Plan de Continuidad de Negocio Como Base del Éxito Organizacional

Mora Yomayuza David Felipe
Bogotá
Universidad Piloto de Colombia
david.morayz@gmail.com

Abstract- ***The Business Continuity Plan is the first recovery system in an organization against threats and security events. Currently, the guide of normativity and the best practices are fundamental aspects to develop a business continuity plan. According to this, we define a methodology to design and develop a business continuity plan based on the important role in an organization of any economic activity and size. Finally, we identified the main features of BCP, although nowadays it is not considered as a relevant implementation inside of a organization***

Keywords- business, risk, impact, threat, security,

Resumen- **El plan de continuidad de negocio se considera la primera arma de defensa para una organización ante cualquier tipo de incidente que se presente ya que permite restaurar los procesos más críticos ante cualquier interrupción. La normatividad y guías de buenas prácticas son aspectos importantes a tener en cuenta para el desarrollo de cualquier plan de continuidad, finalmente como resultado de este trabajo se habla de la importancia de su implementación, y se definen pasos básicos para el desarrollo y diseño de un plan para cualquier organización sin importar su tamaño o actividad económica. Se concluye que un plan de continuidad es de vital importancia para las organizaciones, aunque en la actualidad no es visto como una necesidad**

Palabras Claves- activos, seguridad, informática, amenaza, riesgo continuidad

I. Introducción

En la actualidad la información es llegada a considerar como uno de los activos o recursos más valiosos e importantes para cualquier tipo de organización sin importar su actividad económica, de esta depende la prestación de sus servicios, así como decisiones vitales para la organización, compras, gestión de proveedores todo depende de información, por esta razón es importante garantizar que esta se encuentre bajo los tres pilares de la seguridad de la información, los cuales son la integridad, confidencialidad y la disponibilidad de la información y de los sistemas de información que hagan uso de la misma para el momento de almacenar y procesar la información sea cual sea el método se deben adoptar estrategias y políticas que aseguren la información [1].

El siguiente articulo presenta un análisis de los beneficios y aspectos importantes que brinda para una organización el diseñar e implementar un plan de continuidad de negocio, como lo es la identificación de procesos críticos de la organización, así como las amenazas y riesgos a los que están expuestos todo esto de la mano de los objetivos misionales de la organización, con un único objetivo que es el de continuar con la prestación de los procesos y servicios de la organización reduciendo el impacto lo máximo posible.

II. Preliminares

Plan de Continuidad del Negocio*:* BCP por sus siglas en inglés (Bussines Continuity Plan) *"es un documento claro, conciso y detallado que especifica cómo deben actuar las personas y departamentos de la empresa (no solo IT), para responder ante una situación crítica de modo que el impacto para la empresa sea el menor posible" [2].* Otra definición interesante es la que presenta la compañía de seguridad informática ESET donde dice que un ***"BCP*** *debe contemplar las acciones que una empresa debe seguir para* ***recuperar y restaurar las actividades críticas del negocio*** *en un tiempo prudencial y de manera progresiva regresar a la normalidad; garantizando en todo momento la* ***integridad, confidencialidad y disponibilidad*** *de la información" [3].*

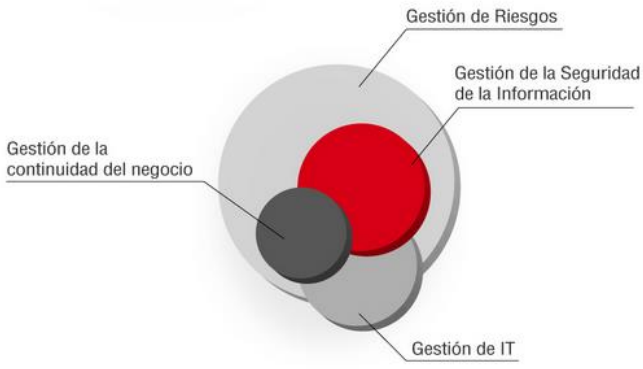

Figura 1. Gestion de la Seguridad de la Informacion[2].

El plan de continuidad de negocio es solo una parte o una herramienta de la seguridad de la informacion, como vemos en la figura 1 es una de las varias formas de gestion de la seguirdad de la informacion, y puede ser usado en conjunto con el Plan de Recuperacion de Desastres (DRP) para un mayor analisis de escenarios [2].

La continuidad de negocio o el desarrollo normal de los procesos en una organización en ocasiones se ve afectado por riesgos que provienen de factores internos y externos, naturales, errores humanos o simplemente por la caída de un servicio como el servicio de internet por parte del proveedor o un corte de energía, en la página de la British Standards Institution, BSI por sus siglas en ingles es una organización que tiene con fin la creación de normas comerciales que ayudan a las organizaciones a mejorar el rendimiento, reducir el riesgo y generar un crecimiento para las organizaciones encontramos un reporte anual realizado en asociación con BCI (Business Continuity Institute) el cual identifica las amenazas que más afectan a las organizaciones en el mundo año tras año[4]

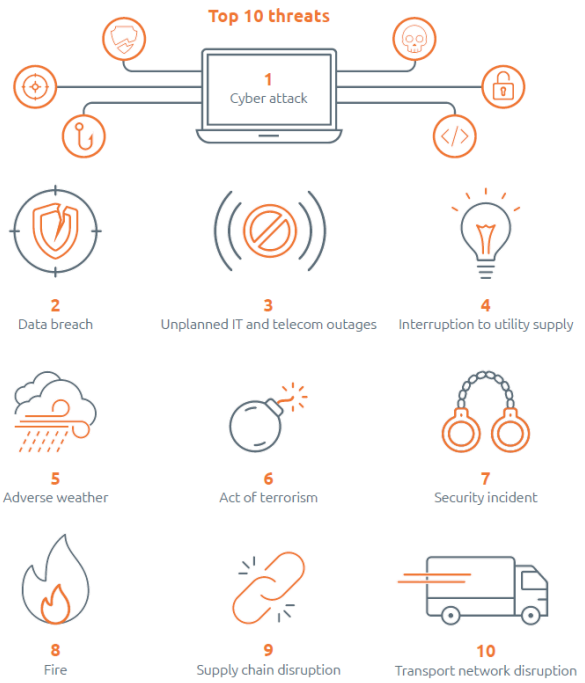

Figura 2. Top 10 de Amenazas segun BCI [5]

De acuerdo a figura 2 se puede ver las 10 amenazas más comunes para las organizaciones, según esto las amenazas se pueden categorizar de la siguiente manera:

Desastres Naturales
- Mal Clima
- Terremotos
- Inundaciones

Accidentales
- Fallas tecnológicas
- Fallas de estructura física
- Explosiones
- Incendios

Intencionales (internos)
- Violación de Datos
- Borrado de Datos

Tecnológicos
- Ataques
- Virus
- Malware
- Pérdida de Información

Es imposible llegar a determinar el número de amenazas que logran afectar la productividad y operación de una organización ya que estas pueden llegar a ser desde una gran catástrofe hasta una pequeña fuga de información por parte de un empleado, colocando en apuros a la organización. Tendiendo en cuenta que los avances tecnológicos no se detienen y a diario están innovando todas las organizaciones deben ir a la par de estos para poder satisfacer las necesidades del mercado, con base en un factor importante en la actualidad y es la información, la cual hoy en día es de vital importancia para cualquier organización sin importar su razón social o actividad económica, lo que hace que el área de tecnología de la organización tenga la necesidad de proteger y brindar un soporte a la organización.
Además, que en la actualidad no solo las personas se preocupan por la protección de sus datos, sino que la legislación ya tiene leyes y directivas que obligan a las organizaciones a cumplir con estas para garantizar la integridad y confidencialidad de la información. El no cumplimiento de estas trae consigo consecuencias desde grandes multas hasta incluso ir a la cárcel.

Por tal motivo es importante contar con una estrategia de prevención con tal de minimizar las consecuencias, la cual es la creación de un BCP efectivo que se pueda probar y desarrollar, así como también debe ser evaluado y periódicamente actualizado con el fin de que el mismo tenga una mejora continua. Un BCP puede ser denominado un aspecto de seguridad preventiva en la gestión de la seguridad de la información.

Se puede resumir que un plan de continuidad de negocio es un modelo o una guia que busca que los procesos, y servicios brindados por una organización continuen prestandose de manera continua y en caso de que exista alguna interrupcion o falla esta sea restablecida en el menor tiempo posible, asi como definir los responsables de este reestablecimiento, con el objetivo de reducir o minimizar el daño producido por estas iterrupciones el no contar con un Plan de Continuidad de Negocio representa mucho más que arriesgar datos e información de la organización que pueden ser comprometidos sino también todo esto representa pérdidas de dinero, tiempo, seguridad y confianza no solo para la organización sino también para los usuarios de la misma, así como también puede afectar la imagen de la organización.

Year	Top five threats
2016	1. Cyber attack 2. Data breach 3. Unplanned IT & telecom outages 4. Act of terrorism 5. Security incident
2017	1. Cyber attack 2. Data breach 3. Unplanned IT & telecom outages 4. Security incident 5. Adverse weather
2018	1. Cyber attack 2. Data breach 3. Unplanned IT & telecom outages 4. Interruption to utility supply 5. Adverse weather

Figura 3. Principales amenazas a las organizaciones a través de los 3 últimos años [5].

Así mismo en este informe se puede ver cuáles son las interrupciones más comunes para las organizaciones, en la figura está el top 5 de las interrupciones más significativas a lo largo de los últimos 3 años. En la figura 4 se pueden ver las 10 más significativas para el año 2018 estas son las interrupciones no planificadas de TI y de telecomunicaciones (67%), el clima adverso (50%) y la interrupción del suministro de servicios públicos (43%). Es interesante ver que los ataques cibernéticos solo ocupan el cuarto lugar (37%) cuando se trata de medir las interrupciones, mientras que son la principal preocupación para los profesionales. Esto es consistente con los resultados del año 2017 y podría deberse al hecho de que los ataques cibernéticos pueden tener un impacto muy alto, como por ejemplo la campaña de ransomware WannaCry que logró afectar a varias organizaciones en todo el mundo. La disponibilidad de talentos / habilidades clave (22%) completa los cinco primeros, a pesar de no ser una de las diez principales preocupaciones para los profesionales en la actualidad, en este reporte participaron 657 organizaciones de 76 países. [5]

Figura 4. Top 10 de Interrupciones segun BCI [5].

Análisis de Impacto del Negocio (BIA) por sus siglas en ingles *Business Impact Analysis*,

El RTO, Objetivo de Tiempo de Recuperación es el tiempo máximo que la organización puede tolerar para la recuperación de los datos en caso de algún evento, es decir este indica el tiempo tolerable en que los servicios o información vuelva a su estado operacional, el otro aspecto vital para el plan de continuidad es el RPO o Punto Objetivo de Recuperación en el cual se establece la cantidad o el volumen de datos que se pueden perder y que la organización está dispuesta a tolerar perder sin que le afecte de gran manera este aspecto está relacionado de manera directa con las copias de seguridad de los datos. [6]

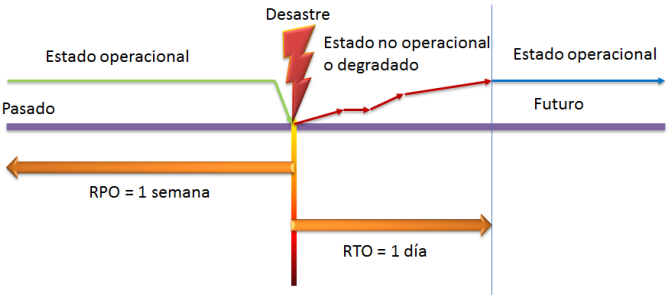

Figura 5. Tiempo Objetivo de Recuperación vs Punto Objetivo de Recuperación [7].

En la figura 5 se ve representado un incidente y la interacción del tiempo y el punto de recuperación. La relación entre el RPO y el RTO es que prácticamente la una depende de la otra ya que el RPO está relacionado con las copias de seguridad para mantener la continuidad del negocio, es importante para determinar la frecuencia con que se realizaran las copias de seguridad. Mientras que el uno habla del tiempo máximo de los datos que deben ser respaldados la otra habla del tiempo máximo que la organización tolera para restablecer sus operaciones. [7].

Es importante tener en cuenta que entre más bajo sea el tiempo establecido del RPO será mucho mayor el costo de los planes adoptados para la recuperación de información ya que estas se deberán realizar más a menudo, así como también la ejecución de pruebas de correcto funcionamiento de las copias de seguridad.

CREACIÓN DE UN BCP

El diseño e implementación varía de acuerdo a la organización, según su tamaño, actividad, muchas guías e incluso páginas en la web definen pasos para el diseño y desarrollo de un BCP, estas varían desde 4 hasta más de 10 pasos como vemos en las tablas 1,2,y 3 donde definen estos pasos:

ESET (4 Pasos)
1. Identifica y ordena las amenazas
2. Realiza un análisis del impacto en la empresa
3. Crea un plan de respuesta y recuperación
4. Prueba el plan y refina el análisis

Tabla 1. Pasos para un BCP definidos por ESET [8].

Foro de Profesionales Latinoamericanos de Seguridad (13 Pasos)

1. Documenta al personal clave y las copias de seguridad.
2. Identifica quien puede trabajar desde casa.
3. Documenta los contactos externos.
4. Documenta el equipo crítico.
5. Identifica documentos críticos.
6. Identifica opciones de equipo contingente.
7. Identifica tu localización contingente.
8. Prepara una guía de "Cómo hacer".
9. ¡Pon toda la información junta!
10. Comunícalo
11. ¡Prueba el plan!
12. Prevé que puede que tengas que cambiar el plan.
13. Revisa y revisa.

Tabla 2. Pasos para un BCP definidos por el foro de Profesionales Latinoamericanos de Seguridad [9].

Foro de Cooperación Económica Asia-Pacífico (12 Pasos)
1. Determinar el Propósito y alcance de tu PCN y selecciona al líder y equipo responsable de llevarlo a cabo
2. Determinar las Actividades Prioritarias de tu empresa y los Tiempos de Recuperación Ideales
3. Determinar qué necesitas para la continuidad de tus Negocios
4. Evaluación de Riesgos- Conozca sus escenarios de riesgos
5. No olvidar protección previa al desastre y métodos de mitigación
6. Respuesta de Emergencia ante el desastre
7. Estrategias para Continuidad de Negocios Temprana
8. Estar preparado financieramente
9. La práctica hace que el plan sea funcional
10. Revisión continua y mejoramiento del Plan

Tabla 3. Pasos para un BCP definidos por el Foro de Cooperación Económica Asia-Pacífico [10].

Existe un sin número de guías, foros y sitios web donde es posible encontrar pasos para la creación de un plan de continuidad, cada uno de estos define

III. Objetivo del plan de continuidad de negocio

Brindar la capacidad a la organización de continuar con los procesos de negocio con normalidad o al menos a un nivel mínimo aceptable en caso de producirse una interrupción o eventos como desastres naturales, manifestaciones sociales, fallas tecnológicas o fallas humanas que afecten o interrumpan los procesos de negocio disminuyendo el impacto ante cualquier incidente.

IV. Beneficios del plan de continuidad de negocio

Un plan de continuidad de negocio trae consigo muchos beneficios para cualquier organización sin importar su tamaño o actividad económica, aunque muchas veces las organizaciones lo ven como un gasto este debería considerarse como una inversión para la organización ya que no se debe ver desde el punto de cuánto cuesta sino cuánto podría llegar a perder la organización en cualquier incidente de estos. [11]

- Mejora y ayuda a mantener una buena imagen de la organización para con sus empleados y sus clientes.
- Eficiencia organizacional, ya que ayuda a establecer, implementar y mejorar los procesos de la organización, ya que brinda un enfoque organizado para las acciones de respuesta y mejora.
- Mantiene la continuidad de negocio y la prestación de productos y servicios brindando así un soporte o una confiabilidad tanto para el negocio como para sus clientes
- Identificación de los activos y recursos más relevantes o importantes para garantizar la prestación de sus servicios.
- Evaluación e identificación de los riesgos a los que está expuesta la organización sus recursos y sus activos.
- Identificación de los servicios más críticos de la organización.
- Brinda una rápida acción de respuesta ante cualquier incidente que se presente en la organización y que afecte el correcto desarrollo de sus procesos.
- Evita la perdida de dinero y costos innecesarios a causa de las afectaciones de los servicios críticos.

V. Resultados

Pasos para la creación de un BCP

Para la realización de un plan de continuidad de negocio de manera correcto se definen al menos los siguientes pasos para su desarrollo, es importante inicialmente definir el alcance de y realizar un análisis de toda la organización con el fin de identificar todos los procesos y recursos críticos que necesita la organización para su correcto funcionamiento.

1. Inventario de activos y recursos de la organización

Primero que todo se debe realizar un inventario de todos los activos de tecnología y recursos que son necesarios e interfieren en el desarrollo de los procesos y prestación de servicios de la organización, así mismo se debe realizar una categorización de los mismos, para establecer cuáles de estos activos o recursos son los más críticos tanto para el desarrollo de las actividades de la organización sino también para establecer el orden de restablecimiento en caso de incidentes. Además de esto se deben establecer las relaciones entre los procesos con el fin de identificar así mismo la dependencia entre los mismos, así como de aplicaciones, sistemas de información e infraestructura TI necesaria.

2. Análisis y Evaluación de Riesgos

Una vez identificados los activos y recursos más críticos de la organización, se procede a realizar un análisis de riesgos con el fin de identificar, analizar y evaluar las amenazas que pueden ocasionar incidentes o interrupciones que afecten la continuidad de negocio, lo importante es identificar el máximo de riesgos a los que se encuentra expuesta la organización, garantizando así que no existan amenazas no evaluadas o identificadas que atenten con los objetivos de negocio de la organización.
Una vez identificadas las amenazas debemos identificar las vulnerabilidades que tiene la organización las cuales son las debilidades que se pueden ser materializadas y convertir las amenazas en un riesgo real que traiga consigo consecuencias desastrosas para la organización.
Una vez identificado los puntos críticos de los procesos y servicios, se deben evaluar todos los escenarios posibles en los cuales la materialización de alguna de las amenazas se convierta en riesgos, de acuerdo a los escenarios se identifican también la existencia de controles existentes para las amenazas identificadas. Todo este análisis debe evaluar los escenarios de peor caso, así como tener en cuenta las amenazas más representativas.

3. Análisis de Impacto del Negocio (BIA)

Luego de realizar la evaluación de riesgo se debe realizar un análisis de impacto del Negocio, BIA el cual es parte fundamental para el desarrollo del BCP, dentro de este análisis es importante la definición de dos aspectos de gran importancia que ayudan al análisis e identificación de la criticidad de los procesos de la organización estos son el RTO (Objetivo de Tiempo de Recuperación) y RPO (Punto Objetivo de Recuperación).

Una vez definidos estos dos aspectos se deberá establecer el impacto tanto de las operaciones de negocio como del impacto financiero para la organización en caso que se presente alguna interrupción. Por lo que se deben establecer los procesos y recursos afectados y las consecuencias que traerá para la organización enfatizando en los procesos críticos para la organización.

Al final del análisis BIA junto con la evaluación de todos los aspectos podemos establecer o dar una prioridad a los procesos de la organización de acuerdo al impacto que este pueda tener, con el criterio básico de que a mayor impacto generado para la organización mayor será su prioridad, es decir que también según su tiempo de recuperación y operación es que se define su criticidad e importancia para la organización y del plan de continuidad de negocio ya que estos procesos serán los que más tendrán relevancia para su restauración y continuidad.
Además de la identificación de los procesos más críticos también están los sistemas de información críticos para la correcta operación, los clientes y proveedores de la organización, los recursos necesarios para el restablecimiento de las operaciones y las épocas más críticas de operación de negocio de la organización [12].

Al final del análisis del BIA debe resultar un informe en el que se encuentren los resultados consolidados de todo este análisis en general así:

- Listado de los procesos críticos de la organización.
- Listado de los recursos críticos de la organización.
- Listado de prioridades de los sistemas de información y aplicaciones de la organización.
- Listado de los tiempos RTO, RPO, de cada uno de los procesos de la organización.
- Impactos financieros y operacionales de las interrupciones.

4. Acciones Correctivas

A medida del desarrollo de un plan de continuidad de negocio, es posible identificar fallas y vulnerabilidades de los sistemas de información o en la ejecución de procesos que tiene la organización, sobre las cuales se pueden ir tomando acciones correctivas para su optimización y mejoramiento.

5. Plan de Acción de Respuesta y Comunicaciones

En el plan de acción de respuesta del BCP se deben proponer inicialmente como utilizar el plan, los procedimientos a desarrollar en caso de incidentes o interrupciones, con el fin de brindar seguridad al personal de la organización en primera medida y así mismo a la información, debe proponer y ejecutar acciones que permitan mitigar el impacto de los riesgos y la probabilidad de que una amenaza sea materializada. Debe estar definido los responsables de las acciones a ejecutar paso a paso de los procedimientos de respuesta que sean propuestos y definidos en el plan para cada uno de los procesos críticos del negocio y los escenarios allí evaluados como por ejemplo el proceso de restauración al punto anterior de un sistema de información, todos los procedimientos y pasos a seguir deben ser claros para evitar realizar procedimientos erróneos que pueden afectar o tener un mayor impacto a la organización. Estas soluciones o acciones de respuesta deben ser acciones posibles y eficaces para las situaciones de emergencia que se presenten y que permitan cumplir el objetivo principal del BCP el cual es retornar las operaciones y servicios de la organización en el menor tiempo posible. Las acciones y procedimientos de respuestas para la continuidad deben depender y tener en cuenta también la criticidad de cada uno de los procesos a restablecer, el costo de la acción o solución, pero sobretodo los tiempos y puntos de recuperación objetivos ya definidos (RPO, RTO).

Otro aspecto importante son los procedimientos de comunicaciones por lo que se debe establecer un ***Plan De Comunicaciones En Eventos De Crisis*** para el momento de presentarse un incidente que represente interrupciones en los procesos de la organización es de vital importancia saber qué hacer, a quien informar y los medios por los que se debe o se tiene para realizar dicha comunicación [13], por lo que en este plan se deben definir aspectos básicos para la comunicación como lo son:

- Canales de comunicación
- Documentación de lo sucedido
- Establecer sistemas de notificación o comunicación

- Identificar y conocer los responsables del BCP
- Generar comunicados preliminares sobre la emergencia y finales.

6. Concientización y capacitación del BCP

Una vez desarrollado un plan de continuidad de negocio el tenerlo no garantiza a la organización que este sea efectivo el restablecimiento de los procesos o aplicaciones críticas del negocio de manera correcta y como se debe ejecutar, por esto es importante delegar a responsables que puedan y tenga la capacidad y competencias necesarias para tomar decisiones y puedan ejecutar el plan de continuidad ante cualquier interrupción es por eso que la capacitación y concientización a todo el personal de la organización es una parte muy importante para que el objetivo de este se cumpla con éxito ya que es necesario que los empleados conozcan del plan y el cómo actuar ante cualquier incidente.
Es importante dentro del plan de continuidad definir un comité o un equipo para que sean estos los responsables y tengan roles definidos para momento de poner en acción el mismo. Así como para definir pequeños equipos que sean encargados de distintos campos o aspectos a desarrollar para la evaluación y desarrollo del plan de continuidad, a continuación, vemos una propuesta de los equipos de continuidad de negocio, cabe notar que es solo una propuesta y que el desarrollo de un BCP cambia para cada organización según las necesidades y procesos que esta tenga [13].

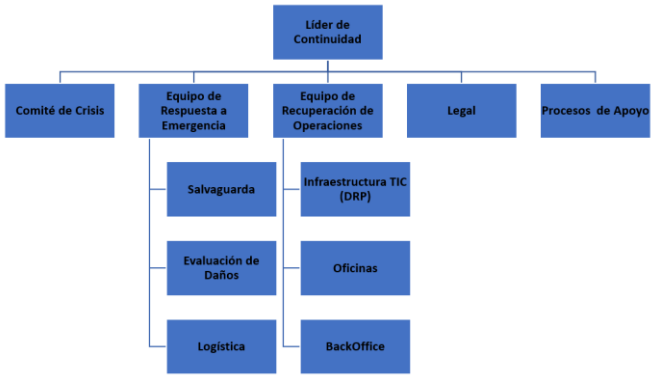

Figura 6. Propuesta de Equipos de Continuidad del Negocio [13]

Dentro de esta propuesta de equipo de continuidad de negocio se establece que debe haber un líder de continuidad el cual tendrá las siguientes funciones responsabilidades:

- Mantener información actualizada de los terceros proveedores críticos de La Organización
- Realizar periódicamente pruebas y ejercicios de los planes de continuidad
- Comunicar al Comité de Crisis la situación de contingencia o crisis presentada.
- Ser el enlace entre los equipos de soporte a la respuesta de emergencia y el equipo de Crisis
- Coordinar la reunión y acciones del Comité de crisis.
- Definir con el Comité de Crisis las comunicaciones a difundir al interior y exterior de La Organización.
- Coordinar y monitorear la fase de respuesta.
- Coordinar la recolección de información sobre el evento.
- Conducir el retorno a la normalidad.

Los demás miembros de equipos tendrán funciones más específicas en la evaluación de los incidentes, equipos de respuesta que se encargan de proteger la información, evaluar los daños, así como equipos encargados de la recuperación o restablecimiento de las operaciones, teniendo en cuenta infraestructura TIC, comunicaciones, oficinas y oficinas alternas para garantizar la continuidad de negocio [13].

7. PRUEBAS "Evaluación, Actualización y Mejora del BCP"

Además de la capacitación y concientización de como emplear el BCP y sus responsables es indispensable realizar pruebas a este plan con el fin de garantizar su funcionamiento y asegurar que los procedimientos allí establecidos corresponden a la realidad de nada sirve tener los mejores dispositivos o herramientas de recuperación o backup si al momento de usarlos estos no funcionan, además que en temas de TI día a día están en continuo evolución por lo que surgen nuevas amenazas, nuevas herramientas que pueden ser usadas para apoyar el BCP de manera más eficaz y efectiva, la aparición de tecnologías emergentes derivadas del desarrollo del internet como la virtualización de infraestructura informática, masificación de comunicaciones móviles.

Dicha virtualización ofrecida por empresas como VMware, Microsoft, Oracle y Google, brindan interfaces con gran facilidad de uso, y altas prestaciones de entornos simulados de distintos sistemas operativos o dispositivos de almacenamiento según la necesidad de cada organización. Esto reduce de manera notable el costo de operación y desarrollo de muchos procesos ya que evita el adquirir un computador por cada sistema operativo que se necesite, sino que en un solo dispositivo se pueden tener varios de ellos para trabajar.

Otra gran herramienta es la nube o computación en la nube la cual permite el procesamiento y almacenamiento de datos los cuales se encuentran alojados en servidores remotos lo que representa la mitigación notable del riesgo a diferencia de tener datacenter locales y propios de la organización, representando otro tipo de vulnerabilidades y amenazas que no se tienen al usar herramientas alojadas en la nube. Además, que esta brinda un fácil acceso a la información y su capacidad de escalabilidad cada que sea necesario. Por ejemplo, durante la creación de Backups de los dispositivos estas copias pueden ser alojadas en servidores virtuales externas lo cual representa la mitigación de la perdida de datos.

Cada que sea puesto a prueba el BCP se debe evaluar su eficacia, y en caso de haber fallas o inconvenientes se deben comunicar al líder de continuidad para el estudio posibles soluciones con el fin de garantizar el restablecimiento de los procesos más críticos de negocio y evitar las fallas en futuras interrupciones. Este mejoramiento debe ser periódico y debe tener un responsable el cual es el oficial de seguridad de la información, por lo que es recomendable para un BCP implementar el ciclo PHVA el cual es una estrategia de mejora continua de la calidad en cuatro pasos (Planear – Hacer – Verificar – Actuar) siendo esta una de las principales

herramientas de mejoramiento continuo para las organizaciones [14].

VI. NORMATIVIDAD

La normativa en seguridad informática tiene como fin de cuidar los datos e información personal de los usuarios y clientes, así como la regulación de la forma en que las organizaciones utilizan y tratan la información de los usuarios. En la mayoría de entes regulatorios y compañías que brindan marcos de gestión, guías de buenas prácticas y metodologías para el desarrollo de planes de continuidad de negocio, entre las más importantes y reconocidas están las siguientes:

ISO 27001
Esta norma que hace parte de la familia de las IS 27000, la cual es una norma que brinda la capacidad de garantizar la confidencialidad e integridad de los datos y de la información para las organizaciones, así como los procesos de los sistemas que las procesan, esta norma o estándar es brinda el sistema de gestión de la seguridad de la información está en especial permite a la organización la evaluación del riesgo y la aplicación de los controles necesarios para su erradicación o mitigación. Esta norma ofrece herramientas que ayudan a la implementación y desarrollo de los planes de continuidad, así como algunos pasos a seguir en casi de incidentes de seguridad [15].

ISO 22301
Esta norma de la ISO está especializada en la gestión de Continuidad del Negocio creada por especialistas en el tema la cual proporciona un marco de referencia para la gestión de la continuidad de negocio en las organizaciones. Especifica los requisitos para la protección, así como para reducir los tiempos de interrupción, garantizar a la organización que se recupere de incidentes, ayuda a la identificación y gestión de las amenazas a las que se encuentra expuesta la organización, minimizar los impactos que generan los incidentes, minimizando el tiempo de inactividad causado por un incidente y reduce el tiempo de recuperación de sus procesos y servicios a su normalidad generando una imagen confiable para empleados, proveedores y usuarios [16].

COBIT
"Objetivos de Control para Información y Tecnologías Relacionadas" Cobit es un marco de buenas prácticas reconocido a nivel internacional para la gestión y control de la información en sistemas de TI, este marco se enfoca también en el gobierno de TI, objetivos de control, medidas de desempeño, contingencia, aspectos críticos de éxito y modelos de madurez, el marco de COBIT es una herramienta más que ayuda a tener un adecuado enfoque en la creación desarrollo e implementación de un plan de continuidad Cobit tiene 4 divisiones o dominios y en especial en su apartado DS4, hace referencia a objetivos de control específicos que aseguran la continuidad del negocio y de las operaciones de una organización [17].

ITIL
"La biblioteca de infraestructura de TI" brinda un marco para la gestión de servicios de TI en cuanto a la planificación, aprovisionamiento, diseño, implementación, operación, soporte y mejora de los servicios de TI adecuados para las necesidades del negocio. ITIL proporciona un marco integral, consistente y coherente de buenas prácticas en la gestión de los servicios de TI y otros procesos relacionados. Dentro de sus objetivos de control se encuentran algunos que brinda apoyo a la continuidad de servicios de TI y disponibilidad de los servicios que en conjunto con otras normas y guías son de gran ayuda para el desarrollo de un BCP.
Aunque esta guía no entra en detalles de los procesos ni como se deben hacer, si nos brinda unos procesos básicos de gestión para el desarrollo y control [18].

NIST SP 800-34
El Instituto nacional de Estándares y Tecnologías NIST brinda un documento guía con la cual brinda a las organizaciones a comprender el propósito, proceso y un formato del desarrollo de planes de contingencia de los sistemas de información a través de directrices y practicas reales. Además, proporciona información de antecedentes sobre las interrelaciones entre la planificación de contingencias del sistema de información y otros tipos de planes de contingencia relacionados con la seguridad y la gestión de emergencias, la capacidad de recuperación de la organización y el ciclo de vida del desarrollo del sistema de contingencia [19].

VII. CONCLUSIONES

El éxito de cualquier organización sea cual sea su actividad algo primordial es la prestación de sus servicios, ya que de ellos depende el beneficio económico, es esta la principal razón para la adopción de un plan de continuidad de negocio.

La mayoría de las organizaciones no cuentan con un plan de continuidad de negocio porque no lo ven como una necesidad sino más bien como un gasto, además que en la actualidad la seguridad de la información no representa una necesidad por lo que no existe la asignación de recursos para este tipo de estrategias de respaldo y aseguramiento de la información en las organizaciones. Lo que podría resumirse como una adecuada gestión de la seguridad de la información.

La implementación y uso en conjunto de los distintos estándares, guías que hacen referencia a la continuidad de negocio como ISO 22301, ITIL O Cobit, en el desarrollo de un BCP es importante, ya que cada uno de ellos se enfoca en un aspecto distinto por ejemplo mientras que Cobit nos brinda detalles más específicos sobre objetivos de las pruebas de recuperación, ITIL por su parte solo da unas pautas básicas sin entrar en detalle, y la hizo es un marco general que en conjunto con estos dos estándares sería un perfecto conjunto para el desarrollo de un plan de continuidad de negocio.

Los BCP a menudo son confundidos con los planes de recuperación de desastres ya que los dos son parecidos salvo que el plan de continuidad indica cómo seguir con los procesos mientras se vuelve al estado normal de los negocios

mientras que el plan de recuperación de desastres como recuperarse después de un desastre, ambos con el fin de la continuidad de negocio por lo que es aconsejable desarrollar en conjunto.

AGRADECIMIENTOS

Agradecimientos especiales al docente Ing. Ramiro Merchán, experto en Planeación de la Continuidad del Negocio (CISA, CBCP)

REFERENCIAS

[1] "Pilares de la Seguridad de la Información: confidencialidad, integridad y disponibilidad | Firma-e", *Firma-e.com*, 2014. [Online]. Available: https://www.firma-e.com/blog/pilares-de-la-seguridad-de-la-informacion-confidencialidad-integridad-y-disponibilidad/. [Accessed: 11- Nov- 2018].

[2] S. IT, "Plan de Continuidad de Negocio o BCP", Secureit.es, 2018. [Online]. Available: https://www.secureit.es/procesos-y-gobierno-it/continuidad-de-negocio/. [Accessed: 07- Nov- 2018].

[3] C. Amaya, "Continuidad del negocio: ¿cómo responder ante una contingencia?", WeLiveSecurity, 2018. [Online]. Available: https://www.welivesecurity.com/la-es/2012/07/18/continuidad-negocio-como-responder-ante-emergencia/. [Accessed: 07- Nov- 2018].

[4] "Sistemas de gestión y estándares de calidad | BSI Group", *Bsigroup.com*. [Online]. Available: https://www.bsigroup.com/es-CO/. [Accessed: 11- Nov- 2018].

[5] *Horizon Scan Report 2018*. https://www.bsigroup.com/es-CO/gestion-de-la-continuidad-del-negocio-iso-22301-/reporte-horizon-scan-2018/ 2018.

[6] "Pasos a seguir para realizar un análisis de impacto en nuestro negocio", *INCIBE*, 2017. [Online]. Available: https://www.incibe.es/protege-tu-empresa/blog/pasos-seguir-realizar-analisis-impacto-negocio. [Accessed: 11- Nov- 2018].

[7] Revista Datacenter, *Cual es la diferencia entre el rto y rpo.*. 2012.

[8] S. Cobb, "4 pasos para armar un Plan de Continuidad del Negocio", WeLiveSecurity, 2014. [Online]. Available: https://www.welivesecurity.com/la-es/2014/05/14/gestion-continuidad-negocio-cuatro-pasos/. [Accessed: 12- Nov- 2018].

[9] O. Ávila, "Como crear un plan de continuidad del negocio", Forodeseguridad.com. [Online]. Available: http://www.forodeseguridad.com/artic/segcorp/7230_bcp_plan_continuidad_negocios.htm. [Accessed: 12- Nov- 2018].

[10] Guía para Desarrollar un Plan de Continuidad de Negocios. Mexico: Guía para Desarrollar un Plan de Continuidad de Negocios, p. 7.

[11] C. Montserrath, "ISM | ¿Cuál es el objetivo de tener un Plan de Continuidad de Negocio?", *ISM*, 2017. [Online]. Available: https://www.ismgrc.com/objetivo-continuidad-de-negocio/. [Accessed: 11- Nov- 2018].

[12] *Guía para realizar el Análisis de Impacto de Negocios BIA - MinTIC*, 2nd ed. Bogotá, 2015.

[13] R. Merchán Patarroyo, "Continuidad de la Cadena de Suministro", Universidad Piloto de Colombia, 2018.

[14] Y. Sanchez, "Ciclo PHVA", *www.gerencie.com/ciclo-phva.html*, 2017. [Online]. Available: https://www.gerencie.com/ciclo-phva.html. [Accessed: 11- Nov- 2018].

[15] "ISO 27001 - Software ISO 27001 de Sistemas de Gestión", *ISOTools*, 2013. [Online]. Available: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/. [Accessed: 11- Nov- 2018].

[16] "ISO 22301", *Software ISO Tools*. [Online]. Available: https://www.isotools.org/normas/riesgos-y-seguridad/iso-22301/. [Accessed: 11- Nov- 2018].

[17] "COBIT 5", *Isaca.org*. [Online]. Available: http://www.isaca.org/COBIT/Pages/COBIT-5-spanish.aspx. [Accessed: 11- Nov- 2018].

[18] "Proyectar con COBIT e ITIL el plan de recuperación de desastres", *SearchDataCenter*, 2009. [Online]. Available: https://searchdatacenter.techtarget.com/es/consejo/Proyectar-con-COBIT-e-ITIL-el-plan-de-recuperacion-de-desastres. [Accessed: 11- Nov- 2018].

[19] R. Toro, "¿Cómo utilizar la serie SP 800 de la norma ISO 27001?", *PMG SSI - ISO 27001*, 2016. [Online]. Available: https://www.pmg-ssi.com/2016/05/como-utilizar-serie-sp-800-norma-iso-27001/. [Accessed: 12- Nov- 2018].

AUTOR

Mora Yomayuza David Felipe, ingeniero de telecomunicaciones de la Universidad Militar Nueva Granada, estudiante de especialización en Seguridad Informática de la Universidad Piloto de Colombia.