Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

ANÁLISIS DE UN PLAN DE CONTINUIDAD DE OPERACIONES PARA UNA ORGANIZACIÓN/PYME CON SEDE EN CIUDAD DE GUATEMALA

Rafael Ernesto Siney Guamuch
Asesorado por el Ing. Mario José Bautista Fuentes

Guatemala, junio de 2017

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

ANÁLISIS DE UN PLAN DE CONTINUIDAD DE OPERACIONES PARA UNA ORGANIZACIÓN/PYME CON SEDE EN CIUDAD DE GUATEMALA

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

RAFAEL ERNESTO SINEY GUAMUCH
ASESORADO POR EL ING. MARIO JOSÉ BAUTISTA FUENTES

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO EN CIENCIAS Y SISTEMAS

GUATEMALA, JUNIO DE 2017

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Pedro Antonio Aguilar Polanco
VOCAL I	Ing. Angel Roberto Sic García
VOCAL II	Ing. Pablo Christian de León Rodríguez
VOCAL III	Ing. José Milton de León Bran
VOCAL IV	Br. Jurgen Andoni Ramírez Ramírez
VOCAL V	Br. Oscar Humberto Galicia Nuñez
SECRETARIA	Inga. Lesbia Magalí Herrera López

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Murphy Olympo Paiz Recinos
EXAMINADOR	Ing. César Augusto Fernández Cáceres
EXAMINADOR	Ing. Ludwing Federico Altán Sac
EXAMINADOR	Ing. Oscar Alejandro Paz Campos
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

ANÁLISIS DE UN PLAN DE CONTINUIDAD DE OPERACIONES PARA UNA ORGANIZACIÓN/PYME CON SEDE EN CIUDAD DE GUATEMALA

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería en Ciencias y Sistemas, con fecha febrero de 2016.

Rafael Ernesto Siney Guamuch

Guatemala, 05 de julio de 2016

Ingeniero
Carlos Azurdia
Revisor de Trabajo de Graduación
Escuela de Ciencias y Sistemas
Facultad de Ingeniería

Respetable Ing. Azurdia

Por este medio hago de su conocimiento que he revisado el trabajo de graduación del estudiante **RAFAEL ERNESTO SINEY GUAMUCH,** titulado: **"ANÁLISIS DE UN PLAN DE CONTINUIDAD DE OPERACIONES PARA UNA ORGANIZACIÓN/PYME CON SEDE EN CIUDAD DE GUATEMALA"**, y a mi criterio el mismo cumple con los objetivos propuestos para su desarrollo, según el protocolo.

Sin otro particular, me suscribo de usted.

Atentamente,

Mario José Bautista Fuentes
Ingeniero en Ciencias y Sistemas
Colegiado No. 10,017
Asesor de Trabajo de Graduación

Mario Jose Bautista Fuentes
Ing. En C.C Y Sistemas
Colegiado- 10017

Universidad San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería en Ciencias y Sistemas

Guatemala, 3 de Agosto de 2016

Ingeniero
Marlon Antonio Pérez Türk
Director de la Escuela de Ingeniería
En Ciencias y Sistemas

Respetable Ingeniero Pérez:

Por este medio hago de su conocimiento que he revisado el trabajo de graduación del estudiante **RAFAEL ERNESTO SINEY GUAMUCH** con carné **199911983,** titulado: **"ANÁLISIS DE UN PLAN DE CONTINUIDAD DE OPERACIONES PARA UNA ORGANIZACIÓN/PYME CON SEDE EN CIUDAD DE GUATEMALA",** y a mi criterio el mismo cumple con los objetivos propuestos para su desarrollo, según el protocolo.

Al agradecer su atención a la presente, aprovecho la oportunidad para suscribirme,

Atentamente,

Ing. Carlos Alfredo Azurdia
Coordinador de Privados
y Revisión de Trabajos de Graduación

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
INGENIERIA EN CIENCIAS Y SISTEMAS
COORDINACION TESIS

ESCUELA DE INGENIERÍA EN CIENCIAS Y SISTEMAS

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÌA
ESCUELA DE INGENIERÍA EN
CIENCIAS Y SISTEMAS
TEL: 24767644

El Director de la Escuela de Ingeniería en Ciencias y Sistemas de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer el dictamen del asesor con el visto bueno del revisor y del Licenciado en Letras, del trabajo de graduación ***"ANÁLISIS DE UN PLAN DE CONTINUIDAD DE OPERACIONES PARA UNA ORGANIZACIÓN/PYME CON SEDE EN CIUDAD DE GUATEMALA",*** *realizado por el estudiante RAFAEL ERNESTO SINEY GUAMUCH aprueba el presente trabajo y solicita la autorización del mismo.*

"ID Y ENSEÑAD A TODOS"

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCION DE INGENIERIA EN CIENCIAS Y SISTEMAS

Ing. Marlon Antonio Pérez Türk
Director
Escuela de Ingeniería en Ciencias y Sistemas

Guatemala, 7 de junio de 2017

Universidad de San Carlos
de Guatemala

Facultad de Ingeniería
Decanato

Ref.DTG.D.271.2017

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería en Ciencias y Sistemas, al trabajo de graduación titulado: **ANÁLISIS DE UN PLAN DE CONTINUIDAD DE OPERACIONES PARA UNA ORGANIZACIÓN/PYME CON SEDE EN CIUDAD DE GUATEMALA,** presentado por el estudiante universitario: **Rafael Ernesto Siney Guamuch** y después de haber culminado las revisiones previas bajo la responsabilidad de las instancias correspondientes, se autoriza la impresión del mismo.

IMPRÍMASE.

Ing. Pedro Antonio Aguilar Polanco
Decano

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANO
FACULTAD DE INGENIERIA

Guatemala, junio 2017

/cc

ACTO QUE DEDICO A:

Dios	Quien es mismo ayer hoy y por siempre, fuente de amor y sabiduría, que me ha guiado hasta el día de hoy y a quien debo mi vida y mis logros.
Mis padres	Rafael Siney y Lucia Basilia Guamuch de Siney, quienes con su esfuerzo, amor, dedicación y ejemplo me formaron y apoyaron de forma incondicional, para siempre seguir para adelante y de quienes he aprendido a ser emprendedor y a quienes amo con todo mi corazón, este triunfo es para mis padres.
Mis hermanos	Luis, como parte fundamental en mi formación profesional y amigo incondicional, Silvia, por ser mi amiga y consejera.
Mi esposa	Leslly Cortéz, por su apoyo y motivación para alcanzar mis metas, compartir conmigo cada momento de mi vida y ser parte de la música que alegra mi vida.
Mis amigos	Quienes me han acompañado en cada etapa, y sé que he contado con una amistad sincera con cada uno de ellos.

USAC Por ser mi casa de estudios y fuente de formación profesional, así como al pueblo de Guatemala quien con su contribución ha logrado formar profesionales.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

GLOSARIO

Access point	Dispositivo de red, punto de acceso (AP, por sus siglas en inglés) para ampliar red de forma inalámbrica.
Área roja	Categorización hecha para sectores con mayores índices de violencia y criminalidad.
Backups	Copias de respaldo de sistemas de información.
Big data	Término utilizado para definir grandes volúmenes de *data*, transformada a información para su análisis.
Carpetas compartidas	Información compartida en un servidor de archivos, para uso de varios usuarios.
Cloud computing	Computación en la nube, donde se proveen diferentes servicios por medio de Internet.
Escala mercalli	Escala para determinar intensidad de sismos, determinado por los efectos y daños causados.
Falla geológica	Fracturas en la corteza terrestre.

Firewall	Cortafuegos que puede ser por *hardware* o *software* para limitar accesos a una red como un dispositivo de seguridad.
GB	Medida de almacenamiento, por sus siglas en inglés Gigabyte, equivalente a 1000 MB.
Hardware	Las partes físicas, tangibles, de cualquier recurso de tecnología.
IMAP	Protocolo de correo electrónico, por sus siglas en inglés Internet Message Access Protocol, donde se mantienen correos electrónicos en un servidor de correo, y se sincronizan de la misma forma en distintos dispositivos.
INE	Por sus siglas, Instituto Nacional de Estadística, encargado de recolectar, elaborar y publicar estadísticas oficiales para Guatemala.
Infraestructura de red	Término utilizado para definir detalles de una topología, o tipo, de red.
INSIVUMEH	Por sus siglas, Instituto Nacional de Sismología, Vulcanología, Meteorología e Hidrología, institución que monitorea dichos fenómenos y eventos en Guatemala.

Intranet	Término utilizado para referirse a redes internas, únicamente para el personal de una organización.
ISP	Por sus siglas Internet Service Provider, refiriéndose a las entidades proveedoras de Internet.
IT	Por sus siglas Information Technology, lo referente a tecnologías de la información.
Linux	Sistema operativo basado en Unix.
MySQL	Base de datos de código abierto, parte de la familia de Oracle.
PC	Se refiere a computadoras personales, por sus siglas Personal Computer.
PYME	Por sus siglas, Pequeña y Mediana Empresa, para determinar un tipo de empresa en el mercado.
RAID 1	Tipo de almacenamiento, generalmente en servidores, también llamado “espejo”, en que la información esta almacenada de la misma forma que en el arreglo de discos.
RDP	Protocolo de acceso remoto a equipos, por sus siglas, Remote Desktop Protocol.

Router	Dispositivo de red encargado de transportar paquetes de un punto a otro, según tabla de ruteo, y también puede funcionar como servidor DHCP.
SaaS	Siglas en inglés para Software as Service, utilizando el software como un servicio.
SAN	Siglas para definir Storage Área Network, dedicado exclusivamente para el almacenamiento en la red.
Servidor	Equipo de cómputo dedicado para compartir recursos de hardware/software con otros equipos en la red local.
Cliente/Servidor	Sistema en que su base de datos está instalada en un servidor, y cada equipo posee *software* independiente que se conecta al servidor.
Sistema IGSS	Se refiere al sistema de planillas del Instituto Guatemalteco de Seguridad Social.
Sistema ISR	Se refiere al sistema del Impuesto Sobre la Renta de la Superintendencia de Administración Tributaria (SAT).
Sistema *web*	O aplicación *web*, es un sistema alojado en un servidor al cual se puede acceder desde cualquier navegador, sin necesidad de estar instalado en cada equipo.

Software	Programa informático, intangible.
SQL Server	Administrador de base de datos relacional, parte de la familia Microsoft.
Switch	Dispositivo de red para comunicar varios equipos en una red local.
TCP/IP	Protocolo de red utilizado para la comunicación entre equipos, tanto en red local como externa, Internet.
UDP	Protocolo de red utilizado para la comunicación, donde no importa el orden de los paquetes transmitidos.
VPN	Por sus siglas en inglés, Virtual Private Network, o red privada virtual, para conexión a una red privada por medio de Internet, a través de túneles encriptados.
Windows	Sistema operativo desarrollado por Microsoft.

RESUMEN

En el presente trabajo de investigación se detalla el análisis de cómo la interrupción de operaciones puede ser generada por diferentes situaciones, por lo que se deben evaluar distintos tipos de riesgo, tanto naturales como de índole social, enfocados en la delimitación para el área metropolitana de la Ciudad de Guatemala.

El trabajo está dividido en tres capítulos, los cuales describen las fases que se deben seguir para establecer un plan de continuidad de negocio/operaciones. Posteriormente se presenta el análisis en el entorno guatemalteco, y finalmente se da una introducción a cómo los servicios en la nube, o software como un servicio, han cobrado auge en los últimos tiempos.

Para el análisis en el entorno guatemalteco se tomaron como base fases ya existentes, sin embargo, se hace una pequeña adaptación al medio local, considerando una implementación más sencilla para una PYME, con escaso recurso económico, de tiempo, de personal, o sin de un departamento de IT.

El plan propuesto busca ser una herramienta de retroalimentación inmediata sobre procesos a seguir en medio de una situación, ya sea grave o leve, que haya provocado la interrupción de operaciones de alguna forma, por medio de la identificación de grados de exposición al riesgo. Finalmente, se da un vistazo rápido sobre el tema de servicios en la nube, como una medida que se ha estado utilizando en los últimos años como forma de mantener conectado y comunicado al personal de una empresa durante todo el tiempo, en todo lugar, con disposición a su información crítica y en cualquier dispositivo.

OBJETIVOS

General

Realizar un análisis de un plan de continuidad de operaciones a partir de un análisis de riesgos para un área determinada, clasificando escenarios posibles, y que este sirva de ejemplo para poder realizar el mismo análisis, como una herramienta o instrumento, para otras áreas dentro de la Ciudad de Guatemala.

Específicos

1. Respaldar de forma comprobada escenarios posibles, a partir de riesgos por desastres naturales, o bien, por índole social.

2. Tener un panorama general para la creación de procesos como parte de un plan de continuidad de operaciones.

3. Crear o modificar instrumentos ya existentes, de uso fácil para el análisis de riesgos, clasificando sistemas de información por medio de métricas de exposición al riesgo y prioridades de recuperación.

INTRODUCCIÓN

Las políticas de seguridad de la información constituyen un tema que ha cobrado auge en los últimos años, no solo en grandes empresas multinacionales o grandes corporaciones bancarias y financieras, sino también en las pequeñas empresas u organizaciones en las que se consideran de vital importancia para la continuidad de sus operaciones.

En muchas organizaciones se realizan tareas de respaldo de forma programada y automática, en otras de forma manual y empírica, sin embargo, lo importante en medio de cualquier incidente es que existan las copias de seguridad y no tanto cómo se hayan hecho, sin dejar a un lado la forma en la que se hacen las copias de respaldo. Estas deben ser implementadas de la mejor manera posible, siempre dentro de las políticas de seguridad de la información de la organización. Sin embargo, el contar con *backups*, o copias de respaldo, solo es un primer paso, por lo que en medio de cualquier situación o problema externo que afecte a la organización, se pone en riesgo la continuidad de operaciones de la misma.

Por este motivo, en medio de un incidente que interrumpe las operaciones de una organización, si esta no cuenta con un plan estructurado para restablecer las mismas, es decir, un plan que ponga en funcionamiento todos los sistemas de información de vital importancia para las operaciones, la organización corre el riesgo de que algunos de los sistemas de información no se restablezcan en absoluto, no se restablezcan de forma correcta, o bien, todo esto no se realice en un tiempo prudencial y aceptable.

Así también puede existir una serie de escenarios que compartan los mismos procesos para que exista continuidad de operaciones, aunque también puede que varíen según el tipo de incidente, por lo que de no existir un análisis de riesgos enfocado en los tipos de incidentes que pueden afectar a una organización, se pueden crear planes de continuidad de operaciones no adecuados.

1. GESTIÓN DE LA CONTINUIDAD DE OPERACIONES

1.1. Enfoque dentro de un Sistema de Gestión de Seguridad de la Información (SGSI)

Debe definirse qué es un Sistema de Gestión de Seguridad de Información (SGSI), que refiere todo lo relacionado a la seguridad de la información dentro de una organización. En los últimos años, debido a múltiples amenazas, la mayoría de organizaciones se ha empezado a preocupar por asegurar sus datos y tener protegida toda su información sensible, y esto ha ido aumentando cada vez más en las PYMES (Pequeñas y Medianas Empresas), pues muchas de ellas poseen sistemas de seguridad que funcionan de forma eficiente.

Alberto G. Alexander menciona que "un SGSI nos debiera permitir determinar con objetividad qué requiere ser protegido, por qué, de qué debe ser protegido y como protegerlo"[1]. De esta forma, un SGSI busca de forma eficaz y eficiente dar solución a eventos detectados, y que estos no sean recurrentes, tomando acciones para que al ocurrir eventos se esté preparado para afrontar los mismos.

Pueden encontrarse varias definiciones de un SGSI. Peltier lo define como "la preservación de la confidencialidad, integridad y disponibilidad de la información"[2]. En esta definición cabe resaltar la palabra "disponibilidad", donde comienza a verse que el asegurar la información no lo es todo; es una gran

[1] ALEXANDER, Alberto G. *Diseño de un sistema de gestión de seguridad de* información. p. 176.
[2] PELTIER, Thomas R. *Information security risk analysis*. p. 296.

parte del todo, pero al momento de cualquier incidente que provoque la interrupción de operaciones se debe también asegurar la disponibilidad de la información.

El modelo ISO 27001:2005 define al SGSI como “la parte del sistema de gestión global, basada en una orientación a riesgo de negocio, para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información”[3].

En el modelo ISO 27001:2005, por medio de los objetivos de control de la sección A.14, se estipula que un SGSI debe contar con un plan de continuidad del negocio, por lo que el gestionar un plan para la continuidad de operaciones es un aspecto importante a considerar dentro de la organización, así como lo es el asegurar la información desde el principio.

1.2. Enfoque del plan de continuidad

Syed plantea un dato interesante al decir que “una empresa que deja de operar por espacio de diez días consecutivos, jamás se recuperará”[4]. Esto da una imagen de los márgenes de pérdida extralimitados dentro de una organización, al no restablecer sus servicios y operaciones de una manera pronta y eficiente.

Al mencionar pérdidas no se refiere exclusivamente a una organización que se dedique a producción o ventas de cualquier tipo, sino que también pueden ser organizaciones no lucrativas en las que las pérdidas se miden por tiempos en los que no se prestan ciertos servicios por no tener acceso a la

[3] ISO27001:2005. *Sistemas de gestión de seguridad de información.*
[4] SYED, Afsar y Akthar. *Business continuity planning methodology*. p. 307.

información, o bien, la falta de acceso a los recursos (económicos, coordinación, entre otros) que la organización provee para su funcionamiento, dado por el no poder acceder a los sistemas de información específicos de cada área de la organización.

Un Plan de Continuidad de Negocio, PCN, mantenido y actualizado constantemente, permitirá asegurar que frente a un incidente o desastre (de cualquier tipo), las operaciones de mayor importancia de la organización no se vean afectadas o interrumpidas. En el caso de las PYME, u organizaciones con falta de recursos, se debe prever que estas operaciones interrumpidas no tengan un tiempo de respuesta de recuperación alto que incida en pérdidas significativas.

Un desastre está definido por la Real Academia Española como "desgracia grande, suceso infeliz y lamentable"[5]. Los desastres son sucesos que no son esperados en ningún momento y cuya ocurrencia no puede ser prevista. Si bien en la Ciudad de Guatemala no existen probabilidades de algún tipo de desastre especifico (tsunamis, maremotos, huracanes y demás), sí existen sucesos o eventos que pueden limitar el acceso a la información o interrumpir algunas operaciones de un negocio, y aunque se han hecho esfuerzos por asegurar la información con creación de copias de respaldo (*backups*) internas y externas, limitar accesos, etc., muy pocas empresas u organizaciones invierten en un PCN para minimizar el posible impacto de un evento.

Hiles hace un comentario muy parecido a Syed, con la diferencia de que él menciona que la organización "nunca se recupera y desaparece del mercado"[6].

[5] Real Academia Española de la Lengua. *Diccionario de la Real Academia Española*. http://dle.rae.es/?id=CUceyCB. Consulta: en 2016.
[6] HILES, Andrew. BARNES, Peter. *Business continuity management*. p. 410.

Entonces, puede decirse que un PCN debe ser capaz de restablecer los servicios y recursos interrumpidos en tiempos de respuesta aceptables para la organización. Hiles habla de un PCN como de "un documento que contiene procedimientos y lineamientos para ayudar a la recuperación y restablecimiento de procesos interrumpidos y recursos al estado de operación normal, en un tiempo prudencial"[7].

1.3. Proceso de un plan de continuidad

Varios autores proponen un ciclo de vida para la implementación y mantenimiento de un plan de continuidad. Entre estos autores se puede mencionar a O'Hehir[8], Hamilton[9], entre otros. Llama mucho la atención que todos estos autores de referencia publican en el 2002, inmediatamente después de la crisis suscitada en el año 2001 después del atentando contra las Torres Gemelas. Esto porque se vio la importancia de todo lo relacionado a SGSI, gestiones de riesgo, planes de contingencia y, por supuesto, como parte de un SGSI, el plan de continuidad de negocio u operaciones.

Todos estos autores mencionados concuerdan que un PCN implica seguir un proceso. En Guatemala muy pocas empresas u organizaciones poseen un PCN, y menos cuando se trata de PYMES, por lo que estos procesos sugeridos por los autores serán adaptados para que sean funcionales dentro de un entorno de PYMES guatemaltecas.

Estas son las fases consideradas como parte del plan de continuidad:

[7] HILES, Andrew. *Business continuity: best practices*. p. 268.
[8] O'HEHIR, Michael. *Business continuity management: what is a business continuity planning strategy?* p. 410.
[9] HAMILTON, Dennis. *Business continuity management: multilateral continuity planning.* p. 410.

- Fase I: análisis del impacto del negocio

Conocida mejor como Business Impact Analysis (BIA), en donde se identifican todos los procesos que apoyan a la misión de la empresa y se analiza el impacto que se tendría si estos procesos son interrumpidos como consecuencia de un evento o desastre.

El instrumento resultante consiste en un informe en el que se muestran las áreas del negocio/organización que son críticas, así como la magnitud del impacto operativo y financiero en la interrupción, y los requerimientos para recuperarse.

- Fase II: gestión del riesgo

En esta fase se evalúan las amenazas existentes, se consideran a detalle las vulnerabilidades y los potenciales impactos de un desastre; además, se identifican los controles necesarios para prevenir, o reducir lo máximo posible, los riesgos de un desastre.

El instrumento resultante consiste en un informe de riesgos y controles. En este informe se identifican las posibles amenazas potenciales que interrumpan al negocio. Se puntualiza en las recomendaciones para hacer el control de los riesgos que pudiesen alterar el funcionamiento de los procesos que se consideraron esenciales durante el análisis de impacto.

- Fase III: desarrollo de estrategias de un PCN

Durante esta fase se examinan los requerimientos y se identifican las opciones para la recuperación de los procesos esenciales, críticos, y los

recursos que fueren necesarios en el caso fueren interrumpidos por cualquier evento.

El instrumento resultante consiste en un informe donde se describen las opciones viables para la recuperación de los servicios interrumpidos y sus recursos. Dada la cantidad de amenazas potenciales se pueden crear distintos escenarios, y sobre cada escenario se crean estrategias para cada uno.

- Fase IV: desarrollo del plan de reanudación de operaciones

Durante esta fase se desarrolla un plan para mantener la continuidad de la empresa/negocio u organización, todo basado en las fases que se realizaron con anterioridad, la fase de análisis de impacto, la gestión del riesgo, y en aspectos planteados para el desarrollo de la estrategia.

El instrumento resultante es un informe con los lineamientos y procedimientos concretos para la recuperación y restablecimiento de los recursos que han sido afectados, todos aquellos procesos esenciales y críticos que fueron interrumpidos.

- Fase V: ensayo del PCN

Durante esta fase se efectúa el ensayo del plan creado, para poder determinar su efectividad y evaluar los resultados, con el fin de poder tomar medidas correctivas o que mejoren aún más el plan, de forma que se pueda actualizar.

El instrumento resultante de esta fase únicamente son los registros que resultan de las pruebas, para poder demostrar que los ensayos se han

realizado y si estos han estado dentro de los márgenes considerados como aceptables para la organización, y también, de ser necesario, poder realizar ajustes al plan de reanudación de operaciones para que esté en el punto que la empresa/organización desea.

2. PROCESO DE UN PCN

2.1. Fase I – análisis del impacto del negocio (BIA)

Mejor conocido como Business Impact Analysis (BIA), busca analizar el impacto de un desastre dentro de la organización, en cada una de sus áreas y en cada uno de sus procesos críticos o esenciales. Entonces, como lo menciona Alberto G. Alexander, un análisis de impacto identifica:

- Las funciones y procesos que son esenciales para que la empresa/organización se mantenga “a flote”. Dentro de una organización o empresa existe un sinfín de procesos, pero dentro de todos estos procesos se deben determinar cuáles son los procesos clave para que la empresa continúe en funcionamiento. Estos deben estar dentro del plan de continuidad (PCN).Para los otros procesos encontrados que no fueron categorizados como claves, sí habrá planes de recuperación a poner en marcha, mas no estarán dentro del plan de continuidad del negocio.

- Las consecuencias de la interrupción de los procesos clave.

- Estimación, los más aproximada posible, de los tiempos de recuperación, cuando exista la interrupción de los procesos clave.

- Los requerimientos de los recursos necesarios e indispensables para la recuperación y funcionamiento de los procesos categorizados como claves.

En el informe que se genera en el BIA se presenta la información básica sobre los procesos críticos, de tiempos de recuperación y los recursos requeridos, con el fin que la organización cuente con buenos planes de continuidad.

2.1.1. Métodos para la recolección de información

Se debe tener un método de recolección ordenado y estructurado, de forma que sea fácil la recolección de la información que se desea. Hiles recomienda tres métodos: encuestas, entrevistas y talleres[10].

- Encuesta: utiliza un conjunto de preguntas que se envían a las distintas unidades, o áreas, en la organización. Este método permite a los encuestados la flexibilidad de poder completar las preguntas a su conveniencia, sin embargo, se tienen dos desventajas: una es la falta de precisión y confiabilidad de las respuestas porque puede que los encuestados no comprendan las preguntas; la otra desventaja es que las respuestas pueden tardar más del tiempo esperado, tardando más de lo deseado en la recopilación de la información.

- Entrevistas: la información se recolecta personalmente, entrevistando a una o más personas dentro de cada unidad/área. La interacción entre la persona que entrevista con la persona entrevistada minimiza los riesgos de interpretar mal las preguntas. Lo que puede constar con este método es dependiendo de los recursos que se tomen: recurso tiempo, recurso persona, o bien coordinación con las personas a ser entrevistadas.

[10] HILES, Andrew. *Business continuity: best practices*. p. 268.

- Talleres: este método permite a un grupo de personas trabajar de manera colectiva para proveer información en conjunto. Puede ser una muy buena forma para obtener la información, sin embargo, la dificultad en este método es lograr el compromiso de cada área de la organización para la cooperación y participación en el taller, aún más cuando estas actividades no son consideradas como prioridad en las labores diarias del personal, situación bastante común dentro de las PYMES guatemaltecas.

2.1.2. Requerimientos de tiempo de recuperación

Según Barnes y Von Roessing se tienen distintos componentes de recuperación de tiempo[11], sobre lo que describen:

- *Maximun Tolerable Downtime* (MTD): consiste en el espacio de tiempo en el que un proceso puede estar sin operar como máximo hasta que la empresa empiece a tener problemas por estas interrupciones.

- *Recovery Time Objective* (RTO): está asociado con la recuperación de recursos, tales como sistemas de computación, equipos de manufactura e infraestructura física. También es el tiempo transcurrido entre una interrupción y la recuperación. Indica el tiempo disponible para recuperar sistemas y recursos interrumpidos.

- *Recovery Point Objective* (RPO): este tiempo está relacionado con la tolerancia que puede tener la empresa con respecto a la pérdida de

[11] BARNES C, James. *A guide to business continuity planning*. p. 183. VON ROESSING, Rolf. *Auditing business continuity: global best practices*. p. 290.

datos, medidos en términos del tiempo entre la última copia de respaldo y el desastre.

- *Work Recovery Time* (WRT): se calcula como el tiempo entre la recuperación del sistema y la normalización de los procesos claves; es el tiempo invertido en buscar datos perdidos y realizar reparaciones.

2.1.3. Proceso metodológico del BIA

Se crea una secuencia de pasos con el propósito de identificar los impactos de una interrupción y determinar los requerimientos para restablecer los procesos críticos que han sido afectados.

2.1.3.1. Paso 1: identificación de funciones y procesos de negocio

Se debe de identificar las funciones y procesos, que apoyan la misión y objetivos. El resultado será un listado de las funciones y procesos, las cuales se convertirán en el foco del análisis de los siguientes pasos del BIA.

2.1.3.2. Paso 2: evaluación de los impactos financieros y operacionales

En algunos casos de organizaciones no lucrativas, el impacto financiero no se refiere a pérdidas por falta de ventas u otros que generen ingresos, si no que se atiende a la falta de control de los recursos económicos bien utilizados y controlados, y a la provisión de los mismos para cumplir con la misión y objetivos de la organización.

En cuanto a los impactos financieros, la medición debe realizarse por cada proceso. La pregunta clave, planteada por Alexander, que debe de realizarse para determinar el impacto es: "¿Cuáles serían la magnitud y la severidad de las pérdidas financieras si el proceso fuese interrumpido después de un desastre?"[12]

El impacto de los procesos se recomienda sea medido acorde al valor de la pérdida y en base a una escala según el nivel de severidad:

- Severidad 0 – Impacto 0
- Severidad 1 – Menor impacto
- Severidad 2 – Impacto intermedio
- Severidad 3 – Impacto mayor

En cuanto a los impactos operacionales, se sigue la misma línea planteada por Alexander; se miden según un esquema cualitativo de la siguiente forma:

- bajo
- mediano
- alto
- altísimo, y
- ninguno

[12] ALEXANDER, Alberto G. *Diseño de un sistema de gestión de seguridad de información*. p. 176.

2.1.3.3. Paso 3: identificación de procesos críticos

La base para poder identificar los procesos críticos se realiza según la clasificación de los impactos realizados anteriormente. Siguiendo como base lo estipulado por Alexander cuando habla sobre el diseño de un SGSI, y utilizando la clasificación de niveles de severidad y de impactos, se identifica el proceso critico cuando cumple con los siguientes puntos:

- La severidad de 2 x 3 se identifica según sus impactos financieros.
- La clasificación de alta se asigna por lo menos a tres de sus impactos operacionales.
- La clasificación de alta se asigna al menos a dos, y una de altísima se asigna a uno de sus aspectos operacionales.
- La clasificación de altísima se asigna por lo menos a dos de sus impactos operacionales.

2.1.3.4. Paso 4: establecimiento de los tiempos de recuperación

Cuando ya se identificaron los procesos críticos se debe determinar para cada uno de ellos el MTD (*Maximun Tolerable Downtime*). Todo esto para obtener el tiempo disponible para poder recuperarse después de una interrupción en los procesos. Los tiempos descritos en la gráfica son los descritos en los requerimientos de los tiempos de recuperación.

MTD no es mayor a la suma de los tiempos RTO y WRT. Para determinar un MTD se debe analizar para cada uno de los procesos cuál es el tiempo máximo que la organización puede soportar, en base en los niveles de impacto. Posteriormente, según los MTD, se debe establecer la prioridad para la

recuperación, para lo que se tiene un orden de menor a mayor, y los menores serán los que tendrán prioridad de recuperación.

2.1.3.5. Paso 5: identificación de requerimientos de recursos

Luego de la identificación de los procesos críticos, deben considerarse los recursos que apoyan a cada uno de estos procesos, y en específico los recursos de tecnología de información que sean considerados vitales para el debido funcionamiento de los procesos críticos.

2.1.3.6. Paso 6: determinación del RTO (Recovery Time Objective)

RTO es la recuperación de los recursos de sistemas, o recursos que han sufrido una interrupción. Es decir, los tiempos para recuperar los recursos de tecnología de información antes enumerados. Se utilizará el cálculo de WRT, que refiere los tiempos requeridos para recuperar los datos, con el fin de volver a la normalidad. Por consiguiente, se procede a enumerar los procesos críticos con sus respectivos requerimientos de TI, y se le asignan los valores de RTO y de WRT.

2.1.3.7. Paso 7: determinación del RPO (Recovery Point Objective)

Esta es la magnitud de la pérdida de datos, es decir, la tolerancia máxima de tiempo que los datos pueden estar perdidos sin afectar el desempeño del sistema.

2.1.3.8. Paso 8: identificación de procedimientos alternos

Esto no es más que identificar procedimientos alternos, generalmente operaciones manuales de forma temporal, para todos los procesos críticos identificados con el fin de que la organización pueda continuar operaciones en caso se presente alguna interrupción.

2.1.3.9. Paso 9: resumen de Informe BIA

En este paso se presentan los resultados de los pasos anteriores. El contenido está dado por:

- Procesos críticos
- Tiempos MTD y su clasificación
- Sistemas y aplicaciones (clasificadas)
- Tiempos de RTO
- Tiempos de RPO
- Procedimientos alternos

2.2. Fase II – definición de gestión del riesgo

La gestión del riesgo consiste en determinar diferentes escenarios en los que se pueden presentar distintas amenazas que pueden interrumpir los procesos vitales o esenciales para la organización. Con base en estos escenarios se desarrollarán estrategias para la continuidad y la reanudación de operaciones.

Hiles contempla la gestión del riesgo como “el cálculo del riesgo, la apreciación de su impacto en el negocio y la posibilidad de ocurrencia”[13], mientras que Barnes define al riesgo como “la probabilidad que una amenaza pueda explotar una vulnerabilidad y causar daño a los activos de una organización”[14]. Por su parte, Von Roessing define una amenaza como “el intento de hacer daño”[15], y Alexander clasifica las amenazas según su naturaleza poniéndolas de la siguiente forma: “naturales, físicas, humanas, tecnológicas, operacionales, sociales”[16].

Continuando el tema, Sheffi define la vulnerabilidad como “una combinación de la posibilidad de una alteración y su potencial severidad”[17], y tratando acerca de los activos de una organización, O’Hehir los define como “todas aquellas cosas a las que la empresa da valor”[18]. Por último, nuevamente Alexander dice “el riesgo se presenta cuando la amenaza y la vulnerabilidad se untan y la amenaza las puede explotar”[19].

En la gestión del riesgo se persigue lograr identificar las amenazas que pueden impedir el normal funcionamiento de las operaciones de la organización. También se quiere evaluar la vulnerabilidad de la organización ante cada amenaza y qué tanto impacto pueda tener sobre las operaciones.

Se pretende también revisar los controles para reducir el riesgo o mitigar las pérdidas, y así mismo calcular el nivel de exposición al riesgo. El fin también

[13]HILES, Andrew. *Business continuity: best practices*. p. 268.
[14] BARNES C, James. *A guide to business continuity planning*. p. 183.
[15] VON ROESSING, Rolf. *Auditing business continuity: global best practices*. p. 290.
[16] ALEXANDER, *Alberto G. Diseño de un sistema de gestión de seguridad de información*. p. 176.
[17] SHEFFI, Yossi. *The resilient enterprise*. p. 352.
[18] O’HEHIR, Michael. *Business continuity management: what is a business continuity planning strategy?* p. 410.
[19] ALEXANDER, Alberto G. *Diseño de un sistema de gestión de seguridad de información*. p. 176.

es determinar los escenarios para los que es necesario desarrollar estrategias y planes de continuidad.

2.2.1. Calculando el riesgo

2.2.1.1. Paso 1: identificación de amenazas

Se desea identificar las amenazas que afectan los activos de la organización. Alexander recomienda detectar las amenazas en dos etapas[20]:

- Análisis de amenazas: se revisan las potenciales amenazas y se enfoca la atención en los siguientes aspectos:
  - Ubicación de instalaciones
  - Seguridad interna y externa
  - Ambiente físico
  - Protección de activos
  - Protección del personal
  - Protección de información
  - Análisis de la cobertura de pólizas
- Análisis de procesos esenciales: se enfatiza en las interrupciones a las que los procesos son vulnerables por la pérdida de recursos básicos como: instalaciones, sistemas de cómputo, registros vitales, telefonía, personal clave, conectividad de la red, equipo especial, materias primas. El objetivo es identificar las funciones organizacionales que tienen la mayor exposición a la interrupción y saber qué recursos son los que dependen de dichas funciones.

[20] ALEXANDER, Alberto G. *Diseño de un sistema de gestión de seguridad de información*. p. 176.

Al final de esta etapa se tendrá una lista con las amenazas y las funciones de la organización, con sus respectivas dependencias en recursos. Las amenazas que aparecen en esta lista fueron las consideradas a atender por parte de la organización, y a las que se les han calculado probabilidad de ocurrencia y el impacto que tendrían en la organización. Hay otras amenazas que la organización puede decidir aceptar y no tomar acción sobre ellas, por su baja probabilidad e impacto.

2.2.1.2. Paso 2: identificación de vulnerabilidades

Según las amenazas detectadas, se identifican las vulnerabilidades, ya que como se mencionó, una vulnerabilidad puede ser aprovechada o explotada por una amenaza y afectar activos. Toda vez se tenga la lista de las vulnerabilidades sobresalientes, se debe saber el grado en el esta puede ser explotada.

2.2.1.3. Paso 3: controles de seguridad

Se deben revisar los controles de seguridad que se poseen para cada uno de los casos de la lista de amenazas y vulnerabilidades, esto porque puede ser que existan políticas de seguridad, estipuladas en algún manual de seguridad de la empresa, y se esté confiando que al momento de cualquier incidente estos controles funcionen correctamente, pero si al momento de ponerlos en práctica estos controles fallan, se convierte en una vulnerabilidad.

Al final de este paso se tendrá una lista de todos los controles de seguridad y el estado de su funcionamiento, así como las observaciones respectivas de los controles que necesiten reforzarse.

2.2.1.4. Paso 4: cálculo del nivel de exposición al riesgo

En el cálculo de la exposición al riesgo se asigna el grado de severidad para cada amenaza potencial. Esto se basa en una escala como la siguiente:

- N/A: No aplica
- B: Bajo = 10
- M: Moderada = 50
- A: Alta = 100

También se asignan los porcentajes de cobertura, lo que es el grado de protección que tiene la empresa frente a una amenaza, que van desde 0 % a 100 %, en seis niveles (0 % - 19 %, 20 % - 39 %, 40 % - 59 %, 60 % - 79 %, 80 % - 99 %, 100 %).

De esto se calcula la exposición al riesgo, (nivel de severidad * (100 % - % cobertura)). Y a partir de estos se pueden representar las exposiciones al riesgo según las amenazas potenciales.

2.2.1.5. Paso 5: determinar escenarios de amenazas

Los escenarios son clasificados del uno (1) al cinco (5), los cuales son de menor a mayor según su complejidad. Para cada uno de los escenarios encontrados se deben realizar estrategias de continuidad, planes de continuidad y ensayo del plan de continuidad. Los escenarios se describen de la siguiente manera:

- Nivel 1: cuando una amenaza afecta la continuidad de funciones de la organización, por ejemplo cuando se da por la pérdida de un recurso crítico en las instalaciones (por energía, sistemas especiales, personal clave o archivos).

- Nivel 2: cuando una amenaza afecta muchas funciones de la organización, por ejemplo cuando se da por alguna situación que evita el acceso a las instalaciones, sin que existan daños en los recursos críticos.

- Nivel 3: cuando una amenaza afecta varias de las funciones de la organización, por ejemplo cuando ocurre la destrucción parcial de uno o más recursos críticos en las instalaciones.

- Nivel 4: cuando una amenaza afecta varias de las funciones de la organización, por ejemplo cuando ocurre la destrucción total de las instalaciones y de los recursos críticos, en accidentes como incendios o explosiones.

- Nivel 5: cuando una amenaza afecta varias de las funciones de la organización, por ejemplo cuando se dan pérdidas que afectan a más de una de las instalaciones de la organización, como datos centralizados, sistemas centralizados, telecomunicaciones, entre otros. También se puede dar por la falta de acceso a las instalaciones por eventos como terremotos, huracanes y otros.

2.3. Fase III – estrategias para la continuidad del negocio

2.3.1. Fase 1:

Se identifican los requerimientos de recuperación como estrategia del plan de continuidad.

2.3.2. Fase 2:

Se identifican las posibles opciones como solución a los requerimientos de recuperación.

2.3.3. Fase 3:

De las posibles opciones se descartarán aquellas que no cumplen con los tiempos de recuperación estipulados en el análisis del impacto del negocio.

2.3.4. Fase 4:

Se evalúan los costos de las opciones seleccionadas, así como también se evalúa su viabilidad y efectividad.

2.4. Fase IV – desarrollo del plan de reanudación de operaciones

Este plan contiene los procedimientos que las organizaciones o empresas deben seguir para minimizar el impacto al momento de una crisis, siempre recordando que el objetivo del plan de reanudación es la recuperación de procesos críticos en tiempos determinados. Varios autores, como Hamilton, coinciden en que el plan debe abarcar: respuesta inicial y evaluación, medidas

de contingencia provisionales, aprovisionamiento de recursos, reanudación de operaciones y, por último, reconstitución[21].También los autores definen equipos, o grupos, para responsabilizarse de las actividades del plan:

- Equipo comando: es el equipo encargado de dirigir el plan de reanudación o continuidad.

- Equipo de respuesta: son las personas que están relacionadas con las instalaciones y con el área de seguridad.

- Equipo departamental: son los gerentes que coordinan actividades por departamentos.

- Equipo de tecnología de información: son las personas a cargo del área de tecnología de la información de la empresa/organización, que conocen todas las áreas de la organización y entran en función inmediata para restablecer infraestructura, sistemas e información.

- Equipo de apoyo: equipo designado para ayudar en diversas actividades durante cualquier incidente.

Un equipo bien estructurado y que trabaje de forma eficiente tendrá como fin un plan bien realizado, es decir que funcione ante una crisis. Así mismo, los autores recomiendan para formar equipos tomar en cuenta factores como:

- Tamaño de la organización
- Ubicación de las instalaciones
- Estructura organizacional

[21] HAMILTON, Dennis. *Business continuity management: multilateral continuity planning.* p. 410.

- Cultura organizacional
- Escenarios potenciales de amenazas
- Estrategias de continuidad
- Conocimiento especializado

2.5. FASE V – ensayo del plan de continuidad del negocio

Esta fase es muy importante para la organización. Su objetivo es validar, asegurar y obtener confiabilidad sobre el plan de continuidad, para que este funcione como se había previsto. También se pretende encontrar debilidades que pueden existir en el plan de continuidad, para poder corregirlas. Existen distintos tipos de ensayos que se pueden realizar, entre los cuales, para los fines de este estudio y por cuestiones de costo y esfuerzo, se pueden tomar en cuenta:

- Lista de chequeo: solo se revisa el plan y se chequea la disponibilidad de los recursos necesarios o requeridos para cuando se ejecute el plan.

- Paseo de revisión: cuando existe una reunión y verbalmente se describen las actividades que se realizarían al momento de una interrupción o desastre.

- Simulación: se simula una interrupción de servicios, o una interrupción de uno de los procesos críticos, para crear un escenario. Con este ejercicio se pone en práctica la ejecución del plan y se valida su funcionamiento.

3. ANÁLISIS PARA UNA ONG/PYME CON SEDE EN CIUDAD DE GUATEMALA

Según el Banco Interamericano de Desarrollo (BID) una empresa se puede catalogar por su número de empleados, como se puede ver en la tabla I.

Tabla I. **Tipos de empresa**

Tipo de Empresa	**Número de Empleados**
Micro	De uno a cinco
Pequeña	De seis a veinticinco
Mediana	De veintiséis a cincuenta
Grande	De cincuenta y uno en adelante

Fuente: *Banco Interamericano de Desarrollo (BID).*
https://es.wikipedia.org/wiki/Peque%C3%B1a_y_mediana_empresa. Consulta: abril de 2016.

El Ministerio de Economía y la Cámara de Industria de Guatemala también definen el criterio por cantidad de empleados (ver tabla II), aunque la catalogación también se da por cantidades de activos y ventas de una empresa. En este análisis adquiere un particular interés la cantidad de empleados de la organización, variando de forma mínima con lo estipulado por el BID. Dada la descripción anterior, el presente trabajo se centrará en una pequeña y mediana empresa, considerada por la cantidad de empleados.

Se adaptará el análisis de un plan de continuidad con el fin de obtener una serie de procesos adecuados a la organización antes mencionada, siempre tomando como base los estatutos, parámetros y fases descritas anteriormente por los distintos autores, en especial por Alberto G. Alexander.

Tabla II. **Tipos de Empresa – Industria**

Tipo de empresa	Empleados (Criterio de la Cámara de Industria para el Programa de Bonos)	Empleados (Criterio del Ministerio de Economía)
Microempresa	1-5	1-10
Pequeña empresa	6-50	11-25
Mediana empresa	51-100	26-60

Fuente: *Ministerio de Economía*.
https://es.wikipedia.org/wiki/Peque%C3%B1a_y_mediana_empresa. Consulta: abril de 2016.

Sin embargo, esta adecuación implica la simplificación de algunos puntos de cada proceso del análisis de la gestión para la continuidad de operaciones, con el fin de que este sea más asequible y pueda realizar de una forma sencilla, eficiente y tener resultados en un tiempo mínimo. Con esto se expresa que el análisis preliminar pueda realizarse en el máximo de dos semanas.

3.1. FASE I – Análisis de impacto de negocio recomendado (BIA)

3.1.1. Método para la recolección de información

Según lo estipulado anteriormente sobre el tamaño de la organización en cuestión, se recomienda realizar la recolección de información por medio de entrevistas, dado que de esta forma se tendrá más acercamiento con los empleados y se podrán observar las actividades que realizan; así mismo se podrán explicar de una mejor forma las preguntas a cada empleado para poder llenar el cuadro resultante con la información que se necesita para el análisis.

3.1.2. Tiempos de recuperación

Para los tiempos de recuperación se mantendrán los estipulados en esta sección, con la diferencia que estarán orientados no solo al proceso, sino que al recurso IT que se utilice. Por ejemplo, para un sistema, las preguntas serían las siguientes:

- *Maximun Tolerable Downtime* (MTD): ¿cuánto sería el máximo de tiempo que puede estar sin trabajar/acceso al sistema?

- *Recovery Time Objective* (RTO): en caso pudiera trabajar en el sistema, aunque no tenga la data, ¿cuánto tiempo esperaría para poder trabajar y luego el equipo IT cargar la data?

- *Recovery Point Objective* (RPO): si se perdiera información, que no se recuperara, ¿cuánto es el máximo de tiempo tolerable de la pérdida de información, a partir del último *backup*?, es decir que si al momento de un evento en el que se pierda la data, el último *backup* se realizó hace una semana, 2 días, 1 día, etc., esto es tolerable para la organización, porque ya sea que lo puede trabajar de nuevo (aunque implique mayor esfuerzo para el usuario) o bien sea información de la que se pueda prescindir.

- *Work Recovery Time* (WRT): ¿cuánto tiempo esperaría para tener la información recuperada ya cargada en el sistema?

3.1.3. Procesos BIA

A diferencia de la metodología anterior, la cual iba formando por partes el análisis de los procesos críticos del negocio y puede que necesitara más de una intervención o entrevista, con los empleados se presenta una forma similar, optimizando pequeños aspectos que se aprovechan durante la entrevista, para no tener que volver a consultar con el empleado y realizar las preguntas correspondientes y anotaciones que posteriormente llevarán a concluir en procesos críticos.

Por eso durante un mismo paso de entrevista se realizarán varios pasos de los mencionados anteriormente, en la sección de la definición del proceso para desarrollar un análisis del impacto del negocio (BIA). Si bien es cierto que anteriormente algunos pasos solo se realizaban para los procesos críticos, el evaluar todos los aspectos para todos los procesos también dará un panorama general de todos los procesos, aun cuando el resultante solo sean los procesos críticos.

3.1.3.1. Paso 1:

Durante este paso, por medio del método de recolección de información seleccionado (entrevista), se realizará:

- Identificación de funciones y procesos de negocio, que se realizará por usuario, con datos del departamento al que pertenece, y listando los procesos/funciones que realiza.

- Para cada proceso o función enumerada se debe obtener:

- Evaluación de impactos financieros, para cada uno de los procesos y con base en una escala de 0 a 3, siendo 0 ninguno, 1 menor, 2 intermedio, 3 mayor. La pregunta propuesta es: ¿existe alguna pérdida económica o efecto económico negativo si este proceso se interrumpe?

- Evaluación de impactos operacionales, o de trabajo. La pregunta propuesta es: ¿qué tanto afectará sus labores la interrupción de este proceso?, usando la escala 0 ninguno, 1 bajo, 2 mediano y 3 alto.

- Tiempos de recuperación. Se determina para cada uno de los procesos enumerados el MTD correspondiente. Utilizando la pregunta planteada anteriormente, ¿cuánto sería el máximo de tiempo que puede estar este proceso interrumpido?

- Identificación de requerimientos de recursos. Se hace referencia específicamente a los recursos de tecnología que utilice para realizar el proceso enumerado; cabe resaltar que puede ser que para un proceso/actividad/función se utilice más de un recurso de tecnología, por lo que se enlistará en diferentes líneas cada recurso, siempre bajo la raíz del proceso.

- Ahora, para cada recurso IT, se debe obtener la siguiente información:

    - Determinación del RTO: ¿cuánto tiempo esperaría para poder trabajar con este recurso y luego el equipo IT cargar la data? Y WRT ¿cuánto tiempo esperaría para tener la

información recuperada ya cargada en el sistema?, lo que será estimado por el usuario, pero el equipo de TI validará la información con respecto a tiempos para poner a funcionar los recursos de tecnología.

- Determinación del RPO. Dato proporcionado por el empleado según la frecuencia de la copia de respaldo: ¿cuánto es el máximo de tiempo tolerable de la pérdida de información, a partir del último *backup*?

Partiendo de este paso se creará un listado de procesos y recursos IT que apoyan a dicho proceso (ver tabla III).Así podrán determinarse procesos críticos y recursos IT. Estos serán parte de un plan de continuidad.

Tabla III. **Procesos y recursos de tecnología**

Usuario	Depto. /Proyecto	Procesos	Imp.Finan	Imp. Trabajo	MTD (días)	Recursos IT Indispensable	RTO	WRT	RPO
Usuario 1	Compras	Compra	1	3	3	Correo	1 día	2 día	5 días
						Paquetes Ofimática	1 día	N/A	N/A
						Servidor de archivos	1 día	2 día	0 días
						Información	1 día	2 día	0 días
						Sistema Web interno	2 día	1 día	0 días
						Internet	0.5 día	N/A	N/A
Usuario 2	Contabilidad	Pago de planilla	3	3	2	Sistema de planillas	1 día	1 día	1 día
						Sistema de IGSS	1 día	1 día	1 día
						Sistema Web interno	1,5 día	0,5 día	0 días
						Internet	0,5 día	N/A	N/A

Continuación de la tabla III.

		Llevar libros	0	2	3	Sistema contable	2 días	1 día	0,5 día
						Paquetes Ofimática	1 día	N/A	N/A
						Servidor de archivos	1 día	2 día	0 días
						Internet	2 día	N/A	N/A
						Correo	2 día	1 día	5 días
Usuario 3	Recepción	Entrega de docs.	0	0	5	Sistema Web interno	3 días	2 días	0 días
						Internet	0.5 día	N/A	N/A
						Correo	1 día	4 día	5 días

Fuente: elaboración propia.

3.1.3.2. Paso 2:

Durante este paso se realizará:

- Identificación de los procesos críticos según los niveles de severidad asignados a los impactos financieros y operacionales, es decir que si en cualquiera de los casos poseen severidad/impacto 2 ó 3, se considerarán como críticos.

- Validación de los tiempos de recuperación, obteniendo la prioridad de recuperación, según el proceso que posea un menor MTD.

El resultado será una lista basada en los procesos críticos y recursos de tecnología que apoyan a cada proceso (ver tabla IV). También el enfoque que

muestra este análisis se basa en los recursos de tecnología que apoyan a los procesos críticos para cumplir con los objetivos organizacionales.

3.2. FASE II – Gestión del riesgo

Después de analizar la estructura organizacional de algunas pequeñas y medianas empresas, así como organizaciones no gubernamentales que pueden ser catalogadas como medianas por la cantidad de personal con que cuentan, puede decirse que muchos servicios se proveen por terceros, o dicho de otra manera, se subcontratan con el fin de reducir costos para la organización.

Uno de estos servicios que se subcontratan en la mayoría de los casos, incluso puede correrse el riesgo de decir que en el 90 % de las PYMES en Guatemala, es el de personal de TI. Esto porque muchas veces la cantidad de personal no amerita tener un departamento de TI dentro de la organización.

Tabla IV. **Ejemplo de procesos críticos y recursos con prioridad de recuperación**

Usuario	Depto. / Proy.	Procesos	Impacto Financiero	Impacto Trabajo	MTD (días)	Recursos IT Indispensable	Prioridad recuperación
Usuario 1	Compras	compra	1	3	**3**	Correo	**2**
						Paquetes Ofimática	
						Servidor de archivos	
						Información	
						Sistema Web interno	
						Internet	
Usuario 2	Contabilidad	pago de planilla	3	3	**2**	Sistema de planillas	**1**
						Sistema de IGSS	
						Sistema Web interno	
						Internet	

Fuente: elaboración propia.

Por lo tanto, para tratar de dar una estructura organizacional genérica o estándar, y muchas veces roles adoptados por una misma persona dentro de la organización, puede decirse que aquello que coincide en la mayoría de PYMES en Guatemala es:

- Recursos Humanos/Administración/Operaciones
- Ventas/Servicios
- Dirección/Gerencia
- Producción/Proyectos
- Finanzas/Contabilidad

A partir de la fase I del análisis de impacto en la organización, de los departamentos y procesos críticos detectados, y por supuesto de los recursos IT que son útiles para el desempeño de estos procesos, se identifican las amenazas que pueden existir y afectar a los recursos en los que se apoyan varios procesos.

Una de las formas propuestas es detectar la amenaza que puede existir en cada recurso de tecnología, y posteriormente hacer una lista de las amenazas. Si una amenaza se repite más de una vez para un recurso solo se lista una vez, y esta amenaza se puede considerar con severidad alta.

En el análisis de gestión de riesgo, al igual que en la fase I, se simplifica el proceso haciéndolo más asequible a una pequeña y mediana empresa guatemalteca que no posee muchos recursos para un análisis más exhaustivo. Con recursos se hace referencia no solo a un recurso económico, más bien, se abarcan los recursos del tiempo y el recurso de capital humano. De forma genérica se mencionarán algunas amenazas a considerar en las PYME, y al momento de tener el análisis inicial se pueden ir agregando a la lista.

3.2.1. Paso 1: identificación de amenazas

Ahora bien, con el fin de considerar distintos escenarios y amenazas, se toman en cuenta ciertos indicadores que ayudarán con el análisis de gestión de riesgos, siempre considerado únicamente para la Ciudad de Guatemala (encaso se desee hacer a nivel nacional, otro departamento, o municipios aledaños, se deberán realizar un análisis similar).

Como forma de justificación se analiza por qué son consideradas ciertas amenazas, y al final se enumerarán y agregarán otras que son consideradas como amenaza dado que de suceder se interrumpen procesos críticos, por ejemplo: falla del servicio de Internet por parte del ISP (Internet Service Provider), ocasionando problemas de comunicación, sistemas web, correos electrónicos, transacciones *online*, entre otros.

3.2.1.1. Violencia

Si bien es cierto que la Ciudad de Guatemala no está dentro de las diez (10) ciudades más peligrosas del mundo, según el más reciente informe de la organización civil mexicana Seguridad, Justicia y Paz, y otras fuentes de noticieros como BBC, Guatemala se encuentra dentro de las 50 ciudades más violentas del mudo, según la misma organización Seguridad Justicia y Paz[22], así como según la revista Forbes en México[23] y otros medios de comunicación como La Tribuna de Honduras[24].

[22] *Seguridad, justicia y paz*. http://www.seguridadjusticiaypaz.org.mx/sala-de-prensa/1356-cara c as-venezuela-la-ciudad-mas-violenta-del-mundo-del-2015. Consulta: abril de 2016.
[23] *Forbes en México*. http://www.forbes.com.mx/las-50-ciudades-mas-violentas-del-mundo/#gs. N0oIq8A. Consulta: abril de 2016.
[24] *La Tribuna*. http: // www.latribuna.hn/ 2016 /01 /29/las-50-ciudades-mas-violentas-del-mundo/. Consulta: abril de 2016.

Se hace mención de esto porque estando la Ciudad de Guatemala propensa a cualquier acto de criminalidad, debe ser considerado como una amenaza el hecho de que en esta puedan ocurrir toda clase de desastres, como lo son el robo de equipos de cómputo, o bien la pérdida inesperada de personal clave para la organización, esto sin considerar la ubicación exacta de la instalación de la PYME.

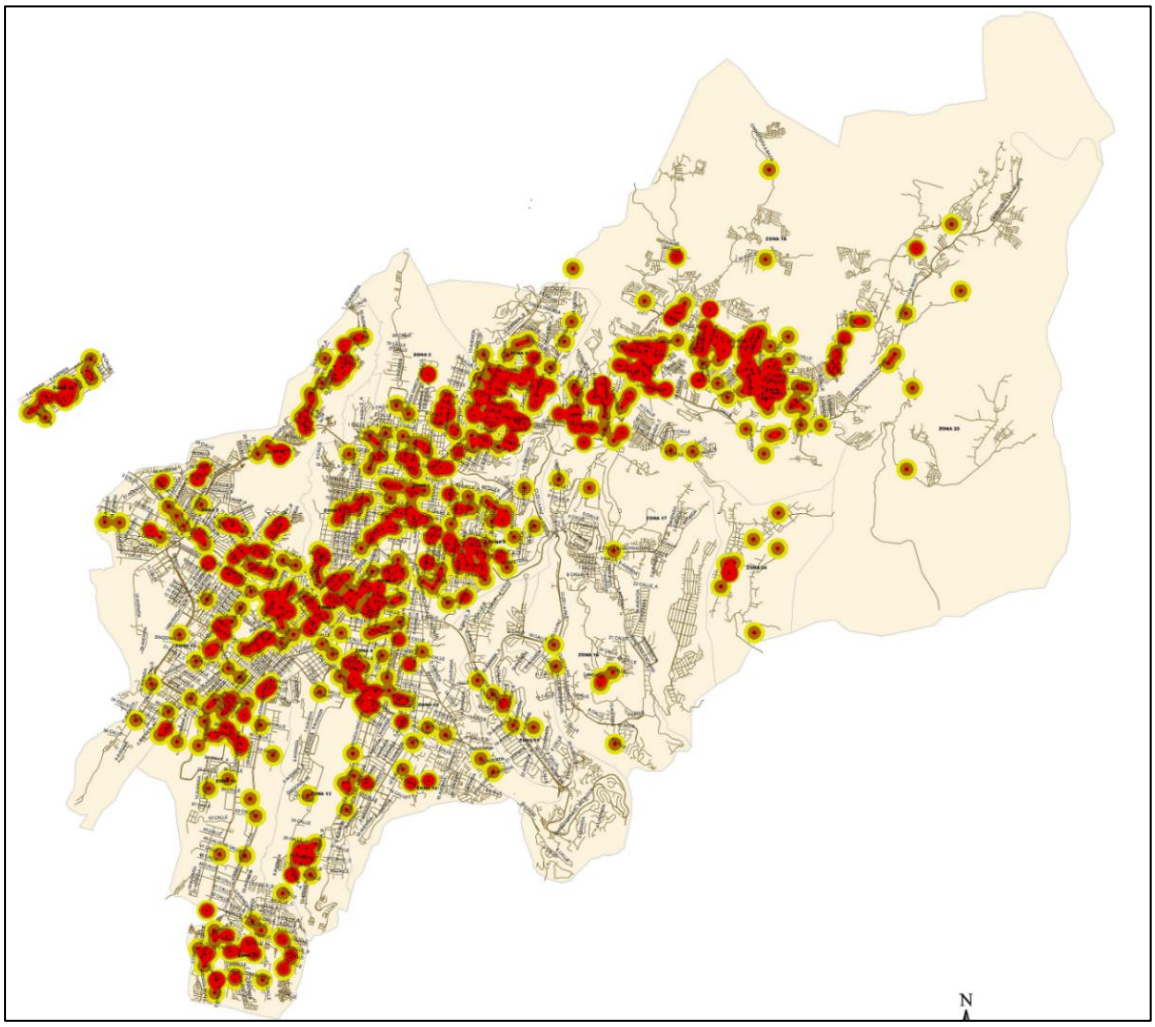
Sin embargo, también se debe considerar la vulnerabilidad de las instalaciones según su ubicación. Para ello la organización que realice este análisis deberá considerar si las instalaciones de la organización están ubicadas en un área donde frecuentemente ocurren hechos de violencia. Así que si las instalaciones de una organización se encuentran en alguna de estas zonas, aumenta la probabilidad de ser afectada por esta amenaza.

En cuanto a este punto, tomando datos de diferentes fuentes, como referencia principal los datos proporcionados por la PNC (Policía Nacional Civil), se han determinado áreas rojas. Según el mapa (ver figura 1) se puede observar como áreas rojas:

- Zona 1
- Zona 2
- Zona 3
- Zona 4
- Zona 5
- Zona 6
- Zona 7
- Zona 8
- Zona 11
- Zona 12

- Zona 18
- Zona 19
- Zona 21
- Algunos índices en la zona 9

Figura 1. **Mapa de áreas rojas**



Fuente: *Oficina GIS (PNC)*. www.gt.embjapan.go.jp/map/AREAS%20ROJAS%202009%20GUATEMALA.pdf. Consulta: mayo de 2016.

Según el reporte estadístico de la Secretaría Técnica Del Consejo Nacional De Seguridad, en el 2015 (figura 2) se pueden observar mayores índices de criminalidad por zonas, en los que sobresalen las zonas 1, 2, 4, 5, 6, 7, 11, 12, 18, 19, 21.De las dos fuentes consultadas anteriormente, se puede decir que hay pocos índices en sectores de la zona 12, y menores aún en la zonas 10 y 13, y todavía mejor catalogadas las zonas 14, 15, 16 y 17, pudiendo catalogar estas últimas como zonas menos vulnerables a las amenazas de tipo criminal, siendo las mejores zonas para ubicar las instalaciones de una empresa.

Tabla V. **Índice de criminalidad por zonas**

	Zona 1	Zona 2	Zona 3	Zona 4	Zona 5	Zona 6	Zona 7	Zona 8	Zona 9	Zona 10	Zona 11	Zona 12	Zona 13	Zona 14	Zona 15	Zona 16	Zona 17	Zona 18	Zona 19	Zona 21	Zona 24	Zona 25	Total
Muertes Violentas	12	1	5	1	7	24	9	0	4	0	3	7	1	0	0	3	4	14	3	14	2	1	115
Heridos en forma violenta	37	4	9	15	14	23	17	6	5	1	4	12	2	1	2	10	5	19	10	13	3	2	214
Robo a residencias	2	3	2	0	2	3	4	1	0	3	4	7	1	0	2	8	3	2	1	3	0	0	51
Robo a comercios	5	0	0	0	4	1	3	2	2	4	3	2	1	1	0	1	0	1	0	0	0	0	30
Robo de vehiculos	23	13	8	2	23	10	34	8	4	11	45	36	9	3	5	3	1	3	10	7	0	0	258
Robo de motocicletas	49	8	6	12	16	9	34	2	15	9	17	37	5	1	0	3	1	8	3	3	0	1	239
Robo de armas	4	0	1	1	2	3	3	0	0	6	5	4	0	0	0	0	1	2	0	2	3	0	37
Robo a peatones	33	3	5	1	1	4	6	3	2	3	8	2	2	1	0	0	0	1	2	2	0	0	79
Robo a buses	1	0	0	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3
Denuncias delitos sexuales (violaciones)	1	0	0	0	0	0	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	3
Secuestrados	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
Denuncias violencia intrafamiliar	2	0	2	1	2	0	1	0	0	0	2	0	1	0	0	0	0	5	0	1	0	0	17

Fuente: *Secretaría Técnica Del Consejo Nacional De Seguridad*. http://stcns.gob.gt/index.php/reporte.html. Consulta: mayo de 2016.

Según lo anterior se puede catalogar una amenaza por pérdida de equipo, o por robo/hurto, y puede ser considerado como vulnerabilidad, pero la cobertura variará según la ubicación de la empresa. Es decir, para una empresa con instalaciones en zona 15, por ejemplo, su cobertura será mayor (80 %– 99

%) con respecto a una empresa con instalaciones en zona 8 (según el mapa) o zonas 1, 7, 11 (según tabla) con cobertura (0 %– 19 %).

3.2.1.2. Sismos

La ciudad de Guatemala está afectada por fallas múltiples. Todas estas fallas pueden estar clasificadas como fallas activas y no activas. Las fallas que se consideran activas poseen un mayor potencial de ser activadas durante un sismo (o terremoto).

Tal y como se puede observar en la figura 3, las fallas en el área metropolitana pueden llegar a ocasionar que cualquier sismo llegue a ser bastante sensible. Por este motivo es que se deben considerar los sismos como una posible amenaza que puede llegar a afectar los procesos de cualquier organización, causando su interrupción.

Figura 2. **Fallas geológicas en el área metropolitana de Guatemala**

Fuente: *Mapa en sitio web ArcGIS*.
www.arcgis.com/home/webmap/viewer.html?webmap=b55265b68d2645c88cb4cc6e06a117be.
Consulta: mayo de 2016.

Según Prensa Libre, en lo que va del año 2016 el INSIVUMEH ha reportado 90 sismos con magnitudes desde los 3 grados hasta los 5,1 grados en todo el territorio nacional, siendo más sensibles en la parte sur del país.

Con el fin de obtener datos concretos para considerar los sismos como una amenaza para la interrupción de operaciones, se obtuvieron datos estadísticos referentes a sismos en la Ciudad de Guatemala como epicentro (ver tabla V).

Tabla VI. **Sismos reportados**

Año	Mes	Guatemala		
		No.	Magnitud	
			Max.	Min.
2014	Enero	5	3,6	2,9
2014	Febrero	3	3,1	2,6
2014	Marzo	5	3,8	2,6
2014	Abril	4	3,2	2,6
2014	Mayo	1	3,8	3,8
2014	Junio	2	2,6	2,4
2014	Julio	5	3,7	2,6
2014	Agosto	7	3,3	2,3
2014	Septiembre	4	3,3	2,7
2014	Octubre	12	3,3	1,8
2014	Noviembre	3	4,0	3,2
2014	Diciembre	1	4,3	4,3
	Total	**52**		
	Max (grados)	**4,3**		
	Min (grados)	**1,8**		

Fuente: *INE – INSIVUMEH*. www.ine.gob.gt/index.php/estadisticas/caracterizacion-estadistica. Consulta: mayo de 2016.

Según el Instituto Nacional de Estadística (INE), en los últimos datos oficiales reportados en sus informes descargados del sitio oficial, quienes a su vez obtienen datos del Instituto Nacional de Sismología, Vulcanología, Meteorología e Hidrología (INSIVUMEH), solo en un año en la Ciudad de Guatemala se reportaron hasta 52 sismos, siendo el máximo en este caso de 4,3, y el mínimo de 1,8 (en escala Richter).

De la misma forma se pueden observar mapas de amenazas sísmicas para la Ciudad de Guatemala, y así observar el impacto que pudieran tener

estas fallas sobre la Ciudad de Guatemala, considerando la falla de Mixco(ver figura 4), la falla de Santa Catarina Pínula (figura 5), y la falla de Jalpatagua (figura 6). El objetivo de esto es fundamentar por qué se consideran estas como amenazas latentes que pueden llegar a provocar la interrupción de operaciones, por su repercusión en recursos de tecnología en los cuales se apoya.

Para las imágenes de los mapas de amenazas sísmicas se utiliza la escala de Mercalli (ver tabla VI).Estos mapas fueron elaborados por la Agencia de cooperación Internacional de Japón (JICA), bajo el programa de Cooperación Técnica del Gobierno de Japón y el Gobierno De la República de Guatemala. Como se puede observar en estos, siempre se refleja el área de la ciudad de Guatemala y cuál sería el impacto de las distintas fallas sobre esta, pudiendo tomar nota de qué fallas distintas tienen un impacto sobre toda el área metropolitana. La gravedad puede variar según la falla, pero aun así cualquiera de ellas abarca prácticamente toda la ciudad de Guatemala, pudiendo decir que en cualquier momento pueden llegar a ser destructivas, y ocasionar incluso el destrozo de instalaciones, o bien limitar el acceso a las mismas.

En los distintos mapas, el color rojo indica que es un área que puede tener un impacto destructivo, y esto es en la mayoría de zonas de la ciudad. El resto de igual forma afectado por impacto muy fuerte, color amarillo, y fuerte, color verde.

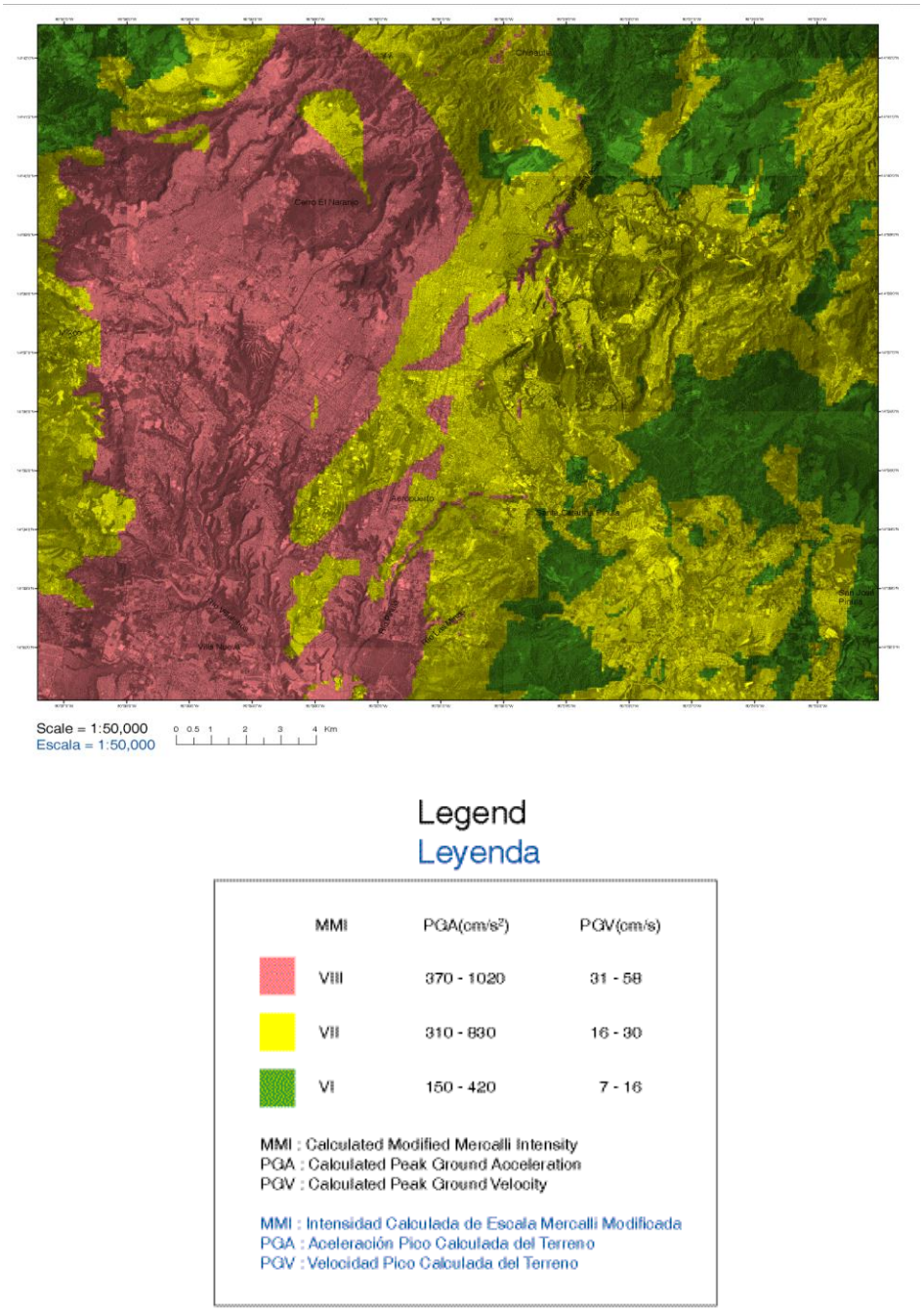
Tabla VII. **Escala de Mercalli según clasificación**

V - *Poco fuerte*.	Sacudida sentida casi por todo el país o zona. Algunas piezas de vajilla o cristales de ventanas se rompen; pocos casos de agrietamiento de aplanados; caen objetos inestables. Se observan perturbaciones en los árboles, postes y otros objetos altos.
VI - *Fuerte*.	Sacudida sentida por todo el país o zona. Algunos muebles pesados cambian de sitio y provoca daños leves, en especial en viviendas de material ligero.
VII - *Muy fuerte*.	Ponerse de pie es difícil. Muebles dañados. Daños insignificantes en estructuras de buen diseño y construcción. Daños leves a moderados en estructuras ordinarias bien construidas. Daños considerables en estructuras pobremente construidas. Sistema tradicional de construcción (adobe) dañado. Perceptible por personas en vehículos en movimiento.
VIII - *Destructivo*.	Daños leves en estructuras especializadas. Daños considerables en estructuras ordinarias bien construidas, posibles derrumbes. Daño severo en estructuras pobremente construidas. Sistema tradicional de construcción (adobe) seriamente dañado o destruida. Muebles completamente sacados de lugar.

Fuente: *Escala sismológica de Mercalli*.
https://es.wikipedia.org/wiki/Escala_sismol%C3%B3gica_de_Mercalli. Consulta: mayo de 2016.

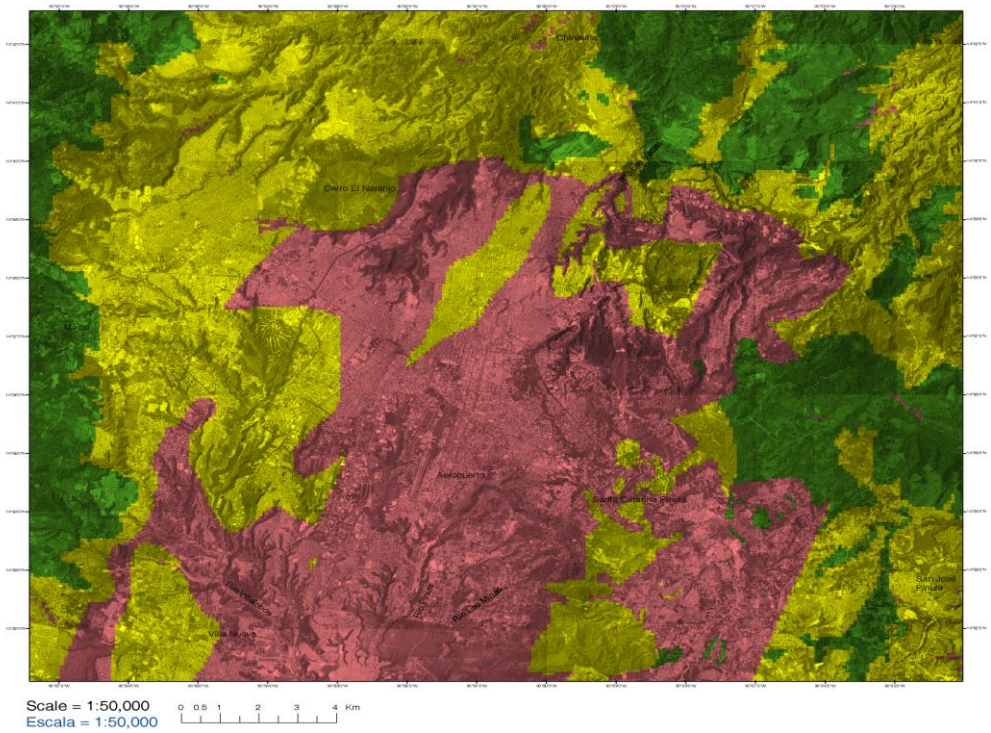
Por tanto, los sismos son una amenaza que siempre debe ser considerada por cualquier organización, pues puede llegar a tener impactos en los procesos de la organización, provocando pérdida de instalaciones, equipo o acceso a las mismas.

Figura 3. **Mapa de amenaza sísmica (Falla de Mixco)**



Fuente: *INE – INSIVUMEH*. www.insivumeh.gob.gt/Mapa_Amenaza_sismica.html. Consulta: junio de 2016.

Figura 4. **Mapa de amenaza sísmica (Falla de Santa Catarina Pínula)**



Legend
Leyenda

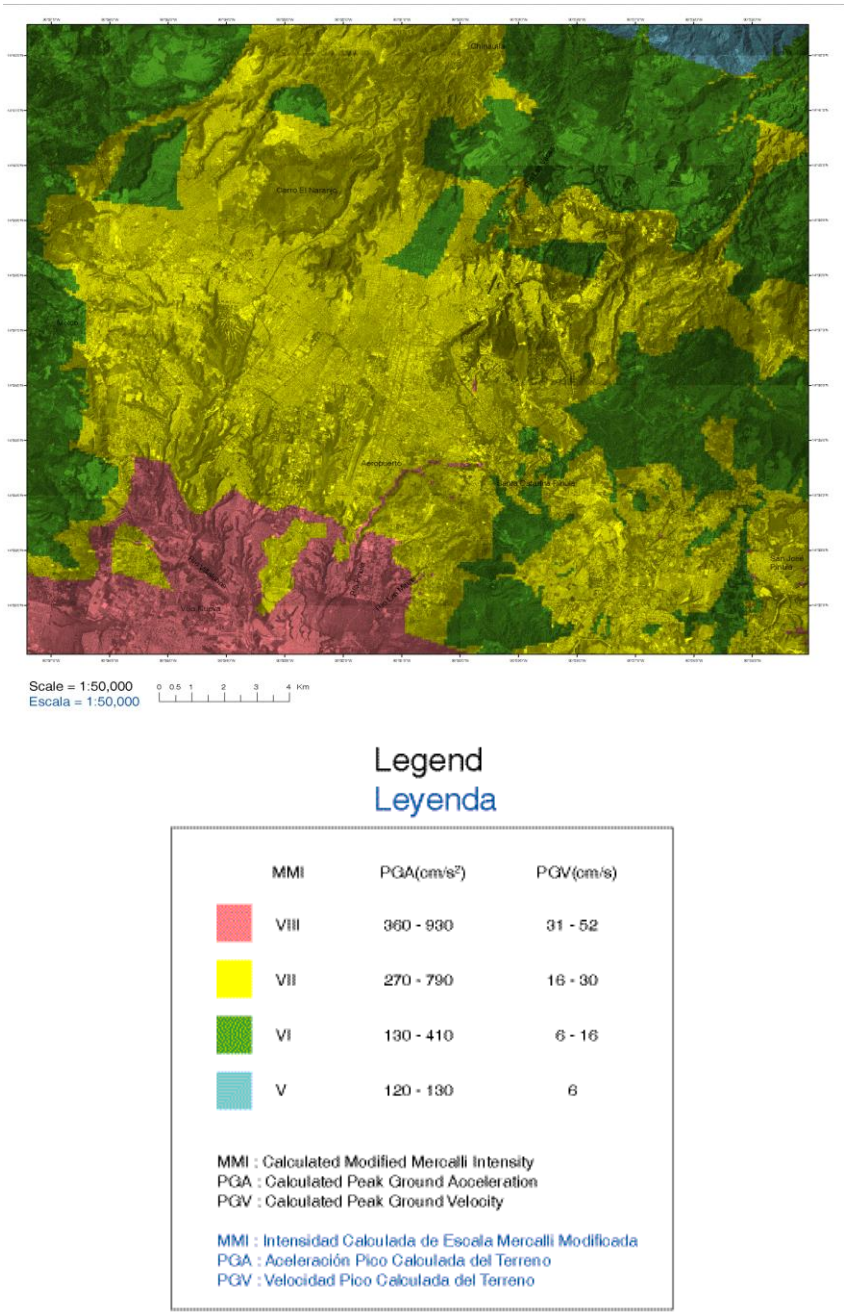
MMI	PGA(cm/s²)	PGV(cm/s)
VIII	370 - 1020	31 - 57
VII	360 - 860	16 - 30
VI	170 - 360	8 - 16

MMI : Calculated Modified Mercalli Intensity
PGA : Calculated Peak Ground Acceleration
PGV : Calculated Peak Ground Velocity

MMI : Intensidad Calculada de Escala Mercalli Modificada
PGA : Aceleración Pico Calculada del Terreno
PGV : Velocidad Pico Calculada del Terreno

Fuente: *INSIVUMEH – JICA*. www.insivumeh.gob.gt/Mapa_Amenaza_sismica.html. Consulta: junio de 2016.

Figura 5. **Mapa de amenaza sísmica (segmento oeste de la Falla de Jalpatagua)**



Fuente: *INSIVUMEH – JICA*. www.insivumeh.gob.gt/Mapa_Amenaza_sismica.html. Consulta: junio de 2016.

3.2.1.3. Amenazas que limitan el acceso a las instalaciones

Específicamente son incidentes climatológicos o sociales que impiden la libre locomoción o limitan el lograr llegar a las instalaciones de la oficina. Se pueden mencionar:

- Manifestaciones: según un medio de radio fusión, Emisoras Unidas, durante todos los meses ha existido noticia sobre alguna manifestación realizada, o amenaza de manifestación a realizar.(Ver tabla VII).

Tabla VIII. **Manifestaciones en la ciudad**

Año	Mes	Noticias de Manifestaciones
015	Agosto	6
015	Septiembre	6
015	Octubre	1
015	Noviembre	2
015	Diciembre	1
016	Enero	2
016	Febrero	1
016	Marzo	1
016	Abril	1
016	Mayo	2
016	Junio	3
	Promedio	**2,36**

Fuente: elaboración propia.

Según la información que se recopiló proveniente de este medio de comunicación, puede observarse una tendencia de cada mes para la ciudad capital, siendo la más afectada la zona 1, por ser la ubicación del palacio de gobierno (Palacio Nacional de la Cultura) y del Congreso de la República de Guatemala, así como de otras instancias de Gobierno.

Aun así, generalmente las manifestaciones se trasladan de un punto a otro de forma pacífica, pero ocupando vías de tránsito en calles o avenidas principales, que pueden ser utilizadas para movilizarse hacia instalaciones de la organización, limitando así la libre locomoción, y a esto debe sumársele los ocasionales bloqueos. Sin embargo, estas manifestaciones son temporales, pero pueden retrasar procesos por horas, así que dependerá de la organización tomar esta como una amenaza para un plan de continuidad de operaciones, ya que estas no se interrumpen definitivamente o por un tiempo muy prolongado. Sin embargo, el objetivo de este análisis es llegar a considerar las amenazas más significativas que pueden conducir a la interrupción de operaciones, por lo que una organización siempre debería tomar en cuenta esta amenaza, con baja probabilidad de ocurrencia, si en algún momento esta puede llegar a explotar vulnerabilidades por no haberlas considerado.

- Inundaciones de vías principales: la Ciudad de Guatemala posee varios antecedentes de inundaciones en vías principales, ya sea porque los sistemas de drenaje de la ciudad son rebasados, o bien, por estar estos mismos llenos de desechos, por falta de educación de los residentes de la ciudad.

Sin embargo, este hecho podría ser considerado con el mismo plan que limita el acceso a las instalaciones, ya que específicamente en la ciudad de Guatemala no existen antecedentes de catástrofes por inundaciones que

puedan provocar la destrucción de instalaciones, aunque sí existen antecedentes sobre inundaciones en las vías principales que puedan limitar el acceso a las mismas. (Ver figura 7).

Figura 6. **Calzada San Juan, zona 7 de la capital**

Fuente: Prensa Libre. *Calzada San Juan Inundada*. Consulta: julio de 2016.

3.2.1.4. Amenazas que no afectan al área de la ciudad de Guatemala

Existen amenazas que para la ciudad de Guatemala no aplican, ya sea por su ubicación geográfica, sistema climático u otros factores. Sin embargo,

para otras áreas del país si deberían ser consideradas, por dar un ejemplo se mencionados:

- Inundaciones (destrucción): la ciudad de Guatemala no está afectada directamente por catástrofes por inundación que puedan llegar a dañar instalaciones, esto debido a su ubicación geográfica, ya que se encuentra a 100 Km del mar. Como se mencionó anteriormente, en la ciudad no se posee antecedente de alguna catástrofe causada por inundación, pero ríos que suelen salirse de su cauce sí se encuentran fuera de la ciudad, o bien a inmediaciones de la misma.

- Incendios forestales: en el área de la ciudad de Guatemala, solamente existen pequeñas áreas forestales, por lo que no es una amenaza latente un incendio forestal. Sin embargo, en otras áreas del país esta sí debería considerarse, puesto que puede que las instalaciones estén ubicadas cerca de un área forestal.

Las áreas con más cobertura forestal son las que se encuentran en las inmediaciones de la Ciudad de Guatemala, como se observa en la figura 8, mapa del Instituto Nacional de Bosques (INAB), con lo que se respalda la postura de no considerar un incendio forestal como una amenaza para la interrupción de operaciones de una empresa u organización citadina.

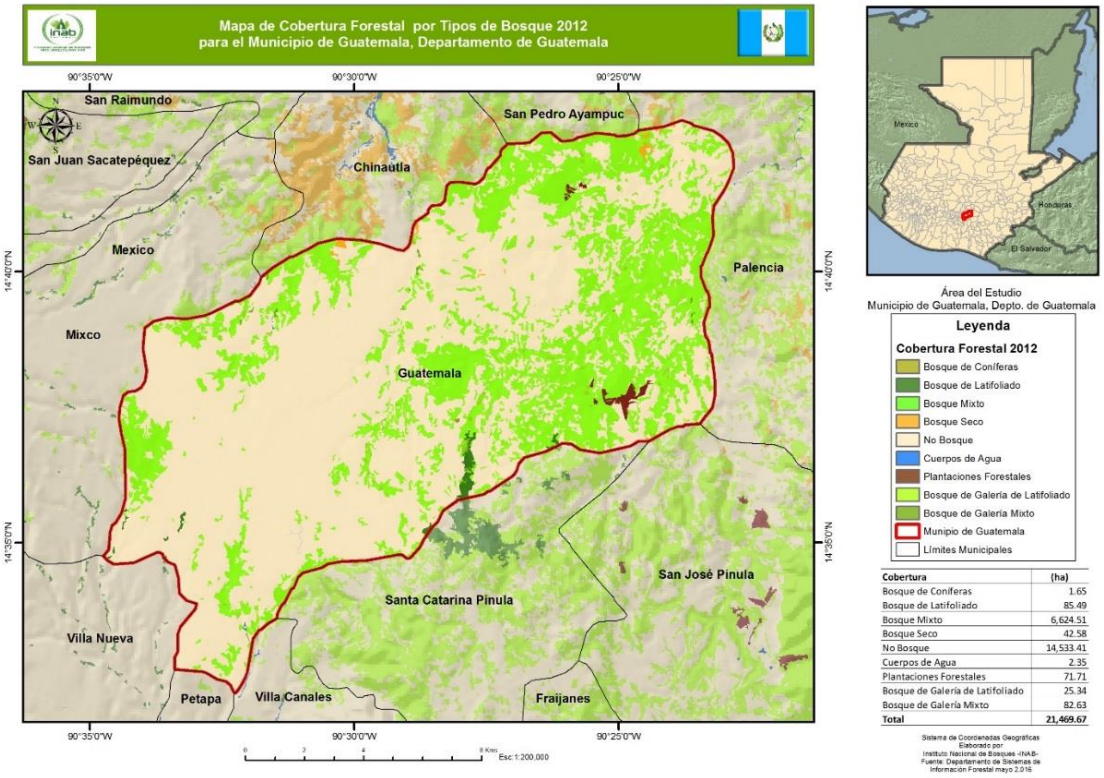
3.2.1.5. Resultado de amenazas para la ciudad de Guatemala

En resumen, estas son las amenazas que se consideran genéricas para la ciudad de Guatemala, entre las cuales algunas requieren mayor atención que

otras, pero el objetivo es que se pueda tomar como base para el desarrollo de un plan de continuidad de operaciones:

- Violencia
- Sismos
- Manifestaciones
- Inundaciones de calles o avenidas principales de la ciudad
- Pérdida de personal clave

Figura 7. **Mapa de la cobertura forestal de la ciudad de Guatemala**



Fuente: *Instituto Nacional de Bosques (INAB).* www.sifgua.org.gt/Cobertura.aspx. Consulta: junio de 2016.

Otras amenazas que pueden darse son:

- Fallas del proveedor de Internet. Actualmente este servicio es vital para las operaciones de una organización, ya no solo en comunicación, si no que muchos sistemas están basados en este tipo de servicio, cuya falta puede provocar la interrupción de varios procesos.
- Pérdida de datos.
- Fallas irreparables del equipo de cómputo.
- Fallas en sistema eléctrico.
- Pérdida de sistemas. Se hace referencia a los diferentes sistemas que apoyan los procesos críticos; la organización los utiliza para cada área de trabajo.

3.2.2. Paso 2: revisión de controles

Se hace referencia a las amenazas detectadas, y se determina qué controles se están utilizando para que la organización sea menos vulnerable ante alguna de las amenazas mencionadas. En este caso la PYME deberá tomar el listado anterior, del paso 1, y para hacer este proceso más sencillo solo se nombrará si existe un control y si este se encuentra en un funcionamiento correcto.

- Violencia: ¿qué control se posee si existe un acto de violencia que afecte a un miembro de la organización, o si existe algún robo de equipo? En este apartado se puede nombrar si se poseen seguros sobre activos, si existen equipos comodines para reponer el equipo robado, o si existen copias de seguridad actualizadas y cuánta es la regularidad de las copias de respaldo.

- Sismos: se indaga si existe un sismo que afecte la destrucción de instalaciones. Se puede nombrar si se posee algún tipo de garantía sobre equipos y qué tipos de garantía son, también si hay seguros sobre activos, o si existen copias de seguridad actualizadas y fuera de las instalaciones de la oficina.

- Manifestaciones: se indaga si el acceso a las instalaciones está limitado por el máximo tiempo permitido. Se debe de preguntar si existe alguna medida para que el equipo de trabajo funcione desde fuera. También se pueden nombrar las diferentes áreas de trabajo y evaluar en cuáles es posible realizarlo, y qué medida existe (si es que existe) para llevarlo a cabo, ya que hoy en día esto es posible a excepción de departamentos de producción u otros, dependiendo de los fines de la organización.

- Inundaciones de calles o avenidas principales de la ciudad: se indaga si se realiza lo mismo que en lo referente al punto anterior.

- Perdida de personal clave: se debe preguntar si existe una persona capaz de realizar las actividades de otra. Se puede mencionar si a la información que manejan las personas pueden acceder otras personas de mayor rango, siempre con las autorizaciones correspondientes, y considerando políticas de seguridad de la información de la organización.

- Fallas del proveedor de Internet:¿existe algún proveedor de Internet (ISP) alternativo en caso falle uno? El fin es tener alta disponibilidad para este servicio, HA *(High Availability)*.

- Pérdida de datos: ¿existen copias de respaldo, tanto para la información como para la data de los sistemas que apoyan a los procesos críticos?

Se debe especificar si se posee *script* para creación de copias de seguridad o copias de respaldo.

- Fallas irreparables de equipo de cómputo: ¿existe garantía de los equipos? ¿Se puede ampliar sobre el tipo de garantía? Hay garantías que cubren cualquier daño del equipo, aun cuando no fuera por daños del fabricante.

- Falla en sistema eléctrico: ¿existen UPS, u otra fuente de alimentación eléctrica? Para UPS se deben tener listas con tiempo de antigüedad.

- Falla de sistemas: se debe especificar si es aplicación (cliente/servidor) o *web* de instalación independiente (solo en el equipo que lo utiliza).Se debe también listar para cada uno de los sistemas que apoyan a los procesos críticos si se posee instaladores del sistema, o base de datos, o si existe ubicación especial de los instaladores.

3.2.3. Paso 3: Cálculo del nivel de exposición al riesgo

Los cálculos de cobertura son independientes del grado que la organización evaluada posea frente a cada amenaza, siempre siguiendo el rango propuesto por los autores mencionados anteriormente, y en base a que se está adaptando a una PYME guatemalteca. La cobertura, que indica qué cobertura tiene la organización frente a la amenaza evaluada, se mantiene en seis niveles (0 % 19 %, 20 % 39 %, 40 % 59 %, 60 % 79 %, 80 % 99 %, 100%). Y el grado de severidad, que indica si esta amenaza llegara a ocurrir y pudiera explotar alguna vulnerabilidad qué tan severo sería para la organización, se mide según estos niveles: alta = 100, moderada = 50 y baja = 10.

Al momento de crear la lista de potenciales amenazas también se clasificarán según su nivel, desde los menos graves hasta los más complejos, con la diferencia que para el fin de las PYME en Guatemala únicamente se llegará al nivel 4, dado que generalmente solo se posee una única instalación/oficina, aunque siempre queda abierto para el caso de una empresa u organización que tenga subsedes o proyectos en otros departamentos.

- Nivel 1: afecta la continuidad por la pérdida de un recurso crítico
- Nivel 2: afecta muchos procesos por evitar el acceso a las instalaciones
- Nivel 3: afecta varios procesos porque destruye recursos críticos
- Nivel 4: se da por la destrucción de las instalaciones

Un ejemplo de una organización puede verse en la tabla VIII. Este análisis es diferente para cada organización, dependiendo de sus vulnerabilidades y controles existentes, y agregando el nivel como última columna. Para el nivel de exposición siempre se utiliza la propuesta por Alexander, siendo esta: severidad * (100 % de cobertura), tomando siempre el menor número del rango).

Este cálculo de exposición al riesgo también servirá para saber si la organización posee un plan de contingencia ante el desarrollo de uno de estos incidentes que pudiera llegar a explotar las vulnerabilidades, por ejemplo, como la violencia tiene una exposición al riesgo de 80, la empresa debe preguntarse qué se debe hacer para que un acto de violencia no llegue a afectar tanto, y así reducir esta exposición al riesgo, tomando medidas como: poseer seguro de activos, poseer copias de seguridad actualizadas de los equipos (depende cuál es el RPO), entre otros.

Para el caso de sismos, con una exposición al riesgo de 100, la empresa debe preguntarse qué controles debe realizar como plan de contingencia ante

un sismo, por ejemplo, si posee copias de respaldo fuera de las instalaciones de la empresa, con qué regularidad se realizan (cumpliendo con el RPO aceptado), si existe la certeza de que estas copias podrían funcionar correctamente cuando se lleguen a necesitar, si el servidor se encuentra en un sitio seguro dentro de las instalaciones (donde no podrá caerse y causar daños a los discos duros y provocar pérdida de la información, por ejemplo). En el caso de sismos, prácticamente se realiza una evaluación completa de todos los recursos utilizados dentro de las instalaciones de la empresa.

Tabla IX. **Cálculo de exposición al riesgo y escenario de amenaza (nivel)**

Amenazas	Severidad			Cobertura						Exposición del Riesgo	Nivel
	B = 10	M=50	A=100	0-19%	20-39%	40-59%	60-79%	80-90%	100%		
Violencia			100		20 %					80	3
Sismos			100	0 %						100	3 y 4
Manifestaciones	10				20 %					8	2
Inundaciones de calles	10				20 %					8	2
Pérdida de personal clave.			100	0 %						100	1
Fallas del proveedor de Internet		50						80 %		10	1
Pérdida de datos			100			40 %				60	1
Fallas de equipo de cómputo	10						60 %			4	1
Falla en sistema eléctrico	10							80 %		2	1
Pérdida de sistemas (cliente/servidor)			100		20 %					80	1
Pérdida de sistemas (Web)			100				60 %			40	1
Pérdida de sistemas (Instalado PC)			100	0 %						100	1

Fuente: ALEXANDER G., Alberto. *Diseño de un SGSI*. p. 86.

3.3. FASE III – Desarrollo de estrategias

Para el desarrollo de estrategias para la continuidad de operaciones de la organización se tenían cuatro fases (que se resumirán en un cuadro). Ahora el enfoque será en los recursos de tecnología que apoyan a los procesos críticos. Esto se puede realizar por área. Se dará una vista general de lo que podría adaptarse a PYMES en la Ciudad de Guatemala, tomando recursos de tecnología genéricos en cualquier organización, como se puede observar en la tabla IX. Sin embargo, esta lista debe ser tomada de la lista de recursos de tecnología, obtenida en el análisis de impacto en la primera fase.

También cabe resaltar que esta lista debe generarse con base en los recursos de tecnología que pueden verse afectados por algunas de las amenazas o escenarios considerados en la fase anterior, tomando como prioridad las que están más expuestas.

En este ejemplo se ha agregado la columna de costos, donde se pondrán las diferentes opciones con sus diferentes costos, y el cuadro final resultante únicamente tendrá el costo de la opción seleccionada para cubrir el requerimiento de recuperación. Los valores de la columna “Costo Aprox.” son solo con fines de ejemplificar, y también pensando que la organización no posee ninguno de estos recursos con anticipación como forma de contingencia, ya que en la mayoría de PYMES no se poseen servicios alternos de Internet, no se poseen equipos comodines, es decir, equipos sin uso y que pueden ser utilizados para cualquier otra actividad. En caso de que la PYME ya posea alguno de estos recursos, se debe obviar el valor del costo.

Tabla X. **Requerimientos de recuperación**

Recurso de Tecnología critico	Requerimiento de recuperación	Opciones	Costo	Costos Aprox.
Internet	ISP alternativo, y tipo de servicio	Proveedores locales	Costo de cada proveedor	Q. 500,00
Correo Electrónico	Soporte de alta disponibilidad, correo alternativo	Servicio de *hosting*, servidor alternativo	Costo de proveedores	Q. 2 000,00
Sistemas Web (Intranet)	Ubicación alterna, instaladores, *backups*	Equipo local, servidor virtual	Costo de proveedores, Costo de equipo	Q. 4 000,00
Servidor (Carpetas Compartidas)	*Backups*, servidor alternativo, instaladores	Discos de alta capacidad de respaldo	Costo de equipo y discos	Q.1 500,00
Sistema Contable (Cliente/Servidor)	Ubicación alterna, instaladores, *backups*	Equipo PC/Portátil	Costo de equipo	Q. 8 000,00
Sistema Específico de la organización	Instaladores, nueva ubicación, *backups*			
Sistema ISR	Instaladores, nueva ubicación, *backups*	Equipo comodín	Costo de equipo	Q. 5 000,00
Sistema Planillas				
Sistema IGSS				
Red interna (Intranet)	*Routers, Access Point, Switch*	Diferentes marcas, sin importar que sean SOHO	Costo de proveedores	Q. 1 500,00
Impresoras en Red	Impresora alternativa con protocolos de red	Diferentes marcas	Costo de proveedores	Q. 1 500,00
			Total	**Q.24 000,00**

Fuente: elaboración propia.

3.4. FASE IV – Desarrollo del plan de reanudación de operaciones

Dado que en PYMES generalmente no existe un departamento de tecnología de la información, se tiende a subcontratar servicios de TI, o bien puede ser que este conste de una sola persona como soporte técnico, entonces se debe conformar un equipo que tome las iniciativas de respuesta inicial,

acompañado de gerentes/jefes de departamento con la suficiente autoridad para la toma de decisiones dentro de la organización.

Por lo tanto, se recomienda que este equipo responsable de ejecutar y supervisar el plan de reanudación esté conformado por el gerente de operaciones, gerente financiero y responsable del área de tecnología de la organización. El gerente de operaciones, o administrador, para dirigir todas las decisiones de tipo administrativas y de coordinación con el personal, y como canal de comunicación con los demás empleados. El gerente financiero, por los gastos que estén bajo presupuestos destinados a este plan de reanudación, y para que se cumpla con los requerimientos solicitados para la recuperación de recursos. Finalmente, el encargado IT, por ser el ejecutor de todos los pasos para el restablecimiento de recursos y tener a su disposición toda la información de sistemas y tecnologías utilizadas.

Para cada uno de los escenarios de amenazas detectados se realizan fases para la reanudación de actividades, por ejemplo, la amenaza que puede causar un mayor impacto es la de un sismo, por su grado de exposición al riesgo, ya que esta puede afectar no solo acceso a instalaciones, sino que puede ser que ocurra pérdida o destrucción de áreas de instalaciones, lo que conlleva a una serie en cadena de las demás amenazas como pérdida de equipo, de red interna, de acceso a sistemas en servidores locales y demás.

Se mencionará la amenaza de un sismo con el fin de considerar los pasos del plan de reanudación de operaciones, como un panorama general, ya que al momento de realizarlo para una PYME en específico se deben considerar situaciones muy propias de la PYME. Sin embargo, se mencionarán aspectos genéricos que aplican a cualquier PYME, y que se podría decir que son hasta de sentido común.

Para esto también cabe resaltar que las medidas de contingencia que se deberían haber tomado deben estar funcionando de forma correcta, ya que el objetivo de este plan de reanudación de operaciones, es únicamente establecer las operaciones utilizando lo ya realizado por un plan de contingencia ante fallos, y cumpliendo con los tiempos de recuperación, considerando que se ha cumplido con las medidas de seguridad de información. Por ejemplo, si existen repositorios de instaladores actualizados, si existe repositorio de copias de seguridad, si los servidores se encuentran protegidos de forma correcta, etc. Todo plan de reanudación de operaciones va íntegramente relacionado con un plan de contingencia ante fallos realizado con anterioridad. Como ejemplo se nombrarán las fases de reanudación de operaciones, considerando que se han interrumpido operaciones por un sismo.

3.4.1. Respuesta inicial

Se debe realizar una evaluación y una lista de chequeo del funcionamiento de todos los recursos que apoyan los procesos críticos dentro de la oficina, tomando como base el listado realizado durante el análisis de impacto. Por ejemplo, los aspectos para revisión podrían ser:

- Servidores (aplicaciones cliente/servidor, *web*, datos)
- Red interna (Protocolos TCP/IP, UDP)
    - *Firewalls*
    - *Routers/Access point*
    - *Switchs*

- Bases de datos (SQL Server, MySQL, etc.)
- Impresoras (con protocolos de red)

Se supone que de este chequeo inicial resulta que la empresa no estaba preparada para sismos, y el servidor de aplicaciones tuvo daños irreparables en cuestiones de hardware y este mismo servidor tenia servicios de servidor de archivos y de directivas de grupo para el dominio. En Guatemala, las PYMES generalmente cuentan con un único servidor y este tiene configurados varios servicios.

3.4.2. Medida de contingencia provisional

- Se debe tener un documento con la lista de todos los servicios y aplicaciones configurados en este servidor.
- Se debe tener un documento con información de última copia de respaldo del servidor, de todo lo que este posea: directivas de grupo, información, bases de datos, aplicaciones.
- Debe existir un equipo que pueda ejercer las funciones de un servidor.

3.4.3. Aprovisionamiento de recursos y reanudación

- Se debe poseer fuera de oficinas, en la nube, o en cualquier otro medio externo, un repositorio de los instaladores de todos los sistemas utilizados por la empresa, clasificados por área con un documento que identifique la versión del software y usuarios. Este documento, así como el repositorio, deben actualizarse constantemente.

- El equipo a utilizar ya debería tener instalado todo lo que posea el servidor, con el fin de solo cargar la data y últimas copias de seguridad generados. Esto se considera porque en las PYME no se tienen otros servidores o discos que hayan funcionado como espejo (RAID 1), ya que la PYME prefiere aprovechar espacio o capacidad en lugar de seguridad.

- Se debe cargar primero la información actualizada de políticas de grupo de dominio (directivas de grupo), para tecnología Microsoft. Se puede utilizar el siguiente enlace sobre directivas de grupo:https://technet. microsoft.com/eses/library/hh147307(v=ws.10).aspx

- Posteriormente se carga la información de servidor de archivos y la instalación de software.

- Al mismo tiempo se debe proceder con la recuperación del servidor, siguiendo los tiempos de recuperación estipulados para cada sistema de información que está instalado en el servidor. Puede existir un margen de error sobre la pérdida de datos, aceptado por la empresa, pues toda empresa nunca deseará perder ningún porcentaje de información, sobre todo de la información sensible.

- Si fuese necesaria la compra de equipo debe estar dentro de la aprobación del gerente financiero y gerente general/director.

3.4.4. Reconstitución

Este no será más que el proceso en el que se tiene la garantía que el servidor se encuentra nuevamente en funciones óptimas, se han restablecido todos los servicios y regresará a su uso en condiciones normales, es decir, trasladando toda la información del equipo utilizado durante la contingencia provisional.

3.5. FASE V – Ensayo del plan de continuidad

Tomando como base el equipo responsable de encabezar las actividades de reanudación de operaciones, se deberá acordar reuniones periódicas, de preferencia dos veces al año, cada 6 meses, para evaluar y realizar un paseo de revisión sobre los procedimientos que se deben seguir en el PCN, para cada una de las amenazas detectadas, evaluando los canales de comunicación que deben existir, la seguridad de la información, los recursos necesarios (si siguen siendo los mismos de la última reunión), si se sigue estando en los mismos grados de exposición al riesgo en ciertos escenarios, para ir haciendo las modificaciones y mejoras al plan.

Se seleccionó el “paseo por revisión” por su facilidad de realización y por no implicar costo alguno para la empresa, no haciendo referencia solo a una inversión económica, sino también a una inversión de mucho personal y de tiempo.

4. *CLOUD SERVICES* COMO RECURSO PARA LA REDUCCIÓN DE TIEMPOS DE RECUPERACIÓN Y COMO MEDIDAS DE CONTINGENCIA

Todo el proceso realizado anteriormente requiere una serie de controles y planes realizados a la medida de cada empresa. Sin embargo, actualmente existen diversas herramientas, tecnologías actuales, que pueden ser utilizadas para el trabajo en cualquier PYME, y que reducen el riesgo a la mayoría de amenazas descritas anteriormente (sismos, violencia, inundaciones, entre otras), no solo ante la pérdida de información, como medida de contingencia y como parte de un plan o gestión de seguridad de la información, sino también como parte de un plan de continuidad de operaciones.

Por ejemplo, una forma muy común de trabajo fuera de oficinas centrales ha sido por medio de VPN *(*Virtual Private Network*)* y el trabajar en la red de la empresa. Esto algunas veces puede acarrear complicaciones para una PYME si esta no posee el personal técnico adecuado, infraestructura adecuada y configuraciones adecuadas. Siempre es importante cuidar la seguridad del acceso a la información, así que este aspecto no se debe descuidar en ninguna de las herramientas a utilizar.

Con tecnología actual, que forme parte del plan de contingencia y la vez forme parte de un plan de continuidad, se hace referencia a los *cloud services* (servicios en la nube), también conocidos como *cloud computing* (computación en la nube). Y entra en juego también el concepto de SaaS, por sus siglas en inglés, Software as a Service.

Con SaaS se logra dar acceso a aplicaciones de usuarios finales por medio de Internet, sin que se haya tenido que realizar una fuerte inversión en infraestructura tanto de hardware como de software. Con Cloud Computing, SaaS, se obtienen varias características dentro de las que se pueden mencionar:

- Alta escalabilidad: que ofrece distintas características según las demandas de los usuarios. Estas pueden ir aumentando según sus necesidades, y el usuario final no interviene en las distintas ampliaciones de infraestructura (servidores, hardware, software).

- Actualizaciones automáticas: dado que todo puede ser manejado desde la nube, las actualizaciones son parte del servicio en el que no interviene directamente el usuario final ni personal IT de la empresa.

- Accesibilidad y persistencia: estos factores también han sobresalido, porque muchas empresas, desde pequeñas hasta grandes, están tendiendo a migrar todos sus servicios a la nube. También proporcionan estabilidad, poseen una gran infraestructura de *data centers* para los que una empresa común necesitaría invertir fuertes cantidades de dinero para implementarlos. Son accesibles desde cualquier lugar (dentro y fuera de las instalaciones) y también desde cualquier equipo. Y, finalmente, persistencia, que no refiere servicios variables, sino que permanecen constantes sin que existan pérdidas, pudiendo ser recuperados o utilizados en cualquier momento en el que se requieran.

De esta forma, las pequeñas y medianas empresas hoy en día tienen a su alcance herramientas que las ponen en un alto nivel de seguridad y al mismo tiempo de competitividad en el mercado.

La utilización de estos servicios también depende del volumen de información que manejan las PYME, y de la capacidad de inversión que posean. Por ejemplo, para un servicio de almacenamiento en la nube de una pequeña empresa que maneja un volumen de información de 2GB promedio, no se necesita lo mismo que una empresa que maneja volumen de 50GB de información, y es aquí donde se puede ver la importancia de la escalabilidad de los servicios en la nube, pues cuando la empresa de 2GB de volumen empiece a crecer no necesitará realizar una gran inversión en almacenamiento de servidores o SAN *(*Storage Area Network*),* si no que realizará un *upgrade* a sus servicios en la nube, sin tener mayor complicaciones de configuraciones, tiempos de implementación e inversión monetaria.

Cuando se tratan de pequeñas empresas con un volumen no alto de almacenamiento se pueden tener opciones libres como:

- *Google Drive* (almacenamiento)
- *Dropbox* (almacenamiento)
- *Team Drive* (almacenamiento compartido con control de cambios)

También están el manejo de correos por medio de dominio adquirido por la misma empresa, así como un *hosting* de contrato anual. Estos pueden configurarse con protocolo de correo IMAP *(*Internet MessageAccess Protocol*)*, con lo que se busca tener acceso a los mismos correos desde cualquier ubicación, aunque muchas veces se puede tropezar con limitantes como soporte de ancho de banda del *hosting* y de almacenamiento en el *hosting*. Esta última limitante ha ido desapareciendo con el transcurso del tiempo, pero aun así las sincronizaciones pueden ocasionar conflictos de comunicación entre el dispositivo configurado como IMAP y el servidor de correos, por lo que esto

puede llegar a ser funcional cuando no son muchas las conexiones que se hacen al servidor.

Ahora bien, si se considera un volumen mayor a 20GB se pueden considerar servicios en la nube más robustos y con características integradas de alta calidad, para poder disponer de estos servicios en cualquier ubicación del país, e incluso fuera de las fronteras de Guatemala.

Para una PYME con mayores necesidades, y que al mismo tiempo busque mejorar sus planes de contingencia y a la vez buscar la continuidad de operaciones frente a cualquier amenaza, se pueden recomendar soluciones corporativas en la nube. Para empresas con infraestructuras más robustas y con capacidad de inversión mayor se podrían considerar:

- AWS *(*Amazon Web Services*)*
  - Servidores virtuales
  - Almacenamiento
  - Bases de datos
  - Redes

- Google Cloud Platform
  - Almacenamiento y Bases de datos
  - *Compute*
  - Redes *(Networking)*
  - *Big Data*

Sin embargo, para PYMES, que son el fin de este análisis, se pueden considerar soluciones como:

- Google for Work
    - Almacenamiento
    - Calendarios
    - *Sites*
    - Llamadas y videoconferencias
    - Correo
    - Colaboración (Docs)
    - Capacidad móvil

- Office 365 Business Essential
    - Almacenamiento
    - Calendario
    - Llamadas y videoconferencias
    - Correo
    - *Office online*
    - Capacidad móvil

- Servidores Virtuales (Windows, Linux) – Con BD SQL, MySql – Existen variedad de proveedores, aunque no a gran escala como AWS y Google *Cloud Platform*.

Con la lista de recursos de tecnología que apoyan los procesos críticos, obtenida del análisis de impacto, se realizará nuevamente un breve análisis sobre los recursos que han sido cubiertos al momento de realizar una migración a servicios en la nube. Para este ejemplo se tomará la lista de recursos críticos que se utilizó para el desarrollo de estrategias, que es la unificación de los recursos de tecnología de los diferentes procesos críticos.

Tabla XI. **Recursos de tecnología críticos con servicios en la nube**

Recurso de tecnología critico	**Requerimiento de recuperación**	**Opciones**
Internet	ISP alternativo	Proveedores locales
Correo Electrónico	*Cloud Services*	Cero pérdida de data y accesible en cualquier momento
Sistemas Web (Intranet)	*Servidor Virtual*	Cero pérdida de data y accesible en cualquier momento
Servidor (Carpetas Compartidas)	*Cloud Services*	Cero pérdida de data y accesible en cualquier momento
Sistema Contable (Cliente/Servidor)	Ubicación alterna, instaladores, *backups*	Utilizar servidor virtual como medio de contingencia
Sistema específico de la organización	Instaladores, nueva ubicación, *backups*	
Sistema ISR	Instaladores, nueva ubicación, *backups*	Utilizar servidor virtual como medio de contingencia
Sistema Planillas		
Sistema IGSS		
Red interna (Intranet)	*Routers, Access Point, Switch*	Diferentes marcas, sin importar que sean SOHO
Impresoras en red	Impresora alternativa con protocolos de red	Diferentes marcas

Fuente: elaboración propia.

Como se puede observar en la tabla X, marcados en verde, algunos procesos que son considerados críticos dentro de cualquier empresa están cubiertos por servicios en la nube, tanto como parte de un plan de contingencia como por un plan de continuidad de operaciones, ya que al momento de ocurrir cualquiera de las amenazas listadas, estos recursos permanecerán funcionando, pues no dependerán directamente de la infraestructura de la empresa. También se puede observar que hay recursos que no están migrados a servicios en la nube y que siempre necesitarán de un servidor local para su utilización dentro de la empresa, sin embargo, están en un tono de verde más claro, ya que estos sí pueden ser instalados en cualquier momento en un servidor virtual y ser utilizados por medio de escritorio remoto, protocolo RDP *(*Remote Desktop Protocol*),* como una medida de contingencia provisional del plan de reanudación de operaciones; y así se cargará la *data* de la última copia

de respaldo generada para estos sistemas, copias de respaldo que sí estarán en un servicio de almacenamiento en la nube.

De esta forma, los recursos críticos marcados en azul son para los que se deben seguir manteniendo en planes de continuidad de operaciones de forma actualizada y monitoreada, y se reducen los recursos críticos para los que se debe tener plan de continuidad de operaciones (ver tabla XI).

Tabla XII. **Recursos críticos resultantes**

Recurso de tecnología critico	Requerimiento de recuperación	Opciones
Internet	ISP alternativo	Proveedores locales
Red interna (Intranet)	*Routers, Access Point, Switch*	Diferentes marcas, sin importar que sean SOHO
Impresoras en red	Impresora alternativa con protocolos de red	Diferentes marcas

Fuente: elaboración propia.

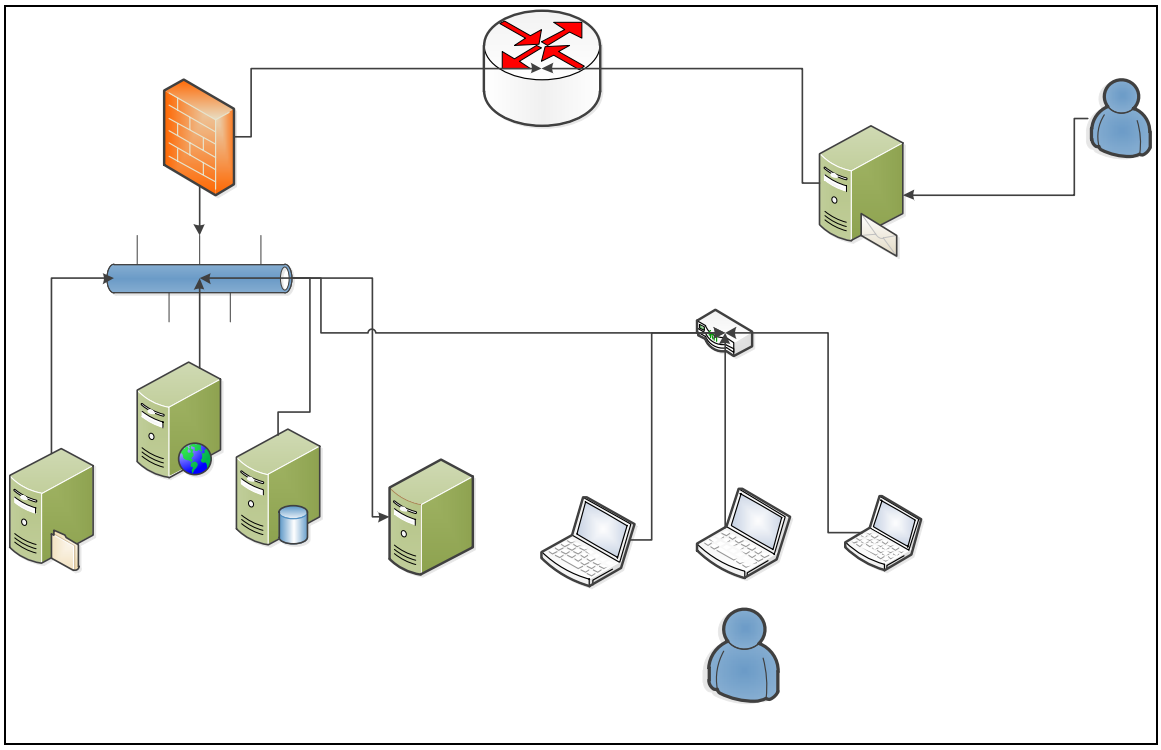
Al mismo tiempo, al tener servicios en la nube se puede volver a realizar el análisis del cálculo de exposición al riesgo, de la sección 3.2.3, por amenaza, y se podría observar que también habrá una reducción en los grados de exposición al riesgo.

En un diagrama de infraestructura de red de una PYME(ver figura 9), generalmente se utiliza un mismo servidor para varios servicios, sin embargo los servicios se garantizan únicamente cuando se está dentro de las instalaciones, de lo contrario se limita muchas veces a servicio de correo electrónico, que generalmente esta albergado en un *hosting*.

Sin embargo, al migrar a servicios en la nube disminuye no solo la inversión en mantenimiento de *hardware* dentro de las instalaciones, si no que

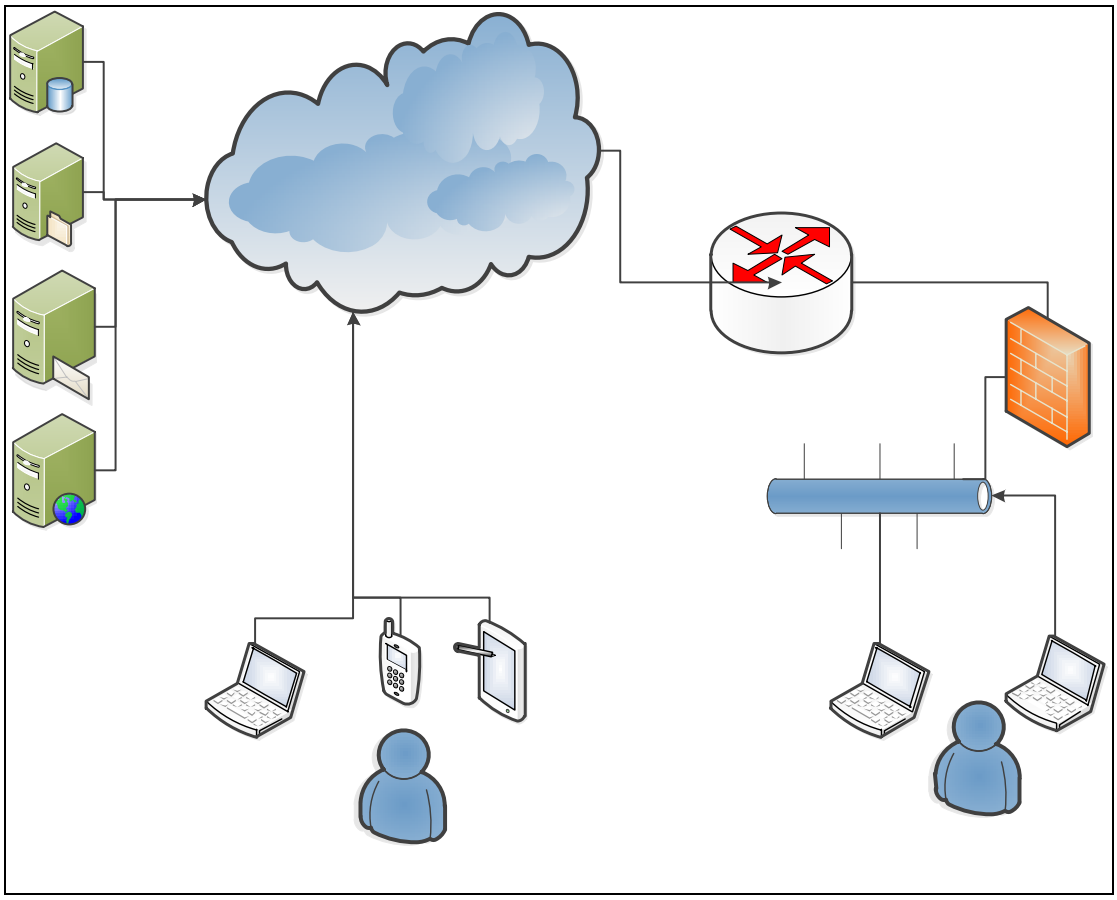
aumenta la productividad fuera de las instalaciones físicas de la empresa, de tal forma que también se provee acceso a los mismos servicios tanto dentro como fuera y desde diferentes dispositivos(ver figura 10).

Figura 8. **Diagrama de infraestructura de red**



Fuente: elaboración propia.

Figura 9. **Diagrama de red con servicios en la nube**



Fuente: elaboración propia.

CONCLUSIONES

1. Un plan de continuidad de operaciones va íntegramente relacionado con un SGSI, incluyendo todos los controles realizados para asegurar la información de la empresa, como creación de copias de respaldo.

2. El plan de continuidad de operaciones hace uso de todas las medidas de seguridad que haya tomado la empresa y busca crear un plan para restablecer los servicios y recursos de tecnología en el menor tiempo posible (tiempos aceptados por la empresa).

3. Uno de los puntos clave de este análisis es la determinación de las amenazas según la región que se esté evaluando, a partir de una ubicación geográfica de las mismas, la cual puede variar.

4. Los cálculos de exposición al riesgo dan un valor agregado a la empresa que esté realizando un análisis de este tipo, ya que a partir de ellos se puede determinar ante qué tipo de amenaza posee una vulnerabilidad mayor. También pueden revelarse casos en los que la empresa no ha prestado todavía atención y esté vulnerable, por ejemplo, ante un tipo de amenaza que llegue a afectar los recursos de tecnología y que provoque una interrupción de procesos críticos.

5. Las tecnologías recientes, como la migración de servicios a la nube, pueden llevar a una empresa a minimizar el grado de exposición al riesgo, y a partir de ello realizar un nuevo análisis de plan de continuidad

de negocio (PCN) para los recursos de tecnología que no pueden migrarse a la nube.

RECOMENDACIONES

1. Las instituciones que fueran a desarrollar un plan de continuidad deben realizar un análisis acorde a su ubicación geográfica, pues incluso estando dentro de la ciudad capital su grado de exposición al riesgo puede variar; no es lo mismo una empresa que está ubicada en la zona 1 o zona 3, a una empresa ubicada en la zona 15 o zona 16, ya que la amenaza ante indicios de violencia, o manifestaciones, es mayor.

2. Dado que este análisis se realizó únicamente para la Ciudad de Guatemala, área metropolitana, para otra ubicación geográfica se debe realizar un análisis similar acorde a las amenazas en dicha ubicación, por ejemplo: erupción de volcanes, arena volcánica, inundaciones, derrumbes, entre otros, siguiendo el mismo proceso adaptado para una PYME.

3. La empresa debe asegurarse que los controles de seguridad de la información se estén llevando a cabo correctamente, ya que estos serán utilizados posteriormente en un plan de continuidad de operaciones, este se encarga de restablecer los servicios de manera acorde al análisis del impacto del negocio, sobre procesos críticos y recursos de tecnología.

   Toda empresa u organización que no posea mucho poder de inversión puede optar por servicios en la nube de acuerdo a sus capacidades y uso, utilizando servicios libres pero con menor capacidad que un servicio pagado. Esto además de asegurar su información fuera de las

instalaciones de la empresa, asegurará la continuidad en cualquier otra ubicación

BIBLIOGRAFÍA

1. ALEXANDER, Alberto G. *Diseño de un Sistema de Gestión de Seguridad de Información.* Bogotá, Colombia: *Óptica ISO 27001:2005*. 2007.176 p.

2. ÁLVAREZ, Carlos; DE LEÓN, Irene. *Sismo de 4.5 grados es asociado a falla de Jalpatagua.* [en línea]. <http://www.prensalibre.com/ guatemala/comunitario/sismo-sacude-el-centro-del-pais>. [Consulta: abril de 2016].

3. ArcGIS. *Fallas geológicas en la zona metropolitana de Guatemala.* [en línea]. <https://www.arcgis.com/home/webmap/viewer.html?webmap=b55265b68d2645c88cb4cc6e06a117be>. [Consulta: marzo de 2016].

4. CASTAÑÓN, Mariela. *Las diez zonas más peligrosas de Guatemala.* [en línea]. <http://lahora.gt/hemeroteca-lh/las-diez-zonas-mas-peligrosas-de-guatemala/>. [Consulta: abril de 2016].

5. BETANCOURT CANCHIGNIA, Erika Fernanda; SALGUERO VÉLIZ, Juan Francisco. *Propuesta un plan de continuidad del negocio (BCP). Caso de aplicación*. Quito, Ecuador: Escuela Politécnica Nacional, 2014. 147 p.

6. CHEN, Jin Jun; WAN, Lizhe. *Special issue: cloud computing.* Journal of Computer and System Sciences. Australia: View Editorial Board, 2012. 391 p.

7. Emisoras Unidas. *Manifestaciones.* [en línea]. <https://emisorasunidas.com/etiqueta/manifestaciones/>. [Consulta: junio de 2016].

8. Embajada del Japón en Guatemala. Oficina Gis PNC. *Áreas rojas. Municipio de Guatemala. Delitos contra la vida.* [en línea]. <http:// www.gt.emb-japan.go.jp / map / AREAS % 20ROJAS%202009% 20 GUATEMALA.pdf>. [Consulta: abril de 2016].

9. ESPINOSA DÍAZ, Yessica; FIGUEROA ROCHÍN, Claudia; LIZALDE MARTÍNEZ, Félix; SEPÚLVEDA RODRÍGUEZ, Jesuán. *Plan de continuidad académica utilizando tecnologías de información comunicación y colaboración ante una contingencia en una institución de educación superior*. México: Universidad Autónoma de México, 2012. 19 p.

10. GASPAR MARTÍNEZ, Juan. *El plan de continuidad de negocio*. Madrid, España: Diaz de Santos, 2006. 223 p.

11. _____. *Planes de contingencia*. Madrid, España: Diaz de Santos, 2004. 256 p.

12. INSIVUMEH. *Mapa de amenaza sísmica.* [en línea]. <http://www.insivumeh.gob.gt/Mapa_Amenaza_sismica.html>. [Consulta: abril de 2016].

13. La Tribuna. *Las 50 ciudades más violentas del mundo.* Tegucigalpa, Honduras, 2016. [en línea]. <http://www.latribuna. hn/2016/ 01/29/las-50-ciudades-mas-violentas-del-mundo/>. [Consulta: abril de 2016].

14. MENDOZA ESCAMILLA, Viridiana. *Las 50 ciudades más violentas del mundo.* [en línea]. <http://www.forbes.com.mx/las-50-ciudades-mas-violentas-del-mundo/>. [Consulta: junio de 2016].

15. Microsoft. *Directiva de grupo para principiantes.* [en línea]. <https:// tech net. microsoft.com / es-es / library / hh147307 (v=ws.10) .aspx>. [Consulta: agosto de 2016].

16. PITÁN, Edwin. *Inundaciones por intensa lluvia en la capital y Mixco.* [en línea]. <http://www.prensalibre.com/guatemala/comunitario/lluvias-causan-inundaciones-en-la-metropoli>. [Consulta: junio de 2016].

17. Real Academia Española de la Lengua. *Diccionario de la Real Academia Española*. [en línea]. <http://dle.rae.es/?id=CUceyCB>. [Consulta: agosto de 2016].

18. ROUSE, Margaret. *Software as a Service (SaaS)*. [en línea].http://searchcloudcomputing.techtarget.com/definition/Software-as-a-Service>. [Consulta: mayo de 2016].

19. Wikipedia. *Pequeña y mediana empresa.* [en línea]. <https://es.wikipedia.org/wiki/Peque%C3%B1a_y_mediana_empresa>. [Consulta: abril de 2016].