CONTINUIDAD DEL NEGOCIO

Rodríguez Pinilla, Oscar Javier

Oscar.rodriguez.pinilla@gmail.com
Universidad Piloto de Colombia.

Abstract— *This document describes general concepts, details the behavior of its elements and the deepening of the basic components of business continuity, highlighting the benefits and importance of this in organizations, showing statistics that show organizations that Threats are there and that these can materialize in any type of company, the best method of defense is to be prepared and although the company has the best controls and risk mitigation policies there is always the possibility that this is materialized in the organization and Before this we must be clear how to act.*

Resumen— *En este documento se describen conceptos generales, se detalla el comportamiento de sus elementos y la profundización de los componentes básicos de la continuidad del negocio, exaltando los beneficios y la importancia de este en las organizaciones, mostrando estadísticas que le demuestran a las organizaciones que las amenazas están ahí y que estas se puedan materializar en cualquier tipo de compañía. El mejor método de defensa es estar preparados, aunque en la compañía tenga los mejores controles, políticas de mitigación de riesgo, siempre existe la posibilidad que este sea materializado en la organización y ante esto hay que tener claro cómo actuar.*

Keywords— *BIA bussines impact analysis, RTO recovery time objective, RPO recovery point objective, DRP disaster recovery plan, BCP business continuity plan, SDO service delivery objective, maximum tolerable cut, interruption window, hot site, warm sites, cold site, Maximum tolerable cuts, RAID redundant array of independent disks, CIO chief information officer.*

Palabras claves— *BIA análisis de impacto al negocio, RTO objetivo de tiempo de recuperación, RPO punto objetivo de recuperación, DRP plan de recuperación de desastres, BCP plan de continuidad del negocio, SDO objetivo de prestación de servicios, cortes máximos tolerables, ventana de interrupción, sitio caliente, sitios cálidos, sitio frío, cortes máximos tolerables, raid matriz redundante de discos independientes, CIO jefe de oficina de información.*

I. INTRODUCCIÓN

Los avances tecnológicos se presentan a diario, las empresas deben ir a la vanguardia de estos para abarcar las necesidades de la industria, en los últimos años la sociedad le ha dado trascendencia a la información, por lo que hoy se puede definir como de vital importancia para una organización independientemente su actividad económica. En la actualidad las empresas están expuestas a un gran número de riesgos informáticos; esto lleva a que las áreas de la tecnología realicen un trabajo reiterativo por proteger su integridad, confidencialidad y disponibilidad.

Dentro de la gestión del riesgo el ítem más importante es tener continuidad del negocio, puesto que el riesgo se puede minimizar, pero no desaparecer, la continuidad del negocio busca amortiguar en lo posible ese riesgo, ya sea residual, el que se deriva de un control débil o mal gestionado.

Según los datos reportados en accounting software, describen las causas de la pérdida de datos, las cuales se relacionan en la siguiente imagen.

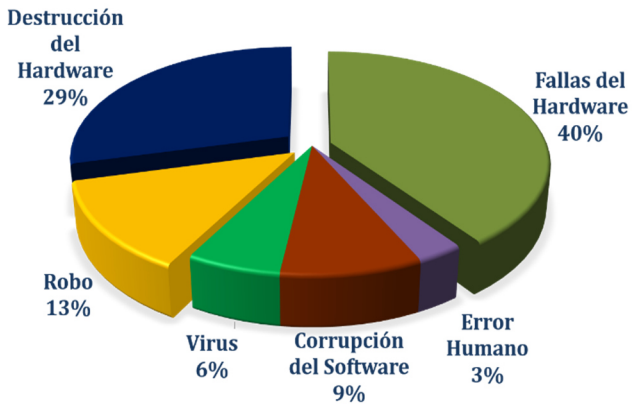

Figura 1. Porcentaje pérdida de datos [1].

Otra estadística realizada y publicada por la Boston Computing Network menciona lo siguiente:

- 6% Las PC'S sufren algún evento de pérdida de datos en cualquier año.
- 30% de todas las empresas que tienen un gran incendio se queden fuera del mercado en un año.
- El 31% de los usuarios de PC'S han perdido todos sus archivos debido a eventos fuera de su control.
- 34% De las empresas no logran probar sus copias de seguridad en cinta, y de las que sí lo hacen, el 77% han encontrado problemas en éstas.
- 60% De las empresas que pierden sus datos cerrarán dentro de los siguientes 6 meses después del desastre.
- Las empresas que no son capaces de reanudar sus operaciones dentro de los diez días siguientes de un desastre, no es probable que sobrevivan.
- Cada semana 140,000 discos duros dejan de funcionar en los Estados Unidos y la recuperación de cada unidad puede ser bastante costosa y no se garantiza el funcionamiento [2].

Estas estadísticas muestran lo vulnerable y susceptible a perder datos, servicios y aplicaciones críticas si no se toman las medidas de protección pertinentes.

II. DESARROLLO DEL TEMA

El primer paso para una adecuada continuidad del negocio lo da el BIA (bussines impact analysis), en el cual se identifican, analizan y se priorizan los tipos de impacto; estos pueden ser (económico, de imagen empresarial, de cumplimiento, entre otros) de acuerdo con las funciones de la organización. El objetivo principal del BIA es construir una base con los procesos de alta criticidad para la organización dándole una priorización.

La clasificación de las operaciones y procesos de la organización se puede dar de la siguiente manera.

Crítico
Estas funciones no pueden realizarse a menos que sean reemplazadas por capacidades idénticas. Las aplicaciones críticas no pueden ser reemplazadas por métodos manuales. La tolerancia a la interrupción es muy baja. Por lo tanto, el costo de la interrupción es muy alto.

Vital
Estas funciones pueden realizarse manualmente sólo por un período breve de tiempo. Hay mayor tolerancia a la interrupción que con los sistemas críticos, por lo tanto, los costos de interrupción son un poco más bajos considerando que las funciones son restauradas dentro de un marco de tiempo determinado.

Sensible
Estas funciones se pueden realizar manualmente, a un costo tolerable y por un período prolongado de tiempo. Aun cuando se pueden realizar manualmente, por lo general es un proceso difícil y requiere de personal adicional para llevarlas a cabo.

No Sensible
Estas funciones pueden ser interrumpidas por un período prolongado de tiempo, a un costo muy pequeño o nulo para la compañía que requiere de poco o ningún esfuerzo para ponerse al día cuando son restauradas.

En el BIA se realiza una evaluación de los procesos y sistemas del negocio, con el objetivo de identificar:

- Áreas, funciones y/o procesos sensibles a interrupciones.
- Interdependencia entre procesos internos y externos.
- Impactos financieros de las interrupciones.
- Impactos operacionales de las interrupciones.
- Sistemas de información críticos para la operación.
- Clientes y proveedores críticos de la organización.
- Recursos necesarios para la recuperación de operaciones.
- Épocas críticas para la operación del negocio.

Dentro del análisis se estiman los recursos para aquellos procesos misionales más críticos y vitales, para ello se define un RTO (objetivo de tiempo de recuperación) en el cual define el tiempo máximo tolerable dentro del cual se recuperan datos, si se produce un desastre en el RTO se tolera tiempo, pero no se permite que haya alguna pérdida de datos [3]. Y un RPO (punto objetivo de recuperación) hace referencia al volumen de datos en riesgo de pérdida que la organización considera tolerable [4]. Esto indica el punto más anticipado en el tiempo al cual es aceptable recuperar los datos. Por ejemplo, si el proceso puede permitir perder los datos hasta cuatro horas antes del

desastre, entonces la última copia de respaldo debería ser hasta cuatro horas antes del desastre o de la interrupción y, por tanto, las transacciones durante RPO y la interrupción deberán ser ingresadas después de la recuperación.

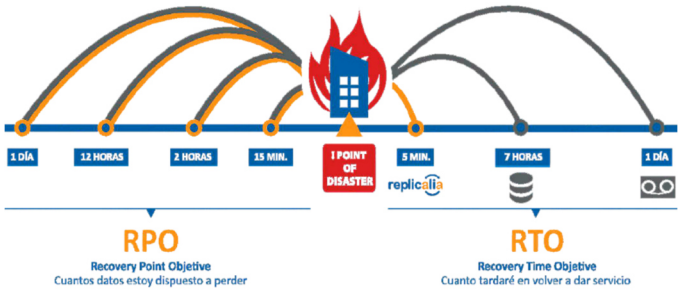

Figura 2. Escalas de rpo y rto [5].

Cuanto más bajo sea el tiempo de recuperación requerido, más elevado será el costo de las estrategias de recuperación. Adicional de RTO y RPO hay otros ítems importantes para definir.

- Ventana de interrupción: El tiempo que una organización puede esperar, desde el punto de falla, hasta la restauración de servicios/aplicaciones críticas. Después de ese tiempo, las pérdidas progresivas causadas por la interrupción no son aceptables.
- Objetivo de prestación de servicios (SDO): El nivel de servicios a proveer durante el modo de proceso alterno, hasta que se restaure la situación normal. Esto está directamente relacionado con las necesidades del negocio.
- Cortes máximos tolerables: El tiempo máximo que la organización puede soportar procesar en modo alterno.

La siguiente tabla muestra una forma simple de clasificar las aplicaciones y servicios en función del RTO y RPO.

- Nivel 1: Aplicaciones o servicios responsables de la generación de ingresos de la organización (Color verde, impacto alto).
- Nivel 2: Aplicaciones o servicios que tienen importancia, pero no impactan de manera sensible las operaciones core de la organización (Color morado, impacto moderado).
- Nivel 3: Aplicaciones o servicios de monitoreo y administración de TI (Color amarillo, impacto leve).
- Nivel 4: Aplicaciones o servicios de ambientes de calidad, desarrollo o pruebas (Color celeste, impacto bajo).

		RTO			
		TIER # 1 APPS < 15 MIN	TIER # 2 APPS < 1 HORA	TIER # 3 APPS < 4 HORAS	TIER # 4 APPS < 24 HORAS
RPO	P1 < 15 MIN				
	P2 < 1 HORA				
	P3 < 2 HORAS				
	P4 < 12 HORAS				

	Aplicaciones criticas de las cuales dependen de forma directa la generacion de ingresos
	Aplicaciones importantes, sin embargo no impactan de forma directa la generación de ingresos
	Aplicaciones de gestión, administración y monitoreo de la plataforma informatica
	Aplicaciones propias de ambientes de desarrollo, pruebas y aseguramiento de calidad

Figura 3. Tabla clasificación aplicaciones y servicios [6].

Teniendo el RPO y el RTO claramente definidos, se debe realizar un plan de recuperación de desastres DRP (disaster recovery plan) también conocido como BPC o BPCP plan de continuidad del negocio o de procesos del negocio, en el cual se describe como la organización debe actuar ante la posibilidad de la explotación de una amenaza o desastre los cuales impiden el funcionamiento normal de la operación de la organización, un plan de recuperación de desastres, se compone de todas las precauciones instauradas para minimizar al máximo los efectos que pueden traer la materialización de una amenaza o de un desastre y la organización pueda restablecer lo más rápido posible las funciones críticas de la organización.

El plan de recuperación de desastres ha evolucionado en el tiempo convirtiéndose en un aspecto cada vez más fundamental debido a la complejidad de los sistemas actuales y a la vital importancia de estos en las organizaciones, el DRP no es una fórmula estándar aplicable por igual a todas las compañías este varía de

acuerdo con el tipo del negocio, procesos involucrados y nivel de seguridad deseado.

"A pesar del número de desastres conocidos desde el 9/11, sólo el 50% de las empresas informan que tienen un plan de recuperación de desastres. De aquellos que sí lo tienen, casi la mitad nunca han puesto a prueba su plan, lo que equivale a no tener ninguno"[7].

En las organizaciones no solo es importante tener un plan de recuperación de desastres, también es fundamental realizarle pruebas a este para garantizar el funcionamiento del DRP y asegurar a la organización que los procesos o aplicaciones críticas del negocio se podrán restablecer en el tiempo previsto en los objetivos de los RPO y RTO.

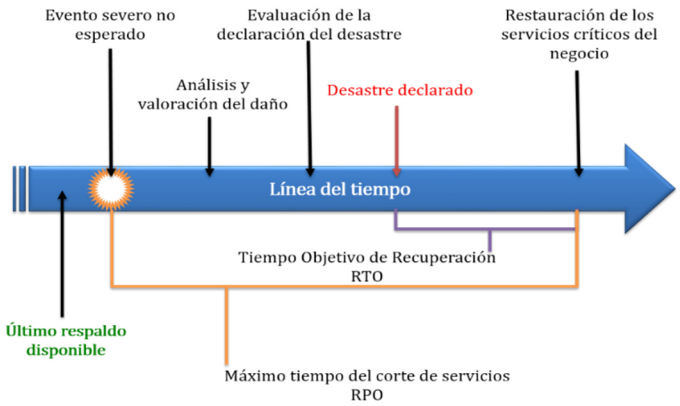

Figura 4. Línea de tiempo DRP [8].

Para la implementación de un DRP se deben seguir las siguientes fases (Análisis, diseño, capacitación, pruebas y recuperación). En el análisis se toman los datos recopilados en el BIA y los objetivos trazados en el RTO y RPO. En el diseño se plantea una solución de acuerdo con los datos y tiempos recolectados en la fase de análisis, documentar esta, asignar responsables de cada proceso, capacitar a los empleados encargados de restablecer los procesos de la organización, se establecen tácticas de comunicación en toda la organización para fomentar la cultura de seguridad en esta. A las posibles soluciones planteadas se les debe realizar pruebas para validar la efectividad de estas y hacer las posibles modificaciones en las fallas encontradas, en la fase de recuperación se ejecuta la solución planteada en la fase de diseño y se realiza un reporte con los resultados de este.

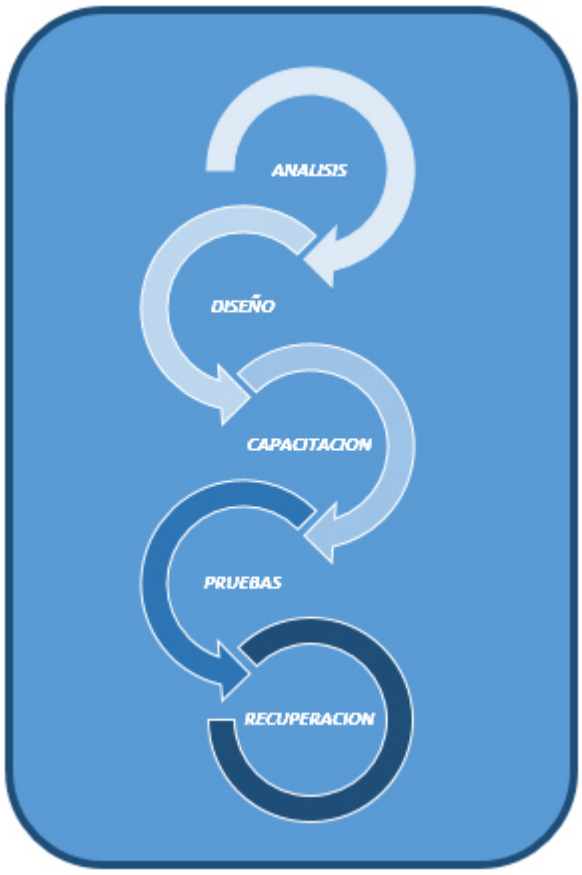

Figura 5. Fases del plan de recuperación de desastres [8].

III. ALTERNATIVAS DE RECUPERACIÓN

Las interrupciones de los servicios y aplicaciones más prolongadas, por ende, tienen un alto costo, particularmente las que afectan a las instalaciones físicas core de la organización, las alternativas de recuperación a estas requieren la disponibilidad de un sitio alterno al primario (offsite), para estos se destacan los siguientes tipos.

HotSite

Se configuran totalmente y están listos para operar dentro de varias horas. El equipo, red y software del sistema deben ser compatibles con la instalación primaria que está siendo respaldada. Las únicas necesidades adicionales son el personal, programas, archivos de datos y documentación. Los costos asociados con el uso de un hotsite de terceros por lo general son elevados, pero más bajos que crear un sitio redundante y con frecuencia son costos justificables para aplicaciones críticas. El hotsite está destinado para operaciones de emergencia durante un período limitado de tiempo y no para uso prolongado [9].

Warm Sites
Estos están parcialmente configurados, por lo general con conexiones de red y equipo periférico seleccionado, como, por ejemplo, unidades de discos y otros controladores, pero sin la computadora principal. Algunas veces un warm site está equipado con una CPU menos potente que la que se usa generalmente. El supuesto detrás del concepto warm site es que la computadora puede por lo general obtenerse rápidamente para una instalación de emergencia y como la computadora es la unidad más cara, dicho acuerdo es menos costoso que un hot site [9].

Cold Site
Es un edificio vacío equipado con energía eléctrica, aire acondicionado, conexiones telefónicas, el agua, etc, pero sin computadoras, equipo de oficina y muebles. Un sitio frío ofrece una respuesta menos oportuna a un desastre porque debe convertirse en un hot-site para su uso [10].

Sitios móviles
Son como una especie de "remolque" especialmente diseñado para ser transportado rápidamente a un lugar de negocio o a un sitio alterno para proveer una instalación acondicionada y lista para el procesamiento de información [9].

Acuerdos con otras organizaciones
Este es un método usado con menos frecuencia entre dos o más organizaciones con equipos o aplicaciones similares. Bajo el acuerdo típico, los participantes prometen proveerse mutuamente tiempos de computadoras cuando surja una emergencia [9].

Para equipos de telecomunicaciones dentro de las estrategias usadas para la prevención de desastres en red incluyen:

Direccionamiento alternativo
Método para direccionar información a través de un medio alterno como, por ejemplo, cable de cobre o fibra óptica. Esto involucra el uso de distintas redes, circuitos o puntos si la red normal no estuviera disponible [9].

Direccionamiento diversificado
El método de encaminar el tráfico a través de instalaciones divididas de cable o instalaciones duplicadas de cable. Esto se puede lograr con fundas de cables diferentes y/o duplicados. Si se usan fundas diferentes de cables, el cable puede estar en el mismo conducto y por lo tanto sujeto a las mismas interrupciones que el cable al que está respaldando [9].

Diversidad de red de largo alcance
Software de re direccionamiento automático y líneas redundantes que proveen recuperación instantánea si ocurriera un corte en sus líneas [9].

Para mejorar la tolerancia a fallos en almacenamiento se opta por configurar arreglos redundantes de discos independientes (RAID) estos se pueden configurar por niveles de acuerdo con la cantidad de discos y a la necesidad de la organización.

Nivel 0
Arreglo de discos con datos distribuidos sin tolerancia a fallas: Mejora el desempeño creando lo que parece ser un disco entre varios manejadores de disco separados físicamente.

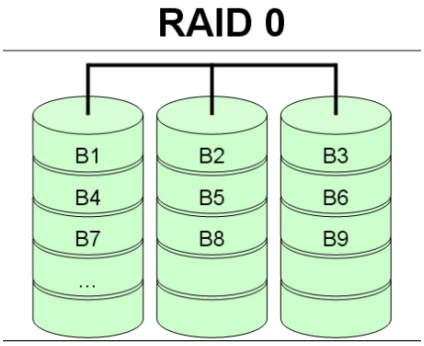

Figura 6. RAID 0 [11].

Nivel 1
Mirroring, Permite que una copia exacta de información en un área de disco, sea copiada a otra. Una vez establecidos, los datos grabados en el disco también se graban en el espacio libre de la otra mitad del disco espejo.

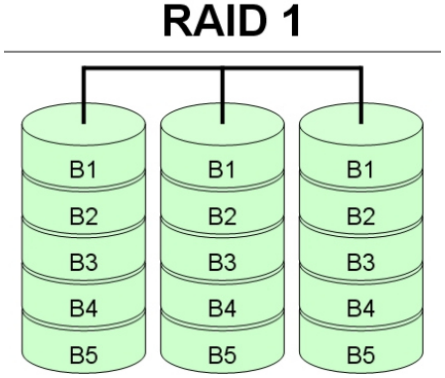

Figura 7. RAID 1 [11].

Nivel 2
Cifrado de curva elíptica con código de hamming (ECC): Es el proceso de intercalar datos en múltiples drives incluyendo información de paridad creada usando la técnica del código de hamming.

Nivel 3
Transferencia paralela con paridad: usa paridad a nivel de byte en dispositivos (drives) dedicados y datos de usuario distribuidos a través de los múltiples dispositivos.

Nivel 4
Discos de datos independientes con bloques de paridad compartida: Similar al nivel 3 pero usa paridad a nivel de bloque y disk striping, en vez de byte dentro de un bloque.

Nivel 5
Discos de datos independientes con bloques de paridad distribuida: Hace una distribución tanto de los datos, como de la información de paridad entre los múltiples discos a nivel de bloque.

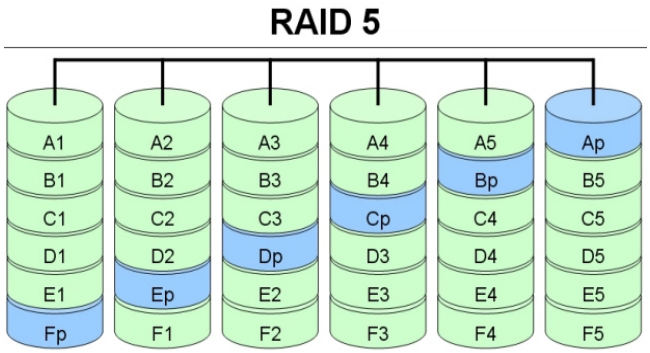

Figura 8. RAID 5 [11].

IV. INTERRUPCIONES Y DESASTRES

Estos ocasionan que los procesos y aplicaciones críticas de la organización queden inoperantes durante un lapso de tiempo, impactando negativamente las operaciones de la organización, estas pueden tardar desde minutos hasta meses dependiendo la extensión del daño.

Un desastre puede ser por causas naturales como (terremotos, inundaciones, tornados, tormentas eléctricas, incendios), los cuales causan daño a las instalaciones de TI de la organización o al área en donde se encuentra la organización y se pueden categorizar de la siguiente forma:

Categoría 1
Esta categoría incluye escenarios que sólo afectan a la organización y por tanto la entidad debe ser responsable de hacer frente al incidente por sus propios medios (una falla de un equipo de comunicaciones).

Categoría 2
Esta categoría incluye escenarios en los que la responsabilidad en la reanudación es compartida entre la entidad y otras organizaciones, dentro del marco legal existente (un corte prolongado de energía eléctrica).

Categoría 3
Hace referencia a situaciones extremas que por su elevada magnitud podrían provocar situaciones legales de excepción, tales como un estado de emergencia nacional (desastre natural, pandemia).

Los eventos de interrupción de servicios proporcionados por terceros y de los más comunes que son causados por seres humanos involuntariamente o precipitadamente como hackers, virus ataques físicos provocados.

Causas de interrupciones del sistema

- Ausencia de personal: cuando un funcionario o el contratista no puede asistir a desarrollar las actividades del cargo.
- No acceso al sitio de trabajo: se presenta cuando el funcionario por algún evento externo no puede asistir al sitio de trabajo (huelgas, paros, fallos de transporte).
- Caída de sistemas: cuando el software o hardware falla y hay interrupción de este.

Un buen plan de continuidad del negocio tomará en cuenta todos los tipos de acontecimientos que impacten tanto en las instalaciones de procesamiento de los sistemas de información críticos como las funciones organizacionales normales de operación del usuario final. Para escenarios de peor caso, se requieren estrategias de marcha atrás de corto y largo plazo. Para el corto plazo, se puede necesitar instalación del procesamiento alterno para satisfacer las necesidades operativas inmediatas, como en el caso de un desastre natural mayor. En el largo plazo, para recuperación ante desastres, se debe considerar una nueva instalación permanente, equipada para proveer la continuidad del

servicio de procesamiento de los sistemas de información de manera regular.

El Instituto de Continuidad del Negocio (BCI) en colaboración con la compañía BSI genera reportes anuales (informe horizon scan) que identifican las amenazas a las que se enfrentan las organizaciones de todo el mundo, también mide la resiliencia de los profesionales de la continuidad del negocio, en el estudio participaron 568 empresas de 74 países.

En el 2016 para el horizon scan, las 5 principales amenazas fueron:

- Ataques cibernéticos – 85%.
- Fuga de datos – 80%.
- Cortes no planeados de TI –77%.
- Interrupción del suministro de la red – 57%.
- Actos de terrorismo – 55%.

Según el informe horizon scan del 2017 publicado en febrero del año en curso, arroja los siguientes datos acerca de las interrupciones y amenazas. Para el 2017 participaron 726 organizaciones de 79 países [12].

Top 10 threats \ Las 10 principales amenazas

1. Cyber attack \ Ataque cibernético.
2. Data breach \ Violación de datos.
3. Unplanned it and telecom outage \ Desconexión no planificada de TI y telecomunicaciones.
4. Security incident \ Incidente de seguridad.
5. Adverse weather \ Clima adverso.
6. Interruption to utility supply \ Interrupción a la provisión de servicios públicos.
7. Act of terrorism \ Acto de terrorismo.
8. Supply chain disruption \ Interrupción de la cadena de suministro.
9. Availability of talents/key skills \ Disponibilidad de talentos / habilidades clave.
10. New laws or regulations\ Nuevas leyes o reglamentos.

Top 10 disruptions \ Las 10 principales interrupciones

1. Unplanned it and telecom outages \ Pérdidas no planificadas de TI y telecomunicaciones.
2. Adverse weather \ Clima adverso.
3. Interruption to utility supply \ Interrupción a la provisión de servicios públicos.
4. Cyber attack \ Ataque cibernético.
5. Security incident \ Incidente de seguridad.
6. Transport network disruption \ Interrupción de la red de transporte.
7. Availability of talents/key skills \ Disponibilidad de talentos / habilidades clave.
8. Supply chain disruption \ Interrupción de la cadena de suministro.
9. Data breach \ Violación de datos.
10. New laws or regulations \ Nuevas leyes o reglamentos.

Top 10 trends \ Las 10 principales tendencias

1. Use of internet for malicious attacks \ Uso de Internet para ataques maliciosos.
2. Influence of social media \ Influencia de las redes sociales.
3. Loss of key employee \ Pérdida de empleado clave.
4. New regulations and increased regulatory scrutiny \ Nuevas regulaciones y mayor escrutinio regulatorio.
5. Prevalence and high adoption of internet dependent services \ Prevalencia y alta adopción de servicios dependientes de Internet.
6. Political change \ Cambio político.
7. Increasing supply chain complexity \ Aumento de la complejidad de la cadena de suministro.
8. Potential emergence of a global pandemic \ Emergencia potencial de una pandemia mundial.
9. Changing consumer attitudes and behaviour \ Cambiar las actitudes y el comportamiento de los consumidores.
10. Slow economic growth and its impact on investment \ Crecimiento económico lento y su impacto en la inversión.

El reporte arroja las siguientes conclusiones;
(69%) Más de 2 de cada 3 organizaciones incluirán como parte de su análisis el top de tendencias incluido en el horizon scan.

(21%) 1 De cada 5 organizaciones aumentará su presupuesto para la continuidad del negocio en 2017.

(63%) Más de 2 de cada 3 organizaciones utilizan ISO 22301 para orientar su programa de continuidad de negocio.

V. PRUEBAS Y MANTENIMIENTO

Se deben realizar pruebas al plan de continuidad del negocio definido para corroborar el buen funcionamiento de este, garantizando que la

organización entienda como debe ser ejecutado y validar en cuales etapas requiere mejoras o plantearlas nuevamente, las pruebas deben ser programadas con el fin de interrumpir o afectar lo mínimo las operaciones de la organización.

"No se debe olvidar que quizás lo más importante de un BPC es que sea probado. De nada sirve tener los mejores servidores de respaldo si al momento de restablecer los servicios críticos, estos no funcionan; o tener un canal de datos dedicado si no se lo puede restablecer a tiempo, o peor aún, tener funcionales los servicios del negocio dejando vulnerable la información de la empresa" [13].

En las pruebas se debe verificar:

- Desempeño del plan y del personal involucrado.
- Capacitación, concientización y coordinación de personal interno y terceros si se requieren.
- Medir tiempos de respuesta del plan y del personal.
- Medir el desempeño de las actividades, sistemas, procesamiento entre otros.
- Documentar los resultados exaltando los puntos a mejorar.
- En la documentación se debe detallar tiempo, cantidad y exactitud.

El mantenimiento del plan de continuidad del negocio debe ser periódico y tener un responsable, por lo general en las organizaciones el responsable es el CIO (chief information officer) dentro de las actividades de mantenimiento se encuentran las siguientes.

- Desarrollar el plan periódico de revisión y pruebas del plan y publicarlo en la organización
- Exigir revisiones no formales cuando la plataforma de TI sea modificada o alterada significativamente, como las siguientes:
    - Adquisición de equipos nuevos.
    - Actualizaciones de sistemas.
    - Actualización de aplicaciones.
    - Cambios de personal.
    - Estrategia del negocio.
    - Cambios en las ubicaciones físicas.
- Participar en las pruebas programadas del plan.
- Realizar programa de concientización al personal.

A continuación, una descripción de los tipos de pruebas a realizar al plan de continuidad del negocio:

1. Revisión estructurada del plan.
2. Prueba de la lista de verificación.
3. Simulaciones.
4. Prueba en paralelo.
5. Prueba de interrupción completa.

VI. BUENAS PRÁCTICAS EN CONTINUIDAD DEL NEGOCIO

Algunas de las entidades o institutos que nos pueden ayudar con mejores prácticas en el desarrollo de planes de continuidad de negocio son:

BCI

El Business Continuity Institute (BCI) es el instituto líder en el mundo para la continuidad del negocio, establecido en 1994, la asociación BCI, a través de la membresía corporativa, ofrece a las organizaciones la oportunidad de trabajar con el instituto para promover las mejores prácticas en continuidad de negocios y aumentar su perfil corporativo en el ámbito global de BC. Tiene como meta fortalecer el papel de BCI como "el líder global del pensamiento" para la continuidad y la resiliencia.
www.thebci.org

DRII

Promueve una base conocimiento común en la continuidad del negocio y de recuperación planificada ante desastres en las organizaciones de cualquier tamaño y sector de actividad industrial a través de la educación, la asistencia y la publicación de recursos y estándares fundamentales. El DRI coopera adicionalmente con el sector público y privado para promover las mejores prácticas profesionales.
www.drii.org

COBIT

(Control objectives for information and related technology), es el marco aceptado internacionalmente como una buena práctica para el control de la información de TI y los riesgos que conllevan. COBIT se utiliza para implementar el gobierno de IT y mejorar los controles de TI. Contiene objetivos de control, directivas de aseguramiento, medidas de desempeño y

resultados, factores críticos de éxito y modelos de madurez.
www.isaca.org/COBIT/Pages/default.aspx

ISO 27001
Es una norma internacional emitida por la organización internacional de normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.
www.iso.org

ITIL
Aboga por que los servicios de ti estén alineados con las necesidades del negocio y apoyen sus procesos centrales. Proporciona orientación a organizaciones e individuos sobre cómo utilizar la TI como una herramienta para facilitar el cambio, la transformación y el crecimiento del negocio.
La mejora de la gestión de servicios de TI de ITIL está respaldada por un esquema de certificación que permite a los profesionales demostrar sus habilidades en la adopción y adaptación del marco para atender sus necesidades específicas.
www.axelos.com/best-practice-solutions/itil

ISO 22301
Especifica los requisitos para un sistema de gestión encargado de proteger a su empresa de incidentes que provoquen una interrupción en la actividad, reducir la probabilidad de que se produzcan y garantizar la recuperación de su empresa.
La norma pretende implantar un sistema integral de gestión de la continuidad del negocio que mantenga de forma continuada un proceso integral y sistemática de:

- Prevención.
- Protección.
- Preparación.
- Mitigación.
- Respuesta.

www.iso.org/standard/50038.html

NIST SP 800-34
Guía de planificación de contingencias para sistemas de tecnología de información (IT), se publicó por primera vez en junio de 2002, y proporciona instrucciones, consideraciones para la planeación de contingencia de TI del gobierno. Aunque diseñado para sistemas federales, el NIST SP 800-34 se ha utilizado como guía para la planificación de contingencias en gran parte del sector privado.
www.csrc.nist.gov

VII. CONCLUSIONES

La implementación del plan de continuidad del negocio debe realizarse con el apoyo de la dirección general de la organización, para facilitar el cumplimiento de los objetivos trazados.

El plan de continuidad del negocio debe evolucionar de acuerdo con la variación de tecnología o procesos de la organización, este no debe permanecer estático, se debe probar cíclicamente, replanteándolo en caso de encontrar fallas para que cumpla a satisfacción con lo requerido por la organización.

La falta de un plan de continuidad del negocio puede causar severos impactos financieros, buen nombre, disminución de clientes a la organización que muchas no están preparadas para asumir.

En la mayoría de empresas tienen la falsa creencia que el backup es un plan continuidad del negocio, cuando en realidad un backup es solamente una copia de datos, por tanto, no garantiza que las operaciones core de la organización en caso de desastre puedan restablecerse y así continuar con sus operaciones de manera normal.

El plan de continuidad del negocio debe estar alineado con los requisitos de la organización para que este perdure a lo largo del tiempo.

"El único sistema seguro es aquel que está apagado y desconectado" Gene spafford, científico de la computación.

VIII. REFERENCIAS

[1].The balance, Reseña e información de software, disponible en www.thebalance.com.
[2].Boston computing network, estadistica de pérdida de datos, disponible en www.bostoncomputing.net.
[3].Symantec, glosario respuesta de seguridad, disponible en www.symantec.com.
[4].Software greenhouse, conceptos de continuidad del negocio, disponible en www.swgreenhouse.com.
[5].Replicalia, continuidad del negocio como servicio, disponible en www.replicalia.com.
[6].VMware, recuperación de desastres informáticos, disponible en www.vmware.com.

[7].Datacenter, plan de recuperación de desastres, disponible en www.searchdatacenter.techtarget.com.
[8].Albe, beneficios de implementar un DRP, disponible en www.grupoalbe.com.
[9].Bsc, estrategias de seguridad, disponible en www.bscconsultores.cl.
[10].Bd, definiciones, disponible en www.businessdictionary.com.
[11]. Recuperación de datos, términos de RAID, disponible en www.recuperaciondedatos.com.
[12].BSI-BCI, informe anual horizon scan 2017 continuidad de Negocio, disponible en www.bsigroup.com.
[13]. Eset, como responder ante una contingencia, disponible en www.welivesecurity.com.