LA CONTINUIDAD DEL NEGOCIO EN PROCESOS Y SERVICIOS – PYS

Lemaitre Vargas, Orlando Esteban
orlandolemaitrev@gmail.com
Universidad Piloto de Colombia

Resumen **–** Este documento presenta un análisis de las problemáticas que se presentan en una PYME como es Procesos y Servicios SAS, es una Empresa cuyo "Core" de Negocio es la digitalización de documentos, por lo tanto, el volumen de información que se procesa y se mantiene es un factor decisivo, el digitar la información en los aplicativos de los clientes con base en la información procesada y luego almacenar esa información para mantenerla disponible. También examinar el análisis de costo beneficio sobre lo que implica generar los Backup´s, las condiciones del negocio de frente a los clientes y los marcos legales y contractuales que impactan a la Empresa.

Índice de Términos **-** Activo, amenaza, ataque, impacto, incidente, riesgo, vulnerabilidad, modelo PHVA, MECI, PYS, Core, Backup(´s), GB, TB, SARO, SI, ANS.

Abstract **-** This document presents the analysis of the problems that arise in an PYME such as Processes and Services, being a Company whose Business Core is the digitization of documents and therefore the volume of information that is processed and maintained as a decisive factor, enter the information in the clients' applications based on the information processed and then store that information to keep it available. Review the cost-benefit process involved in generating the Backup's, the business conditions facing the clients and the legal and contractual frameworks that impact the Company

Keywords **-** Active, threat, attack, impact, incident, risk, vulnerability, model PHVA, MECI, PYS, Core, Backup (´s), GB, TB, SARO, SI, ANS.

I. INTRODUCCION

A. Procesos y Servicios SAS.

Con diminutivo PYS. Es una PYME Colombiana, con sede en Bogotá D.C., la cual lleva una trayectoria de 25 años de trabajo en el sector comercial, con un frente de negocio que consiste en la digitalización de la información, la cual se digita en los aplicativos de los clientes con los cuales se tienen relaciones comerciales. Basadas en contratos, y los ANS que circunscriben los pormenores que los mismos establecen. Muchas veces se ha dicho que: "El papel está en vía de extinción en Colombia" pero hemos podido confirmar que el papel en Colombia tiene por lo menos unos 25 años más de vida, precisamente porque fuera de las ciudades principales y el sector privado, el manejo del papel en el país se mantiene y esa información tendrá que sufrir la trasformación a digital y eso garantiza que exista un mercado para PYS.

B. La Información.

A PYS, le llega información en documentos muchas veces en condiciones deplorables, en un completo desorden y generalmente agrupada en bolsas, cajas, AZ o simplemente con bandas de caucho. Estos documentos, son limpiados, alistados, organizados, agrupados y finalmente digitalizados por medio de escáneres de alta velocidad y alta definición. Una vez digitalizada, esta es revisada por dos grupos de personas, los digitalizadores y luego los supervisores de calidad digital, con el objetivo que la imagen capturada del documento sea clara, completa y no tenga zonas borrosas o difusas, es decir 100% veraz y fidedigna, fiel copia del documento original o fuente.

C. El Proceso.

Una vez con la imagen digitalizada, con 100% de Calidad, esa imagen es tomada por los Digitadores, los cuales van a digitar la información que presenta la imagen en los aplicativos de los clientes, una vez digitada, hay un proceso de revisión por parte de los supervisores del proceso, los cuales hacen verificación de la información que los Digitadores han introducido basados en procesos de muestreo. Por consiguiente, la imagen debe permanecer almacenada para ser entregada en medios magnéticos o copiada en los servidores de almacenamiento del cliente, pero esa información debe estar disponible para consultas posteriores ya sea PYS, por el cliente de acuerdo con lo contratado o cumpliendo con el marco legal.

D. Las Imágenes.

Estas son el corazón de la información; la imagen es el origen de lo que se plasma en los aplicativos de los clientes. Para PYS es un tema del día a día, debido a que la imagen debe permanecer disponible para los Digitadores y para los procesos de revisión, y también se le debe entregar al cliente. He aquí, el problema principal, como almacenar un enorme número de imágenes de varios clientes, que a hoy pueden llegar a pesar **12 TB de información creciendo día con día.**

II. LOS MARCOS LEGALES, CONTRACTUALES Y DE ANS´S

A. Marco Legal.

El marco legal para Colombia lo regula la Ley General de Archivo que es la Ley 594 del 2000 y el MinTIC que es el encargado de hacerla cumplir tanto en el ámbito de gobierno como en el sector privado. El Estatuto Mercantil en su artículo 48 dispone que "todo comerciante conformará su contabilidad, libros, registros contables, inventarios y estados financieros en general, a las disposiciones de este código y demás normas sobre la materia. Dichas normas podrán autorizar el uso de

microfilmación, faciliten la guarda de su archivo y correspondencia. Así mismo será permitida la utilización de otros procedimientos de reconocido valor técnico - contable, con el fin de asentar sus operaciones, siempre que facilite el conocimiento y prueba de la historia clara, completa y fidedigna de los asientos individuales y el estado general de los negocios". Esta norma señala, en primer lugar, que los comerciantes tienen la obligación de ajustar sus libros y papeles de comercio a las normas vigentes sobre la materia, y en segundo lugar, permite la utilización de distintos mecanismos para facilitar la gestión contable de las sociedades, siempre y cuando su uso se configure como la historia clara completa y fidedigna de la situación de los negocios. El Código de Comercio en su artículo 60 refiriéndose a la conservación de libros y papeles del comerciante, establece un término preciso para que los comerciantes hagan uso de cualquier sistema técnico tendiente a garantizar su reproducción exacta, ordenando para tal efecto, que los libros y papeles de comercio sean conservados cuando menos por diez años, contados desde el cierre o último asiento de los documentos o comprobantes. Adicionalmente, el artículo 60 mencionado, impone la obligación según la cual la Cámara de Comercio en donde se encuentran registrados los libros o documentos debe verificar que la copia sea exacta a los originales que se van a destruir, y que el acta que se levante como consecuencia de este trámite debe ir firmada por el secretario de la misma cámara.
A su vez, el artículo 134 del Decreto 2649 de 1993 dispone que "Los entes económicos deben conservar debidamente ordenados los libros de contabilidad, actas, registro de aportes, los comprobantes de las cuentas, los soportes de contabilidad y la correspondencia relacionada con sus operaciones.
Salvo lo dispuesto en normas especiales, los documentos que deben conservarse **pueden destruirse después de veinte (20) años** contados desde el cierre de aquellos o a la fecha del último asiento, documento o comprobante. No obstante, **cuando se garantice su reproducción por cualquier medio técnico, pueden destruirse transcurridos diez (10) años**, y es aquí en donde el proceso Core de PYS hace énfasis, dado que al digitalizar la información el archivo físico voluminoso desaparece para ser reemplazo por archivos digitales.
Tratándose de comerciantes, para diligenciar el acta de destrucción de los libros y papeles de que trata el artículo 60 del Código de Comercio, debe acreditarse ante la cámara de comercio, por cualquier medio de prueba, la exactitud de la reproducción de las copias de los libros y papeles destruidos.

B. Marco Contractual y ANS´s.

Tomando como base, lo que se indica en la norma ISO 27001 en lo que, a custodia de la información en los terceros contratados, los clientes de PYS han incluido en las cláusulas de los contratos firmados estableciendo condiciones en las cuales le están solicitando a la Empresa que su información se maneje con las siguientes variaciones por cliente:

- ✓ No se mantenga por más de 48 horas.
- ✓ No se mantenga por más de tres (03) meses.
- ✓ Se mantenga por los últimos cinco (05) años.
- ✓ Se mantenga una vigente de los últimos seis (06) meses y el resto disponible en consulta histórica por los últimos cinco (05) años.

Como se puede entender las condiciones contractuales establecidas con los clientes, generan un problema mayor desde el punto de vista técnico, dado que cumplir con esas condiciones en el fondo simplemente se traduce en que las Bases de Datos y las imágenes, deben estar disponibles al menos por Cinco (05) años en el caso más extremo en custodia de PYS y disponible "*On Line*" o de inmediato para el cliente. Mantener esta información (Bases de Datos + Imágenes) desde el punto de vista de almacenamiento se traduce en que la data pesa 12 TB actualmente. Manejar ese peso para procesos de Backup, significa que cada copia de seguridad va a tener que poder reconstruir los 12 TB de información, ya sea incremental o completa, administrar ese volumen de información es exactamente de lo que vamos a tratar en este documento más adelante.
Es de acotar que adicional a lo que se establece en los contratos, es muy normal que en los ANS´s que se firman en el marco del contrato a PYS se le exige que la información documental remitida sea procesada máximo en la siguientes 48 o 72 horas sin importar la fecha calendario. Esos ANS´s obligan a que PYS trabaje 7x24x364 de forma que el área de TIC y la Operación deben soportar ese flujo de trabajo bajo las condiciones de los ANS´s.
Eso también obliga a que la capacidad de almacenamiento sea lo suficientemente robusta para poder alojar la información que se está digitalizando. El proceso diario en PYS se promedia en un peso de 30 GB de información, para todos los clientes a los cuales se les presta el servicio.

III. LA CONTINUIDAD DEL NEGOCIO

Dadas las condiciones expresadas en los capítulos I y II, los procesos de continuidad del negocio deben estar enmarcados en las condiciones que requiere PYS, esas condiciones junto con el peso de la Data (Bases de Datos + Imágenes) son reto técnico mayor para el área de TIC de PYS. Detallaremos los que nos enmarca este proceso así:

A. Marco Normativo.

Los procesos de Continuidad del negocio están enmarcados en la norma ISO 22301, la ISO 31000 y la NIST 800-34, en donde se establece qué y cómo se debe implementar un Plan de Continuidad del Negocio, tema que vamos a abordar en profundidad de la siguiente forma.
Aunque no le aplican a PYS estas normativas, con el objetivo de poder cumplir con lo solicitado por los clientes, PYS tiene por objetivo cumplir con las normas que la Superintendencia Financiera de Colombia ha emitido con circulares donde se normatiza la necesidad de que las Empresas generen un Plan de Continuidad de Negocios, que cumplan con los siguientes elementos:

- ✓ Circular 041/2007- SARO: Las Empresas deben definir, implementar, probar y mantener un proceso para administrar la continuidad del negocio que incluya la prevención y atención de emergencias, administración de la crisis, planes de contingencia y capacidad de retorno a la operación normal.

- ✓ Circular 038/2009 – Sistema de Control Interno: Implementar, probar y mantener un proceso para administrar la continuidad de la operación de la Empresa para responder a las fallas e interrupciones específicas de un sistema o proceso y capacidad de

retorno a la normalidad.

- ✓ Circular 042/2012: Exigir que los terceros contratados dispongan de planes de contingencia y continuidad debidamente documentados. La Empresa deberá verificar que los planes, en lo que corresponde a los servicios convenidos, funcionen en las condiciones pactadas.

Además, existen metodologías para el Plan de Continuidad del Negocio fundamentado en el uso de buenas prácticas reconocidas y normas internacionalmente aprobadas basadas en la gestión de riesgos, entre ellas se encuentran DRI International (Disaster Recover Institute International) e ISO 22301, ISO27001, las cuales fueron tenidas en cuenta para la elaboración de este documento.

B. Introducción.

PYS reconoce que existen amenazas significativas ante la posibilidad de la ocurrencia de un incidente o desastre que afecte la operación, como también la necesidad de recuperarse en el menor tiempo posible, garantizando la continuidad de la Empresa.

La Administración del Plan de Continuidad de Negocios es una política que PYS debe implementar, para responder organizadamente a eventos que interrumpen la normal operación de sus procesos y que pueden generar impactos sensibles y críticos en el logro de los objetivos.

C. El Plan de Continuidad del Negocio.

Es una herramienta que mitiga el riesgo de no disponibilidad de los recursos necesarios para el normal desarrollo de las operaciones y como tal hace parte del Sistema de Gestión de Riesgo, ofreciendo como elementos de control la prevención y atención de emergencias, administración de la crisis, planes de contingencia y capacidad de retorno a la operación normal.

1. Objetivo General.
   Asegurar que PYS esté preparado para responder a emergencias o crisis, poder recuperarse de ellas y mitigar los impactos ocasionados, permitiendo la continuidad de los servicios críticos para la operación.
2. Objetivos Específicos.
   - 2.1. Lograr un nivel alto de preparación frente a incidentes o crisis que permita asegurar que se puede proteger la integridad de las personas, los bienes y activos de la Empresa en forma adecuada, realizando una buena administración de la situación.
   - 2.2. Minimizar la frecuencia de interrupciones de la operación de los procesos del negocio.
   - 2.3. Asegurar una pronta restauración de las operaciones afectadas por el evento.
   - 2.4. Reducir las decisiones a tomar en caso de contingencia para evitar cometer errores
   - 2.5. Cumplir los requerimientos de las normas emitidas por la Superintendencia de Sociedades y el MinTIC de Colombia.
3. Alcance.
   La Administración del Plan de Continuidad de Negocios es una disciplina que prepara a la Empresa para poder continuar operando durante un incidente o desastre, a través de la implementación de un plan de continuidad, el cual contempla los lineamientos y los requisitos Empresariales, el desarrollo de fases que componen el plan y las metodologías definidas por PYS para su ejecución, como también el desarrollo de los planes de contingencia, que se realizan de acuerdo con las prioridades establecidas por la Empresa.

De la misma manera, el desarrollo de los planes de continuidad se apoya en las capacidades con las que cuenta PYS para enfrentar situaciones que amenacen o afecten la integridad física de sus colaboradores e instalaciones, los bienes y activos tales como el Plan de Manejo de Emergencias, los mecanismos de protección y seguridad, Manual de Gestión de la comunicación en situaciones de crisis y los demás sistemas de gestión, como son los planes de BCP, DRP, el BIA y el Manejo de las Crisis, que son los elementos que componen un Plan de Continuidad del Negocio, completo.

C. Conceptos Básicos.

1. Administración del Plan de Continuidad de Negocios: Es un sistema administrativo integrado, transversal a toda la organización, que permite mantener alineados y vigentes todas las iniciativas, estrategias, planes de respuesta y demás componentes y actores de la continuidad del negocio. Busca mantener la viabilidad antes, durante y después de una interrupción de cualquier tipo. Abarca las personas, procesos de negocios, tecnología e infraestructura.
2. Incidente de Trabajo: Es un evento que no es parte de la operación estándar de un servicio y el cual puede causar interrupción o reducción en la calidad del servicio y en la productividad.
3. Problema de Continuidad de Negocio: Es un evento interno o externo que interrumpe uno o más de los procesos de negocio. El tiempo de la interrupción determina que una situación sea un incidente, una interrupción, una crisis o un desastre.
4. Planes de contingencia: Conjunto de acciones y recursos para responder a las fallas e Interrupciones específicas de un sistema o proceso.
5. Plan de Continuidad de Negocio (BCP): Conjunto detallado de acciones que describen los procedimientos, los sistemas y los recursos necesarios para retornar y continuar la operación, en caso de interrupción, o crisis.
6. Plan de Recuperación de Desastres (DRP): Es la estrategia que se sigue para restablecer los servicios de tecnología (red, servidores, hardware y software) después de haber sufrido una afectación por un incidente o una catástrofe de cualquier tipo, el cual atente contra la continuidad del negocio.
7. Análisis de Impacto del Negocio (BIA): Es la etapa que permite identificar la urgencia de recuperación de cada área, determinando el impacto en caso de interrupción.
8. Plan de Manejo de Crisis: Va a generar, manejar, administrar o gestionar un evento de crisis, es el proceso mediante el cual la Empresa enfrentará un acontecimiento de importancia que podría generar daño a la organización, sus *stakeholders*, o al público en general.
9. Disponibilidad: La información debe estar en el momento y en el formato que se requiera ahora y en el futuro, igual que los recursos necesarios para su uso.
10. Amenaza: Persona, situación o evento natural del entorno (externo o interno) que es visto como una fuente de peligro, catástrofe o interrupción. Ejemplos:

inundación, incendio, pandemias, robo de datos, ataques informáticos.

11. Vulnerabilidad: Es una debilidad que se ejecuta accidental o intencionalmente y puede ser causada por la falta de controles, llegando a permitir que la amenaza ocurra y afecte los intereses de la Empresa. Ejemplos: Deficiente control de accesos, poco control de versiones de software, entre otros.
12. Riesgo: Es la probabilidad de materialización de una amenaza por la existencia de una o varias vulnerabilidades con impactos adversos resultantes para la Empresa.
13. Frecuencia: Estimación de ocurrencia de un evento en un período de tiempo determinado. Los factores a tener en cuenta para su estimación son la fuente de la amenaza y su capacidad y la naturaleza de la vulnerabilidad.
14. Impacto: Es el efecto que causa la ocurrencia de un incidente o siniestro. La implicación del riesgo se mide en aspectos económicos, imagen reputacional, disminución de capacidad de respuesta y competitividad, interrupción de las operaciones, consecuencias legales y afectación física a personas. Mide el nivel de degradación de uno de los siguientes elementos de continuidad: Confiabilidad, Disponibilidad, Integridad y Recuperabilidad.
15. Control: Es el proceso, política, dispositivo, práctica u otra acción existente que actúa para minimizar el riesgo o potenciar oportunidades positivas.
16. Riesgo inherente: Es el cálculo del daño probable a un activo que esta desprotegido, o sin controles.
17. Riesgo residual: Riesgo remanente tras la aplicación de controles.

D. Estructura del Proceso de Continuidad del Negocio.

Para asegurar una adecuada administración de la continuidad del negocio se debe establecer con base en los procesos de Calidad ISO 9001, una estructura, que incluye la definición de los roles y responsabilidades, tanto de los Líderes de Proceso, como de la Alta Gerencia. Esa administración está conformada por:

1. Comité SARO – SI.

   La gestión de la continuidad de negocio requiere de una estructura organizacional, encargada de promover el desarrollo de los lineamientos definidos en este Capítulo, dado que el Comité SARO (Sistema de Administración del Riesgo Operativo) – SI (Seguridad Informática) debe encargarse de realizar el monitoreo a la gestión del Sistema de Riesgos y es responsable de administrar la continuidad de la operación de la Empresa. A continuación, se mencionan las personas que deberían integrar el comité, su rol y responsabilidad frente a este ítem así:

Tabla I.
Comité SARO – SI.

COMITÉ SARO - SI	
ROL PRIMARIO	ROLES DE CONTINGENCIA
Gerente General de PYS, quien presidirá el Comité	Cualquier Gerente
Analista Admistrativa	Asistente de Calidad
Director de TIC - CISO	Coordinador de TIC
Directora de Recursos Humanos	Jefe de Contabilidad
Director Juridico	Director Comercial
Jefes de Sedes	Coordinadores de Sedes

En caso en que el Comité active el plan de continuidad, podrá invitar a otros funcionarios responsables de actividades que impacten la operación del negocio, caso Supervisores de los Procesos Productivos.

Roles y Responsabilidades del Comité SARO – SI. A continuación, se describen los roles y responsabilidades de los integrantes del Comité en lo respectivo al plan de continuidad; vale aclarar las personas nombradas como principales y sus suplentes (Roles de Contingencia) tienen las mismas responsabilidades, que describiremos de la siguiente forma:

a. Presidente del Comité.
   El presidente del Comité es el encargado de dirigir y liderar todas las actividades de los planes de continuidad del negocio. Es responsable de declarar la contingencia ante el escenario de interrupción, crisis o catástrofe, con base en las decisiones tomadas por el Comité SARO - SI o en situaciones donde amerite realizar su activación inmediata.

b. Asistente Administrativo.
   El Asistente Administrativo, ayuda a coordinar los aspectos logísticos internos cuando la Empresa se encuentre operando bajo contingencia. Es quien ayuda a gestionar en cada una de las sedes y procesos el suministro de elementos esenciales para asegurar el desarrollo de la operación.

c. Director TIC – CISO.
   Es la persona encargada de liderar la recuperación tecnológica, basados en las estrategias de continuidad implementadas. Es el contacto directo entre la Dirección de TIC y el Comité SARO - SI; además, apoya las decisiones tomadas por el presidente del Comité durante la declaración y activación de la contingencia.

d. Jefes de Sedes.
   Son personas encargadas de liderar la

recuperación de procesos de negocio críticos, basados en las estrategias de contingencia. Son el contacto directo entre los procesos de negocio y el Comité SARO-SI; además, colaboran con las decisiones tomadas por el presidente del Comité SARO- SI durante la declaración y activación de la contingencia.

e. Líderes de los Planes de BCP y DRP.
Cada área o proceso Operativo deberá contar con un Líder de BCP y DRP, quien tiene la responsabilidad de actuar y colaborar en el proceso siguiendo el Plan.

2. Oficina de Riesgos.
Se debe crear en PYS una Oficina de Riesgos, que deberá ser conformada por la Asistente de Calidad y el CISO, y que tendrá su cargo las siguientes funciones en el plan de continuidad:
- ✓ Definir e implementar los instrumentos, metodologías y procedimientos tendientes a gestionar efectivamente el BCP o DRP.
- ✓ Suministrar los programas de capacitación para el BCP o DRP
- ✓ Coordinar, apoyar y hacer seguimiento a la gestión del BCP o DRP en cada área, proceso o sede de PYS.
- ✓ Guiar en el desarrollo de las diferentes etapas del BCP, DRP, BIA y Manejo de las Crisis.

3. Elementos que Conforman la Administración del Plan de Continuidad del Negocio.
La Administración del Plan de continuidad del Negocio está conformada por los siguientes elementos:

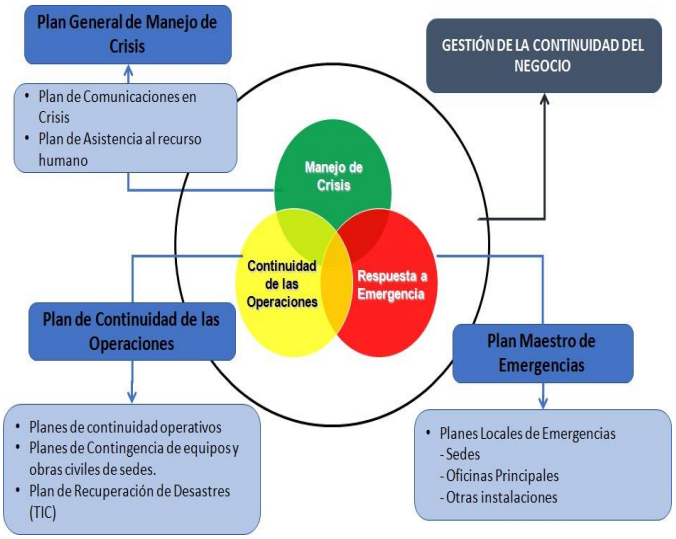
a. Planes de Contingencia de Proceso - BCP, abarcando los escenarios de falta de personal, no disponibilidad del sitio normal de trabajo, falla en los Sistemas de Computo y/o Comunicaciones y no contar con los proveedores críticos del negocio.

b. Planes de Recuperación de Desastres – DRP, el cual contempla las diferentes estrategias definidas para la recuperación de los sistemas y de la Operación en base de mínima Operatividad.

c. Plan de Continuidad del Negocio: Procedimientos y estrategias definidos para asegurar la reanudación oportuna y ordenada de los procesos del negocio, este interrelaciona los planes de BCP, DRP, BIA y Manejo de la Crisis; para ello podemos apreciar la siguiente Fig. 1 en donde se explica mejor la interrelación de estos planes.

d. Capacitación.
En el éxito del Plan de Continuidad es fundamental contar con la participación y el compromiso del personal involucrado en el mismo. La administración de continuidad debe asegurar que todos los funcionarios involucrados reciban capacitación y entrenamiento sobre los procedimientos a seguir en caso de incidentes o desastres, lo cual permite tomar conciencia de la importancia del plan, ya que serán los encargados de ponerlos en funcionamiento en caso de presentarse un evento no deseado. A los jefes de las sedes y a los coordinadores de los procesos, también se les capacitara y concientizara, ya que son los responsables de la correcta ejecución de los planes.
La Oficina de Riesgos (a Crear) suministrara los programas de capacitación, para que sean ofrecidos a todo el personal y dentro de la política de capacitación se contempla suministrar a todos los funcionarios capacitación anual de Plan de Continuidad de Negocios (BCP y DRP).

Fig. 1.
Interrelaciones de los Planes de BCP, DRP y Manejo de Crisis



E. Los Planes para la Continuidad del Negocio en PYS.

1. BIA (*Bussines Impact Analisis*)
El Análisis de Impacto del Negocio (de ahora en adelante se identifica como BIA), es una etapa que permite identificar la urgencia de recuperación de cada área, determinando el impacto en caso de interrupción. Esta actividad conlleva a identificar los procedimientos críticos de la Entidad, los recursos utilizados para soportar las funciones, así como sus proveedores críticos, también determinar los sistemas de Cómputo, de Comunicaciones y de Red críticos y estimar el tiempo que la Empresa puede tolerar en caso de un incidente o desastre.

1.1. Objetivo. El BIA se constituye en el pilar sobre el que se va a construir el Plan de Recuperación de Negocios, es la guía que determina qué necesita ser recuperado y el tiempo requerido para recuperación.

1.2. Alcance. A través del desarrollo del BIA se obtiene la siguiente información:

- ✓ Evaluación de los procedimientos, donde se establece cuáles son primordiales para la continuidad de la Empresa.
- ✓ Determinación de los impactos de una interrupción y cuando empiezan.
- ✓ Priorización y establecimiento del período de tiempo en el que los sistemas, aplicaciones y funciones deben ser recuperados después de una interrupción (RTO).
- ✓ Determinación del orden de recuperación.
- ✓ Establecimiento del tiempo máximo tolerable permitido de pérdida de información ante una interrupción en los sistemas de información (RPO).
- ✓ Definición de los recursos necesarios para el buen desarrollo de los procedimientos a nivel de: Tecnología, personal, infraestructura y soporte proveedores.

1.3. Fases. Para desarrollar la etapa de Análisis de Impacto del Negocio - BIA se ha establecido cumplir con los siguientes pasos:

- ✓ Planeación:
- ✓ Identificación Procesos y Procedimientos.
- ✓ Equipo de Planeación.
- ✓ Metodología.

2. RTO (Tiempo de Recuperación Objetivo).
Con base en la "Encuesta BIA", se puede lograr calcular el tiempo durante el cual un procedimiento puede estar sin operar antes de sufrir impactos considerables para la Empresa. Con base en ello, se fija un Tiempo de Recuperación Objetivo (RTO), que consiste en establecer cuánto tiempo puede permanecer la Empresa sin ejecutar una actividad, el uso de una aplicación o información relevante; que está asociado con el tiempo máximo de inactividad. En consecuencia, la mayoría de las preguntas buscan determinar el tiempo en que se puede impactar la Empresa o los clientes por dejar de realizar el procedimiento ante una interrupción. Como resultado de la evaluación se genera las siguientes valoraciones:

- ✓ Calificación BIA: Indica la sensibilidad en tiempo ante los diferentes impactos analizados por no ejecutarse el procedimiento. Esto se deriva a través de la realización de la "Encuesta BIA".
- ✓ Tiempo Objetivo de Recuperación (RTO): El período de tiempo después de una interrupción, mediante el cual el PYS debe activar sus planes de contingencia y recuperación de las actividades críticas para evitar un impacto significativo.
- ✓ Valor del BIA: Indica la criticidad del procedimiento basado en la Calificación BIA y que impulsa el establecimiento de prioridades de recuperación durante una situación difícil. La tabla de valoración establecida es la siguiente:

Tabla II.
Tabla de Valoración del BIA.

Tabla Valoración del BIA		
Calificación BIA	Tiempo Objetivo de Recuperación (RTO)	Valor del BIA
N - 1AAA	4 Horas	Misión Critica
N - 1AA	8 Horas	Misión Critica
N - 1A	24 Horas	Masivo
Nivel 2	48 Horas	Masivo
Nivel 3	7 días	Medio
Nivel 4	14 días	Medio
Nivel 5	30 días	Bajo
Nivel 6	> 30 días	Insignificante

3. RPO (Punto de Recuperación Objetivo de la información).
El parámetro de Punto de Recuperación Objetivo de la Información determina la periodicidad con la que deben salvaguardarse los datos de los procesos del negocio; cuanto más pequeño sea el RPO más sólido debe ser el mecanismo de protección de datos (Backup, replicación online, etc.).
En la "Encuesta BIA" contiene la pregunta dirigida a establecer el Punto Objetivo de Recuperación (RPO) por procedimiento, la cual permite establecer el apetito de riesgo de pérdida de información ante un incidente tecnológico. Los parámetros de RTO y RPO influyen en la infraestructura de soporte y respaldo que utilice la Empresa.

4. Requerimientos de Infraestructura.
El análisis de los procedimientos está acompañado de la identificación de los requerimientos de personal, recursos y facilidades necesarias para su operación ante un evento de contingencia.
Para ello, se tiene dispuesto la hoja de Cálculo "Requerimientos Tecnológicos" de la "Encuesta BIA", donde el Líder de BCP diligencia la información referente a:

- ✓ Número de colaboradores de tiempo completo para ejecutar el proceso.
- ✓ Recurso humano requerido en contingencia.
- ✓ Aplicativos tecnológicos utilizados en el procedimiento. Con esta información se determina la criticidad de los aplicativos de PYS.
- ✓ Elementos logísticos como son: teléfono, impresora, escáner etc.
- ✓ Otros elementos necesarios en el funcionamiento, como, por ejemplo: Carpeta compartida del área, acceso a los Servidores y Permisos.

5. Análisis de Proveedores Externos.
El BIA identifica la relación del proceso o procedimiento con proveedores externos y en la hoja de cálculo denominada "Información Proveedores" de la "Encuesta BIA" donde se mencionan los proveedores críticos.

6. Aprobación de la Encuesta BIA.
   Cada procedimiento evaluado por la metodología BIA es revisado, analizado y aprobado por el Líder del Proceso y como evidencia se genera el documento "Resultados del Análisis de Impacto de Negocio (BIA)", el cual es firmado por el Líder de Proceso y Líder de BCP del área o proceso.

7. Recopilación de Datos y Documentación de Hallazgos.
   Los resultados de la Evaluación BIA de todos los procedimientos son consolidados por la Oficina de Riesgos. De esta información se producen los siguientes resultados, que deben ser informados al Comité SARO – SI:

   - ✓ Número de procesos y procedimientos evaluados.
   - ✓ Clasificación de los procedimientos por calificación BIA.
   - ✓ Establecimiento de los procedimientos críticos de la Empresa, de acuerdo con la calificación BIA.
   - ✓ Cantidad de recursos humanos requeridos en contingencia: Número de personas que apoyan la contingencia ante una interrupción de las operaciones.
   - ✓ Recursos de Bienes Muebles clasificado por calificación BIA: Se establecen los bienes muebles necesarios en la contingencia, como son: Computadores, teléfonos, escáneres, impresoras y otros elementos necesarios en contingencia.
   - ✓ Dependencia de los proveedores externos en los procesos prioritarios: Definir los proveedores críticos con el fin de involucrarlos en la estrategia de BCP o DRP.
   - ✓ Recursos Tecnológicos: Es necesario suministrar la información de:

     a. Detalle de los aplicativos requeridos.
     b. Establecer el orden de criticidad de los aplicativos.
     c. El punto objetivo de recuperación (RPO).

8. Análisis de Riesgos. En esta etapa se identifican y analizan las posibles amenazas y/o vulnerabilidades de personas, sistemas, infraestructura y procesos que podrían ocasionar riesgos de continuidad para la Empresa, con el fin de medir el nivel del riesgo.

   a. Objetivo.
      La gestión de riesgos de continuidad tiene por función especial reducir la probabilidad de una amenaza potencial o vulnerabilidad y reducir el impacto que puede provocar un evento de desastre o una interrupción significativa en los servicios.
   b. Metodología.
      A continuación, se detalla la Metodología de Análisis de Riesgos, la cual cubre los aspectos relacionados a continuación:

      - ✓ Identificación de riesgos de Continuidad.
      - ✓ Cálculo del riesgo inherente.
      - ✓ Evaluación de controles.
      - ✓ Cálculo del riesgo residual.
      - ✓ Tratamiento del riesgo residual.

9. Identificación del Riesgo.
   El Líder de PCN de cada proceso, área o sede en conjunto con la Oficina de Riesgos procede de la siguiente manera:
   a. Determinar los procesos críticos del área a cargo, resultado que se obtuvo en la etapa de Análisis de Impacto del Negocio (BIA).
   b. Establecer los recursos necesarios para la continuidad de los procedimientos críticos, que también se estimaron en la etapa de Análisis de Impacto del Negocio (BIA).
   c. Describir las posibles amenazas que conlleven a una interrupción en la operación detallando posibles fuentes de peligro, las cuales se deben evaluar identificando si tales situaciones pueden darse en el proceso analizado.
   d. Determinar las vulnerabilidades que tiene el proceso para cada amenaza identificada. Para identificarla es necesario responder esta pregunta: ¿Cómo puede ocurrir una amenaza? Al responderla se definen las distintas situaciones por las que puede ocurrir la misma, evaluando si dentro de PYS puede darse esa circunstancia.
   e. Describir el riesgo contemplando las variables de amenaza y vulnerabilidad.
   f. Enmarcar estas vulnerabilidades en los siguientes factores de la continuidad, de acuerdo a:
      - ✓ Personas.
      - ✓ Infraestructura física.
      - ✓ Infraestructura de tecnología de información.
      - ✓ Procesos.

10. Cálculo de Riesgo Inherente.
    El riesgo de continuidad se evalúa con dos (2) variables de medición, una que expresa el impacto del riesgo si ocurriera y otra que expresa la frecuencia de que el riesgo ocurra.

    - ✓ Frecuencia: Se debe estimar la frecuencia para cada vulnerabilidad del riesgo, según la siguiente escala de medición:
    - ✓ Impacto: El impacto se mide por riesgo y es analizado teniendo en cuenta el nivel de afectación.

    Habiendo valorado tanto el Impacto como la frecuencia del evento de riesgo, los dos puntajes son multiplicados para dar el puntaje de riesgo Inherente. Dado que tanto la Frecuencia como el Impacto son calificados de 1 a 5, el puntaje de riesgo total o inherente es de máximo 25 y el mínimo es 1.

11. Evaluación de los Controles. Este proceso permite evaluar todos los controles asociados a las vulnerabilidades identificadas, garantizando a la Empresa que se apliquen los tipos y niveles adecuados de control para poder dar un adecuado tratamiento al riesgo. Los criterios de evaluación del control son: Oficialidad, Aplicación y Efectividad, a los cuales se les ha asignado un peso de 20, 30 y 50 puntos respectivamente sobre 100.

    - ✓ El criterio de Oficialidad es calificado teniendo en cuenta cuatro (4) variables:
        a. Control no documentado: no aporta valor al total del criterio.
        b. Control documentado: aporta al total del criterio una calificación de 8 puntos.
        c. Control aprobado: aporta al total del criterio una calificación de 8 puntos.
        d. Control divulgado: aporta al total del criterio una calificación de 4 puntos, para un total de 20 puntos.
    - ✓ El segundo criterio es la Aplicación, la cual aporta un total de 30 puntos, siendo necesario seleccionar una de las tres Opciones:
        a. El control nunca se aplica, no aporta valor al total del criterio.
        b. Se aplica a discreción, arroja una calificación de 10.
        c. Se aplica siempre, tiene una calificación de 30.

12. Cálculo del Riesgo Residual. Luego de la valoración de los controles se identifica el efecto de mitigación en frecuencia e impacto del riesgo, para lo cual la Matriz de Riesgo de Continuidad determina el riesgo residual, así:

    - ✓ Ubica el valor del control que se obtuvo sobre la variable de frecuencia en la Tabla "Calificación del Control", estableciendo el efecto de mitigación que indica la columna "Cuadrantes a disminuir en la frecuencia". Este valor se resta a la frecuencia obtenida en riesgo inherente.
    - ✓ De igual manera se procede con los controles dispuestos para disminuir el impacto del riesgo, obtenido el valor del control que se obtuvo sobre la variable de impacto en la Tabla "Calificación del Control", estableciendo el efecto de mitigación que indica la columna "Cuadrantes a disminuir en el impacto". Este valor se resta al impacto obtenido en riesgo inherente.

13. Se multiplica el nuevo valor de frecuencia por el nuevo valor del impacto aplicado los controles, obteniendo así el Riesgo Residual.

14. El Riesgo Residual se ubica en la siguiente Escala de Clasificación del Riesgo:

Tabla III.
Escala del Riesgo.

NIVEL	CLASIFICACIÓN
0-3	Aceptable
4-6	Tolerable
7-15	Grave
16-25	Critico

15. Tratamiento del Riego Residual.
    A partir de la evaluación y análisis de los riesgos, se priorizan de mayor a menor "criticidad", a fin de tomar decisiones de cómo actuar sobre los mismos. Esta metodología pretende actuar sobre los riesgos que estén fuera del rango de aceptabilidad. El tratamiento del riesgo residual debe ir orientado a cualquiera de las siguientes opciones:

    - ✓ Eliminar el riesgo: Cuando se opta por suspender un producto o proceso por una decisión administrativa.
    - ✓ Mitigar el riesgo: Se consigue mediante la optimización de los procedimientos y la implementación de controles tendientes a disminuir la frecuencia de ocurrencia y/o minimizar la severidad de su impacto.
    - ✓ Dispersar o atomizar el riesgo: Se logra mediante la distribución o localización del riesgo en diversos lugares, procesos o personas.
    - ✓ Transferir el riesgo: Actividades y medidas tendientes a transferir a un tercero la responsabilidad por el manejo del riesgo y/o la obligación por las consecuencias financieras del riesgo, en caso de ocurrencia. Esta técnica no reduce la frecuencia ni el impacto, por el contrario, involucra a otro en la responsabilidad. P. e. Pólizas de Seguros, Subcontrataciones.
    - ✓ Asumir el riesgo: Aceptación del riesgo en razón a que los retornos potenciales son atractivos en relación con los riesgos involucrados.

    Para los riesgos que en su calificación residual se clasifiquen como graves o críticos, el Líder del Proceso debe establecer planes de acción que busquen reducir la exposición de la Empresa a través de la creación de nuevos controles o la implementación de modificaciones a los controles existentes. A dichos planes se les hará seguimiento de forma trimestral, y se reportará su avance al Comité SARO-SI, con el fin de tomar las decisiones respectivas para su tratamiento y mitigación.
    Los riesgos clasificados como aceptables y tolerables deben ser evaluados continuamente por los Líderes de Riesgo, garantizando la eficacia de los controles. Si se percibe un incremento en el nivel del riesgo debe ser informado inmediatamente a la Oficina de Riesgos, con el fin de realizar la respectiva reclasificación y acordar acciones.

16. Monitoreo al Mapa de Riesgos de Continuidad.
    Se realiza seguimiento a los riesgos y la efectividad de los controles y planes de acción para determinar el nivel de exposición frente al aspecto de disponibilidad de los elementos que se requieren para la continuidad del negocio.
    El Líder de BCP efectúa seguimiento permanente sobre la implementación de los planes de acción y la verificación de la efectividad de los controles y a la vez identificando nuevos riesgos. Adicionalmente, se realiza monitoreo con frecuencia semestral por parte del Líder de BCP de cada una de las áreas con apoyo de la Oficina de Riesgos y éste es aprobado por el Líder del Proceso. Este monitoreo se realiza en la Matriz de Riesgo de BCP. Dentro del monitoreo, la Oficina de Riesgos debe proponer al Comité SARO-SI las medidas relativas al perfil de riesgo residual, teniendo en cuenta el nivel de tolerancia al riesgo fijado por PYS.

17. Reporte de Incidentes de Continuidad.
    Los incidentes que afecten la continuidad de la operación deben ser reportados por los Líderes de BCP a la Oficina de Riesgos, a través de un formato de "Reportes de Incidentes", dentro de los tres (3) días hábiles siguientes a la ocurrencia del hecho.

18. Plan de Continuidad del Negocio (BCP).
    Este escenario hará referencia a la creación de un plan de continuidad del negocio (o sus siglas en inglés BCP, (por *Business Continuity Plan*), que será un plan logístico para la práctica de se debe recuperar y restaurar las funciones críticas parcial o totalmente interrumpidas dentro de un tiempo predeterminado después de una interrupción no deseada.
    En lenguaje sencillo, un BCP es: el cómo la organización se prepara para futuros incidentes que puedan poner la Empresa en peligro y a su operación a corto y mediano plazo. Las situaciones posibles que analizaremos incluyen desde incidentes locales (como incendios, terremotos, inundaciones, tsunamis etc.), hasta incidentes de carácter regional, nacional o internacional.
    Inicialmente las actividades de planificación y prevención estarán dirigidas hacia las operaciones de TI, que están centralizadas en el Departamento de TIC y su lugar físico concreto primario y de existir el alterno. Para desarrollar el plan de BCP, definiremos la respuesta prevista por el Negocio ante aquellas situaciones de riesgo que le pueden afectar de forma crítica, es decir, impidiendo la operación tecnológica que soporta los procesos de negocio más importantes, porque ya que tarde o temprano se presentará una incidencia de seguridad o algún evento que detenga súbitamente la operación de una empresa. Lo primero que se debe realizar es un análisis del impacto al negocio (BIA). Éste es básicamente un informe que nos muestra el coste ocasionado por la interrupción de los procesos críticos de negocio.
    Una vez obtenido este informe, la Empresa tiene la capacidad de clasificar los procesos de negocio en función de su criticidad y lo que es más importante: establecer la prioridad de recuperación (o su orden secuencial). Los componentes a desarrollar para el BCP son:

    - ✓ Personal requerido.
    - ✓ Áreas de trabajo.
    - ✓ Registros vitales - Backup's de información.
    - ✓ Aplicativos críticos.
    - ✓ Dependencias de otras áreas.
    - ✓ Dependencias de terceras partes.
    - ✓ Criticidad de los recursos de información
    - ✓ Participación del personal de seguridad informática y los usuarios finales.
    - ✓ Análisis de todos los tipos de recursos de información.

    La estrategia para el BCP será una combinación de medidas preventivas y correctivas para:

    - ✓ Eliminar la amenaza completamente.
    - ✓ Minimizar la probabilidad de que ocurra.
    - ✓ Minimizar el efecto.

    Las interrupciones más prolongadas y más costosas y en particular los desastres que afectan a las instalaciones, requieren recuperación por DRP y no por BCP.

19. Plan de Recuperación del Desastre (DRP).
    A diferencia de BCP, el DRP hace referencia de un desastre total y mayor que afecta al negocio. El plan de recuperación ante desastres (del inglés *Disaster Recovery Plan*) es un proceso de recuperación que cubre los datos, el hardware y el software crítico, las comunicaciones y los recursos humanos, para que la Empresa pueda comenzar de nuevo sus operaciones desde 0, en caso de un desastre natural o causado por humanos. Esto incluirá proyectos para enfrentarse a la pérdida inesperada o repentina de personal clave, el propósito primario es la protección y recuperación de datos que soportan el proceso productivo de la organización.
    Existen diferentes riesgos que pueden impactar negativamente las operaciones normales de una organización. Efectuaremos una evaluación de riesgo para ser realizada y ver qué constituye el desastre y a qué riesgos es susceptible la Empresa específicamente, incluyendo:

    - ✓ Catástrofes Naturales o Humanas.
    - ✓ Fuego.
    - ✓ Fallos en el suministro eléctrico, totales o por encima de la tolerancia especificada.
    - ✓ Ataques terroristas.
    - ✓ Ciberataques.
    - ✓ Interrupciones organizadas o deliberadas.
    - ✓ Sistema y/o fallos de TIC.
    - ✓ Error humano crítico.
    - ✓ Virus, amenazas y ataques informáticos.
    - ✓ Cuestiones legales. (sellamientos)
    - ✓ Huelgas de empleados.
    - ✓ Conmoción social o disturbios.
    - ✓ Pandemias Mayores.

20. Plan de Gestión de Crisis.
El Plan de Gestión de Crisis que se va a generar va a manejar, administrar o gestionar un evento de crisis, por el cual se va a generar el proceso mediante el cual la Empresa enfrentará un acontecimiento de importancia que podría generar daño a la organización, sus *Stakeholders*, o al público en general. Como antecedente, el estudio de gestión de crisis nació con los desastres industriales y medioambientales de gran escala de la década de 1980. El Plan de Gestión de Crisis es considerado como el proceso más importante dentro de las relaciones públicas de la Empresa, tres elementos son comunes en una crisis los cuales analizaremos en nuestro Plan:

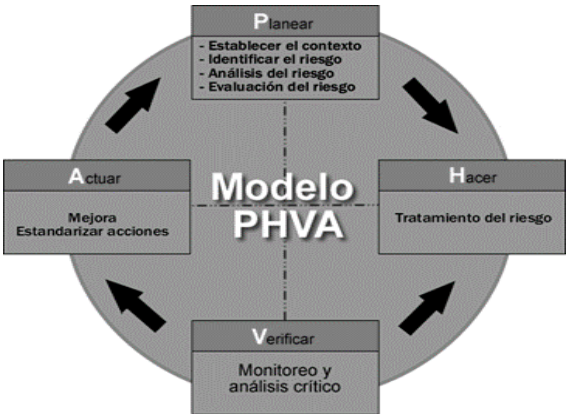
- ✓ Una amenaza a la organización.
- ✓ El elemento de sorpresa.
- ✓ Un corto tiempo de decisión.

La cuarta característica que se analizara es la necesidad de cambio. Si el cambio no es necesario, el acontecimiento podría ser descrito más bien como un fracaso.
A diferencia de la gestión de riesgos, que implica evaluar potenciales amenazas y encontrar las mejores formas de evitar dichas amenazas, el manejo de crisis implica lidiar con amenazas antes, durante, y después de que éstas han ocurrido. Presentaremos un plan como una actividad que, dentro del contexto más amplio de la administración, consistirá en definir las habilidades y técnicas requeridas para identificar, evaluar, entender y soportar una situación de crisis, especialmente desde el primer momento en que ocurre al punto donde se inician los procedimientos de recuperación.

21. Ciclo PHVA para el Manejo del Riesgo.
También conocido como el ciclo de la mejora continua, es una metodología que describe los cuatro pasos esenciales que se deben llevar a cabo de forma sistemática, para lograr la mejora continua, tal y como se observa en la siguiente figura, entendiendo al mejoramiento continuado como la disminución de fallos, el aumento de la eficacia y eficiencia, la solución de problemas, la previsión y eliminación de riesgos potenciales.
Los pasos propuestos en este ciclo PHVA para la gestión de riesgos son las siguientes:

- ✓ Planificar: Es el punto de partida del ciclo, que se debe construir a partir de una línea de base, sobre la cual se van a establecer objetivos de mejora claros, junto con los parámetros de medición que se van a utilizar para gestionar los riesgos.
- ✓ Hacer: Posterior a la planificación se procede con la ejecución de las acciones necesarias para lograr los objetivos propuestos.
- ✓ Verificar: Todo lo que se hace, es susceptible de ser mejorado. Sin embargo, para lograrlo se debe contar con cifras que nos permitan medir y valorar la efectividad de los cambios implementados.
- ✓ Actuar: En este punto se deben tomar las decisiones y desarrollar las acciones necesarias para corregir las desviaciones encontradas en la verificación, esto con el propósito de mejorar continuamente y minimizar los riesgos.

Fig. 2.
Modelo Ciclo PHVA



Ya que los riesgos de pérdida de información, son un tema que representa mayor vulnerabilidad en las Empresas, ellas se concentran cada vez más en identificarlos y gestionarlos. La capacidad de minimizar la ocurrencia de hechos que vulneren la seguridad y reaccionar oportunamente ante intromisiones indeseables, ayudará a las organizaciones a desarrollar las funciones para las cuales fueron creadas, generando mayor confianza entre sus colaboradores, los clientes y el público.
Para PYS es un tema sensible poder desarrollar un adecuado plan de manejo del Riesgo, asegurando la mejor estrategia que logre en lo más profundo simplemente disminuir las pérdidas económicas, y evitar las afectaciones a los colaboradores.

22. Capacitación a los Colaboradores de PYS.
En el éxito del Plan de Continuidad es fundamental contar con la participación y el compromiso del personal involucrado en el mismo. La administración de continuidad debe asegurar que todos los colaboradores involucrados reciban entrenamiento sobre los procedimientos a seguir en caso de incidentes o desastres, lo cual permite tomar conciencia de la importancia del plan, ya que serán los encargados de ponerlos en funcionamiento en caso de presentarse un evento no deseado. A los jefes de las áreas también se les capacita y concientiza, ya que son los responsables de la correcta ejecución de los planes. La Oficina de Riesgos suministra los programas de capacitación, para que sean ofrecidos a todo el personal a través de la Secretaria General Grupo de Talento Humano. Dentro de la política de capacitación incluida en SGC, se contempla suministrar a todos los funcionarios capacitación anual de Plan de Continuidad de Negocios.

23. Pruebas de los Planes de Continuidad del Negocio.
Las pruebas de los planes de BCP, DRP se deben efectuar concienzudamente acogiendo las características de los escenarios a probar que serán los más críticos y los más dañinos y perjudiciales al negocio y se pueden o no efectuar con el Plan de Manejo de Crisis.
Las pruebas se van a efectuar conjuntamente con los funcionarios identificados como críticos, primarios y necesarios junto con sus reemplazos (en caso de que el primario no pueda estar presente) con la supervisión del Comité SARO-SI y la Oficina de Riesgos con el apoyo de las áreas y procesos que soportan la operación en este caso TIC y las otras áreas Operativas del Negocio

24. Tipo de Pruebas.
En la siguiente gráfica se ilustra la metodología que se debe utilizar para la realización de las pruebas del plan de continuidad de negocio proyectado para PYS.

Tabla 4.
Metodología de Pruebas.

TIPO DE PRUEBA	TECNICA UTILIZADA	OPERACIÓN
Integrada	• Creación de un escenario • Seguimiento en vivo de todas las estrategias re recuperación • Con previo aviso. • Apoyo de los proveedores de recuperación	Prueba integrada con todos los elementos que hacen parte del plan de contingencia.
Componentes	• Creación de un escenario • Seguimiento de las estrategias de recuperación • Con previo aviso.	Se ejecutan las estrategias y procedimientos de recuperación de cada uno de los componentes de la infraestructura tecnológica.
Escritorio	• Con previo aviso. • Creación de un escenario.	Se realiza un ejercicio de papel de un escenario de desastre que toma lugar en un salón de conferencia.

25. Plan de Pruebas para PYS.
Para la realización de una Prueba de Estrategia de Continuidad es necesario diligenciar el documento "Plan de Pruebas", conformado por los siguientes pasos:

- ✓ Guion de pruebas: Es el documento mediante el cual se plasma la intención de efectuar la revisión de la estrategia de continuidad estimada para el proceso o servicio determinado, donde se relacionan aspectos de: Objetivo y alcance de la misma, el escenario de interrupción, los resultados esperados, los integrantes de las pruebas y los riesgos asociados a la ejecución de la prueba. Este documento debe desarrollarlo previo a la ejecución de la prueba el presidente del BCP o DRP, y él es responsable del proceso a probar con la ejecución del funcionario encargado del proceso y la supervisión de la Oficina De Riesgos.
- ✓ Paso a paso de la planeación: Este documento relaciona las actividades a efectuar durante la prueba, indicando además los responsables de realizar tales actividades, así como los recursos mínimos necesarios y los tiempos de su realización, para la estimación completa del tiempo de la prueba. Adicional, se deben mencionar los aspectos adicionales que son necesarios para la adecuada realización de la prueba. Al igual que en el anterior ítem, este informe debe ser adelantado previo a la ejecución de la prueba por el Líder del BCP o DRP, responsable del proceso a probar con la ejecución del funcionario encargado y la supervisión de la Oficina de Riesgos.
- ✓ Paso a paso de la ejecución: Este documento contiene las actividades realizadas en el desarrollo de la prueba, que deben ser semejantes a las planeadas a menos que se presenten algún incidente dentro de la prueba. Adicionalmente, se describen los recursos mínimos necesarios, los responsables y los tiempos de ejecución de las actividades. Este informe es elaborado en el momento de la prueba por el Líder de BCP o DRP responsable del proceso a probar con la colaboración del funcionario encargado del proceso.
- ✓ Paso a paso del retorno: En este reporte se relacionan las actividades que se ejecutan para retornar a la operación normal, caso devolución a los puestos de trabajo, captura de las operaciones que no se procesaron en un aplicativo, entre otras.
- ✓ Encuesta de satisfacción: Este informe lo realizan diferentes integrantes de la prueba, donde se busca determinar el grado de satisfacción de la prueba. La conforman aspectos como: duración de la prueba, preparación de la prueba y la comunicación de la misma, y dificultades que se identificaron.

IV. RELACIONES ENTRE LA DATA, LA CONTINUDAD DEL NEGOCIO Y LA GERENCIA

Procesos y Servicios es una Empresa PYME que tiene unas circunstancias que no tienen ni siquiera las grandes empresas, los contratos con los clientes, los ANS´s firmados conexos con los contratos y la necesidad de la operación de mantener una Data (Bases de Datos e Imágenes) es una mezcla que posee unas singularidades, que como "gato caminando entre vidrios" ha logrado superar la Gerencia y el área de TIC. Entremos a detallar esas singularidades de la siguiente forma:

A. Data.

Para PYS, las imágenes que se han procesado para los clientes, tienen un peso aproximado de 12 TB, de las cuales 10 TB están en servidores en la Nube, y los otros 2 TB están en servidores locales los cuales conforman el proceso Operativo de los tres (03) meses vigentes que son el "Día a Día" de la operación.

En cuanto a las Bases de Datos, están todas en las plataformas SQL, MySQL, y Mongodv (Base de Datos No Relacional) y tienen un peso aproximado de 1 TB. Ahora, teniendo en cuenta lo anterior estamos confirmando que el peso total de la Data es

de 13 TB, lo cual es un verdadero reto técnico para los procesos de Backup, por el peso de esa información, para el área de TIC. Los procesos de Backup, de la Data que se encuentra en la nube están tercerizados con los proveedores de las plataformas que usan PYS, MS *Azure* y *GoDDady*, pero incluso transfiriendo el riesgo de los procesos de Backup, PYS en situaciones de indisponibilidad de los servidores puntualmente en *GoDDady* no han podido recuperar las máquinas virtuales en la nube en donde estaba alojada información de más de 8 TB, con consecuencias nefastas para el negocio por la pérdida de la información que no pudieron recuperar en *GoDDady*.

B. La Continuidad del Negocio.

En PYS los procesos de BCP, DRP, BIA y Manejo de Crisis, son planes que están por crear, a la fecha existen procesos de Backup en los Servidores Locales, basados en Tareas Programadas que aseguran los 3 TB, de la Data activa de los últimos tres (03) veces, y una parte de tres (03) TB aproximadamente de la Data Histórica (de más de tres (03) meses atrás), en Discos Duros USB Externos, y aunque este proceso es básico y asegura la copia de la información es sumamente lento dado el peso de la información, junto con la velocidad de Lectura/Escritura de los D.D. USB Externos; de forma que actualmente estos procesos de Backup, están demorando cuatro (04) horas aproximadamente todos los días. Fuera de la demora en los procesos de Backup, se debe sumar el hecho de que al ejecutar el proceso de Backup por medio de la Tarea Programada diaria, el *Performance* del Servidor se deteriora muchísimo, a pesar de que el proceso se lanza a las 2:00 AM, mientras se ejecutan los usuarios (PYS trabaja 7x24x364) no tienen otra alternativa que resignarse a la velocidad que el Servidor puede proveer, y a costa de la perdida de rendimiento en los procesos que los usuarios ejecutan en el Servidor.

C. La Gerencia.

Vamos a partir que los Gerentes de PYS son Ingenieros De Sistemas, de forma que el manejo de los procesos de Backup para ninguno es desconocido o la importancia de los mismos, sin embargo, en el análisis de Costo/Beneficio el costo de ejecutar procesos de Backup local, más rápidos o mejorados supera el Beneficio para PYS. El costo que paga PYS a las plataformas Web es bastante significativo y como ya se evidencio a la hora de tener que recurrir al Backup, no fue posible, claramente por responsabilidad total del administrador de la plataforma web, en este caso puntual *GoDDady*, pero el punto es que la excusa del proveedor fue que no se pudo recuperar la información porque los proceso de Backup, implementados por *GoDDady* son incrementales y por lo pesado de la información el proceso de recuperación del Servidor falló y simplemente no se pudo recuperar el Servidor. Esta situación crítica fue ampliamente debatida con la Gerencia, Calidad, la Operación y el área de TIC, y a pesar de la culpabilidad del proveedor, por ese hecho se tomó la decisión de cambiar y migrar todo de *GoDDady* a MS Azure, ahí se evidenció una alta vulnerabilidad, en los procesos de Backup por el peso de la información que se debe resguardar para los clientes y cumplir con los contratos y los ANS´s firmados.

A hoy, el que un proveedor haya incumplido en una situación de crisis (como ya ocurrió), y a pesar de las medidas de mitigación que se tomaron las pérdidas reputacionales con los clientes y las pérdidas de uso de los colaboradores no se han podido cuantificar.

D. La Gerencia + La Data + PCN

Una vez observado los aspectos que se relacionan en este documento y los pormenores que se tienen para PYS, es cuando entraremos a analizar lo que pasa en este punto donde se interrelacionan todos los ítems. Se da por descontado la mejor intención de la Gerencia, de los Colaboradores, del área de TIC y de los proveedores, dicho lo anterior, analizaremos el punto crítico, los Backup´s. Es claro que el peso de la información de consulta que llega a los 12 TB junto con el manejo de la información del día a día que suma semanalmente un 200 GB, en Data, se suma a las condiciones especiales de la Empresa. La Empresa ha analizado le mejor forma de hacer las copias de seguridad, e incluso se ha transferido el riesgo tomando los procesos de Backup con los terreros en donde está alojada la información en la Web, mirando el contexto, si la información pesa 12 TB, quiere decir que el Backup inicial pesa 12 TB, y aunque es información de consulta lo que significa que los incrementales son muy pequeños, la Data de los procesos diarios son muy grandes, 200 GB semanales es un volumen de información pesado, y el manejo de ella, que incluye mantenerla en los Servidores locales y luego migrarla a la Nube, hace que traslimitar esa información alcanza a saturar el canal de Internet de PYS, y es por ello que los procesos de envío se hacen a la madrugada, pero los usuarios se deben someter al bajo *performance* que se origina por el proceso de copia de la información del ambiente local a la nube. Ese proceso se hace semanalmente por lo que el aumento de la Data en la Nube también se amplía de forma equivalente y genera que las copias se deban actualizar para asegurar esa Data.

El proceso de Backup, es crítico como es claro para cualquier empresa, el análisis del costo / beneficio de mantener las copias, de generarlas de trasmitirlas y de tener la Data disponible para consulta tanto de los usuarios de los clientes como de los colaboradores de PYS, siempre está enmarcada en la pérdida operativa, porque es información histórica de consulta, no de producción actual. Dada las condiciones actuales, la Gerencia y el área de TIC han definido que la mejor forma de mantener un Backup económicamente viable, es alojar esa Data en Discos Duros USB en un servidor Local, y luego almacenar los Discos Duros en una Discoteca de al menos unos 25 Discos en donde está la copia de la Data de varios clientes, este proceso es la forma básica de copias, y la administración acepta pagar la constante compra de los Discos Duros para ese propósito.

En los comités de Gerencia se han analizado varias alternativas para generar las copias de seguridad y el mejor sitio para almacenarlas, encontrando que, desde el punto de vista de la disponibilidad y el valor de mantener copias de la Data histórica, el proceso actual en Discos Duros externos, es el de menor costo, y se logra cumplir con los contratos y los ANS´s de la disponibilidad de la Data histórica. Ahora, un tema a tener en cuenta es el hecho de sostener la Data histórica en ambiente Web; para los clientes se ha convertido en un “Plus” corporativo, utilizar ambientes en la nube, lo que inclina la decisión a la hora de renovar o generar nuevos contratos y esa

es la base por la cual la Gerencia ha sostenido el esquema de Copias y de disponibilidad de la Data, como está ahora, razones que a pesar de que no cumplen algunas normas, si representan un apalancamiento comercial. Dicho todo lo anterior, no queda más que esperar que la forma de hacer los Backup´s se pueda cambiar de alguna manera con nuevas tecnologías, o nuevos procesos operativos, o que la normatividad cambie para que el peso de la Data pueda disminuir, o que la Gerencia analice alternativas para cambiar los contratos y los ANS´s para disminuir la Data de los clientes, y hacer una reingeniería de los Servicios locales de los Servidores, del canal de internet y de las redes LAN de PYS para que se pueda optimizar el *performance* de la plataforma cuando se hacen los procesos de Backup y de migración de la Data a la Web.

REFERENCIAS

[1] Ministerio de TIC Colombia, Guía de gestión de riesgos, Bogotá, 2016
[2] I. 27005, Tecnología de la información. Técnicas de seguridad. Gestión del riesgo de seguridad de la información.
[3] ICONTEC, NTC-ISO/IEC 27001, 2013.
[4] I. ITIL, *Information Technology Infrastructure Library.*
[5] N. G. 73, Gestión del riesgo. Vocabulario.
[6] I. 31010, Gestión del riesgo. técnicas para el proceso de evaluación del riesgo.
[7] I. 31000, Gestión del riesgo. Principios y directrices.
[8] H. Villamil, Gestión de la Seguridad de la Información, 2016.
[9] Manual de Administración del Plan de Continuidad del negocio, ICETEX, Versión 1, 2013.
[10] SGSI, Blog especializado en Sistemas de Gestión de Seguridad de la Información, 2018.
[11] Conservación de Documentos. MinHacienda 1999,https://www.superfinanciera.gov.co/jsp/Publicaciones/publicaciones/loadContenidoPublicacion/id/18362/dPrint/1/c/00

Autor

Orlando Esteban Lemaitre Vargas, graduado en Ingeniería de Sistemas en la Universidad E.C.C.I, Bogotá D.C., Colombia, en el 2016 y candidato a Especialista en Seguridad Informática en la Universidad Piloto de Colombia.