequeñas y medianas empresas PYMES:

Son entidades independientes, “En Colombia el sector empresarial está clasificado en micro, pequeñas, medianas y grandes empresas, esta clasificación está reglamentada en la Ley 590 de 2000 y sus modificaciones (Ley 905 de 2004), conocida como la Ley Mipymes” (Bancoldex, 2014), las características de su clasificación son así; Microempresa: personal no superior a 10 trabajadores, con activos totales o inferiores a 501 salarios mínimos mensuales vigentes, Pequeña Empresa: personal entre 11 y 50 trabajadores, con activos totales a 501 y menores a 5.001 salarios mínimos mensuales legales vigentes, Mediana: personal entre 51 y 200 trabajadores, con activos entre 5.001 y 15.000 salarios mínimos mensuales legales vigentes.

2.3 MARCO LEGAL

Para establecer el marco legal del proyecto se determina mencionar las normas y las regulaciones vigentes que contemplan todo lo relacionado al DRP como la norma de seguridad informática y la ley de protección de datos.

2.3.1 ISO/IEC 27001 y la ISO 22301:2012

La ISO 27001, es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada con base a la norma británica BS 7799-2. Puede ser implementada en cualquier tipo de organización, con o sin

fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. *También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001*. (Kosutic, 2014)

La Norma Internacional ISO 22301:2012 es un estándar que proporciona a empresas y a todo tipo de organizaciones, soluciones y prácticas para asegurar la marcha del negocio ante posibles contingencias. En esta norma, además, se señalan las razones para la implementación de un BCP y se definen conceptos básicos como el BIA, RTO, RPO, activos críticos, crisis, incidencia y las diferentes etapas de unas metodologías de los planes de continuidad.

2.3.2 Protección de los Datos Personales

En el momento de describir, acerca de la protección de la información, se enfatiza, en que es el hecho de la garantía, en tener un control de la propia información, frente a su tratamiento automatizado o no, es decir, no sólo a aquella información alojada en los sistemas informáticos, sino en cualquier soporte que permita su utilización: almacenamiento, organización y acceso.

El 17 de octubre de 2012 el Congreso Colombiano, expidió la Ley 1581 de 2012 y junto con el decreto 1377 de 2013 de la Ley Estatutaria de Protección de Datos Personales, que se hizo obligatoria para las empresas a partir del 18 de abril de 2013, convirtiéndose de esta forma la información dentro las empresas hoy en día en Colombia, en un activo vital y un derecho fundamental, mediante la cual se dictan disposiciones generales para la protección de datos

personales. En esta ley, se regula el derecho fundamental de habeas data y se señala la importancia en el tratamiento de dicha información, cuyo objetivo principal de esta ley es, proteger los datos personales registrados en cualquier base de datos que permita realizar operaciones abarcando entidades públicas o privadas, con el fin de salvaguardar los derechos, deberes fundamentales, procedimientos y recursos para la protección de la información. Este derecho, demanda para su efectiva protección mecanismos que lo garanticen, los cuales no sólo han de depender de jueces, sino de una institucionalidad administrativa que garanticen control y vigilancia tanto en las empresas de sector privado como público, que aseguren la efectiva protección de datos y en razón de su carácter técnico, tengan la capacidad de fijar políticas que busquen la confidencialidad, disponibilidad y usabilidad de la información

2.4 MARCO GEOGRÁFICO

La investigación se desarrolla en Colombia específicamente en la ciudad de Bogotá D.C., iniciando con el desarrollo del diagnóstico del conocimiento y grado de implementación de un plan de recuperación de desastres realizado en empresas de diferentes sectores en el segmento de empresas pequeñas y medianas en Bogotá D.C., a partir de una muestra por sectores no regulados.

3. METODOLOGÍA DE LA INVESTIGACIÓN

Este capítulo establece el tipo de investigación a desarrollar, la población y las fuentes de información que se van a utilizar en el transcurso de la investigación.

3.1 METODOLOGÍA DE ESTUDIO

En esta parte del trabajo se plantea la forma en la cual se va a desarrollar la investigación en cada una de sus etapas para lograr los objetivos planteados.

Enfoque de la investigación

La investigación Cualitativa fue el enfoque a utilizar en la presente tesis, para este método se pretende recoger los discursos de los entrevistados, con el propósito de analizar e interpretar el comportamiento que se presenta en las empresas para el caso de estudio.

3.1.1.1 Técnica e instrumento de recolección de información

Para esta investigación, se empleó, como técnica de recolección de información, la entrevista, y como instrumento de recolección de información, el cuestionario, los cuales fueron dirigidos a un segmento de diferentes empresas pequeñas y medianas en Bogotá D.C., ver tabla 1, donde se

describen los cargos de quienes fueron entrevistados en las áreas de tecnología, en cada empresa, con su respectivo modelo del negocio, con el propósito de realizar un diagnóstico junto con el personal directamente implicado de los procesos, mostrando la necesidad de implementar de un DRP. Ver anexo A.

3.1.1.2 Tamaño de la muestra

Una de las características de la investigación cualitativa es poder realizar una recolección de datos, sin tener una restricción en la medición numérica, para este caso, en la investigación realizada, se determinó un tamaño de la muestra de 7 (siete) empresas de la ciudad de Bogotá D.C., las cuales accedieron a compartir la información de las áreas de tecnología informática, respecto al conocimiento y grado de implementación, acerca de los planes de recuperación de desastres. Es importante resaltar que las empresas seleccionadas, han sido organizaciones donde he laborado, gracias a la profesión en que me he desempeñado como ingeniero de sistemas.

Tabla 1. Entrevistados

	Entrevista 1	Entrevista 2	Entrevista 3	Entrevista 4	Entrevista 5	Entrevista 6	Entrevista 7(EXPERTO)
Cargo	Gerente de Tecnología (GT)	Administrador de base de datos(ABD)	Coordinador de Infraestructura(CI)	Administrador de base de datos	Administrador de base de datos	Administrador de base de datos	Arquitecto de infraestructura (AI)
Modelo del negocio	Seguridad industrial, salud ocupacional y Seguridad Ambiental (SISOSA)	Sector farmacéutico	Seguridad industrial, salud ocupacional y Seguridad Ambiental (SISOSA)	Reparación de celulares a fabricantes	Ofrece servicios de telecomunicaciones a las empresas del sector.	Desarrollo De Software Para Administración Inteligente De Proyectos	Mejores prácticas de la industria para la gestión y optimización de procesos de negocio(GOPN)

Fuente: Adaptación Propia.

Después de realizar el diagnostico al segmento entrevistado junto con las investigaciones realizadas se plantea un Análisis de Impacto del Negocio (BIA) y su relación con las situaciones posibles de riesgo para las áreas de tecnología informática, para finalmente proponer el conjunto de acciones gerenciales necesarias para la implementación del DRP en las empresas pequeñas y medianas no reguladas en Bogotá D.C..

Fuentes de información

Se aplicará la comunicación personal a través de entrevistas individuales, y visitas de observación. Adicionalmente, si se requiere, y es posible, contactar a través de correos electrónicos, las fuentes primarias de información fueron los funcionarios de las empresas, de las áreas de tecnología informática en Bogotá.

4. DESARROLLO DE LA INVESTIGACIÓN

Para el desarrollo de la investigación, se realizó una metodología de 4 (cuatro) etapas donde se establece como se desarrolló el trabajo, En la tablas de la 2 a la 5 se describen las etapas.

Tabla 2. Etapa de Diagnóstico de conocimiento:

Alcance:	Realizar el diagnóstico de implementación del DRP actual por medio de una muestra para empresas pequeñas y medianas en Bogotá D.C.	
Entregables:	**Categorías del Diagnóstico**	Describir las categorías propuestas en el diagnóstico, con sus respectivas subcategorías, detallando una conclusión general del estado de las empresas entrevistadas.
	Conclusión Del Diagnostico	Descripción de una conclusión general del diagnóstico encontrado de las empresas entrevistadas.

Fuente: Adaptación Propia.

Tabla 3. Etapa de acciones gerenciales de implementación del DRP

Alcance:	Desarrollar la guía para la elaboración de planes de recuperación de desastres desde el PMI en las áreas de tecnología informática de las empresas pequeñas y medianas en Bogotá D.C.	
Entregables:	**Acciones gerenciales**	Describir los procesos que se deben tener en cuenta para el desarrollo de un DRP.

Fuente: Adaptación Propia.

Tabla 4. Etapa de análisis de la importancia del DRP en las empresas pequeñas y medianas en Bogotá D.C.

Alcance:	Exponer la importancia por la cual las empresas pequeñas y medianas no reguladas en Bogotá D.C. deben implementar el Plan de Recuperación de Desastres.	
Entregables:	**La mejor inversión para las empresas**	Explicar las formas como se puede demostrar a los directivos de la empresa que implementar un DRP es la mejor inversión.

Fuente: Adaptación Propia.

Tabla 5. Etapa análisis y evaluación de la guía.

Alcance:	Se realiza la evaluación de la guía para la elaboración de planes de recuperación de desastres, desde el PMI en las áreas de tecnología informática de las empresas pequeñas y medianas en Bogotá D.C., por medio de un experto con conocimientos y experiencia en business continuity plan and management bajo las recomendaciones de Disaster Recovery Institute – DRII.	
Entregables:	**Resultado de la evaluación de la guía.**	Para la validación de guía se plantean 10 ítem o preguntas con posibilidades de respuesta: Totalmente de acuerdo, De acuerdo, En desacuerdo, Totalmente en desacuerdo, ítem que se listan posteriormente: 1. Las etapas planteadas en la presente guía son apropiadas. 2. La secuencia de las etapas planteadas en el presente guía son adecuadas. 3. Es correcta y consistente la terminología usada en el presente guía. 4. La presente guía es una herramienta para aporta a la implementación de planes de recuperación de desastres en las empresas en Bogotá D.C. 5. Es posible que guía propuesta contribuya a la mitigación o

		ayude a la reducción de los impactos negativos frente a la perdida de los activos de tecnología informática. 6. Los entregables sugeridos en la guía son los adecuados para documentar el proceso del DRP. 7. El diseño propuesto para el análisis de impacto del negocio es el adecuado. 8. Los cuatro criterios de seguridad descritos en la guía para identificar los riesgos son los apropiados. 9. Conoce la regulación vigente para la implementación del DRP en las empresas. 10. Cree que las empresas en Bogotá D.C. puede tener beneficios con la aplicación la guía del DRP.

Fuente: Adaptación Propia.

4.1 DIAGNÓSTICO DE CONOCIMIENTO Y GRADO DE IMPLEMENTACIÓN EN LAS EMPRESAS ENTREVISTADAS

El desarrollo del diagnóstico se realizó, por medio de entrevistas, ver anexo C, de entrevistas, seleccionando el personal que se encuentra directamente relacionado con la ejecución y desarrollo del Plan de Recuperación de Desastres de cada empresa por ejemplo; los gerentes de tecnología, Administrador de Base de datos y Coordinadores de Infraestructura, dicho personal, que por su trabajo, rol y experiencia de vida, disponen de la información y de una visión especial permitiendo profundizar el diagnóstico en las empresas y de esta forma conocer el estado en que las empresas se encuentran, frente a la implementación de planes de recuperación de desastres.

En el momento de realizar las entrevistas, se analizó en qué empresas se lograría acceder a la información que se requería para el diagnóstico, por lo cual se concluyó determinar un segmento de 7 (siete) empresas de tecnología informática, señalando que en este ámbito laboral fue donde se logró evidenciar la problemática que existe en las empresas, por la falta de implementación de un DRP, ya que una de las responsabilidades de las áreas de tecnología Informática, es garantizar

la protección de la información. Logrando de esta forma por medio del resultado del diagnóstico realizado al segmento de las 7 (siete) empresas entrevigadas, obtener una base fundamental de la investigación que contribuye al desarrollo de la guía para la elaboración de planes de recuperación de desastres desde el PMI en las áreas de tecnología informática de las empresas pequeñas y medianas en Bogotá D.C..

4.1.1 Objetivo Del Diagnóstico

Describir el grado de conocimiento e implementación del Plan de Recuperación de Desastres que se encontró como resultado de las entrevistas realizadas a la muestra seleccionada de empresas pequeñas y medianas en Bogotá D.C.

4.1.2 Técnica De Investigación (La Entrevista)

Para la investigación realizada se seleccionó como técnica de recolección de información "La Entrevista", con el propósito de recopilar la información e implementar el diagnóstico, por lo tanto se seleccionó una muestra de empresas pequeñas y medianas en la ciudad de Bogotá.

Por medio de las entrevistas, se busca recopilar toda la información de lo que está ocurriendo en cada empresa, es decir investigar qué tanto conocen, cómo lo ejecutan o ejercen las estrategias del DRP, entre otros, para que de esta manera se reconstruya la realidad de las empresas frente a un Plan de Recuperación de Desastres, enriqueciendo la información y facilitando la consecución de los objetivos propuestos.

En la tabla 6 se relaciona, el modelo de las preguntas realizadas en la entrevista como los criterios que orientan la investigación y el propósito por el cual se pretende medir o extraer dicha información.

Tabla 6. Composición de la Entrevista.

Categoría	Sub-categoría	Preguntas realizadas	Propósito de la pregunta
Información de la Empresa	Cargo Entrevistado	¿Cuál es el cargo?	Conocer el cargo del entrevistado
Información de la Empresa	Nombre de la empresa	¿Cuál es el nombre de la empresa?	Conocer el cargo el nombre de la empresa
Información de la Empresa	Modelo de Negocio	¿A qué se dedica la empresa?	Conocer a que se dedican las empresas entrevistadas para ser segmentadas, dentro la investigación.
Información de la Empresa	Clientes	¿Cuáles son sus clientes?	Categorizar las empresas o las entidades a las cuales se les presta los servicios las empresas entrevistadas, resaltando la responsabilidad que tienen frente a estas organizaciones garantizando la confidencialidad, disponibilidad e integridad de la información.
Protección de la Información	Método de Salvaguardar	¿Cómo ustedes guardan la información de su empresa y la de sus clientes?	Conocer los métodos en que las empresas pequeñas y medianas empresas salvaguardan la información.
Protección de la Información	Ante un Desastre	Ante un desastre ¿Cómo la empresa protege la información?	Validar si la empresa se encuentra preparada para proteger la información ante desastre.
Protección de la Información	Políticas de seguridad de Información	¿Sabe usted si la empresa dispone de normas o políticas de seguridad de la información?	Analizar cuántas empresas poseen políticas de seguridad de la información.
Protección de la Información	Procedimientos Documentados	¿Los procedimientos en cuanto a seguridad de la información que tiene la empresa se encuentran documentados?	Observar cuántas empresas documentan los procedimientos de seguridad informática.
Protección de la Información	Procedimientos Actualizados	¿Cuándo fue la última vez que estos procedimientos para asegurar la información fueron utilizados o probados?	Observar si las empresas que informan tener documentos o procedimientos de seguridad informática, los actualizan.
Protección de la Información	Periodicidad de Capacitación	¿Cuándo fue la última vez que estos procedimientos para asegurar la	Conocer la periodicidad en las empresas encuestadas, actualizan los

		información fueron utilizados o probados?	documentos o procedimientos.
Personal de la empresa	Conocimientos DRP	¿Cuándo fue la última vez que el personal fue entrenado en el uso de los procedimientos para asegurar la información?	Analizar si está siendo capacitado el personal de las empresas.
Personal de la empresa	Conocimientos	¿El personal conoce la empresa y sabe de las amenazas que pueden afectarla?	Indagar si el personal de la empresa conoce las amenazas que poseen y reconocen el impacto en la que se puede afectar.
Personal de la empresa	Ejecutan Estrategias de Recuperación	¿En caso de un desastre conoce los procedimientos para salvaguardar la información de la empresa?	Conocer los procedimientos que realizan las empresas en el momento de salvaguardar la información dentro la empresa.
Personal de la empresa	Ejecutan Estrategias de Recuperación	¿Por qué no existen estos procedimientos?	Validar el por qué la empresa no posee un Plan de Recuperación de Desastres.
Conceptos	DRP	¿Qué pasaría si la empresa no tiene o no ejecuta un plan de recuperación de desastres?	Validar si el entrevistado conoce las amenazas y los riesgos de no ejecutar un plan de recuperación de desastres.
Conceptos	BIP	¿Un plan de continuidad del negocio es igual a un plan de recuperación de desastres?	Verificar los conocimientos del entrevistado.
Conceptos	Consecuencias de no tener un DRP	En caso de no tener los procedimientos para proteger la información ¿Es factible para la empresa diseñar o ajustar el plan de recuperación de desastres?	Conocer el interés de los entrevistados, frente a la factibilidad de implementar un Plan de Recuperación de Desastres.
Conceptos	Como se implementa un DRP	¿Cómo cree que se debe realizar un plan de recuperación de desastres?	Recopilar información o conocimientos que poseen las empresas en representación de los entrevistados, personas quienes ejercen roles pertinentes en el área de TI, referente a la protección de la información.

Fuente: Adaptación Propia.

4.1.3 Categorías y subcategorías del Diagnóstico

Las preguntas seleccionadas para la entrevista, fueron el resultado de una selección realizada por un experto en entrevistas para el levantamiento de información, junto con el conocimiento que he adquirido durante el trascurso de mi carrera profesional, logrando una clasificación de los temas principales por categorías y subcategorías, obteniendo en el diagnostico el estado de la empresa y grado de conocimiento del entrevistado acerca del plan de recuperación de desastres.

4.1.3.1 Primera categoría: Información de la Empresa

En esta categoría se describen 5 subcategorías relacionadas directamente con la información contextual de las empresas entrevistadas.

1. Cargo Entrevistado: Rol relacionado directamente con el área de tecnología informática, como lo son: Administradores de bases de datos, Gerentes del área de TI, Coordinador de infraestructura.
2. Nombre de la empresa: Por una acción de reserva no se revelan los nombres de las empresas entrevistadas.
3. Modelo de Negocio: Se realizó la entrevista en diferentes modelos de negocio de empresas pequeñas y medianas en las cuales tenemos empresas de: Seguridad industrial, salud ocupacional y Seguridad Ambiental, Sector farmacéutico, Servicio de telecomunicaciones, desarrollo de software, fabricación y reparación de celulares.
4. Factibilidad de diseñar un DRP si no existe: Es importante señalar del muestreo que se realizó de las empresas ninguna actualmente posee un Plan de Recuperación de Desastres, pero en todas ven factible su ejecución.

5. Clientes: En Bogotá D.C. existe un gran porcentaje de empresas pequeñas y medianas, que trabajan para las grandes empresas del país, prestándoles sus servicios, según lo identificamos en las entrevistas y las cuales se mencionan a continuación: Petroleras, Entidades del sector público, Motorola, Samsung, Siemens, Sony, Telefónica, Une, ETB, EMCALI, Metrotel, entre otras.

4.1.3.2 Segunda categoría: Protección de la Información

Proteger la información es proteger el funcionamiento adecuado de las empresas, evitando pérdidas financieras, ya que puede verse afectada por muchos factores tales como robos, incendios, fallas de disco, virus u otros. Desde este punto de vista uno de los problemas más importantes que se deben resolver es la protección permanente de su información crítica, posteriormente se relacionan las 6 subcategorías:

1. Método de Salvaguardar: De los métodos más usados, según las entrevistados, en las empresas, el método para salvaguardar la información es realizado por medio de backup periódicamente en servidores.

2. Ante un Desastre: Conocer cómo las empresas pequeñas y medianas en Bogotá D.C., protegen la información ante un desastre o si realmente conocen la importancia y si realmente se encuentran preparados para enfrentar un desastre.

   Llegando a una observación clara y es que no se encuentran preparados ante un desastre, ya que no poseen o ejecutan un plan de recuperación de desastres y aunque usan algunas

prácticas para salvaguardar la información, nunca serán suficientes sobre el soporte que tienen a la hora de enfrentar un desastre natural o algún tipo de ataque cibernético.

3. Políticas de seguridad de Información: La seguridad de la información, como se ha descrito anteriormente, dentro de las organizaciones es indispensable y de vital importancia, debido a la gran información con la cual se encuentran expuestos.

Según el sistema de la seguridad de la información de la ISO27001, en las empresas se deben implementar políticas y prácticas para el uso de los recursos de información y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el propósito de generar una cultura de cambio y mecanismos de seguridad dentro la organización, siendo la política una guía a seguir para asegurar la información.

Dentro las entrevistas realizadas se determina que en las empresas no se tienen implementadas, políticas de seguridad informática donde identifiquen realmente y protejan los activos de sus empresas, en este caso la información, de forma que prevengan la destrucción, la divulgación, modificación y utilización no autorizada de toda información relacionada con clientes, empleados, precios, bases de conocimiento, entre otros, y si bien es cierto dentro de varias de estas empresas se tiene quizás algunas normas en algunos aspectos o en algunas áreas no están definidos dentro una política de seguridad o de la implementación y mejora continua de un sistemas de gestión de seguridad de la información. Aunque es importante resaltar que dentro las entrevistas

realizadas para el diagnóstico, se encontró solo una empresa que se encuentra iniciando el levantamiento de la política de seguridad.

4. Procedimientos Documentados: La Política de seguridad informática debe estar documentada y es allí donde se describen las técnicas, normas, reglas, procedimientos y prácticas fundamentales para preservar y regular la protección de la información y los diferentes recursos informáticos con que cuenta la Empresa, para este diagnóstico en ninguna de las empresas se encuentran documentadas las políticas de seguridad de la información.

5. Procedimientos Actualizados: No existen procedimientos actualizados, que describan procesos o normas acerca de la seguridad informática dentro en las empresas que fueron entrevistadas.

6. Periodicidad de Capacitación: Detallando el contenido de la entrevistas para esta subcategoría se ha encontrado que las empresas realizan capacitaciones muy esporádicamente acerca de la protección de la información.

4.1.3.3 Tercer categoría: Conocimiento del personal de la empresa acerca del DRP

Dentro de la empresa, cuando deciden implementar un plan de recuperación de desastres, los miembros del equipo del DRP son los que deben conocer a profundidad y detalle, la ejecución de las tareas específicas que deben desarrollase.

En el diagnóstico realizado por medio de las entrevistas con respecto a los temas específicos, se encontraron 3 subcategorías:

1. Conocimientos DRP: Dentro los empleados entrevistados se determina que poseen un conocimiento básico del significado e importancia de un DRP, pero dicho conocimiento no permite ser influyente para la empresa a la hora de incentivar la implementación de un plan de recuperación de desastres, ya que aunque reconocen que proteger los datos de los clientes y sus activos internos debe ser la prioridad, pero esto no se traduce en efectuar una cultura de cambio con estrategias y normas dentro la empresa.

2. Conocimientos BCP: Dentro los empleados entrevistados se determina que poseen un conocimiento básico del significado e importancia de un BCP.

3. Ejecutar Estrategias de Recuperación: No existen Estrategias de recuperación de desastres dentro de las empresas.

4.1.4 Cuarta categoría: conceptos de la entrevista por experto entrevistado.

Los conceptos aportados por el experto entrevistado comprenden 5 subcategorías, las cuales se mencionan posteriormente, donde se nos aclaran por medio de la entrevista realizada, los temas relacionados a la implementación de un DRP, en el siguiente link se podrá evidenciar la entrevista con el experto y los conceptos. http://youtu.be/0zXQkwzf-uk

4.1.4.1 Concepto del experto acerca del DRP:

Conjunto de actividades y procedimientos que hacen posible a una organización responder ante un desastre y reiniciar sus funciones críticas en una condición aceptable, en un período de tiempo determinado, orientado a recuperación de infraestructura y tecnología.

4.1.4.2 Concepto del experto acerca del BCP:

Son todas las actividades y procedimientos que hacen posible a una organización responder a un evento en tal forma que las funciones críticas del negocio continúen sin interrupción o cambio significativo.

Periodicidad de actualización de documentación: Según el marco de referencia COBIT, dirigido a la supervisión y control de las tecnologías de la información, una de las fases de aseguramiento del servicio continuo establece el “Mantenimiento del Plan de Continuidad de TI / DRP”. En esta fase, la Gerencia de TI debe proveer procedimientos de control de cambios para asegurar que el plan de recuperación ante desastres se mantiene actualizado y reflejo. Los requerimientos

actuales del negocio. Esto requiere de procedimientos de mantenimiento del plan de recuperación alineados con el cambio, la administración y los procedimientos de recursos humanos, todo esto orientado a garantizar la seguridad y la disponibilidad de los sistemas de información de las organizaciones.

4.1.4.3 Concepto del experto acerca del BIA:

El propósito fundamental del Análisis de Impacto sobre el negocio, conocido más comúnmente como BIA (Business Impact Analysis) es determinar y entender qué procesos son esenciales para la continuidad de las operaciones y calcular su posible impacto. Este proceso es parte fundamental dentro de la elaboración de un Plan de Continuidad del Negocio. (portal.ccss.sa.cr, 2014)

De acuerdo al Business Continuity Institute se tienen tres objetivos principales al realizar un análisis de impacto:

1. Entender:
    - ✓ Los procesos críticos que soportan el servicio.
    - ✓ La prioridad de cada uno de estos servicios.
    - ✓ Los tiempos estimados de recuperación.
    - ✓ El punto estimado de recuperación

2. Determinar los tiempos máximos tolerables de interrupción.
3. Apoyar el proceso de determinar las estrategias adecuadas de recuperación.

4.1.4.4 Concepto del experto acerca de ¿Cómo se implementa un DRP?

La metodología recomendada para el desarrollo de un plan de recuperación ante desastres o DRP para los sistemas de información críticos de TI, es un proceso comprendido desde el inicio del proyecto hasta la realización de las pruebas. Se considera también realizar un análisis de riesgo, estrategias de recuperación y la definición de roles y responsabilidades. (Metodología para el diseño de un DRP)

Finalmente, se describe una metodología para implementar un DRP, basada en las recomendaciones del NIST (National Institute of Standards and Technology), DRII (Disaster Recovery Institute International) y el BCI (Business Continuity Institute), y también apoyadas en la experiencia de casos prácticos realizados en nuestro país:

1. Inicio del proyecto Plan de Recuperación ante desastres.
2. Análisis de impacto sobre el negocio (BIA).
3. Análisis de riesgos.
4. Desarrollo de estrategias para el DRP.
5. Definición de roles y responsabilidades.
6. Pruebas del DRP.

(Metodología para el diseño de un DRP)

4.1.4.5 Concepto del experto, acerca de las consecuencias de no tener un DRP

Si la empresa no implementa un plan, podría verse inmersa en problemas de reputación con los clientes, proveedores y aliados estratégicos, llegando hasta salir del mercado, es decir que las

empresas en caso de emergencia, llegarían a no contar con la continuidad, arriesgando grandes sumas de dinero equivalentes a horas de trabajo. Según la organización IBM, de las empresas que han tenido una pérdida principal de registros automatizados, el 43 % nunca vuelve a abrir, el 51 % cierra en menos de dos años y sólo el 6 % sobrevivirá a largo plazo (Sánchez N. , celingest, 2013).

Por esta razón somos conscientes de la necesidad de tener un DRP que permite sostener procesos durante y después de una interrupción, a través de estrategias ordenadas que rescaten y protejan los recursos, procesos, roles y responsabilidades dentro la organización. Sin lugar a dudas, el DRP se constituye en una solución para la evaluar riesgos, costos, además de garantizar la continuidad de la información.

4.1.5 Conclusión del Diagnóstico, de las entrevistas realizadas al personal de las empresas.

Después de realizar las entrevistas al segmento de 7 empresas en Bogotá D.C., en las áreas de tecnología, se puede evidenciar, las grandes falencias que presentan frente al compromiso que se debe tener con respecto a la seguridad de la información y esto se demuestra con el corto conocimiento que posee el personal responsable de los procesos que se encuentran asociados con el área de Tecnología, además de la falta de ejecución en las empresas del Plan de Recuperación de Desastres.

4.2 ACCIONES GERENCIALES NECESARIAS PARA LA IMPLEMENTACIÓN DEL DRP CON UN ENFOQUE DESDE EL PMI

El Plan de Recuperación de Desastres debe verse e implementarse como un Proyecto dentro la empresa, en este caso se describen las acciones gerenciales para implementar un DRP, donde se analiza, diseña, construya y administran unas acciones, que permitan ante un caso de desastre recuperar los procesos críticos dentro de la empresa, utilizándose como la guía para la elaboración de planes de recuperación de desastres desde el PMI en las áreas de tecnología informática de las empresas pequeñas y medianas en Bogotá D.C., junto con los entregables mínimos que deben documentarse para el DRP.

Es importante señalar que el enfoque del PMI que se le da a la guía es tangible para todas las etapas de la implementación del DRP, siguiendo las recomendaciones del Project Management Institute (PMI), para cada proceso: iniciación, planeación, ejecución, monitoreo, control y cierre.

En la Tabla 7, se encuentra el enfoque del PMI por medio del mapa de procesos del PMBOK® 2013, con el propósito de tener un acercamiento inicial de los procesos que abarca el proyecto de la implementación de un DRP en las empresas pequeñas y medianas en Bogotá D.C. (Resaltados en Amarillo).

Los criterios para seleccionar, los procesos con sus respectivas actividades, propuestas en la guía, del mapa de procesos del PMBOK®, fueron seleccionados y planteados, por la experiencia al

momento de implementar un DRP en las empresas, según las investigaciones realizadas para este trabajo de tesis.

Tabla 7 Mapa de procesos PMBOK5

	Inicio	Planificación	Ejecución	Monitoreo y control	Cierre
Integración	4.1 Desarrollar el acta de constitución del proyecto.	4.2 Desarrollar el plan para la dirección del proyecto	4.3 Dirigir y gestionar el trabajo del proyecto	4.4 Monitorear y controlar el trabajo del proyecto 4.5 Realizar el control integrado de cambios	4.6 Cerrar el proyecto o fase
Alcance		5.1 Planificar la gestión del alcance 5.2 Recopilar requisitos 5.3 Definir el alcance 5.4 Crear la EDT		5.5 Validar el alcance 5.6 Controlar el alcance	
Tiempo		6.1 Planificar la gestión del cronograma 6.2 Definir las actividades 6.3 Secuenciar las actividades 6.4 Estimar los recursos de las actividades 6.5 Estimar la duraciones de las actividades 6.6 Desarrollar el cronograma		6.7 Controlar el cronograma	
Costos		7.1 Planificar la gestión de costos 7.2 Estimar los costos 7.3 Determinar el presupuesto		7.4 Controlar los costos	
Calidad		8.1 Planificar la gestión de la calidad	8.2 Realizar el aseguramiento de calidad	8.3 Controlar la calidad	
Recursos humanos		9.1 Planificar la gestión de RRHH	9.2 Adquirir el equipo del proyecto 9.3 Desarrollar el		

			equipo del proyecto 9.4 Dirigir el equipo del proyecto		
Comunicaciones		10.1 Planificar la gestión de las comunicaciones	10.2 Gestionar las comunicaciones	10.3 Controlar las comunicaciones	
Riesgos		11.1 Planificar la gestión de riesgos 11.2 Identificar los riesgos 11.3 Realizar el análisis cualitativo de riesgos 11.4 Realizar el análisis cuantitativo de riesgos 11.5 Planificar la respuesta a los riesgos		11.6 Controlar los riesgos	
Adquisiciones		12.1 Planificar la gestión de adquisiciones del proyecto	12.2 Efectuar las adquisiciones	12.3 Controlar las adquisiciones	12.4 Cerrar las adquisiciones
Interesados	13.1 Identificar a los interesados	13.2 Planificar la gestión de los interesados	13.3 Gestionar la participación de los interesados	13.4 Controlar la participación de los interesados	

Fuente: Extraído certificación pm ajustada por el autor

4.2.1 GUÍA GENERAL PARA LA ELABORACIÓN DE PLANES DE RECUPERACIÓN DE DESASTRES

Inicialmente, con el propósito de estructurar la guía, se listan las etapas con sus respectivas actividades propuestas, para la elaboración de planes de recuperación de desastres como se muestra en la tabla 8:

Tabla 8. Etapas y Actividades de la Guía.

	Inicio	Planificación	Ejecución	Monitoreo y control	Cierre
Actividades del proyecto	**1.** Identificar la necesidad de la implementación de DRP dentro la empresa. **2.** Identificar a los interesados	**1**. Elaborar un diagnóstico de los componentes de hardware y software. **2**. Realizar un levantamiento de información al personal involucrado en los procesos. **3**. Elaboración del plan donde se incluya el alcance, cronograma y costos del proyecto. **4**. Elaboración e identificación de los riesgos del proyecto.	**1.** Realizar un Análisis del Impacto al Negocio (BIA- Business Impact Analysis) **2.** Realizar la evaluación de los Riesgos. **3.** Identificar las estrategias, por medio de manuales y protocolos. **4.** Definir los roles y responsabilidades o funciones. **5.** Implementar el DRP	**1**. Ejecutar pruebas y simulacros del DRP. **2**. Capacitar periódicamente al personal. **3**. Realizar el Control de cambios o actualizaciones.	**1**. Cerrar el proyecto.
Entregables	• Acta de constitución del proyecto. • Presentar a los interesados la propuesta de la implementación del DRP	• Diagnóstico actual de hardware y software inicial de la empresa. • Documentación del levantamiento de información del personal involucrado. • Registro de la elaboración del plan donde se incluya el alcance, cronograma y costos del proyecto. • Registro de la	• Análisis de impacto del negocio de la empresa. • Evaluación y análisis de los riesgos de la empresa. • Planteamiento de las estrategias a implementar en el DRP, en manuales y protocolos. • Documentación de los roles y responsabilidades o funciones. • Documento del DRP con la	• Registrar las evidencias de pruebas y simulacros. • Registrar formatos de asistencia a las capacitaciones del personal involucrado. • Registro del formato de control de	

		elaboración e identificación de los riesgos del proyecto.	descripción de las estrategias con los procedimientos delimitados por tiempos y respectivo responsable.	cambios y actualización del DRP.	

Fuente: Adaptación Propia.

4.2.1.1 Inicio

En la etapa de inicio se debe **identificar la necesidad de la implementación del DRP dentro la empresa** y de esta forma ser expuesta a **los interesados** de la empresa, con el propósito de contar con su respectiva aprobación y dar inicio al proyecto.

Entregable: Presentar a los interesados la propuesta de la implementación del DRP y Realizar Acta de constitución del proyecto.

4.2.1.2 Planificación

En esta etapa se brindan todas las bases para realizar el DRP porque es allí donde se describen los objetivos que la empresa busca en casos de contingencias y los alcances de la recuperación, además se planea y se ejecuta la **elaboración un diagnóstico de los componentes de hardware y software**, seguido de un **levantamiento de información al personal involucrado en los procesos** dentro la empresa en el área de Tecnología Informática, Este diagnóstico se puede diseñar o validar por medio de entrevistas y visitas donde se verifique la información del diagnóstico.

Con el propósito de garantizar que la implementación del DRP se desarrolle con éxito en las empresas, es importante realizar la elaboración del **plan para la dirección del proyecto**, donde se incluya el **alcance, cronograma y costos,** identificando además **los riesgos** que puede presentar la ejecución del mismo.

- **Entregable:** Diagnóstico actual de hardware y software inicial de la empresa, documentación del levantamiento de información del personal involucrado en los procesos del área de tecnología informática y registro de la elaboración del plan donde se incluya el alcance, cronograma, costos y riesgos del proyecto.

4.2.1.3 Ejecución

En la etapa de ejecución se presentarán cuatro (4) actividades las cuales nos aportarán en forma tangible en el desarrollo del DRP, las cuales se describirán a continuación:

4.2.1.3.1 Primera actividad en la etapa de Ejecución:

Análisis del Impacto al Negocio (BIA- Business Impact Analysis)

Después de conocer el estado actual de la empresa, además de reconocer qué tan preparados están ante una contingencia, se prosigue a conocer la pérdida que puede soportar la empresa y la velocidad en que estas pérdidas van escalando con base al tiempo en que se tarda en reactivar la operación. El propósito de esta etapa es **realizar un Análisis del Impacto al Negocio (BIA- Business Impact Analysis)** en donde a través de un proceso de evaluación se identifiquen los procesos críticos de la empresa junto con el daño o pérdida que puede causar.

Entregable: Análisis de impacto del negocio.

Posteriormente se describe una propuesta de un diseño del Análisis de Impacto del Negocio (BIA)

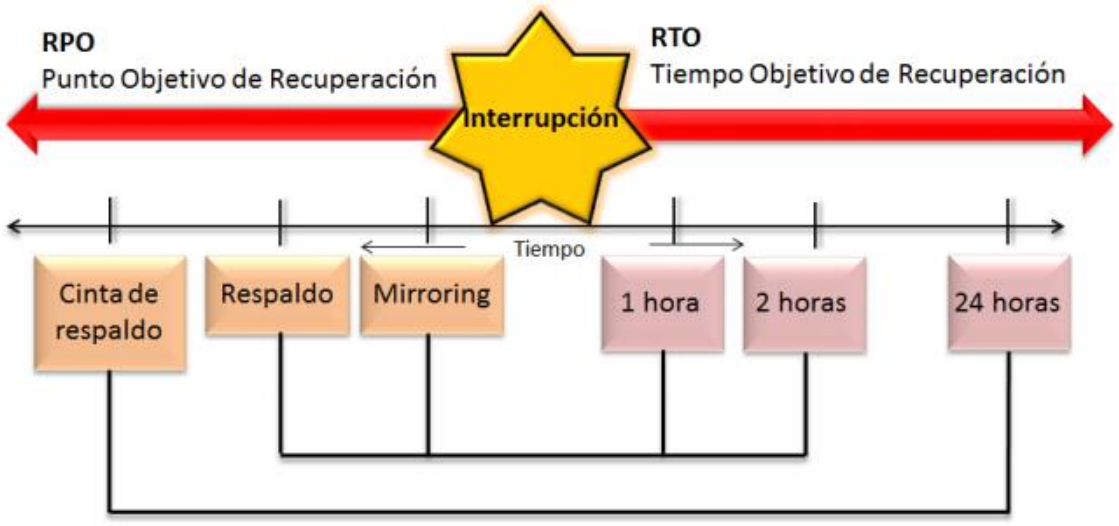
Propuesta de un diseño del análisis de impacto del negocio (BIA)

El Análisis de Impacto sobre el Negocio (BIA) tiene como propósito identificar los procesos críticos y recursos que soportan que puedan afectar la continuidad de las operaciones en las

empresas específicamente en el área de Tecnología Informática, procesos de los cuales indefectiblemente deben regresar al funcionamiento después de una situación de desastre.

Dentro de los objetivos de BIA se debe establecer y determinar el RPO (Recovery Point Objective) considerado como el volumen de datos en riesgo de pérdida que la empresa considere tolerable. Igualmente se debe establecer el RTO (Recovery Time Objective) en el cual se estipula y se expresa el tiempo durante el cual la empresa puede tolerar la falta de funcionamiento de los servicios que ofrecen dentro y fuera de la empresa sin afectar la continuidad del negocio, determinando de esta manera, qué opciones dentro del DRP se deben establecer para poner en ejecución cuando ocurra un evento inesperado y afecte las operaciones o servicios de la empresa; de esta manera logramos *identificar los tiempos objetivos de recuperación y el impacto asociado con la interrupción de los procesos por un determinado periodo de tiempo.* (BILA, 2014) Ver ilustración 4.

Ilustración 4. La relación entre RTO y RPO



Fuente: (Vasquez, ERNST &YOUNG, 2014)

En el momento de realizar el planteamiento del Análisis del impacto en una empresa se deben tener en cuenta los siguientes procesos:

Análisis de la información del área de tecnología informática de la empresa

En el momento de realizar un análisis de información, lo que se busca es, realizar un levantamiento de información del área de tecnología informática con el propósito de identificar los procesos que realizan transversales a la organización, además el impacto que generaría la interrupción de cada proceso, identificando los sitios físicos, los sistemas de información, es decir, el inventario de hardware y software que administran junto con la información que se posee interna y externa.

Los elementos a considerar en el momento realizar el inventario son: *sistemas telefónicos, redes locales, redes wan, redes man, internet, infraestructura física, aplicaciones, hardware, bases de datos, sistemas operativos, firewalls, switches, routers, etc*. (Ferrer, Sisteseg)

Procesos críticos

Después de haber realizado el levantamiento de información y conocer los procesos del área de tecnología, se procede a identificar los procesos críticos, con la descripción de sus respectivas consecuencias para la organización en el momento que este proceso falle, Los procesos críticos demandan no sólo mayor atención, sino además requieren un mayor nivel de inversión para asegurarse de que no fallen o incluso para evitar que su criticidad golpee a la operación, en forma de ejemplo los procesos críticos dentro el área de tecnología son: *redes, comunicaciones, desarrollo y soporte técnico, administrador de bases de datos, sistemas de seguridad de la información, soporte de redes, etc*. (Sánchez N. , Plan de recuperación ante desastres (DRP), 2013)

Probabilidad de interrupción

Para cada proceso crítico señalado anteriormente se analiza la probabilidad de ocurrencia de la falla causada por motivos internos o externos.

Posteriormente se muestra en la tabla 9, un ejemplo de cómo puede realizarse un análisis de probabilidad de ocurrencia.

Tabla 9. Criterios para un análisis de una probabilidad de ocurrencia.

Criterio	Probabilidad de Ocurrencia
ALTO	9
MEDIO ALTO	7
MEDIO	5
MEDIO BAJO	3
BAJO	1

Fuente: adaptación propia

En esta gráfica se muestra una evaluación de probabilidad de ocurrencia, donde se tienen en cuenta los siguientes parámetros, con calificación de 1 a 10 donde:

Bajo: entre 0 y 2

Medio Bajo: entre 3 y 4

Medio: entre 5 y 6

Medio Alto: entre 7 y 8

Alto: entre 9 y 10

Determinar la mayor criticidad de los procesos

En el momento de determinar la mayor criticidad en los procesos, se debe tener en cuenta la probabilidad de ocurrencia de la falla, que afecta el proceso, por el impacto de la interrupción del proceso, esto permite determinar la criticidad del proceso. A mayor impacto, mayor criticidad,

una vez establecido el orden de criticidad de los procesos, se determinará cuáles deben continuar operando limitadamente en una situación de desastre o contingencia.

Posteriormente en forma de ejemplo, se pueden realizar −como sugerencia− los siguientes pasos, para hallar la criticidad de los procesos, teniendo en cuenta que los criterios y valores asignados están bajo criterio de cada empresa.

A. Inicialmente se debe seleccionar la probabilidad de ocurrencia y el impacto del proceso, como se muestra en la tabla 10.

Tabla 10. Impacto de un riesgo.

Criterio	Probabilidad de Ocurrencia	Impacto
ALTO	9	10
MEDIO ALTO	7	8
MEDIO	5	6
MEDIO BAJO	3	4
BAJO	1	2

Fuente: adaptación propia

En esta gráfica se muestra una evaluación de probabilidad de ocurrencia y se le asigna el valor al impacto, teniendo en cuenta los siguientes criterios:

Bajo: 2

Medio Bajo: 4

Medio: 6

Medio Alto: 8

Alto: 10

B. Determinando finalmente la criticidad del proceso, que es el resultado de la probabilidad de ocurrencia por el impacto como anteriormente se indicó:

Criticidad del proceso = Probabilidad de Ocurrencia * Impacto

En la tabla 11, se muestran como ejemplo, los valores que pueden determinar la criticidad del proceso y que más adelante, se pueden convertir en un riesgo con diferentes criterios bajo, alto y medio.

Tabla11. Criticidad del riesgo.

BAJO	MEDIO	ALTO
1 – 30	31-60	61 – 90

Fuente: adaptación propia

Estimación de los tiempos objetivos de recuperación

En el momento que ocurra un desastre para cada proceso crítico se establece el tiempo objetivo de recuperación (RTO) de la falla o incidente presentado, sin perder de vista que este tiempo se asocia al impacto de la interrupción del proceso en el negocio. A mayor tiempo objetivo, mayores son las probabilidades de pérdidas económicas, este paso consiste en calcular los costos asociados a las acciones o procesos de la recuperación del servicio.

Secuencia de recuperación

Se establece la secuencia de cómo realizar la recuperación de los procesos, teniendo en cuenta la viabilidad de continuar con dicha operación dentro la empresa y la consecución de un proceso respecto a otro, es decir, cómo se debe actuar, cuando haya una emergencia ocasionada por un riesgo determinado.

4.2.1.3.2 Segunda actividad en la etapa de Ejecución:

La Evaluación de los Riesgos

Es la forma en que se pretende como resultado determinar las estrategias que se deben implementar para afrontar alguna contingencia (siniestro, desastre) que imposibilite el funcionamiento de los servicios informáticos en forma parcial o total de una empresa, al **realizar la evaluación de riesgos** se determina el nivel de la amenaza y el grado en el que la empresa está siendo vulnerable.

Entregable: Evaluación y análisis de los riesgos de la empresa.

Al momento de realizar un planteamiento de una evaluación y análisis de los riesgos limitados únicamente en el área de tecnología informática se deben tener en cuenta los siguientes procesos:

Propuesta de un diseño para realizar una evaluación y análisis de las situaciones posibles riesgo en la empresa para el área de Tecnología Informática.

Un Riesgo Tecnológico es la probabilidad de que un objeto, material o proceso peligroso, una sustancia tóxica o peligrosa o bien un fenómeno debido a la interacción de estos, ocasione un número determinado de consecuencias a la salud, la economía, el medio ambiente y el desarrollo integral de un sistema. (Delgado., 1997), por lo tanto conocer los riesgos a los que están relacionados los activos o los procesos de la empresa en el área de Tecnología informática se convierte en una tarea obligatoria para lograr gestionarlos.

Posteriormente se describen las posibles situaciones de Riesgo que se pueden presentar en las pequeñas y medianas empresas en Bogotá D.C. en las áreas de tecnología Informática, tomando como referencia la ISO/IEC 27000 siendo el conjunto de estándares que proporcionan un marco de la gestión de la seguridad de la información y la norma NIST SP 800-30 donde su objetivo es asegurar los sistemas de información que almacenan, procesan y trasmiten información, además describe cómo permitir y gestionar los Riesgos, mejorando la administración a partir de los resultados del análisis de riesgos

Para el diseño de la evaluación a del análisis de riesgos se tienen en cuenta cuatro criterios de seguridad que posteriormente se mencionan, con el propósito de abarcar las posibles situaciones de riesgo y cubrir los posibles riesgos asociados a las áreas de tecnología informática, además es importante aclarar que todas las situaciones posibles de riesgos, mencionadas como ejemplo en cada uno de los criterios, se obtuvieron, como resultado de la investigación y de los riesgos más comúnmente presentados en las empresas.

Primer criterio: Seguridad organizacional

Es el marco formal de seguridad informática de la empresa, incluye los servicios o contrataciones externas, la infraestructura de seguridad, Integrando el recurso humano con la tecnología, ante situaciones anómalas a la seguridad.

Situaciones Posibles de Riesgo:

- ✓ Pérdida de Información por acceso de terceros o muerte del colaborador de la empresa.

- ✓ Divulgación de la información confidencial de la empresa, ocasionada por despido o renuncia.
- ✓ Acceso no autorizado a los recursos tecnológicos como ejemplo: (aplicaciones o redes)
- ✓ Fallos en respaldos

Segundo criterio: Seguridad lógica

Son los mecanismos y procedimientos, que permiten monitorear el acceso a los activos de información, que incluyen los procedimientos de administración de usuarios, definición de responsabilidades, perfiles de seguridad, control de acceso a las aplicaciones y documentación sobre sistemas, que van desde el control de cambios en la configuración de los equipos, manejo de incidentes, selección y aceptación de sistemas, hasta el control de software malicioso, los cuales contienen virus, el cual es usado para robar información, enviar spam y hasta cometer fraude.

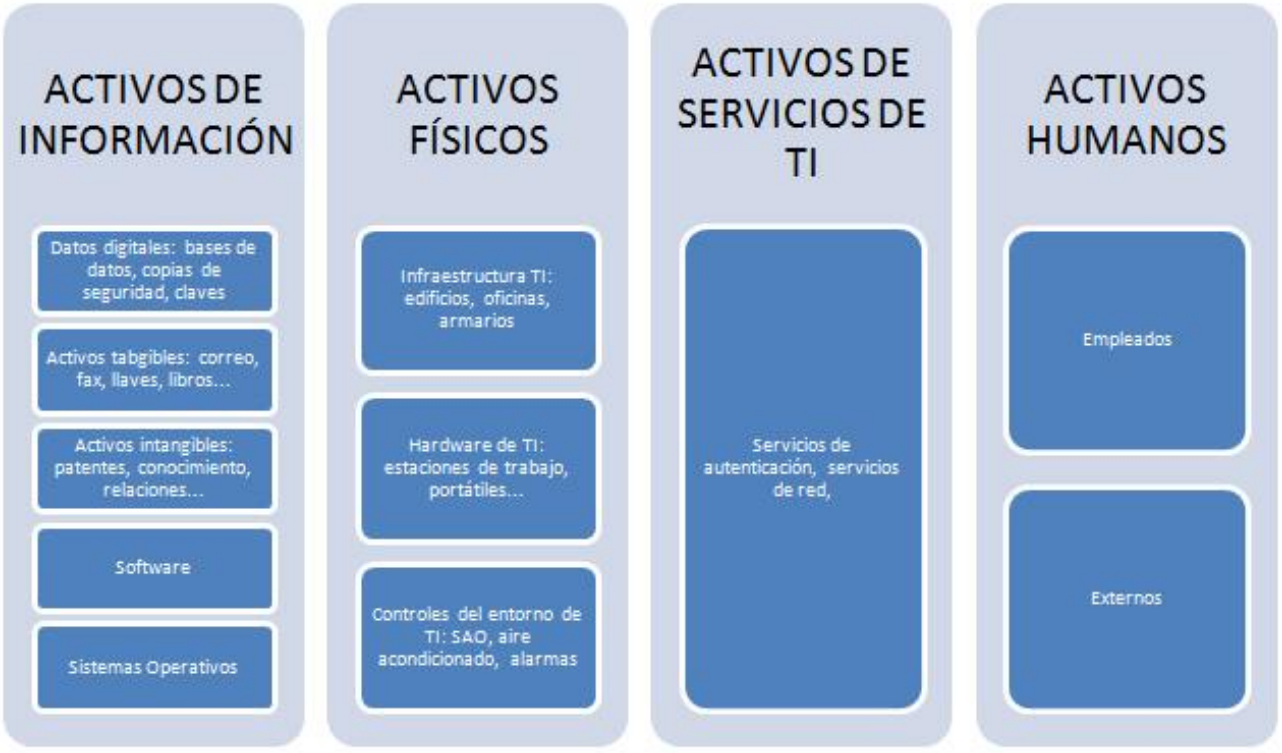
Situaciones Posibles de Riesgo:

- ✓ Códigos maliciosos.
- ✓ Spam.
- ✓ Piratería.
- ✓ Fuga de información.
- ✓ Ingeniería social.
- ✓ Intrusos informáticos.
- ✓ Fallos en software

Tercer criterio: Seguridad de activos

La Seguridad de los activos, contempla los lineamientos que deben seguirse al interior de la empresa, para alcanzar y mantener una protección adecuada de los mismos, pueden clasificarse de la siguiente forma: activos de información, activos físicos, activos de servicios de TI y activos humanos, los cuales deberán estar claramente identificados, por medio de un inventario, para que de esta forma, se pueda ejercer un control adecuado para cada uno, como lo muestra la ilustración 5.

Ilustración 5. Clasificación general de activos



Fuente: (isotools.org, 2013)

Situaciones Posibles de Riesgo:

- ✓ Pérdida de recursos / extravío de activos de IT no inventariados
- ✓ Revelación de datos sensibles
- ✓ Corrupción de Base de datos
- ✓ Falla en migrar la información
- ✓ Interrupciones eléctricas
- ✓ Fallos de hardware

Cuarto criterio: Seguridad física

Para garantizar la seguridad Física se deben identificar y establecer los límites mínimos que se deben cumplir en cuanto a perímetros de seguridad, de tal forma que se puedan establecer controles en el manejo de equipos, transferencia de información y control de los accesos a las distintas áreas, con base en la importancia de los activos.

Situaciones Posibles de Riesgo:

- ✓ Fallas en los servicios públicos
- ✓ Desastres naturales
- ✓ Huelgas
- ✓ Daño a los servidores o la Arquitectura de TI
- ✓ Robo
- ✓ Fallas en los sistemas de comunicación.
- ✓ Incendio

Quinto Criterio: Seguridad legal

Es identificar y establecer los requerimientos de seguridad que deben cumplir todos los empleados de la empresa, socios y usuarios bajo la reglamentación de la normativa interna de políticas y manuales de procedimientos en cuanto al recurso humano, sanciones aplicables ante faltas cometidas, así como cuestiones relacionadas con la legislación del país y contrataciones externas.

Situaciones Posibles de Riesgo:

- ✓ Incumplimiento de los reglamentos internos con respecto a la información de la empresa.
- ✓ Intrusión (hackeo)
- ✓ Virus

4.2.1.3.3 Tercera actividad en la etapa de Ejecución: Las Estrategias

Como efecto de la evaluación de los Riesgos se **identifican las estrategias** y prioridades en el proceso de la recuperación de los servicios, como ejemplo en estas estrategias se describen, por medio de **manuales y protocolos**, los esquemas de recuperación de respaldos, tiempos de recuperación, procesos o servicios indispensables para restaurar o reiniciar la operación de la empresa, identificar las responsabilidades y procedimientos para cada dueño del proceso, es decir, **definir los roles y responsabilidades o funciones.**

Entregable: Planteamiento de las estrategias a implementar en el plan de recuperación de desastres con la documentación de los roles y responsabilidades.

4.2.1.3.4. Cuarta actividad en la etapa de Ejecución:

Implementación del DRP

En esta etapa se construye en primera instancia el **documento** del Plan de Recuperación de Desastres que se desea implementar en la empresa, compuesto por la **descripción de las estrategias y los procedimientos delimitados por tiempos de respuesta**, además se implementa en caso de que aplique la infraestructura o las soluciones necesarias de hardware o software, por ejemplo se puede implementar el almacenamiento de información y respaldo fuera de las instalaciones físicas o también utilizar tecnologías, previniendo la pérdida de información, garantizando la disponibilidad, integridad y confidencialidad de los datos; de esta forma es como se pueden desarrollar las medidas y los procedimientos de reducción de riesgos planteados en el documento, los cuales fueron establecidos para lograr y aportar al cumplimiento de las estrategias y los planteamientos en el BIA realizado en una etapa anterior.

Entregable: Documento del DRP con la descripción de las estrategias con los procedimientos delimitados con los tiempos de respuesta para cada proceso con su respectivo personal responsable.

Es de esta forma donde la etapa de ejecución termina para dar inicio a la etapa de monitorear y controlar el proyecto.

4.2.1.4 Monitoreo y Control

Realizar un seguimiento para comprobar el desempeño y los resultados de la implementación de un DRP, es la mejor forma de verificar si se está desarrollando según lo planeado en el alcance del proyecto, este seguimiento se ejecuta por medio de **pruebas y simulacros***, según el estándar BS25999 para realizar un monitoreo y control, es recomendable probar el DRP cada seis meses y luego proceder a las actualizaciones pertinentes, para asegurar su vigencia. Es indispensable para la ejecución de estas actividades contar con la participación del personal involucrado en cada proceso,* (Latam, 2008) por lo cual es necesario antes de iniciar las pruebas, preparar y **capacitar periódicamente** al personal, con el fin de realizar una prueba completa de todos los procesos, etapas y áreas involucradas en las áreas de tecnología informática, garantizando que las estrategias de recuperación lleguen al fin esperado.

Entregable: Evidencias de las pruebas y simulacros, formato de asistencia a las capacitaciones con el personal o las áreas involucradas de los procesos.

Otro propósito fundamental de la etapa de monitoreo es hacer el **Control de cambios o actualizaciones,** en las áreas en que se vean involucradas todas las actividades previstas por los riesgos, que puedan afectar el proceso de recuperación y un inventario al día de todos los recursos del área de tecnología informática, logrando una nueva actualización del DRP implementado.

Entregable: Formato de control de cambios y actualización del plan de recuperación de desastres y un inventario de los recursos del área de tecnología informática.

4.2.1.5 Cierre

Después de realizar el monitoreo y control del plan de recuperación de desastres y dando cumplimiento al alcance y los objetivos del proyecto junto con la satisfacción de los interesados, se realiza la entrega formal del proyecto.

4.3 ANÁLISIS DE LA IMPORTANCIA DE UN DRP EN LAS ÁREAS DE TECNOLOGÍA INFORMÁTICA PARA LAS EMPRESAS PEQUEÑAS Y MEDIANAS EN BOGOTÁ D.C.

Después de conocer las etapas para implementar un DRP, se desea mostrar la importancia por la cual las empresas pequeñas y medianas no reguladas en Bogotá D.C. deben implementar el Plan de recuperación de desastres.

La mayor razón por la cual las empresas deben evaluar la posibilidad de la implementación de DRP, es evitar que un desastre afecte la continuidad del negocio, es saber cómo reaccionar ante cualquier tipo de amenaza, tanto de actividades internas y externas dentro la organización, pero existe una gran deficiencia de conocimiento en las empresas acerca de la importancia de su implementación, arriesgando grandes sumas de dinero y muchas veces la disponibilidad y perdida de la información.

> D*urante años, las pequeñas y medianas empresas no han conocido la necesidad de contar con un plan de recuperación ante desastres, pero muchas no suelen prestar la atención necesaria a los consejos. De hecho, 74% de las PYMEs a nivel global no cuenta con ningún plan establecido para manejar un desastre que potencialmente podría afectar su negocio.* (Wallace, 2013).

Es evidente que las empresas no tienen una convicción clara con respecto a lo que se enfrentan al no tener un DRP y en el grupo de aquellas que lo tienen implementado en muchas ocasiones ha sido por cumplir con las recomendaciones de un auditor u órdenes de superiores sin tener un pleno convencimiento de lo implementado.

> *En otra encuesta de Symantec sobre la preparación ante desastres en las pymes publicada en mayo de 2012 a escala mundial, el 22% de las pymes ni tiene ni piensa tener un DRP, el 33% está pensando en crear uno y el 45% restante está en ello o ya lo tiene. Entre las que parecen tener claro que no quieren un plan de recuperación ante desastres, la mayoría piensa que no es una prioridad o ni siquiera se han planteado crear uno…¡¡¡más del 50% están sin prevención ante desastres!!!* (Leader, 2012)

En el diagnóstico de las empresas entrevistadas para esta tesis, se evidenció que dichas organizaciones no poseen un plan de recuperación de desastres. Primero, porque no son conscientes de su importancia o no existe el conocimiento adecuado dentro de las áreas de tecnología informática y otra de las posibles causas para no tenerlo, es que en las mayorías de las empresas no consiguen el presupuesto para su implementación, y esta causa radica en que el personal del área de tecnología informática no sabe vender el plan a los directivos de su organización.

Una de las formas para que los directivos de las empresas posiblemente aprueben el desarrollo de este proyecto, debe ser realizando un estudio que demuestre los costos de cuánto perderían por estar fuera de servicio, los costos de tiempo y dinero en los que incurriría la empresa para recuperarse, de forma efectiva en el tiempo adecuado versus lo que les costaría en implementar un DRP llegando a la conclusión de ser más efectivo en costos su implementación.

También se puede demostrar por cada área del negocio, los costos de inversiones en infraestructura que representa cada una y la información que operan, permitiendo aclarar el panorama y no sesgar la criticidad de un producto o servicio, demostrando con un análisis los costos reales de asumir la pérdida de estos procesos y la necesidad de proteger la información de las diferentes áreas de las empresas.

4.3.1 La mejor inversión para las empresas

En las empresas, las áreas de tecnología informática, son las directamente responsables en garantizar la seguridad de la información, área a quien corresponde mostrar los beneficios de implementar un DRP. Para esta labor, en el momento de exponer a los directivos, como un proyecto de “La mejor inversión para la empresa” se debe tener presente;

1. Realizar un análisis costo beneficio de los gastos que conlleva no tener un plan de recuperación de desastres en la empresa, demostrando con valores, las pérdidas que podría ocasionar un riesgo. Para el caso en que los directivos no estén de acuerdo con la inversión por la ausencia de una partida presupuestal asignada a este rubro o la posibilidad de hacerlo, lo que se puede hacer, es estudiar y analizar las diversas

tecnologías disponibles que existen hoy en día, que ayudan a que las empresas disminuyan los esfuerzos de recuperación de desastres y se minimicen costos.

2. Exponer por medio de estadísticas, las estrategias o soluciones que implementan otras empresas; por ejemplo en una encuesta de 95 compañías realizada por la firma Sepaton en 2012, 41% de los encuestados reportó que su estrategia de DRP consiste en un centro de datos configurado activo-pasivo, es decir toda la información está respaldada en un centro de datos completamente configurado con la información crítica replicada en un sitio remoto. El 21% de los participantes utiliza una configuración activa-activa donde toda la información de la compañía se mantiene en dos o más centros de datos. El 18% dijo que aún usan cintas de respaldo; mientras que el 20% restante no tiene o no está planeando una estrategia todavía. (Arbesú, Pasos para un Plan de Recuperación de Desastres (DRP), 2013)

   Otro ejemplo de estrategia recomendada por VMware, es la virtualización, la cual representa un avance considerable al aplicarse en el Plan de Recuperación ante Desastres (DRP). Según la encuesta de Acronis, "*las razones principales por las que se adopta la virtualización en un DRP son: eficiencia mejorada (24%); flexibilidad y velocidad de implementación (20%) y reducción de costos (18%)"* (Arbesú, SearchDataCenter, 2013).

3. Presentar un análisis y selección de las mejores estrategias, que se adecuen a la necesidad y los recursos de la empresa, exponiendo valores o porcentajes de costos de la implementación del DRP. En el momento de seleccionar las estrategias se puede tener en

cuenta toda objeción que se presente por parte de los directivos. Para el caso en que la empresa se pregunte, si se tiene que duplicar el personal, con el temor de tener que aumentar el talento humano, se puede indicar −aunque es viable en caso que se requiera− que no es necesario, ya que existen formas de suplir este recurso, por ejemplo; documentando los procesos de funcionamiento de las aplicaciones de negocio para que cualquier persona los pueda operar.

4. Exponer los tiempos de ejecución de la implementación del DRP, ya que para los directivos de una empresa, siempre será importante conocer los costos y tiempos de un proyecto, por ello es indispensable demostrar un tiempo de ejecución, el cual puede oscilar entre 1 a 3 meses, teniendo en cuenta que la metodología se puede enfocar en lo crítico para las tareas y áreas de negocio más relevantes y para lo cual es importante que las informaciones estén documentadas, probadas e implementadas en un sitio alterno (ojalá en la nube para que pueda estar con una infraestructura mínima que consuma muy pocos recursos y "crezca" en el momento de un desastre").

4.4 ANÁLISIS Y EVALUACIÓN DE LA GUÍA, POR EXPERTOS.

Con el propósito de validar la guía para la elaboración de planes de recuperación de desastres desde el PMI en las áreas de tecnología informática de las empresas pequeñas y medianas en Bogotá D.C., se plantean 10 ítem o preguntas con posibilidades de respuesta: Totalmente de

acuerdo, De acuerdo, En desacuerdo, Totalmente en desacuerdo. Justifique su respuesta. Ítem que se listan a continuación:

1. ¿Las etapas planteadas en la presente guía son apropiadas?
2. ¿La secuencia de las etapas planteadas en el presente guía son adecuadas?
3. ¿Es correcta y consistente la terminología usada en el presente guía?
4. ¿La presente guía es una herramienta para aportar a la implementación de planes de recuperación de desastres en las empresas en Bogotá D.C.?
5. ¿Es posible que la guía propuesta contribuya a la mitigación o ayude a la reducción de los impactos negativos frente a la pérdida de los activos de tecnología informática?
6. ¿Los entregables sugeridos en la guía son los adecuados para documentar el proceso del DRP?
7. ¿El diseño propuesto para el análisis de impacto del negocio es el adecuado?
8. ¿Los cuatro criterios de seguridad descritos en la guía para identificar los riesgos son los apropiados?
9. Si conoce la regulación vigente para la implementación del DRP en las empresas. ¿Cree que las empresas en Bogotá D.C. pueden tener beneficios?
10. ¿Cree que las empresas en Bogotá D.C. puede tener beneficios con la aplicación la guía del DRP?

4.4.1. Análisis descriptivo por variable

Para la evaluación de la guía se contó con la evaluación de un experto en DRP, María Lucía Muñoz Grass, ingeniera Electrónica y de Telecomunicaciones, MBA. Conocimientos y experiencia en el desarrollo de negocios y servicios de DataCenter, y profesional services.

Conocimiento y experiencia en mercado de tecnologías cloud para mediana y gran empresa en Bogotá D.C., Formulación y gestión de proyectos bajo metodología PMI y aplicación de mejores prácticas para la Operación propuestas por ITIL. Desarrollo de planes de continuidad de negocio bajo metodología DRI. Aprendizaje continuo orientado a la generación de soluciones eficientes para el cliente y para la empresa. Facilidad para realizar trabajos en grupo, colaborando en la formulación de comunidades de práctica enfocadas en los objetivos de los proyectos empresariales.

Adicionalmente también fue evaluada por 4 Ingenieros de sistemas con especializaciones en Auditores de sistemas Informáticos con experiencia en implementación y auditoría en DRP, Ariel Garzón, Miguel Barbosa, Eida Maldonado y Carlos Guzmán.

En las tablas 12 hasta la 21, se presenta el resultado por cada una de las preguntas que fueron aplicadas para la evaluación de la guía.

En la tabla 12 se presentan los resultados a la pregunta 1. ¿Las etapas planteadas en la presente guía son apropiadas?

Tabla 12. Resultados pregunta 1

Respuesta	Justifique su respuesta 1.	Evaluador

De acuerdo	Aunque las etapas (son muy usuales) planteadas son apropiadas, se debe tener en cuenta que existen diversidad de Procesos, Hardware, Software, Personal, Comunicaciones, etc. que deben ser especificados para cada caso. Ej. Una empresa con software en la Nube, es diferente a una Empresa con software en un servidor en sus instalaciones.	Auditor 1
Totalmente de acuerdo	Las etapas siguen un orden lógico, y dan cobertura al Proyecto de implementación de un Plan de Recuperación de Desastres.	Auditor 2
De acuerdo	N/A	Auditor 3
Totalmente de acuerdo	N/A	Auditor 4
Totalmente de acuerdo	Cumple las fases con la metodología del DRP Y BCP del DRII y otros referentes como ITIL	Experto

Fuente: adaptación propia

En la tabla 13 se presentan los resultados a la pregunta 2. ¿Las etapas planteadas en la presente guía son apropiadas?

Tabla 13. Resultados pregunta 2

Respuesta	Justifique su respuesta 2.	Evaluador
Desacuerdo	Los Sistemas soportan a los Procesos y estos a los Objetivos, Misión, de la empresa. Por tanto la Secuencia debería ser vista desde lo más General a lo más Específico. Se observa que inician con la parte técnica. Tampoco hay una etapa de viabilidad financiera, donde se especifiquen los recursos monetarios que se requieren para hacer el plan, y para ejecutarlo, Se sugiere también una parte motivadora, justificadora para realizar el plan, especialmente si los dueños de empresas no están conscientes de la importancia del plan.	Auditor 1

Totalmente de acuerdo	Las etapas siguen un orden lógico.	Auditor 2
Totalmente de acuerdo	N/A	Auditor 3
De acuerdo	N/A	Auditor 4
Totalmente de acuerdo	Es la secuencia recomendada por los estándares Internacionales	Experto

Fuente: adaptación propia

En la tabla 14 se presentan los resultados a la pregunta 3. ¿Es correcta y consistente la terminología usada en el la presente guía?

Tabla 14. Resultados pregunta 3

Respuesta	Justifique su respuesta 3.	Evaluador
De acuerdo	Se sugiere colocar un Glosario con traducciones de términos o siglas en Inglés-Español	Auditor 1
Totalmente de acuerdo	Por el lenguaje y la redacción utilizada.	Auditor 2
De acuerdo	N/A	Auditor 3
Totalmente de acuerdo	N/A	Auditor 4
Totalmente de acuerdo	La traducción de conceptos y definiciones son las correctas.	Experto

Fuente: adaptación propia

En la tabla 15 se presentan los resultados a la pregunta 4. ¿La presente guía sirve como herramienta para aportar a la implementación de planes de recuperación de desastres en las empresas en Bogotá D.C.?

Tabla 15. Resultados pregunta 4

Respuesta	Justifique su respuesta 4.	Evaluador
De acuerdo	N/A	Auditor 1
Totalmente de acuerdo	Es un documento que puede ser utilizado como material de apoyo en cualquier empresa que desee llevar a cabo un proyecto de implementación de planes de recuperación de desastres.	Auditor 2
Totalmente de acuerdo	N/A	Auditor 3
De acuerdo	N/A	Auditor 4
De acuerdo	Sugiero para segunda fase sustentar el cómo se puede implementar a bajo costo, acorde con el presupuesto de TI de las empresas medianas en Bogotá D.C.	Experto

Fuente: adaptación propia

En la tabla 16 se presentan los resultados a la pregunta 5. ¿Es posible que la guía propuesta contribuya a la mitigación o ayude a la reducción de los impactos negativos frente a la pérdida de los activos de tecnología informática?

Tabla 16. Resultados pregunta 5

Respuesta	Justifique su respuesta 5.	Evaluador
En desacuerdo	Se debe tener presente, que en caso en que un accionista, dueño o inversionista no sea consciente de los aportes para su negocio o empresa que influye implementar el DRP, no se realiza o se hace como una condición impuesta. Además hacerles ver la importancia de las pruebas o simulacros.	Auditor 1
En desacuerdo	La guía es solo un documento de apoyo para la implementación de un DRP, la mitigación o reducción de los impactos negativos frente a la pérdida de los activos de tecnología informática se logra cuando se implementa el DRP.	Auditor 2
Totalmente de acuerdo	N/A	Auditor 3
De acuerdo	N/A	Auditor 4
Totalmente de acuerdo	Si se aplica correctamente.	Experto

Fuente: adaptación propia

En la tabla 17 se presentan los resultados a la pregunta 6. ¿Los entregables sugeridos en la guía son los adecuados para documentar el proceso del DRP.?

Tabla 17. Resultados pregunta 6

Respuesta	Justifique su respuesta 6.	Evaluador
De acuerdo	Faltan algunos, ver respuestas anteriores.	Auditor 1
De acuerdo	Son consistentes con las fases.	Auditor 2
Totalmente de acuerdo	N/A	Auditor 3
De acuerdo	N/A	Auditor 4
Totalmente de acuerdo	De acuerdo con el DRII	Experto

Fuente: adaptación propia

En la tabla 18 se presentan los resultados a la pregunta 7. ¿El diseño propuesto para el análisis de impacto del negocio es el adecuado?

Tabla 18. Resultados pregunta 7

Respuesta	Justifique su respuesta 7.	Evaluador
De acuerdo	Faltaría un motivador y justificador.	Auditor 1
Totalmente de acuerdo	Cobertura del BIA	Auditor 2
De acuerdo	N/A	Auditor 3
De acuerdo	N/A	Auditor 4
Totalmente de acuerdo	Contenido necesario para un BIA	Experto

Fuente: adaptación propia

En la tabla 19 se presentan los resultados a la pregunta 8. ¿Los cuatro criterios de seguridad descritos en la guía para identificar los riesgos son los apropiados?

Tabla 19. Resultados pregunta 8

Respuesta	Justifique su respuesta 8	Evaluador
De acuerdo	Hay conceptos muy generales que solo pueden entender personas que manejen el tema, y que deben ser más específicos para cada caso, o con un lenguaje más sencillo para que sea entendido e interiorizado para personas como dueños, líderes de otras áreas, etc.	Auditor 1
De acuerdo	Por la cobertura de los aspectos de seguridad.	Auditor 2
De acuerdo	N/A	Auditor 3
De acuerdo	N/A	Auditor 4
Totalmente de acuerdo	Son los recomendados	Experto

Fuente: adaptación propia

En la tabla 20 se presentan los resultados a la pregunta 9. Si conoce la regulación vigente para la implementación del DRP en las empresas, ¿ Considera que la guía cumple con la normatividad?

Tabla 20. Resultados pregunta 9

Respuesta	Justifique su respuesta 9.	Evaluador

De acuerdo	Aunque una guía nunca puede suplir una normatividad, legalmente dicho.	Auditor 1
N/A	No conozco muy bien la regulación vigente.	Auditor 2
De acuerdo		Auditor 3
Totalmente de Acuerdo	N/A	Auditor 4
Totalmente de Acuerdo	Si, los sectores regulados deben el DRP y el BCP y esta guía está acorde con los estándares recomendados.	Experto

Fuente: adaptación propia

En la tabla 21 se presentan los resultados a la pregunta 10. ¿Cree que las empresas en Bogotá D.C. pueden tener beneficios con la aplicación la guía del DRP.?

Tabla 21. Resultados pregunta 10

Respuesta	Justifique su respuesta 10.	Evaluador
De acuerdo	Sí puede ayudar la guía, pero lo más importante es el acompañamiento, la puesta en práctica, la ejecución, los resultados, la concientización y la apropiación. Ejemplo de esto son los planes en Aeronáutica, Gas and Oil, donde son bastantes estrictos y muy bien realizados. También otro ejemplo es en Japón en la parte de Infraestructura debido a su entorno sísmico. La Normatividad "Obliga" pero no concientiza. En	Auditor 1

	Colombia hay muchos ejemplos de cómo la gente se salta la normatividad.	
Totalmente de acuerdo	Por los beneficios que posee la empresa al estar preparada en caso de presentarse un desastre. Mitigación de los riesgos.	Auditor 2
De acuerdo	N/A	Auditor 3
De acuerdo	N/A	Auditor 4
Totalmente de acuerdo	Es necesario que las empresas en Bogotá D.C. sean más conscientes de la prevención de riesgos informáticos y esta guía es una herramienta útil para su negocio.	Experto

Fuente: adaptación propia

4.4.2. Análisis de las respuestas en desacuerdo con la guía.

Posteriormente se realiza un análisis de las 3 respuestas, en que los expertos estuvieron en desacuerdo con la propuesta de la guía.

Pregunta 2.

¿La secuencia de las etapas planteadas en el presente guía son las adecuadas?

Respuesta del Auditor 1.

Los Sistemas soportan a los Procesos y estos a los Objetivos, Misión, de la empresa. Por tanto la Secuencia debería ser vista desde lo más General a lo más Específico. Se observa que inician con la parte técnica. Tampoco hay una etapa de viabilidad financiera, donde se especifiquen los recursos monetarios que se requieren para hacer el plan, y para ejecutarlo, Se sugiere también una parte motivadora, justificadora para realizar el plan, especialmente si los dueños de empresas no están conscientes de la importancia del plan.

Análisis.

Para esta guía lo que se pretende, según como se planteó en el objetivo general es proponer un diseño de un plan de recuperación de desastres de las áreas de Tecnología Informática desde El Project Management Institute (PMI) dirigida para un segmento de empresas pequeñas y medianas en Bogotá D.C., presentándose de una forma general y no detallada, ahora para el punto de vista en que no existe una etapa de viabilidad financiera, según los estándares internacionales del DRP no existe una etapa donde se valide la viabilidad financiera dentro del plan de recuperación de desastres, sin embargo en la tesis se dispuso de un capítulo dónde se analiza la importancia de un DRP en las áreas de tecnología informática para las empresas pequeñas y medianas en Bogotá D.C., donde se concluye sobre los beneficios de los costos al implementar un DRP en las empresas, además es importante aclarar que para definir un costo, éste se debe tener determinado ante una situación particular tanto interna como externa de la empresa en la que se desea implementar.

Para el caso en que se siguiera tener un “motivador” éste haría parte de un rol dentro el proyecto en el que sólo según la empresa lo decide disponer, aunque este rol ya se encuentra inmerso

dentro del área de tecnología de las organizaciones, quienes son un factor importante en el momento de vender a los interesados el proyecto para que éste llegue a ser aprobado.

Nota: Para la pregunta número 2 de la evaluación de la guía, de los 5 encuestados, entre ellos 4 auditores y 1 experto se obtuvo una sola respuesta en desacuerdo.

Pregunta 5

¿Es posible que la guía propuesta contribuya a la mitigación o ayude a la reducción de los impactos negativos frente a la pérdida de los activos de tecnología informática?

Respuesta del Auditor 1.

Si un accionista, dueño o inversionista no es consciente de los aportes para su negocio o empresa, no se realiza o se hace como una condición impuesta. Además hacerles ver la importancia de las pruebas o simulacros.

Análisis:

Según lo que argumenta el auditor 1 en la justificación de la respuesta es que para los inversionistas, dueños o accionistas, pueden que al no ser conscientes de la importancia de implementar el DRP en empresa consideren que esta guía no contribuye a la mitigación o ayude a la reducción de los impactos negativos que pueden presentar las empresas, pero es importante aclarar que esta guía se presenta como un diseño en el momento de implementar el DRP en las empresas, es decir cuando ya se han mostrado a los inversionistas, dueños y accionistas la importancia de invertir en este proyecto, mostrándoles los aportes para su empresa.

Respuesta del Auditor 2.

La guía es solo un documento de apoyo para la implementación de un DRP, la mitigación o reducción de los impactos negativos frente a la pérdida de los activos de tecnología informática se logra cuando se implementa el DRP.

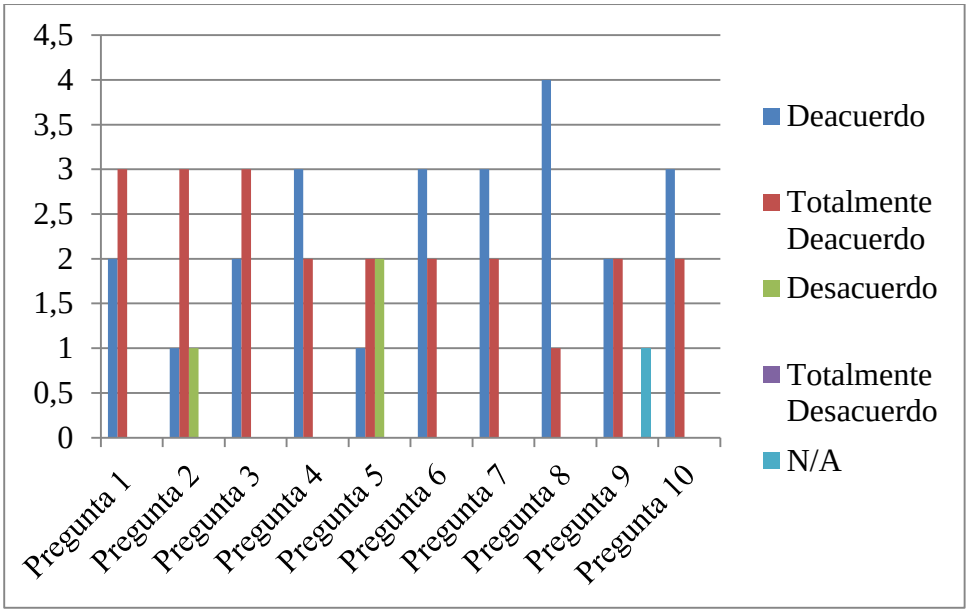
Análisis:

Es importante aclarar que en la pregunta no se especificó que la guía propuesta al ser implementada contribuye a la mitigación o ayuda a la reducción de los impactos negativos frente a la pérdida de los activos de tecnología informática, por lo tanto el Auditor 2 manifestó estar en desacuerdo si solo la guía se deja como un documento y no se implementa en la empresa.

Nota: Para la pregunta número 5 de la evaluación de la guía, de los 5 encuestados, entre ellos 4 auditores y 1 experto se obtuvo 2 respuestas en desacuerdo

En la siguiente ilustración 6, se muestra la gráfica de la evaluación de la guía, verticalmente se encuentra el número de respuestas que se encuentran en: desacuerdo, totalmente de acuerdo, desacuerdo, totalmente desacuerdo o N/A cuando no aplica, según el color que corresponda y verticalmente aparecen las 10 preguntas que correspondían a la encuesta.

Ilustración 6. Gráfica de la evaluación de la guía por los expertos



Fuente: adaptación propia

Con el propósito de complementar, la sugerencia realizada por el experto, De cómo se puede mitigar costos al momento de implementar un DRP, se describen 3 aspectos, con sus respectivos ejemplos, para ayudar a reducir costos al momento de implementar un DRP, sin necesidad de hacer grandes inversiones:

1. Recurso humano: este aspecto es fundamental al momento de implementar el DRP y más cuando se trata de reducir costos, ya que el personal de las empresas es el que tiene gran participación en la ejecución de los procesos, cómo ejemplo para salvaguardar la información de la empresa, se propone el mantener habilidades y conocimientos de protección de información a todos los empleados del área de tecnología informática, para evitar en la eventualidad de que alguien falte, el no tener como responder ante un servicio, por esto es importante que exista otra persona que conozca los procesos o actividades de los sistemas hardware o software, también se propone evitar los accesos remotos desde fuera de la oficina, seleccionar personal capacitado para los procesos

críticos y finalmente realizar configuración de accesos a los sitios o sistemas de acuerdo a los perfiles y cargos de los empleados.

2. Hardware y software: lo que se pretende mostrar en este aspecto es que se debe garantizar, que los sistemas sean tolerantes a fallos, que puedan continuar brindando con el servicio por medio de sistemas, que compartan carga de trabajo para evitar recursos ociosos y bajo desempeño, para ello se pueden realizar controles preventivos, para garantizar la disponibilidad continuamente de las aplicaciones, y como último ejemplo están los Hot sites: Normalmente está configurado con todo el hardware y el software requerido para iniciar la recuperación de los sistemas a la mayor brevedad.

3. Información: Buscar sitios de recuperación externos, pero al mismo tiempo, tener métodos de recuperación interna −cómo Backus− que se realicen periódicamente. Levantar procedimientos y manuales, buscar el medio para que la información pueda estar en su mayoría digitalmente, y finalmente se pueden hacer acuerdos con los proveedores y clientes para la protección de la información.

4.4.3. Conclusiones de la evaluación de la guía.

Finalmente se realiza un análisis de la evaluación de la guía realizada por los auditores y el experto.

- ✓ La guía presenta las etapas apropiadas que se deben tener en cuenta para la implementación de un DRP, cumpliendo con las fases de la metodología DRII.

- ✓ Este documento puede ser utilizado como material de apoyo en cualquier empresa que desee llevar a cabo un proyecto de implementación de planes de recuperación de desastres.

- ✓ El diseño propuesto del análisis de impacto del negocio tiene un contenido adecuado que sirve como un apoyo a la hora de realizar el BIA en las empresas.

- ✓ Es necesario que las empresas en Bogotá D.C. sean más conscientes de la prevención de riesgos informáticos y esta guía es una herramienta útil para su negocio, ya que podrá estar preparada para cualquier emergencia.

5. CONCLUSIONES Y RECOMENDACIONES GENERALES

- ✓ Después de realizar el diagnóstico de conocimiento y grado de implementación de DRP en el segmento de empresas pequeñas y medianas en Bogotá D.C. se evidenció en las

entrevistas las falencias que presentan frente al compromiso que se debe tener con respecto a la seguridad de la información y esto se demuestra con el corto conocimiento, que posee el personal responsable o encargado de los procesos que se encuentran asociados con el área de Tecnología, además de la falta de ejecución en las empresas del Plan de Recuperación de Desastres.

- ✓ El conjunto de acciones gerenciales, propuestas en la guía para la implementación del DRP en las empresas pequeñas y medianas no reguladas en Bogotá D.C., es un diseño que puede ser utilizado como material de apoyo en cualquier empresa que desee llevar a cabo este proyecto, ya que esta guía cuenta con las etapas apropiadas que cumplen con la metodología DRII.

- ✓ Al realizar la validación del plan de recuperación de desastres por un experto en DRP y 4 auditores de sistemas informáticos se consideró que la guía cumple con el objetivo general de proponer un diseño para la elaboración de planes de recuperación de desastres desde el PMI en las áreas de tecnología informática de las empresas pequeñas y medianas en Bogotá D.C.

GLOSARIO

Plan de Continuidad de Negocio (BCP):

"Son los planes logísticos para la práctica de cómo una organización debe recuperar y restaurar sus funciones críticas parcial o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción no deseada o desastre" (Reyes, 2009).

Fenómeno natural:

Un fenómeno natural es un cambio de la naturaleza que sucede por sí solo sin intervención directa del hombre, son aquellos procesos permanentes de movimientos y de transformaciones que sufre la naturaleza. (DRP, 2014)

Desastre natural:

Los desastres naturales siempre se presentan por la acción del hombre en su entorno y hace referencia a las enormes pérdidas materiales y de vidas humanas, ocasionadas por fenómenos naturales como los terremotos, inundaciones, Tsunamis, deslizamientos de tierra, deforestación, contaminación ambiental y otros". (DRP, 2014)

Plan de Recuperación de Desastres (DRP):

Es la estrategia que se seguirá para restablecer los servicios únicamente del área de Tecnología Informática (Hardware y Software) después de haber sufrido una afectación por una catástrofe natural, epidemiológica, falla masiva, daño premeditado, ataque de cualquier tipo el cual atente contra la continuidad del negocio. (InBEST, 2014)

PMI:

El Project Management Institute (PMI) es una de las asociaciones profesionales de miembros más grandes del mundo que cuenta con medio millón de miembros e individuos titulares de sus

certificaciones en 180 países. Es una organización sin fines de lucro que avanza en la profesión de la dirección de proyectos a través de estándares y certificaciones reconocidas mundialmente, a través de comunidades de colaboración, de un extenso programa de investigación y de oportunidades de desarrollo profesional. (americalatina.pmi.org, 2015)

PMBOK:

Es el conjunto de conocimientos en Dirección, Gestión, Administración de Proyectos generalmente reconocidos como «buenas prácticas», y que se constituye como estándar de administración de proyectos. (wikipedia, 2015)

Plan de Contingencia:

El plan de contingencia, "Contempla cómo reaccionar ante una contingencia que pueda afectar la disponibilidad o los servicios ofrecidos por los sistemas informáticos" (SISTESEG, 2012).

Riesgo:

En términos del Riesgo Tecnológico, existe consenso generalizado en definirlo como: la posibilidad de pérdidas derivadas de un evento relacionado con el acceso o uso de la tecnología, que afecta el desarrollo de los procesos del negocio y la gestión de riesgos de la organización, al comprometer o degradar las dimensiones críticas de la información (Ej. confidencialidad, integridad, disponibilidad) (Franco, 2013).

Análisis de Impacto:

Un análisis de impacto en el negocio (BIA) es una parte clave en el proceso del plan de recuperación de desastres, ya que analiza las funciones criticas del negocio, e identifica y cuantifica el impacto que implica no tener esas funciones disponibles para la empresa, "*será la guía que determine qué necesita ser recuperado y el tiempo que tarde dicha recuperación, actividades que en el Plan de Continuidad de Negocios se convierten quizás en las más difíciles y críticas por realizar adecuadamente."* (Camelo, 2010)

TI:

La tecnología informática es el "*Estudio, diseño, desarrollo, innovación puesta en práctica, ayuda o gerencia de los sistemas informáticos computarizados, particularmente usos del software y hardware*" (wikipedia, 2015).

Amenaza:

La amenaza "Corresponde a un fenómeno de origen natural, socio-natural, tecnológico o antrópico en general, definido por su naturaleza, ubicación, recurrencia, probabilidad de ocurrencia, magnitud e intensidad" (DRIDN, 1992), este fenómeno puede afectar las operaciones de TI, de las empresas.

Seguridad de la información:

"Es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma" (ISO/IEC 27011, 2008).

Acción correctiva:

"Es aquella que llevamos a cabo para eliminar la causa de un problema" (Calidad Total, 2013).

Acciones preventivas:

Son aquellas "acciones que se anticipan a la causa, y pretenden eliminarla antes de su existencia. Evitan los problemas identificando los riesgos. Cualquier acción que disminuya un riesgo es una acción preventiva" (Calidad Total, 2013).

RTO:

Tiempo Objetivo de Recuperación (RTO, Recovery Time Objective) es el tiempo que pasará una infraestructura (Tecnológica, Logística, Física) antes de estar disponible, es decir *"Expresa el tiempo durante el cual una organización pueda tolerar la falta de funcionamiento de sus aplicaciones y la caída de nivel de servicio asociada, sin afectar a la continuidad del negocio"* (BILA, 2014).

RPO:

Punto Objetivo de Recuperación (RPO, Recovery Point Objective) *"Determina el objetivo de posible pérdida máxima de datos introducidos desde el último backup, hasta la caída del sistema, y no depende del tiempo de recuperación"* (BILA, 2014).

Servidor:

"Es un nodo que, formando parte de una red, provee servicios a otros nodos denominados clientes" (wikipedia, 2014).

Criticidad:

Es un estado de una reacción la cual, "Es usada para mostrar el impacto del riesgo sobre los factores críticos de éxito de un proyecto, generalmente se usa como el medio principal para priorizar los riesgos" (Barber, 2009).

Probabilidad:

La probabilidad según el diccionario de la real academia Española, es un método por el cual se obtiene la frecuencia de un acontecimiento determinado mediante la realización de un experimento aleatorio, es decir la medida de cuan es posible que un evento ocurra, pero cuando hablamos de un concepto especifico al plan de recuperación de desastres hace referencia a "*un estimado de cuan probable es que un riesgo impacte un proyecto"* (Barber, 2009).

BIBLIOGRAFÍA

Ali H. Al- Badi, Rafi Ashrafi, Ali O. Al- Majeeni, Pam J. Mayhew, (2009) "IT disaster recovery: Oman and Cyclone Gonu lessons learned", Information Management & Computer Security, Vol. 17 Iss: 2, pp.114 – 126.

(Abarca R, 2012)Bell, Judy. "Why Some Recovery Plans Won't Work." Disaster Recovery Journal. Spring 2003: 30 - 32.

Abarca R, Carlos,Oficina estrategica de proyectos. Experiencia Banco Nacional, 2012)

Alvarez, Alonso, Arquero, Hidalgo Mantenimiento óptimo de equipamientos universitarios.

Arbesú, lizzette Pérez, Pasos para un Plan de Recuperación de Desastres (DRP), 2013

Arcos, psicologia aplicada a la seguridad informatica, 2011

Aristizabal Botero, Carlos Andrés, metodologia y investigacion, guia didactica y modulo, 2008

Bancoldex, pymes, 2014

Barber, Carlos Miguel, sostenibilidad o sustentabilidad, 2009

BILA, Gestión de continuidad del negocio, 2014

Barrantes, Generando idinteficación y uso de variables e indicadores, 2006)

Bounds, Gene. “Preparing for the Worst: A Best Practices Guide to Disaster Recovery Planning.” April 2003. URL: http://www.contingencyplanning.com/PastIssues/apr2003/5.cfm (07 June 2003).

Camelo, Leonardo, seguridad de la informacion en Colombia, 2010.

CIIFE, centro internacional,para investigacion de el niño, 2014

Charles E. Adie, Natural Hazards Research and Applications Information Center, Boulder University of Colorado Holistic Disaster Recovery DIANE Publishing, 1/09/2001 – 2002.

C.G. Rudolph, "Business Continuation Planning/Disaster Recovery: a Marketing Perspective", IEEE Communications Magazine, 1990, Vol. 28, No. 6, pp. 25-28.

Musson and E. Jordan Business and Computer Contingency Planning in Australia, 1997.

Con12, Continuidad del Negocio y Recuperación de Desastres, 2012

Cuellar, Leila, Planeacion estratégica de proyectos, 2010)

Disasters Volume 31, Issue 4, pages 508–515, December 2007.

(DRP, consultores de desastres naturales, 2014)

Disaster Recovery Planning: Project Plan Outline.” Computing & Networking Services, University of Toronto. URL: ttp://www.utoronto.ca/security/drp.htm (05 June 2003).

Delgado, Alexander Solís, Modulo de capacitacion de desastres y emergencias tecnológicas,1997)

D.R. Smith, W.J. Cybrowski, F. Zawislan, et al, "Contingency/ Disaster Recovery Planning for Transmission Systems of the Defense Information System Networks", IEEE Journal on Selected Areas in Communications, 1994, Vol. 12, No. 1, pp. 13-22.

Departamento Nacional de Planeación, prosperidad para todos, 2010

Emergency Management Guide for Business and Industry, 1996 :Federal Emergency Management Agency.

Ferrer, Metodología para el diseño de un Plna de Recuperación de Desastres o DRP, 2014

Franco IT, Governance Risk & Compliance, 2013

Frank Cervone, (2006) "Disaster recovery and continuity planning for digital library systems", OCLC Systems & Services: International digital library perspectives, Vol. 22 Iss: 3, pp.173 – 178.

Fitz-Gibbon, Thomas P. "Disaster Recovery Planning for Call Centers." ontingency Planning and Management. March 2003: 26 – 28.

Gabaldón, Arnoldo José, Desarrollo sustentable, la salida a América Latina, 2006

Gaspar, Planes de contigencia: la continuidad del negocio en las organizaciones.

Goh Moh Heng, (1996) "Developing a suitable business continuity planning methodology", Information Management & Computer Security, Vol. 4 Iss: 2, pp.11 – 13

Herriott, Larry. “Business Contingency Planning Is…” PHH Corporation. URL: http://www.drj.com/new2dr/w3_006.htm (05 June 2003).

Hervías, Victor, Gestionando la Continuidad de nuestro negocio, 2010.

Ivancevich, Daniel M., Dana R. Hermanson, and L. Murphy Smith. "The Association of Perceived Disaster Recovery Plan Strength with Organizational Characteristics." Journal of Information Systems 12.1 (1998).

ISO/IEC 27011, 2008

Jordan and A. M. Whiteley "HRM practices in information technology management", Proceedings of the 1994 ACM SIGCPR (Special Interest Group on Computing Personnel Research) Conference, pp.57 -64 1994.

Jacques Botha, Rossouw Von Solms, (2004) "A cyclic approach to business continuity planning", Information Management & Computer Security, Vol. 12 Iss: 4, pp.328 – 337

Kunene, Glen. "Create a Disaster Recovery Plan." URL: http://archive.devx.com/enterprise/articles/drecovery/IBM_BCRS/Demarco-1.asp (07 June 2003).

J. D. Couger and R. A. Zawacki Motivating and Managing Computer Personnel, 1980.

John Rittinghouse, PhD, CISM, James F. Ransome, PhD, CISM, CISSP Digital Press, Business Continuity and Disaster Recovery for InfoSec Managers 8/04/2011 - 408 páginas.

J.R Hackman and G.R. Oldham "Development of the Job Diagnostic Survey", Journal of Applied Psychology, vol. 60, no. 2, pp.159 -170 1973

Mintzberg, Henrry, Planeación estratégica 2007

Miranda, Juan José, El desafio de la gerencia, principios y orientasciones del PMI, 2006)

Manager's Guide to Contingency Planning for Disasters: Protecting Vital Facilities and Critical Operations Kenneth N. Myers. Wiley, 1999.

Michael Whitman, Herbert Mattord, Andrew Green Principles of Incident Response and Disaster Recovery Cengage Learning, 16/04/2013 - 576 páginas.

N. Uddin and D. Engi, "Disaster Management System for Southwestern Indiana", Natural Hazards Review, 2002, Vol. 3, No. 1, pp. 19-30.

P. Fallara, "Disaster Recovery Planning", IEEE Potentials, 2004, Vol. 22, No. 5, pp. 42-44.

P.E. Hayes and A. Hammons, "Disaster Recovery Project Management", Proceedings of IEEE 47th Petroleum and Chemical Industry Conference, Sep. 2000, pp. 55-63.

Project Management Institute, 2008,

Questions and Information Systems Thomas W. Lauer; Arthur C. Graesser; Eileen Peacock. Lawrence Erlbaum Associates, 1992.

Ramirez, Augusto, La teoría del conocimiento, una visión actual, 2009.

Real Academia Española, Diccionario de la lengua Española, 1992.

Revista Tecnológica, 2014 Reyes, Rene, Rebista Tecnológica, 2009

Rethinking Management Information Systems: An Interdisciplinary Perspective Wendy Currie; Bob Galliers. Oxford University Press, 1999.

Rao, Lila; McNaughton, Maurice; Osei-Bryson, Kweku-Muata; and Haye, Manley, "The Role of Ontologies in Disaster Recovery Planning" (2009). AMCIS 2009 Proceedings. Paper 713. http://aisel.aisnet.org/amcis2009/713

Sánchez Natalia, Plan de recuperación ante desastres (DRP), 2013

The Disaster Recovery Handbook: A Step-by-Step Plan to Ensure Business Continuity and Protect Vital Operations, Facilities, and Assets Michael Wallace; Lawrence Webber. American Management Association, 2011.

Tipton, H. and Krause, M. Information Security Management Handbook 4th Edition. NY: Auerbach Publications, 2000. 581 – 596.

K. Wang, R.D. Su, Z.X. Li, et al, "Robust Disaster Recovery System Model", Wuhan University Journal of Natural Sciences, 2006, Vol. 11, No. 1, pp. 170-174.

Kirvan, Paul. “What's Wrong with BCP?” January 2003. URL: http://www.contingencyplanning.com/PastIssues/janfeb2003/1.cfm (06 June 2003).

K. Hardy "Contingency Planning", Business Quarterly, vol. 56, no. 4, pp.26 -28 1992

USA", Information & Management, pp.41 -46 1990.

Wing S. Chow, Wai On Ha, (2009) "Determinants of the critical success factor of disaster recovery planning for information systems", Information Management & Computer Security, Vol. 17 Iss: 3, pp.248 – 275.

W. Lam, "Ensuring Business Continuity", IT Professional, 2002, Vol. 4, No. 3, pp. 19-25.

Documentos Electrónicos

http://www.uci.ac.cr/Biblioteca/Tesis/PFGMAP505.pdf

http://searchdatacenter.techtarget.com/es/cronica/Pasos-para-un-Plan-de-Recuperacion-de-Desastres-DRP

http://www.sisteseg.com/files/Microsoft_Word_-_METODOLOGIA_PLAN_RECUPERACION_ANTE_DESASTRES_DRP.pdf

http://www.abovesecurity.com/pdf/Folleto_Disaster_Recovery_Plan_ES.pdf

http://bilait.co/blog/

http://www.sisteseg.com/sindustrial.html

http://www.iso27000.es/sgsi.html

http://es.wikipedia.org/wiki/Plan_de_recuperaci%C3%B3n_ante_desastres

www.ISO27001.es

http://www.ifrc.org/es/introduccion/disaster-management/sobre-desastres/que-es-un-desastre/

http://www.ciifen.org/index.php?option=com_content&view=category&layout=blog&id=86&Itemid=128&lang=es

http://www.iso27001standarD.C.om/es/

ANEXOS

Anexo A. Análisis de Información.

Categoría	Sub Categorías	Entrevista 1	Entrevista 2	Entrevista 3	Entrevista 4	Entrevista 5	Entrevista 6	Entrevista 7(EXPERTO)
Información de la Empresa (IE)	**Cargo Entrevistado(CE)**	Gerente de Tecnología (GT)	Administrador de base de datos(ABD)	Coordinador de Infraestructura(CI)	Administrador de base de datos	Administrador de base de datos	Administrador de base de datos	Arquitecto de infraestructura (AI)
	Nombre de la empresa(NE)	Consejo Colombiano de Seguridad(CCS)	Copservir Ltda(CL)	Consejo Colombiano de Seguridad(CCS)	Grupo de Tecnología Móvil GTM	OSP INTERNATINAL CALA	eTask Servicios de Colombia	AVANXO(A)
	Modelo de Negocio (MN)	Seguridad industrial, salud ocupacional y Seguridad Ambiental (SISOSA)	Sector farmacéutico del país(F)	Seguridad industrial, salud ocupacional y Seguridad Ambiental (SISOSA)	Reparación de celulares a fabricantes	Ofrece servicios de telecomunicaciones a las empresas del sector.	Desarrollo De Software Para Administración Inteligente De Proyectos	Mejores prácticas de la industria para la gestión y optimización de procesos de negocio(GOPN)

	factibilidad de ejecutar un DRP si no existe	Sí, es absolutamente viable, a medida que las compañías crecen empiezan a generar conciencia en el plan de recuperación de desastres, para desarrollar las iniciativas.	En este momento es vital el diseño de un plan de recuperación de desastres, debido a la gran cantidad de información que se maneja y a la importancia que esta tiene para la operación del negocio. Adicional a esto con una buena implementación se garantiza que al presentarse una caída se restablezca en un tiempo más corto.	La empresa ya se encuentra implementando el DRP y los procedimientos para saber cómo enfrentar un desastre que atente con la información.	Se puede tener debido a que aún se guardan datos en papel, se puede recuperar de desastres, pero sería muy lento y traumático para la operación de la organización	Sí es factible para la empresa ajustar el plan actual de recuperación de desastres	Se dificulta el diseño y ejecución de planes de recuperación	
	Clientes (C)	Empresas(E)	Personas(P)	Empresas(E)	Empresas(E)	Empresas(E)	Empresas(E)	Empresas(E)
Protección	**Metodo de Salvagu**	Backup(B), Servidores(S)	Servidores(S), USB	Backup(B), Servidores(S)	Backup(B), Servidores(S), **Disco**	Servidores(S),	Bases de datos alojadas en	Sitio alterno (Off-site)(OS)

	ardar(MS)				**de espejo**		servidores (S) con respaldo internacional.	
	Ante un Desastre(AD)	la empresa no cuenta con un Plan de recuperación(NDRP)	la completitud de la información que se recoge a diario.(CB)	3 Tipos de copia de seguridad (CB)	Realiza un backup del servidor, del cual se tienen 2 copias una se almacena en la empresa y la otra en una locación ubicada a más de 20 km de la sede administrativa.(CB)	• Protección información de la empresa: Redundancia servidor y equipos de los empleados. • Protección información de los clientes: Redundancia servidor, dd portable y equipos de los empleados. • Para las cuentas de correo electrónico, nuestro proveedores google. Por lo tanto la seguridad de la información correspondiente a las cuentas de correo electrónico están dispuestas a la	El manejo de almacenamiento y mantenimiento de la información de la empresa se encuentra subcontratado a una empresa con sede en los Estados Unidos. Esta empresa es responsable de garantizar la disponibilidad de la información ante cualquier eventualidad.	Administración de operaciones" de la norma ISO 27001 (AO)

						protección que ofrece google.		
	Políticas de seguridad de Información(PSI)	Si, la gerencia de tecnología ha diseñado una política de seguridad la cual ha sido socializada los días lunes en las reuniones de calidad a toda la organización, a partir de esta política se han diseñado planes para salvaguardar la información. Básicamente porque la seguridad es una prioridad	Actualmente no se cuenta con políticas definidas y socializadas a las personas que intervienen en el proceso, Se cuenta con manuales desactualizados para el manejo de los diferentes medios de recopilación y salvaguarda de información. (PIPSINO)	Actualmente se encuentran implementando las políticas de seguridad de la información y realizando el levantamiento de los proceso para salvaguardarla con una matriz de riesgos que pretende mitigar la pérdida de la información que la empresa posee y que el área de infraestructura hace	Además de las políticas de administración y cuidado de la información de acceso al servidor que se documentan desde hace 2 años, se brindan a nivel de cada aplicación, contable y financiera, y de equipos por medio de los perfiles que maneja cada uno de éstos.(PIPI SISI)	Cómo política de seguridad se tiene lo siguiente:a. Se ha designado un administrador de la plataforma de incidentes. Este administrador será el encargado de abrir un nuevo proyecto en dicha plataforma; también puede borrar un proyecto y dar de alta a quien tendrán perfil de administrad	No. El mantenimiento y cuidado de la información se encuentra contratado con un tercero por lo que esta información no es de dominio de la mayoría de los empleados.	Básicamente porque la seguridad es una prioridad para las organizaciones y legítimamente lo es (legalmente). Proteger los datos de los Clientes y sus activos internos debe ser la prioridad No. 1.Debe ser una prioridad proteger los datos contra accesos no autorizados, robos o daños con el fin de garantizar la confidencialidad, integridad, disponibilidad y confiabilidad de los mismos.

		para las organizaciones y legítimamente lo es (legalmente). Proteger los datos de los Clientes y sus activos internos debe ser la prioridad No. 1.Debe ser una prioridad proteger los datos contra accesos no autorizados, robos o daños con el fin de garantizar la confidencialidad, integridad, disponibilidad y confiabilidad de los mismos.		parte de esta labor ya que Por medio de la implantación de estas medidas o controles de alguna forman se podrá reducir el impacto producido por un evento determinado.(PIPSISI)		or.b. Hay una persona encargada de hacer las actualizaciones al software realizado por cada proyecto. c. Hay un rol de DBA encargado de hacer las actualizaciones de base de datos por cada proyecto. Ninguna otra persona podrá hacer actualizaciones sino este encargado. d. Existe una plataforma para subir la información de desarrollos, actualizaciones y nueva documentación. Cómo política de seguridad se tiene lo siguiente:a. Se ha designado un administrad		

						or de la plataforma de incidentes. Este administrador será el encargado de abrir un nuevo proyecto en dicha plataforma; también puede borrar un proyecto y dar de alta a quien tendrán perfil de administrador.b. Hay una persona encargada de hacer las actualizaciones al software realizado por cada proyecto. c. Hay un rol de DBA encargado de hacer las actualizaciones de base de datos por cada proyecto. Ninguna otra persona podrá hacer actualizaciones sino		

						este encargado. d. Existe una plataforma para subir la información de desarrollos, actualizaciones y nueva documentación.		
	Procedimientos Documentados(PD)	No, actualmente no se encuentran documentados en detalle los procedimientos de protección de la información.(PIPDN)	No han sido actualizados y por lo tanto ya no aplican con los nuevos procesos.(PIPDN)	Actualmente no se encuentran documentados estos procesos, ya que están en este proceso. (PIPDN)	Las políticas de administración y acceso al servidor, si se tienen documentado, al igual que las que tiene el software contable Siigo. (PIPDS)	Actualmente no se encuentran documentados estos procesos. (PIPDN)	Actualmente no se encuentran documentados estos procesos. (PIPDN)	
	Procedimientos Actualizados (PA)	En julio del 2013 la política de seguridad de la información junto con la política de clasificación de la información fueron	No se han realizado pruebas a estos procedimientos, se definen fechas para ejecución de simulacros pero no se cumplen.	No tengo conocimiento con exactitud de cuando se inició o se actualizo el levantamiento de estos procesos. (PIPAN)	Actualizado hace unos meses (PIPAS)	Hace dos años se estableciero n estas políticas o normas por parte del líder de desarrollad ores.	No se tiene la información.	

		actualizadas, pero como tal los procedimientos en detalle hasta ahora se van a empezar a realizar (PIPAN)	(PIPAN)					
	Periodicidad de Capacitación (PC)	Mensualmente(M)	Esporádicamente(E)	Semanalmente(S)	No define. (ND)	No define. (ND)	No se tiene la información.	Entrenamientos Regulares (ER)
Personal de la	**Conocimientos DRP(CDRP)**	Básico(B)	Formación Profesional (FP)	Básico(B)	Básico(B)	Básico(B)	Básico(B)	

	Ejecutan Estrategias de Recuperación (EER)	No existen procedimientos para salvaguardar esta información en medio de un desastre, por lo tanto no sabríamos como responder organización y a nuestros clientes ante un desastre, estamos encaminados a la realización de estos procesos con gran urgencia ya que conocemos la gran importancia de tener implementado el Plan de Recuperación de Desastres en la organización.(NE)	La gerencia de sistemas no ha establecido estos protocolos en la operación diaria, (NE)	No los conozco hasta el momento, ya que lo que tengo entendido hasta ahora los están desarrollando(NE)	políticas de administración y cuidado de la información de acceso al servidor que se documentan desde hace 2 años, se brindan a nivel de cada aplicación, contable y financiera, y de equipos por medio de los perfiles que maneja cada uno de éstos (SE)	Actualmente el servidor que contiene la información principal se encuentra en las instalaciones de Medellín. Se ha pensado en instalar un servidor robusto en OSP Bogotá para replicar la información. Esto con el fin de no tener los servidores en el mismo recinto.	No tienen estrategias de Recuperación de Desastres.	Las estrategias de recuperación están basadas en los resultados obtenidos luego de la realización del BIA (Business Impact Análisis), en donde también se consideran los valores de los tiempos máximos permitidos de no disponibilidad (MTD), el RPO y el RTO Las estrategias de recuperación están basadas en los resultados obtenidos luego de la realización del BIA (Business Impact Análisis), en donde también se consideran los valores de los tiempos máximos permitidos de no disponibilidad (MTD), el RPO y el RTO.Realizando también un análisis de todos los datos obtenidos en las entrevistas, el entendimiento de los procesos de negocio, el BIA, el MTD, el RPO y el RTO, se procede a consolidar una matriz ordenada con prioridades de recuperación de los diferentes sistemas considerados como críticos, considerando:• Sistemas telefónicos • Redes Locales• Redes WAN• Redes metropolitanas y/o regionales• Internet• Personas• Infraestructura física• Aplicaciones• Hardware• Bases de datos• Sistemas operativos• Firewalls• IDS-IPS• Switches• RoutersLas estrategias a seguir se

								describen a continuación:1. Hot sites: Normalmente está configurado con todo el hardware y el software requerido para iniciar la recuperación a la mayor brevedad.2. Warm sites: En esta opción no se incluyen servidores específicos de alta capacidad.3. Cold sites: En esta opción sólo se tiene aire acondicionado, potencia, enlaces de telecomunicaciones, y otros.4. Acuerdos recíprocos con otras organizaciones.5. Mirror site: Se procesa cada transacción en paralelo con el sitio principal.6. Múltiples centros de procesamiento.(EBBIA)
	DRP	El plan de recuperación de desastres es un proceso de recuperación que cubre los datos, el hardware y el software crítico, para que un negocio pueda comenzar de nuevo	El DRP está enfocada a la recuperación ante un proceso netamente del área de TI (CDRP2)	Plan de recuperación de desastres se encarga del área de Tecnología hardware y software pero que al igual es trasversal a toda la organización. (CDRP3)	No define. (ND)	No define. (ND)	El plan de continuidad de negocio debe tener en cuenta otros aspectos diferentes a la manifestación de un desastre	conjunto de actividades y procedimientos que hacen posible a una organización responder ante un desastre y reiniciar sus funciones críticas en una condición aceptable, en un período de tiempo determinado, orientado a recuperación de infraestructura y tecnología (CDRP4)

		sus operaciones en caso de un desastre natural o causado por humanos (CDRP1)						
	BCP	El BCP es el cómo la empresa se prepara para futuros incidentes o desastres como incendios, terremotos, inundaciones etc., Que la puedan poner en peligro, para todas las áreas de la compañía. C	Abarca todo un plan de recuperación ante desastres como la planeación para el restablecimiento de la operación(CBCP2)	El plan de continuidad de negocio abarca todas las áreas de la organización (CBCP3)	Un plan de continuidad del negocio es aquel que se realiza para continuar con la productividad de la compañía cuando el flujo normal es alterado e incluye al de recuperación de desastres el cual tiene como objetivo restaurar el flujo normal de trabajo.	No define. (ND)	Los planes de continuidad del negocio deben ponerse en práctica a diario, como mecanismos para afianzar el negocio y encaminarlo hacia objetivos puntuales que le permitan a la compañía mantenerse vigente, activa y competitiva.	Son todas las actividades y procedimientos que hacen posible a una organización responder a un evento en tal forma que las funciones críticas del negocio continúen sin interrupción o cambio significativo. (CBCP4)

	Periodicidad de actualización de documentación (PAD)							Según COBIT, una de las fases de aseguramiento del servicio continuo establece el "Mantenimiento del Plan de Continuidad de TI / DRP". En esta fase, la Gerencia de TI debe proveer procedimientos de control de cambios para asegurar que el plan de recuperación ante desastres se mantiene actualizado y refleja los requerimientos actuales del negocio. Esto requiere de procedimientos de mantenimiento del plan de recuperación alineados con el cambio, la administración y los procedimientos de recursos humanos, todo esto orientado a garantizar la seguridad y la disponibilidad de los sistemas de información de las organizaciones. (SCOBIT)

	BIA	Análisis de impacto del negocio BIA para poder identificar los riesgos a los cuales estamos expuestos, queremos determinar y entender qué procesos son esenciales para la continuidad de las operaciones y calcular su posible impacto. (BIA1)						El propósito fundamental del Análisis de Impacto sobre el negocio, conocido más comúnmente como BIA (Business Impact Analysis) es determinar y entender qué procesos son esenciales para la continuidad de las operaciones y calcular su posible impacto. Este proceso es parte fundamental dentro de la elaboración de un Plan de Continuidad del Negocio. De acuerdo al Business Continuity Institute se tienen tres objetivos principales al realizar un análisis de impacto: • Entender: o Los procesos críticos que soportan el servicio. o La prioridad de cada uno de estos servicios. o Los tiempos estimados de recuperación (RTO). o El punto estimado de recuperación (RPO). • Determinar los tiempos máximos tolerables de interrupción (MTD). • Apoyar el proceso de determinar las estrategias adecuadas de recuperación. (BIA2)

	Como se implementa un DRP	Una metodología recomendada para el desarrollo de un plan de recuperación ante desastres o DRP para los sistemas de información, es implementar un proceso comprendido desde el inicio del proyecto hasta la realización de las pruebas, como realizar un análisis de riesgo, estrategias de recuperación y la definición de roles y Responsabilidades.	Se debe como primera instancia hacer una familiarización de cada uno de los procesos que hacen parte del área de sistemas, Adicional a esto se debe tener claro cuáles son los actores que intervienen en cada una de las áreas de TI. Posterior a esto se debe establecer la metodología que se debe seguir, generando responsabilidades para cada uno de los actores. Se deben contemplar una evaluación de riesgo, análisis de impacto de negocio y Cronograma de ejecución de pruebas.	1. Establecer un equipo para el proyecto del plan de recuperación de desastres2. Analizar el impacto del negocio con el BIA.3. Buscar las estrategias de recuperación de los riesgos hallados en el análisis de impactos.4. Documentar los procesos.5. Realizare pruebas y manteniendo del DRP.6. Comunicar el DRP a los colaboradores del CCS.	El plan de recuperación de desastres deben estar cómo estimar el desastre, qué hacer por cada sector en la empresa que fue afectado y cuáles de éstos son críticos para el negocio, así como qué hacer para recuperar cada uno de éstos de acuerdo a su estado.	No define. (ND)	El plan de recuperación de desastres debe garantizar la continuidad de los servicios prestados por la empresa independientemente del desastre ocurrido. La afectación a nivel interno de la compañía, por causa del desastre debe ser transparente a los clientes y usuarios. El plan debe incluir respaldo de la información, planes de contingencia que permitan la continuidad de los servicios IT, mantenimiento preventivo de	• METODOLOGÍA PARA EL DISEÑO DE UN PLAN DE RECUPERACIÓN ANTE DESASTRES O DRPLa metodología recomendada para el desarrollo de un plan de recuperación ante desastres o DRP para los sistemas de información críticos de TI, propone un proceso comprendido desde el inicio del proyecto hasta la realización de las pruebas. Se considera también realizar un análisis de riesgo, estrategias de recuperación y la definición de roles y responsabilidades.Existen metodologías basadas en las recomendaciones del NIST (National Institute of Standards and Technology), DRII (Disaster Recovery Institute International) y el BCI (Business Continuity Institute), también apoyadas en la experiencia de casos prácticos realizados en nuestro país:1. Inicio del proyecto Plan de Recuperación ante desastres.2. Análisis de impacto sobre el negocio (BIA).3. Análisis de riesgos.4. Desarrollo estrategias de recuperación para el DRP.5. Definición de roles y responsabilidades.6. Pruebas del DRP.• EVALUACIÓN DE RIESGO Y GESTIÓN DEL RIESGOo Identificar amenazas sobre los

							respaldos.	sistemasLas entidades a nivel nacional, en Colombia, por ejemplo, enfrentan numerosas amenazas comunes tales como el potencial de falla de un servidor o la pérdida del fluido eléctrico; pero también enfrentan otras amenazas que son específicas para esta entidad o son únicas consideradas desde el punto de vista de su impacto potencial.Para la identificación de las amenazas a las que pueden enfrentarse los procesos críticos del sistema se deben realizar entrevistas con expertos de la organización, quienes suministrarán información sobre cuáles son las amenazas con mayor impacto, desde la perspectiva de continuidad del servicio y de sus procesos y sistemas críticos, las que podrían llegar a afectar el sistema, es decir, que podrían causar pérdida financiera por demandas, pérdida de imagen por la degradación del servicio.o Identificar vulnerabilidades de los sistemasUna de las preocupaciones más importantes de los profesionales de la seguridad de la información es el aumento en la cantidad de vulnerabilidades encontradas en los sistemas tecnológicos, las cuales son

								el blanco predilecto de herramientas de software cada vez más poderosas en su capacidad de ocasionar daños a los sistemas de información y la infraestructura que los soporta.Lo anterior nos lleva a pensar que se necesita contar con una estrategia más coherente y efectiva para mitigar esta inquietante y crítica amenaza, por tanto en el marco del proyecto de implementación del DRP, se le informará a la empresa de las vulnerabilidades de software asociadas a sus sistemas de información y elementos considerados como críticos en la prestación de sus servicios. Se establece, de esta manera, el conjunto de vulnerabilidades que posee cada proceso crítico del servicio de la entidad que al ser explotadas por una amenaza afectarían la operación del sistema o Cálculo de la probabilidad de ocurrencia de un eventoNos podemos ayudar para determinar la probabilidad de ocurrencia de ciertos eventos, como el caso de una pérdida de potencia, falla en las comunicaciones, información obtenida de ciertas publicaciones tecnológicas como Information Week e Infosecurity News, CERT, SANS, ASIS, NFPA, EIA

								e ISO, entre otros, junto con experiencias de casos colombianos.

	Consecuencias de no tener un DRP	Si la empresa no implementa un plan, podría verse inmersa en problemas de reputación con los proveedores terceros aliados estratégico o salir del mercado, es decir que en caso de emergencia llegaríamos a no contar con la continuidad y recursos de los servicios que préstamos, arriesgando grandes sumas de dinero equivalentes a horas de trabajo, ya que la disponibilidad de la información es escasa y en casos de alto riesgo, esta llegaría a perderse. Somos	Los principales sucesos a que se expone una organización al no tener implementado un plan de recuperación ante desastres seria.• Perdida de información vital para la organización.• Los tiempos de respuesta para poner en marcha el negocio después de una caída se incrementan considerablemente.• Pérdida de clientes ocasionada por la no respuesta oportuna a sus solicitudes.	Con los procedimientos que actualmente tenemos no garantizamos que la información de toda la organización y la de los clientes este salvaguardada a un 100% Las estrategias de recuperación están basadas obviamente en los resultados obtenidos luego de la realización del BIA.	No se podrá acceder a la información de la empresa por lo cual se tendría que reconstruir la información a partir de las copias de ingreso de equipos (Si el desastre no los afectó), al igual que los contables.	No define. (ND)	Se pone en riesgo la continuidad de los servicios, lo que puede acarrear sanciones de tipo penal, además de multas, de acuerdo con los Acuerdos a Nivel de Servicio que tiene la compañía con sus clientes.	La gestión de riesgo es un punto central en la definición de una estrategia de seguridad perfectamente alineada con la visión de las empresas, dentro de su entorno de operación. La metodología de evaluación del riesgo es el resultado de la combinación de diferentes propuestas existentes en la industria, y utiliza métodos tanto cualitativos, como cuantitativos, los cualitativos permiten agilidad en el proceso y facilidad en la asignación de valores de impacto o riesgo, y los cuantitativos permiten la precisión y exactitud necesarias a la hora de tomar decisiones de tipo financiero, por ejemplo, en el caso de la selección de los controles adecuados, para mitigar un posible evento negativo en la operación y continuidad de los procesos. Para esta actividad se considera COBIT, ITIL, ISO 27001, entre otras.Riesgo – Probabilidad – Impacto – Acción para mitigar

		conscientes de la necesidad de tener un DRP que permite sostener procesos durante y después de una interrupción, a través de estrategias ordenadas que rescatan y proteja los recursos, procesos, roles y responsabilidades dentro la organización. Sin lugar a dudas, el DRP se constituye en una solución para la evaluar riesgos, costos, además de garantizar la continuidad de la información.						

Anexo B. Respuestas de la evaluación de la guía por el experto.