RECOMENDACIONES PRÁCTICAS DURANTE LA ACTIVACIÓN DEL BCP

Suescún Méndez Hollman Andrés
hollmanand@hotmail.com
Universidad Piloto de Colombia

Abstract- **The implementation of a Business Continuity Plan is a complex challenge for organizations that support their day to day operations on technical platforms. Companies are urged to put in place strong and sustainable processes to mitigate risk in the event of natural disasters, cyber-attacks and accidental or intentional interruption of the service. In return, said strategies establish the guidelines for a quick recovery of business operations, reducing the risk to both reputation and finances. Additionally, BCP drills help identify gaps in processes, additional system configurations or even the need to acquire extra technology resources. This can include training as well as change management. This exercise further allows the business to mitigate the risks associated with technical interruptions of the service. However, in some instances during this BCP exercise, unforeseen technical issues may arise. Those issues will be analyzed by the undersigned expert and identified in this article.**

***Resumen*— La implementación de un Programa de Gestión de Continuidad del Negocio es un reto complejo para las organizaciones que sustentan sus procesos corporativos sobre infraestructuras tecnológicas. La gran importancia de mantener sus operaciones durante un evento de desastre natural, ataque cibernético o interrupción accidental o intencional de un servicio tecnológico obliga a las organizaciones a establecer estrategias para mitigar los riesgos asociados a tales circunstancias, dichas estrategias, a su vez, establecen las pautas para el diseño de los procedimientos que permiten la reanudación oportuna y ordenada de los servicios tecnológicos de vital importancia para el negocio, con un mínimo impacto económico o reputacional. De esta forma un ejercicio dedicado de identificación de necesidades del negocio, análisis de riesgos, adquisición y configuración de recursos tecnológicos, capacitación y concientización del personal permiten transferir, evadir, reducir o aceptar los efectos negativos, riesgos y consecuencias derivados de una interrupción de las operaciones. Sin embargo, en algunas ocasiones, durante las pruebas de continuidad o incluso durante los procedimientos de contingencia correctamente establecidos surgen problemas técnicos derivados de riesgos no contemplados que, de acuerdo a la experiencia del suscrito, serán identificados en el presente artículo.**

***Índice de Términos*—Acuerdos de Nivel de Servicio, análisis de impacto del negocio, comité de crisis, condiciones normales de operación, líder de continuidad, housing, máximo tiempo de caída tolerable, plan de continuidad del negocio, plan de recuperación de desastres, punto de recuperación objetivo, recursos necesarios para le recuperación de operaciones, sistema de gestión de la seguridad de la información, tiempo de recuperación objetivo.**

I. INTRODUCCIÓN

Es responsabilidad del líder de continuidad del negocio determinar el escenario de desastre de acuerdo con la información por él recolectada luego de la ocurrencia de un evento catastrófico para inmediatamente presentar un informe al comité de crisis con el fin de determinar cuál será el plan de contingencia que se debe activar para superar la crisis. El Análisis de Impacto del Negocio (BIA) contiene los protocolos de comunicación requeridos para que los diferentes especialistas que tienen asignadas responsabilidades dentro del Plan de Continuidad del Negocio (BCP) entren en acción de acuerdo a los procedimientos de contingencia y emergencia establecidos. El Plan de Recuperación de Desastres (DRP) entra en acción mediante la ejecución de los planes de contingencia, diseñados y probados por los propietarios de los activos afectados, momento en el cual, pueden surgir ciertos imprevistos que el autor ha identificado a partir de la experiencia práctica adquirida durante la activación y ejecución de pruebas de continuidad de los procesos corporativos y servicios tecnológicos. Identificar y proponer alternativas de mitigación de los riesgos asociados con los imprevistos anteriormente citados y que pasan inadvertidos a los equipos de respuesta y recuperación de operaciones por la falta de experiencia y experticia técnica y operativa de quienes evalúan y elaboran los planes de recuperación de desastres se convierte en el eje central del presente artículo.

Durante los ejercicios programados de pruebas de los BCP se debe evaluar la eficacia y eficiencia de los procedimientos técnicos de restauración y las tareas de aseguramiento del recurso humano y físico de las compañías durante un evento catastrófico o contingencia técnica de los servicios tecnológicos que soportan los procesos core del negocio, para tal fin, generalmente, se utilizan ambientes tecnológicos mixtos de pruebas y desarrollo que aunque sean idénticos a los ambientes productivos en cuanto a hardware y software no permiten reproducir las condiciones técnicas y de operación de los ambientes productivos ya que generalmente no se contemplan circunstancias relacionadas con el personal quienes pueden sufrir afectaciones físicas o mentales, verse afectados por el simple hecho de transportarse entre diferentes sitios de operación o inclusive cuando se produzcan pérdidas

humanas, condiciones muy diferentes a las presentes durante pruebas programadas de los planes de continuidad.

Una vez un evento de consecuencias para una organización ocurre, se generan múltiples incidentes que producen incertidumbre entre los especialistas encargados de poner en marcha los planes generales de manejo de crisis, el plan maestro de emergencia y los planes de continuidad de las operaciones, el objetivo del grupo de es mitigar la incertidumbre generada mediante el uso de los procedimientos de contingencia, emergencia, comunicaciones y asistencia al recurso humano preestablecidos de acuerdo a las capacidades y experiencia de los líderes de continuidad del negocio. Muchos son los recursos teóricos disponibles para elaborar planes de continuidad del negocio que se ajusten a las necesidades de las empresas, sin embargo, al ser eventos inesperados, probabilísticos y de consecuencias catastróficas sobre los activos tecnológicos y físicos, ocasionan altos niveles de incertidumbre que solo la experiencia de los funcionarios que participan en su activación puede llegar a solucionar mediante la principal cualidad que pueden la experiencia desarrollar, la resiliencia.

En los siguientes apartados se expondrán imprevistos que pueden presentarse durante el despliegue de un DRP al igual que las guías prácticas para asegurar el cumplimiento del MTD, RTO y RPO, contemplando los principales sucesos que la teoría presenta de manera general y que la práctica puede ilustrar detalladamente.

II. ESCENARIOS DE DESASTRE

La identificación del escenario de desastre le permite al comité de crisis establecer el plan de continuidad o contingencia que se requiere desplegar, de la misma manera que los procedimientos técnicos y recursos humanos que intervendrán en la respuesta esperada. A continuación, se describirán los posibles escenarios de desastre, así como los controles tomados de la norma ISO 27001 que permiten mitigar los principales riesgos asociados a ellos para posteriormente identificar los imprevistos que comúnmente se presentan independientes de la calidad de los planes de continuidad.

A. Escenarios que afectan el plan de contingencia técnica.

Las indisponibilidades se presentan por fallos en las soluciones de alta disponibilidad del hardware que soporta los sistemas de información, deficientes procedimientos de control de cambios durante pasos a producción en las aplicaciones, planes de mantenimiento deficientes o inexistentes, procedimientos de gestión de capacidad y disponibilidad de la infraestructura inadecuados, inseguridad en el cableado estructurado, falta de seguimiento y revisión de los servicios brindados por terceros e inclusive sobre carga laboral y deficientes procesos de contratación del recurso humano que cumplen tareas de administración tecnológica. El principal mecanismo para evadir los riesgos asociados con este escenario es la implementación de un conjunto de controles alineados con el BCP y SGSI de la organización, los cuales deben ser debidamente documentados y monitoreados para verificar su implementación. A continuación se listan los controles tomados de la ISO/IEC 27002:2013 [1] que, de acuerdo con la experiencia, permiten disminuir la posibilidad de ocurrencia de activación del plan de contingencia técnica.

1) *Uso aceptable de los activos*: Se deben identificar los activos tecnológicos documentando e implementando reglas para el uso aceptable activos e instalaciones de procesamiento de información.

2) *Medios removibles:* Se deben implementar procedimientos para la gestión de medios removibles con el fin de que estén disponibles en caso de requerir restauraciones de datos.

3) *Derechos de acceso:* Se debe restringir y controlar la continua asignación y uso de derechos de acceso privilegiado, para prevenir daños por falta de experticia técnica.

4) *Suministro eléctrico:* Los equipos se deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.

5) Seguridad en el cableado: El cableado eléctrico y de comunicaciones que brinda soporte a los sistemas de información se debe proteger contra interceptación, interferencia o daño.

6) Operaciones: Los procedimientos de operación se deben documentar y poner a disposición de los usuarios que los necesiten.

7) *Control de cambios:* Se deben controlar los cambios en los sistemas de información e infraestructura que soportan los procesos del negocio.

8) *Gestión de la capacidad:* Se debe realizar gestión de capacidad para asegurar el desempeño requerido de los sistemas.

9) *Programas de mantenimiento:* Ejecución de programas de mantenimiento preventivo durante ventanas programadas de servicio.

10) *Políticas de respaldo:* Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas y

realizar pruebas de restauración de los mismos de acuerdo con una política preestablecida.

11) *Ambientes de pruebas y desarrollo:* Cuando se realizan cambios en las plataformas de operación que afecten aplicaciones críticas del negocio se deben realizar en ambientes de pruebas y desarrollo para no afectar ambientes productivos.

12) *Seguimiento a proveedores:* Los supervisores de contratos deben hacer seguimiento, revisión y auditoría a la prestación de servicios por parte de proveedores o terceras partes.

13) *Alta disponibilidad:* Se deben implementar mecanismos de alta disponibilidad para cada uno de los componentes de hardware que soportan sistemas de información.

Todos y cada uno de estos controles deben estar debidamente implementados y probados tanto en la plataforma de hardware productiva como en la plataforma de hardware destinada a soportar los ambientes de contingencia, con el fin de cumplir satisfactoriamente los máximos tiempos de caída tolerables por los procesos del negocio (MTD) así como los puntos de restauración objetivo (RPO).

B. Escenarios de Activación del Plan de Recuperación de Desastres.

La característica primordial de este escenario es la prolongada indisponibilidad de servicios tecnológicos. Generalmente la responsabilidad de restaurar los servicios tecnológicos afectados es compartida entre miembros de la organización y un proveedor de servicios externo. Las causas más comunes para la activación de DRP son cortes en los canales de comunicación con el centro de datos principal, pérdida de las propiedades de operación en el mismo por fallas ambientales, eléctricas, de comunicaciones u operativas y la ocurrencia de eventos imprevistos que ocasionen que los funcionarios de la compañía no puedan laborar en las instalaciones u oficinas corporativas. Dentro de esta categoría igualmente se pueden clasificar los ciberataques. Los principales controles que permiten evadir los riesgos asociados a este escenario son:

1) *Redundancia en comunicaciones:* Los canales de datos redundantes deben ser contratados con distintos proveedores, las acometidas de los medios físicos de transmisión deben utilizar diferentes rutas de acceso a los edificios.

2) Certificaciones de los centros de datos: La contratación de centros de datos con nivel TIER4 asegura que todas sus condiciones ambientales de operación están perfectamente diseñadas con los mecanismos de redundancia, mantenimiento y administración más idóneos. Las edificaciones certificadas bajo esta denominación, cumplen con los requisitos de sismo resistencia y ubicación pertinentes.

3) *Control de acceso físico:* Las áreas de almacenamiento y procesamiento de datos, al igual que las oficinas donde laboran los empleados de una organización se deben proteger mediante controles de acceso adecuados para asegurar que solo se permita el acceso a personal autorizado.

4) *Firewall, IDS e IPS:* Se deben implementar controles de detección, de prevención y de recuperación contra códigos maliciosos o ataques de denegación de servicio. Los sistemas de detección y prevención de intrusos implementados dentro de una solución de firewall perimetral son la principal recomendación.

5) *Planes de capacitación:* Todos los usuarios de la red de datos de la organización, deben tomar conciencia de las consecuencias que puede acarrear la indisponibilidad de servicios tecnológicos a causa de la ejecución de códigos maliciosos. Las organizaciones están en la obligación de capacitar a sus empleados en aspectos referentes a la seguridad de la información.

7) *Gestión de vulnerabilidades:* Se deben identificar y tratar las vulnerabilidades técnicas mediante la ejecución de técnicas que permitan determinar el grado de exposición de la organización a estas vulnerabilidades y tomar las medidas pertinentes para tratar el riesgo asociado. Se recomienda que el análisis de vulnerabilidades sea contratado con proveedores externos especializados.

8) *Acuerdos de nivel de servicio:* Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red e incluirlos en los acuerdos de nivel de servicio, ya sea que los servicios se presten internamente o se contraten con proveedores externos.

9) *Matriz de responsabilidades ante incidentes:* Se deben establecer responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes que generen afectación de los servicios tecnológicos.

10) *Centros de Datos alternos:* Se deben implementar centros de datos con el nivel de redundancia necesario para responder a desastres. Se recomienda que la ubicación de los centros de datos alternos evite afectaciones relacionadas con pérdidas de conectividad en los centros de datos principales.

11) *Auditorías y planes de mejora:* La organización debe verificar a intervalos regulares los controles de continuidad

anteriormente descritos con el fin de asegurar que son válidos y eficaces durante situaciones adversas.

La reducción del riesgo para esta categoría de desastre está asociada con la implementación de centros de datos alternos, sitios alternos de operación y planes de contingencia técnica probados y actualizados. El cumplimiento de los MTD, RTO y RPO dependen directamente de los servicios de centros de datos alternos contratados y de la efectividad de los planes de contingencia técnica, de un adecuado diseño del BIA y de la retroalimentación obtenida en los ejercicios y pruebas realizadas al DRP.

C. Escenarios de desastres naturales o pandemias.

En este escenario los riesgos se analizan desde las lecciones aprendidas en desastres ocurridos en otras regiones. Las indisponibilidades de servicios tecnológicos pueden tomar meses y estar sujetas al estado de salud de los funcionarios y a las medidas gubernamentales establecidas, de acuerdo con la gravedad del desastre. Los controles específicos asociados a la mitigación de riesgos para este escenario son los mismos descritos en el anterior apartado, pero no son suficientes por lo que se recomienda implementar medidas encaminadas a la sobrevivencia de la organización, como por ejemplo acuerdos de carácter legal con los clientes, pólizas de seguros, centros de datos alternos en zonas geográficas remotas, y, por supuesto, un eficiente y maduro BCP.

III. ¿LA TEORÍA ES SUFICIENTE?

Una vez descritos los posibles escenarios de desastre, es importante determinar los procedimientos necesarios para identificar qué plan se debe activar en caso de una contingencia y bajo qué parámetros se desplegará. La teoría y las principales fuentes bibliográficas referentes a la Continuidad del negocio ilustran las maneras en que se deben enmarcar las circunstancias de contingencia, pero se debe tener muy en cuenta que existen un sin número de incidentes que originan confusión al momento de decidir, por parte del comité de crisis, qué plan debe ser desplegado.

Basándose en la experiencia, a continuación, se describen circunstancias poco contempladas en la teoría general de BCP las cuales pueden contribuir a evitar inconvenientes durante su activación.

A. Aspectos administrativos.

La activación de los planes de continuidad del negocio por causas derivadas de fallas en la infraestructura tecnológica y en el mantenimiento de aplicaciones y sistemas de información se origina por deficiencias en los procedimientos de mantenimiento, gestión y arquitectura de las plataformas tecnológicas que soportan los procesos críticos del negocio. Basándose en esta última consideración, la resolución de estas deficiencias que pueden afectar la disponibilidad e integridad de nuestros servicios tecnológicos iría de la mano con un constante monitoreo de las condiciones de operación de los componentes de la plataforma, en conjunto, con la evaluación periódica de los procedimientos de mantenimiento y gestión de los sistemas de Información. Teniendo en cuenta estas premisas y considerando el tema central de este artículo, un lector desprevenido podría considerar que dichos temas están por fuera de un plan estratégico de gestión de riesgos y que la solución sería fortalecer los mecanismos de auditoria y mejora continua de los sistemas de gestión tecnológica presentes; esta es una recomendación a posteriori. Pero… ¿qué hacer si los servicios no están disponibles por esta causa? Para utilizar un dicho popular, no hay Santa Lucía que valga cuando toda la organización tiene en la mira al área encargada de la gestión tecnológica a causa de la imposibilidad de realizar las actividades cotidianas y con el agravante de tener a clientes y proveedores presionando por una oportuna atención a sus requerimientos, se debe actuar desde la perspectiva de la continuidad del negocio y para tal fin se presentan las siguientes consideraciones:

1) Informe de incidentes: La primera preocupación es restaurar los servicios afectados en el menor tiempo posible o de acuerdo con el RTO propuesto, identificando la causa de la afectación del servicio. Inicialmente se debe generar un informe conciso y detallado de las causas y consecuencias de la indisponibilidad de servicios, dirigido al líder de continuidad. Sin un adecuado informe de las circunstancias que originaron la interrupción de los servicios y una proyección responsable de las acciones a tomar, el líder de continuidad no podrá informar eficientemente acerca de lo ocurrido a los responsables de los procesos afectados y a los integrantes del comité de crisis, quienes, a su vez, establecerán entre uno de los siguientes componentes del plan de continuación del negocio el o los que se deben activar:

--Plan General de Manejo de Crisis.
--Plan Maestro de Emergencias.
--Plan de Continuidad de las Operaciones.

Hago énfasis en que la adecuada elaboración del informe de indisponibilidad de servicios tecnológicos es el pilar para un adecuado despliegue de los componentes del BCP, dicho plan debe incluir los siguientes datos:

--Hora del incidente.
--Hora de reporte del incidente por parte del responsable.
--Aplicaciones o Sistemas de Información afectados.
--Procesos del negocio afectados.
--Responsables de la restauración del servicio.

--Concepto de los responsables de la restauración acerca del tiempo estimado de recuperación.
--Último backup disponible de los componentes tecnológicos afectados.
--Causa de la afectación del servicio.
--Proveedores involucrados.

Cada uno de los anteriores aspectos debe estar debidamente documentado y soportado. Nunca se debe comunicar incidentes que no puedan ser sustentados con evidencias objetivas y claras, no se debe romper la cadena de suministro, por tal razón, los responsables o especialistas de la infraestructura afectada deberán reportar exclusivamente a su jefe inmediato quién, a su vez, con el informe generado como soporte procederá a informar al líder de continuidad, evitando así, desinformaciones y múltiples versiones de los hechos.

2) Responsabilidades: El comité de crisis debe ser asesorado en aspectos técnicos por el líder de continuidad y el responsable de tecnología. NO es responsabilidad de los especialistas de TI activar los planes de continuidad. Nunca se deben suplantar responsabilidades del comité de crisis, no se deben asumir decisiones por importantes que estas sean; un BCP debe incluir una matriz de roles y responsabilidades, incluyendo suplencias para aquellos casos en que los titulares no se encuentren disponibles durante el incidente. Para aquellos casos en que se requiera tomar una decisión por fuera de las responsabilidades previamente adquiridas, se debe consultar con el líder de continuidad. Estas decisiones deben ser soportadas mediante comunicaciones escritas y firmadas.

3) Experiencias adquiridas: Poner en práctica las experiencias adquiridas durante las pruebas del plan de recuperación de desastres o el plan de contingencia técnica, permite reducir la posibilidad de imprevistos durante eventos de indisponibilidad, asegura el cumplimiento de los tiempos objetivo de recuperación RTO y los puntos objetivos de recuperación RPO. Se recomienda mantener los mismos procedimientos del plan de contingencia técnica durante el despliegue de un plan de recuperación de desastre, esto se traduce en que los planes de contingencia técnica deben operar bajo las mismas condiciones técnicas tanto en el centro de datos principal como en el centro de datos alterno.

4) Presupuestos, inversión e infraestructura: Los líderes de las áreas tecnológicas deben crear estrategias para asegurar inversión en Infraestructura tecnológica de contingencia con el fin de evitar dolores de cabeza futuros ya que entre más se pueda unificar el hardware que soporta los ambientes productivos y los de contingencia, más sencillo y comprensibles se tornaran los planes de contingencia técnica. Como ejemplo, si se tiene una infraestructura de servidores de base de datos en alta disponibilidad en el centro de datos principal, los servidores de contingencia para dicha infraestructura deberían ser lo más parecidos posibles en cuanto a sus especificaciones técnicas, de procesamiento, capacidad de memoria y conectividad de red. En la medida de lo posible y lo económico, se deben integrar las soluciones de alta disponibilidad con las soluciones de contingencia, a modo de ejemplo, si tiene un clúster de servidores para sus bases de datos de misión crítica, busque la arquitectura necesaria para integrar los servidores de contingencia como un tercer nodo del clúster de producción. Esta arquitectura tecnológica le permitirá reducir su RTO, RPO y costos de respaldo de la información, así como ventanas de servicio para pruebas de DRP.

Unificar el hardware que soporta los sistemas de misión crítica de las organizaciones permite facilitar el diseño y la realización del set de pruebas de contingencia técnica y recuperación de desastres proporcionando mejores tiempos de restauración de los servicios tecnológicos afectados y consecuentemente mejores tiempos de vuelta a la normalidad de los mismos. No se deben olvidar los temas relacionados con licencias de software en los ambientes contingentes, de esta manera podrá evitar multas o sanciones por parte de sus proveedores de software o de entes de control que realicen auditorías de derecho de autor.

5) Relaciones con terceros: Recomendación práctica que surge a partir de las relaciones contractuales que se establecen con proveedores de servicios tecnológicos que participan directa o indirectamente en los DRP y planes de contingencia técnica. De nuevo podemos considerar el BCP ideal, donde sean contemplados todos los posibles escenarios de desastre, donde se ha desarrollado un juicioso análisis de riesgos para implementar las mejores estrategias que mitiguen la posibilidad de eventos que generen interrupciones de los servicios vitales de la organización el análisis de impacto al negocio ha involucrado todos los procesos operativos, se ha diseñado ambientes productivos y de contingencia compatibles con las mejores tecnologías disponibles y se han realizado de manera programada y metódica las pruebas de restauración y contingencia de acuerdo con los planes diseñados; el líder de contingencia y el director de TI pueden estar tranquilos porque su gestión y experiencia les dice que sus activos tecnológicos están protegidos en caso de una contingencia o desastre. Pero cabe anotar el siguiente interrogante, ¿Todos los aspectos referentes a la continuidad del negocio estarán igualmente probados y documentados del lado de la infraestructura contratada con los proveedores? Se deben solicitar las pruebas de los esquemas de alta disponibilidad contratados que se ajustan a las certificaciones internacionales que los proveedores de centros de datos y comunicaciones exhiben orgullosamente en sus vitrinas o carteleras; estas pruebas se realizan comúnmente sin la intervención del contratante razón

por la cual, generalmente, se debe confiar en los resultados informados por el proveedor.

Se deben establecer acuerdos de nivel de servicio (ANS) con nuestros proveedores debido a que, sin importar el nivel de redundancia que se contrate siempre existe la posibilidad de que se presente una caída de los servicios soportados. Obras de terceros en las vías públicas rompieron enlaces de fibra óptica, durante pruebas de alta disponibilidad, un error humano ocasionó interrupción en los servicios, se presentó un daño de hardware y el componente redundante por una mala configuración no se activó, un tercero, que actúa como prestador de servicios de nuestro proveedor incumplió sus acuerdos de nivel de servicio (ANS), una ataque terrorista ocasionó indisponibilidad de operaciones en el centro de datos principal y alterno, en fin, existen muchos aspectos que se salen del análisis y control del propietario de la infraestructura tecnológica protegida. En estos casos, las áreas jurídicas de las organizaciones son las que deben actuar. Los contratos de prestación de servicios que intervengan en nuestros planes de continuidad del negocio deben ser especialmente redactados para evitar afectaciones al patrimonio y la reputación del contratante. Los aspectos legales deben estar perfectamente atados al cumplimiento de los ANS establecidos por las áreas de operaciones y de seguridad de la información, toda esta información debe estar consignada en los análisis de impacto al negocio BIA y debidamente aprobados por los responsables de tecnología.

Es muy importante que los especialistas que administran hardware y software de misión crítica estén enterados de los ANS y las penalidades establecidas en los contratos de prestación de servicios tecnológicos, para de esta manera exigir soluciones concretas y oportunas al momento de presentarse indisponibilidades de los servicios contratados. Generalmente los riesgos asociados a la probabilidad de ocurrencia de estos incidentes se deben transferir al tercero mediante comunicaciones explicitas generadas por el oficial de seguridad y aprobadas por el comité de riesgo, de esta manera se evitan mal entendidos y conflictos originados por la aplicación de penalidades de los contratos.

6) Pruebas periódicas: Ya se ha mencionado que un adecuado set de pruebas de los ambientes de contingencia, recuperación de desastres y mecanismos de alta disponibilidad toma vital importancia para obtener los resultados esperados durante un escenario de crisis; es pertinente definir la periodicidad con que se van a realizar estas pruebas con el fin de cumplir con los estándares internacionales bajo los cuales se han construido los sistemas de gestión de seguridad de la información y prevenir que los procesos de auditoría establecen no conformidades mayores por el hecho de no encontrar evidencias de la realización de pruebas funcionales a los DRP.

Los set de pruebas deben ser programados con suficiente tiempo, con el fin de diseñar estrategias que permitan mantener los ambientes de producción disponibles y así no afectar la normal operación de los sistemas de información esenciales del negocio, en estos ejercicios se involucra a los dueños de los procesos de la organización, al líder de continuidad, a los diferentes especialistas que administran la infraestructura afectada, proveedores, mesas de ayuda y usuarios funcionales para de esta manera verificar que los servicios tecnológicos en contingencia técnica cumplen con los requerimientos de las diferentes áreas de la organización a nivel de usuario funcional.

Durante cada una de las pruebas en las que se deben realizar cambios de configuración es muy importante mantener un adecuado mecanismo de control de cambios que nos permita documentar e identificar las configuraciones, direccionamientos, rutas y parámetros que permitan el correcto funcionamiento de nuestros componentes. Un caso práctico, a modo de ejemplo, seria considerar que dentro del BCP se debe contemplar la necesidad de contratar un sitio alterno de operación, para aquellos casos en que los funcionarios de nuestras organizaciones no puedan ingresar a laboral en sus oficinas por amenazas de terrorismo, incendio, inundación, falta de servicios públicos fundamentales, sabotaje, etc. Estas ubicaciones de operación alterna generalmente son contratadas en modo no exclusivo, es decir, están disponibles para varios clientes, las configuraciones de los equipos de contingencia, los enrutamientos que se deben establecer en el firewall del sitio alterno de operación (SAO), el direccionamiento público que cada equipo puede llegar a requerir para conectarse a servicios externos, inclusive los puertos donde cada equipo debe ser conectado pueden ser claros ejemplos de cambios que en determinado momento pueden afectar el funcionamiento de los servicios tecnológicos durante una contingencia técnica.

Mantener un adecuado mecanismo de control de cambios aplicable a las configuraciones del ejemplo presentado anteriormente o a cualquier otro escenario donde puedan ocurrir indisponibilidades de servicios de TI a causa de malas parametrizaciones, nos permitirá actuar eficientemente durante una contingencia y brindar a los usuarios que participan en esta, una reanudación de servicios ágil y oportuna, apegado a nuestros acuerdos de nivel de servicio internos. Esta es una manera precisa de evitar acusaciones de los diferentes procesos de negocio en contra de los funcionarios de tecnología durante eventos de activación del DRP con las implicaciones a nivel directivo que esto ocasiona.

B. Consideraciones durante un desastre.

Las recomendaciones precedentes marcan la ruta para evitar errores de diseño en los BCP por falta de gestión y experiencia del líder de continuidad o del Director de TI, quienes pueden

tener a su cargo realizar las validaciones necesarias para dar cumplimiento a la política de continuidad establecida en la organización. A continuación, se exponen algunas situaciones que pueden presentarse durante un desastre natural o calamidad por eventos de orden público, eventos difícilmente reproducibles durante pruebas de continuidad programadas.

1) Asistencia Familiar: En caso de un desastre natural de alto impacto sobre la infraestructura regional, la integridad física y mental de los familiares de los funcionaros y directivos de la organización pueden verse afectadas de manera significativa, si esto sucede, desplegar las tareas de contingencia técnica va a ser muy difícil o va a sufrir demoras importantes. La principal recomendación para estos casos, es que la entidad incluya dentro de los planes de asistencia al recurso humano a los núcleos familiares de los funcionarios responsables de desplegar los planes de recuperación de desastres, para de esta manera permitir que los especialistas puedan enfocarse en sus responsabilidades profesionales con la seguridad de que sus familias cuentan con atención especializada. Las políticas y mecanismos de acceso remoto deben fortalecerse para soportar procedimientos administrativos en caso de que así lo requieran especialistas y personal administrativo.

2) Suplencias de funciones: En caso de afectación física del personal encargado del despliegue del BCP a causa de afectaciones en el orden público, desastre natural o accidente, el análisis de impacto al negocio BIA debe contemplar la necesidad de emplear funcionarios o proveedores suplentes con las habilidades y el conocimiento necesario para realizar las tareas de contingencia necesarias. Una muy buena práctica recomendable para esta situación es que al menos unos de los sets de pruebas de contingencia técnica sean realizados por el especialista o proveedor suplente.

3) Comunicaciones: Durante un desastre se hace particularmente importante que el sitio alterno de operación se encuentre dentro de las instalaciones del centro de datos principal o centro de datos alterno. Un desastre natural de gran magnitud puede ocasionar afectaciones prolongadas sobre los anillos de fibra óptica de los proveedores de comunicaciones, lo que puede conllevar a que el sitio alterno de operación quede desconectado de la infraestructura de servidores que soportan los servicios tecnológicos. Tener el sitio alterno de operación dentro de las instalaciones de los centros de datos principal o alterno reduce la probabilidad de desconexiones de los usuarios con sus aplicaciones productivas o de contingencia.

4) Seguridad Perimetral: El direccionamiento IP y la seguridad perimetral requerida durante una contingencia o desastre natural para la interconexión del sitio alterno de operación debe ser responsabilidad del proveedor de servicios del centro de dato, la organización cliente requiere el soporte de los especialistas de redes, comunicaciones y seguridad que se encuentran en las salas de operaciones de los centros de datos, lo que es una clara ventaja sobre las situaciones en que los especialistas de red y seguridad propios de la institución afectada deban ocuparse de solucionar temas relacionados con enrutamientos y políticas de firewall y no del soporte requerido por los usuarios en contingencia en aspectos funcionales de los sistemas de información e infraestructura durante un desastre.

5) Desplazamientos seguros: Otro aspecto a tener muy en cuenta es que las salas de operación para usuarios funcionales y especialistas de TI que se encuentran dentro de las instalaciones de centros de datos (principal o contingencia) tiene menor posibilidad de sufrir daños físicos, locativos o de infraestructura de servicios públicos gracias a las especificaciones de TIER implementadas en las ubicaciones que los albergan, trabajar en estas salas permite que el desplazamiento de los especialistas durante afectaciones de los servicios tecnológicos se reduzca significativamente por el hecho de que realizan sus labores de administración en instalaciones contiguas a las salas en que se encuentran instaladas las plataformas de hardware. Los problemas de orden público y desastres naturales generan vandalismo y robos; reducir los desplazamientos del personal reduce el riesgo de afectaciones sobre su integridad física.

IV. CIBERATAQUES

Sin Importar la naturaleza de nuestra organización, se debe contemplar la posibilidad de ser víctima de un ciberataque que afecte la disponibilidad de la información de la organización o que utilice su infraestructura como origen de ataques a terceros. Existe una gran variedad de ataques cibernéticos que pueden afectar nuestros sistemas tecnológicos, pero al mismo tiempo, podemos aplicar un gran número de técnicas para proteger los activos tecnológicos una vez las amenazas hayan vulnerado nuestro firewall perimetral.

Si el ataque cibernético está encaminado a afectar la integridad, disponibilidad y privacidad de la información de nuestra organización, dependemos de un adecuado funcionamiento del equipo de respuesta a incidentes de la seguridad de la información del que se recomienda, haga parte el líder de continuidad, esta pertenencia permite que la dinámica con la que se puede desplegar el BCP sea similar a en casos de desastres, contingencia técnica o ciberataques.

En aquellas situaciones en que se pierde la disponibilidad de nuestra información, se deben aplicar contramedidas que restauren la información afectada con el mínimo punto de restauración objetivo (RPO) posible, de ser necesario, se debe iniciar la respuesta al ataque aislando la subred afectada para proceder con la mitigación de la vulnerabilidad aprovechadas.

Pero, ¿qué pasa si las áreas afectadas hacen parte de un proceso de vital importancia en nuestra organización? En la mayoría de las ocasiones los responsables del proceso de negocio afectado no van a dar espera mientras se realiza la inspección de los equipos pertenecientes a la red o subred afectada. Se debe activar el sitio alterno de operación para los usuarios afectados reinicien su operación de manera controlada y con la seguridad de que el ataque no continuará afectando los nuevos recursos a utilizar; una adecuada gestión de vulnerabilidades que incluya entornos productivos, contingentes y de pruebas y desarrollo, reduce considerablemente la posibilidad de activación de planes de contingencia técnica por ciberataques. Las consecuencias del ciberataque sobre su infraestructura tecnológica determinan la activación del plan de continuidad del negocio, los controles tecnológicos implementados para prevenir la ejecución de códigos maliciosos contribuyen para la no activación de contingencias técnicas, por lo tanto, deben ser continuamente evaluados e incluso implementados sobre plataformas alternas de operación (contingencia, pruebas y desarrollo).

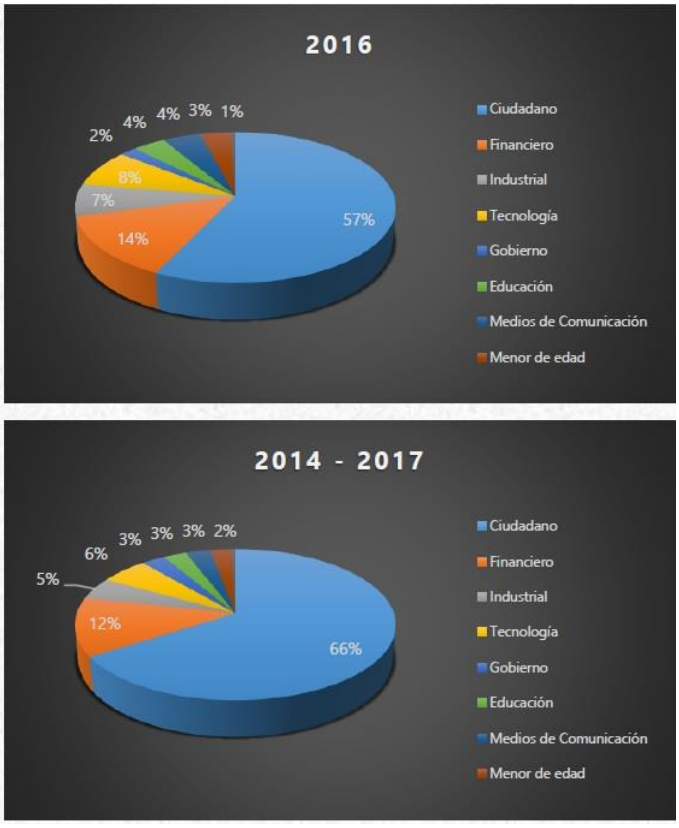

Fig. 1. Ciberataques en Colombia por sectores, tendencias 2014-2017. Obtenida de caivirtual.policia.gov.co

Tomando como referencia el estudio realizado por el centro cibernético de la Policía Nacional de Colombia [2], podemos observar que los ataques cibernéticos han aumentado en el sector representado por los ciudadanos del común, debido a que las campañas de concientización respecto a la protección de la información personal no han dado el resultado esperado, por otra parte se evidencia una disminución en los ataques cibernéticos sobre plataformas tecnológicas corporativas lo que lleva a pensar que los controles adoptados por las áreas tecnológicas están haciendo más dificultando la ocurrencia de ataques informáticos catastróficos. Surge entonces como recomendación implementar controles tecnológicos que no solo mitiguen la probabilidad de que un ataque cibernético logre su cometido, también debemos encaminar nuestros esfuerzos hacia el diseño de soluciones contingentes cuando nuestro perímetro haya sido vulnerado.

Es conveniente mantener una plataforma de servidores virtualizada en la que todos los parches y actualizaciones de seguridad se encuentren aplicados y pertenezca a una red aislada, esta estrategia de contingencia es muy conveniente durante un ciberataque ya que nos permite romper los canales de comunicación con nuestros servidores que soportan roles importantes en la red (DA, DNS,DHCP, SMTP, etc.), detener la inferencia sobre estos servicios y restaurarlos aplicando nuevos direccionamientos IP. Esta estrategia para un DRP es eficiente, de fácil implementación y bastante económica. De esta manera se puede solucionar cualquier ataque de spoofing que es la puerta de entrada para que un atacante genere confusión, caos y denegación de servicio que son las puertas de entrada para el robo de información.

La variedad de recomendaciones técnicas y de gestión hasta aquí propuestas deben ser consideradas por los especialistas de infraestructura y líderes de continuidad en el momento de diseñar los planes de continuidad y así mismo, de activarlos. Son buenas prácticas nacidas de la experiencia durante ejercicios de pruebas institucionales y situaciones reales de contingencia durante la vida profesional del escritor y encaminan al diseño e implementación de un plan de respuesta a los ciberataques. En el siguiente numeral se presentarán algunas recomendaciones de NIST que pueden reforzar aún más los planes de contingencia técnica.

V. INDICACIONES ÚTILES NIST

A. Declaración de una política del plan de contingencia.

La redacción de una política que describa los objetivos del plan de continuidad del negocio es el punto de partida para que todos y cada una de las personas que conforman una organización comprendan sus objetivos y alcance. Esta es la manera más sencilla y viable a la vez, para involucrar a todos los miembros de una organización en la mejora continua de los procesos que permiten mantener la operación de los servicios tecnológicos disponibles. Esta política debe ser publicada y comunicada mediante un eficiente plan de capacitación al personal nuevo y antiguo de la organización para que no se

presenten incidentes en los que los funcionarios expresen desconocimiento operativo de las tareas a realizar durante ejercicios de pruebas del BCP.

La política del plan de contingencia debe estar acompañada de los lineamientos de continuidad del negocio para facilitar la comprensión por parte de los usuarios de las estrategias adoptadas por la organización para el tratamiento de cualquier evento de riesgo operativo que pueda afectar la disponibilidad de los servicios tecnológicos, también se constituye como una recomendación de carácter administrativo que los líderes de continuidad deben adoptar para disminuir los niveles de entropía durante catástrofes. Entre más se pueda involucrar a todos los funcionarios de la organización en los BCP y DRP será mucha más fácil desplegar los planes de respuesta a ciberincidentes y desastres, sin embargo, los aspectos técnicos de los planes de contingencia técnica siempre deben ser de carácter confidencial con el fin de evitar fugas de información que puedan facilitar ataques de denegación de servicio.

B. Roles y responsabilidades.

La definición de responsabilidades es una estrategia comúnmente implementada dentro de los planes de continuidad del negocio y permite mejores tiempos de respuesta a incidentes de seguridad que pueden ocasionar indisponibilidades; es una buena práctica definir las diferentes responsabilidades que componen un gobierno corporativo y de la seguridad de la información para construir desde la punta de la pirámide las funciones requeridas durante una emergencia. Los cargos de líder de continuidad, el comité de crisis, el oficial de seguridad de la información, el equipo de respuesta a emergencias o el equipo de recuperación de operaciones deben ser ejercidos por personal calificado y con la experiencia necesaria para responder a eventos catastróficos ya que generalmente se deben tomar decisiones bajo situaciones de máxima presión y apremio.

NIST propone una diversificación de funciones dentro de del equipo de recuperación de operaciones de acuerdo con las diferentes especializaciones requeridas para la administración de servicios tecnológicos [3]. Es de vital importancia que las organizaciones dentro de sus gerencias tecnológicas establezcan especialidades y no caigan en el error de fomentar la creación de "toderos" técnicos que se caracterizan por acumular el conocimiento necesario para administrar las plataformas tecnológicas, generando cargas laborales desbordadas y demoras por indisponibilidad laboral durante la activación de planes de contingencia y recuperación de desastres. Hay que fomentar la especialización de los funcionarios de TI, impulsando el desarrollo y la investigación por área y contribuyendo al desarrollo de innovación transversal entre especialidades como lo son redes de datos, bases de datos, seguridad de la información, sistemas operativos, gestión de almacenamiento, gestión de usuarios, cableado estructurado e infraestructura eléctrica, desarrollo de software, comunicaciones y gestión de proyectos.

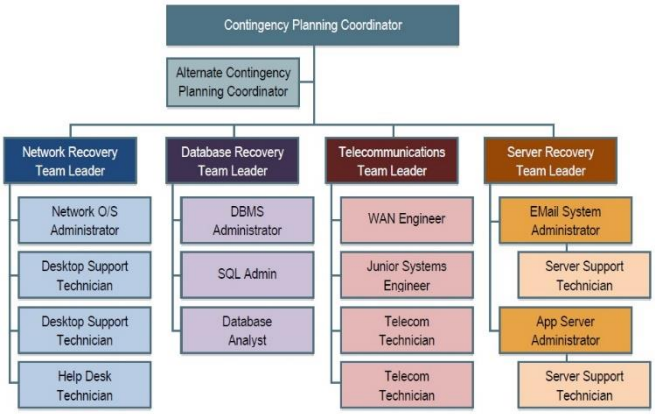

Fig. 2: Roles dentro del equipo de recuperación de operaciones. Obtenida de NIST Special Publication 800-34 Rev 1., paj37.

El entrenamiento en continuidad del negocio debe ser brindado de manera uniforme a todos los especialistas y es responsabilidad de los líderes de las oficinas de TIC que los funcionarios a su cargo se capaciten en estos temas. El siguiente organigrama muestra los roles generales que debe contener un grupo de recuperación de operaciones a nivel técnico.

C. Mantenimiento y control de cambios.

Las infraestructuras tecnológicas, sufren constantes cambios derivados de la depreciación de los equipos, obsolescencia de los sistemas de información, nuevos requerimientos de los procesos del negocio, necesidades de seguridad de la información, crecimientos o reducciones locativas de las organizaciones e incluso cambios de los directivos que las gobiernan. Estos cambios afectan las actividades descritas en los planes de contingencia técnica de manera directa ya que cualquier modificación en el hardware que soportan los sistemas puede representar fallas en los procedimientos de alta disponibilidad, respaldo de la información o sincronización con otros componentes. Bajo este escenario aparece la figura del coordinador de contingencia técnica quien, de acuerdo a la experiencia deberá ser el administrador de la plataforma de hardware o el director de infraestructura.

La responsabilidad de registrar y documentar los cambios o actualizaciones sobre las plataformas tecnológicas e informarlos a los demás especialistas es del coordinador de contingencia técnica. Como ejemplo, el cambio de un sistema de almacenamiento SAN puede afectar la manera como las bases de datos mantienen esquemas de réplica con otras instancias o modifican el mecanismo utilizado por los servidores de archivos para realizar respaldos de la

información, igualmente puede afectar el proceso de grabación de una planta telefónica y sus respectivas tareas de respaldo. Otros casos a reportar son: cambios en los canales de comunicación, cambios de tecnologías de sistemas de alimentación eléctrica ininterrumpida (UPS), actualizaciones de las plataformas web de las aplicaciones, cambios de políticas en los cortafuegos, cambios de número de puerto para acceso a las aplicaciones entre otros. Las bitácoras de cada activo tecnológico deben contener un registro de control que permita identificar si el activo se encuentra dentro de cualquiera de los planes del DRP.

No solo los cambios de infraestructura generan estos inconvenientes, de igual manera los procedimientos de mantenimiento preventivo o correctivos pueden llegar a ocasionar problemas de configuración en los mecanismos de alta disponibilidad o falsas alarmas en las aplicaciones de monitoreo de la infraestructura incluida en el ISCP. Por estas razones y de acuerdo con las recomendaciones de NIST, es importante documentar cualquier cambio en la infraestructura y adicionalmente realizar revisión de cualquier cambio tecnológico que no haya sido reportado y documentado.

D. Resiliencia.

Este término explica la manera como los seres humanos se adaptan a condiciones adversas mediante conductas coherentes y racionables. Esta definición puede ser adaptable a muchas circunstancias del diario vivir humano en las que se requiere toma de decisiones rápida y bajo condiciones de presión. Se presenta la definición de resiliencia del Departamento de Seguridad nacional de los estados unidos (DHS siglas en ingles de Department of homeland security). [4] para utilizarla en el despliegue de un DRP. “La resiliencia es la capacidad de adaptarse y recuperarse rápidamente de cualquier cambio conocido o desconocido en el entorno. La resiliencia no es un proceso, sino un estado final para las organizaciones. El objetivo de una organización resiliente es continuar con las funciones esenciales de la misión en todo momento durante cualquier tipo de interrupción. Las organizaciones resilientes trabajan continuamente para adaptarse a los cambios y riesgos que pueden afectar su capacidad para continuar funciones críticas”. Esta definición aplicada a la teoría de la continuidad del negocio puede ser utilizada redefinida como una característica que las organizaciones deben alcanzar para mantener sus procesos vitales durante cualquier incidente. El fomento de esta característica dentro de una organización complementado con un proceso de mejora continua de los planes de continuidad del negocio se constituye en la vía óptima para la consecución de las políticas de contingencia de las organizaciones.

VI. MEJORA CONTINUA

La implementación de procesos de mejora continua de los BCP es una recomendación adicional que deben tener en cuenta los líderes de continuidad del negocio. El monitoreo y medición de los planes actuales permiten determinar la eficiencia de los mismos de acuerdo con los objetivos esperados por la alta dirección de manera cualitativa, mediante indicadores de gestión especialmente diseñados. El proceso de mejora continua planteado para los planes de continuidad del negocio involucran las etapas que a continuación se describen.

A. Identificar debilidades.

Ya hemos analizado posibles debilidades de nuestro BCP desde el punto de vista técnico y administrativo, ahora, en este apartado, se analizarán los métodos para identificar posibles inconsistencias en los planes de continuidad mediante buenas prácticas conocidas.

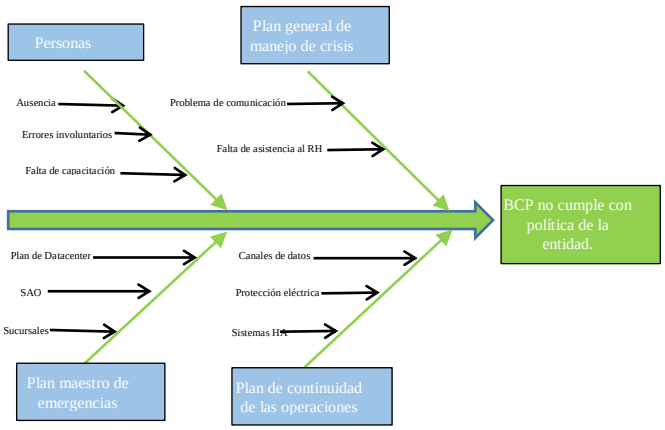

Fig. 3. Diagrama causa y efecto para mejora continua. Propuesto por el autor

La identificación de debilidades mediante auditorías a los informes de ejecución de pruebas de los planes de continuidad surge como una herramienta valiosa para identificar problemas; aplicar un análisis de causa efecto a las diferentes tareas que conforman un plan de contingencia técnica permite determinar las causas de un problema y sus posibles soluciones. El punto central es Asignar importancia a cada factor e identificar aquellas variables particularmente importantes que parecen tener un efecto significativo sobre un problema. Este método de análisis actúa como un identificador de problemas en cada procedimiento presente en el BCP y es de alta importancia al momento de diseñar los indicadores.

B. Definición de planes de mejora.

Para establecer una mejora a partir de la identificación de un problema es necesario determinar cómo vamos a medir el desempeño de un proceso o procedimiento. Generalmente cualquier actividad técnica propia de un plan de contingencia

se mide por unidades de tiempo de principio a fin. El tiempo suele ser el principal indicador para establecer la efectividad de un procedimiento, la recomendación es no olvidar que un BCP está compuesto por un gran conjunto de actividades y responsables a quienes los solos tiempos no interesan. Optimizar los procedimientos para mejorar sus tiempos de ejecución puede ser una solución consecuente, pero no hay que dejar atrás indicadores tan importantes como capacidad de procesamiento, iops por segundo (indicador de escritura lectura) o anchos de banda consumidos ya que son de vital importancia en un escenario de contingencia para determinar mejoras. Definir el plan de mejora está directamente relacionado con la eficiencia de los planes de contingencia y recuperación de desastres y la magnitud en tiempo de utilización de recursos de maquina o red necesarios para cumplir los RTO.

C. Medir la eficiencia.

Debemos obtener un valor cuantificable, valorable y clasificable para establecer la eficiencia de nuestro BCP, pero ¿cuándo podemos realizar estas mediciones?, ¿después de un evento de calamidad mayor?, ¿luego de los test de pruebas?, ¿después de obtener los resultados de las auditorías internas y externas sobre nuestros procesos de continuidad del negocio? Existen múltiples consideraciones referentes a la manera de medir el desempeño de nuestros planes de contingencia; podemos establecer indicadores de eficacia para medir el acierto en la consecución de nuestros objetivos de contingencia planteados; podemos diseñar indicadores para medir la eficiencia en la ejecución de nuestros planes de continuidad estableciendo relaciones entre los objetivos propuestos y los objetivos alcanzados de acuerdo a nuestros análisis de costo-beneficio; también se pueden implementar indicadores de cumplimiento, relacionados exclusivamente con lo asertivos que seamos con el cumplimiento de los RTO y RPO, en fin podemos agregar indicadores de calidad, de evaluación, de productividad para adornar la consecución de los objetivos de nuestro BCP. Existen dos consideraciones claves en el momento de evaluar nuestros procesos de continuidad:

1) ¿Qué estamos midiendo y contra qué?
2) ¿Cómo lo vamos a medir?

Para responder al primer interrogante debemos establecer indicadores considerando a la hora de crearlos en qué escenario van a ser utilizados; en un escenario de pruebas, en una auditoria, en un evento real y qué planes de contingencia técnica se pueden medir. Para establecer las fórmulas que determinarán los indicadores podemos utilizar múltiples variables dependiendo de la naturaleza del evento que dispara la activación de BCP. Simulaciones para auditorias pueden ocasionar desviaciones en nuestros resultados debido a que variables utilizadas, como lo podría ser el tiempo de restauración de una cinta, puede reducirse significativamente por el hecho de que la actividad de medición ha sido programada o simplemente, por la hora del día en que se ejecute ya que la carga del servidor de restauraciones y de las diferentes librerías de cintas cambian de acuerdo con su programación de tareas diarias. La recomendación para este punto es utilizar indicadores diferentes de acuerdo con la circunstancia en la que realizaremos la medición, por ejemplo, utilizar tres indicadores diferentes para auditorias, sets de pruebas y escenarios reales de indisponibilidad.

Los resultados obtenidos en la medición de eficacia de un BCP están directamente relacionados con los cambios en la estructura tecnológica ocurridos desde la medición previa, para volver al ejemplo anterior de la librería de cintas, con el solo hecho de realizar una limpieza al drive de cintas o más aún si es remplazado por uno nuevo, nuestra variable de tiempo, factor del indicador, va a cambiar significativamente; caso similar se puede presentar con servidores, canales de comunicación, tecnologías de discos de almacenamiento, etc. Si se desea mantener una secuencia de mejora continua clara, que permita presentar resultados precisos a los comités directivos pertinentes, debemos por obligación diseñar indicadores de satisfacción del cliente. Estos indicadores permiten realizar una medición integral a nuestro BCP, permitiendo incluir la evaluación a todos los planes implementados, probados o auditados ya que el usuario funcional de las aplicaciones es quien finalmente da su aprobación de manera integral, en caso de que los sistemas de información a los que accede sean restauraos en distintos ambientes. Es así como los mismos usuarios pueden evaluar los planes de asistencia al recurso humano, los planes de comunicaciones, los planes de continuidad de las operaciones incluidos los de TI y por supuesto los planes de emergencia que incluyen desplazamientos entre instalaciones física. Es claro que este tipo de indicador que mide la satisfacción del cliente final que utiliza los servicios tecnológicos y administrativos durante y después de una contingencia son determinadores para un adecuado proceso de medición de nuestro BCP.

D. Análisis de escenarios.

Dentro del proceso de mejora continua del BCP es muy importante tomarse el tiempo para analizar nuevos y diferentes escenarios de contingencia, emergencia y desastre. Condiciones políticas, económicas, sociales, ambientales pueden determinar nuevos escenarios de contingencia, protestas en sectores de la sociedad, demandas legales, nuevas condiciones climatológicas, cambios de líderes políticos entre otros sucesos pueden generar interrupción de la operación de compañías prestadoras de servicios, financieras o gubernamentales.

La mejora continua de los BCP requiere entre otras consideraciones, de un análisis periódico que permita identificar nuevos escenarios de contingencia lo que conlleva a una constante evaluación de nuevos riesgos potenciales que puedan afectar nuestros planes de continuidad. Esta actividad puede ser eficientemente desarrollada con la colaboración de los líderes de proceso de

la organización, quienes están al tanto de los cambios sociales, políticos, económicos y ambientales del entorno donde operan las compañías. Tanto el líder de continuidad, la oficina de riesgos y la oficina de seguridad de la información deben coordinar estas tareas.

Como toda documentación presente en una organización, los planes de continuidad del negocio deben actualizarse de manera controlada pero dinámica de acuerdo con los cambios en la infraestructura de hardware, actualizaciones de los sistemas de información, nuevas contrataciones de housing o colocaction y las mejoras identificadas durante el proceso de revisión. El líder de continuidad del negocio debe cumplir con esta responsabilidad, delegando en quién el disponga, la actualización de los documentos y asegurándose de la difusión y promoción, entre todos los integrantes de la empresa de los cambios realizados. En muchas ocasiones los hallazgos propios de la mejora continua evidencian inconvenientes que deben ser tratados inmediatamente, este proceso se debe convertir en un ciclo que permita afinar cada vez más nuestro BCP.

VII. CONCLUSIONES

1) No existen maneras de predecir la ocurrencia de un evento catastrófico, de falla técnica o ataque cibernético que pueda afectar una plataforma tecnológica encargada de soportar las operaciones de un negocio. Si ha de ocurrir ocurrirá ya que generalmente un evento de contingencia se origina por condiciones naturales, errores humanos en la administración de activos tecnológicos o por pretensiones económicas, políticas, sociales o reputaciones de un atacante.

2) La principal manera de cumplir con las expectativas de los líderes del negocio en lo relacionado con la continuidad operativa de sus organizaciones es establecer las políticas, estrategias y procedimientos que garanticen la continuidad de las operaciones, así como el apoyo y compromiso de los especialistas encargados de liderar y gestionar escenarios de desastres y contingencias.

3) Al ser situaciones proyectadas, se hace complicado prevenir las posibles situaciones que se pueden presentar durante interrupciones de servicios tecnológicos por la causa que sea. Las recomendaciones prácticas presentadas en este artículo pretenden complementar los conocimientos que la teoría brinda a los especialistas responsables que participan en los planes de contingencia técnica en sus trabajos.

4) La resiliencia es la característica más importante que las organizaciones deben impulsar en sus especialistas encargados de las BCP. Adicionalmente el personal encargado del despliegue de los diferentes planes de emergencia y continuidad debe contar con la preparación técnica y experiencia necesaria para afrontar situaciones que pongan en riesgo activos tecnológicos, físicos y sobre todo el recurso humano.

5) Teniendo en cuenta que las experiencias profesionales y la capacitación específica son de vital importancia para responder a eventos de contingencia, incidentes de seguridad, desastres naturales o actos de terrorismo las organizaciones están en la obligación de asegurar que todo el personal que las conforma, cuente con habilidades para brindar primeros auxilios en caso de una emergencia médica, accidente laboral o calamidad derivada de un desastre natural o incidente de oren público, ya que la primera línea de atención es salud humana y esta no debe ser opacada por cualquier procedimiento técnico del que seamos responsables; una vez el recurso humano cuente con los recursos físicos, psicológicos y tecnológicos requeridos para responder a un evento catastrófico, se pueden desplegar todos los planes de contingencias profesionalmente diseñados para asegurar la supervivencia del negocio en el sector económico al que pertenece y bajo el que cumple su responsabilidad social.

REFERENCIAS

[1] ICONTEC, Norma técnica colombiana NTC-ISO-IEC 27001. Bogotá D.C., 2013, pp 15-23.

[2] Policía Nacional de Colombia, Dirección de Investigación Criminal e INTERPOL “Amenazas del Cibercrimen en o Colombia 2016-2017” [en línea] Disponible en: https://caivirtual.policia.gov.co/contenido/informe-amenazas-del-cibercrimen-en-colombia-2016-2017

[3] Swanson M, Bowen P, Wohl Amy, GallupDean, Lynes D. Contingency Planning Guide for Federal Information Systems (NIST Special Publication 800-34),” U.S. Department of Commerce, National Institute of Standards and Technology May 2010 Rev 1 pp. 15–64.

[4] U.S. Department of Homeland security, “DHS Risk Lexicon” septiembre de 2008 [en línea] Disponible en: https://www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf

Autor
Hollman Andrés Suescún Méndez
Ingeniero de Sistemas
Técnico en electricidad y electrónica.
MSCA Windows Server 2012.
ORACLE Solaris 11 System Administrator.
Certificado en ITIL Foundation Examination.
Check Point Certified Security Administrator (CCSA)