PLAN DE CONTINUIDAD DEL NEGOCIO Y DE RECUPERACION ANTE DESASTRES ISO 22301:2019

Estrategia BCP y DRP 2024 por Rodrigo Ferrer

CONTENIDO

RESUMEN

Se busca, en este documento, exponer los pasos requeridos para diseñar e implementar un proceso de Gestión de la Continuidad del Negocio (GCN o BCM por sus siglas del inglés) orientado a diversas organizaciones en Colombia y otras partes del mundo. La metodología propuesta está basada en los estudios realizados por el Business Continuity Institute (BCI) y el Disaster Recovery Institute International (DRII) los cuales han sido las organizaciones líderes a nivel mundial en esta campaña de formación en los temas relacionados con la continuidad del negocio ante diferentes tipos de incidentes.

La continuidad del negocio es una parte fundamental del Gobierno y la gestión del riesgo, por lo tanto, se debe considerar como un proceso dentro de la organización, el cual debe obedecer a una fase de planeación (Planear), seguida por la implementación (Hacer), luego la verificación (Verificar) y, por último, se deben realizar mejoras sobre el proceso (Actuar), conformando así el ciclo PHVA. La GCN debe ser un aspecto importante para considerar en nuestra sociedad moderna globalizada, interconectada y con tecnologías nuevas, como la inteligencia artificial y, además, con una alta presencia de riesgos de tipo tecnológico y de origen natural, que en cualquier momento podrían llegar a materializarse. Por último, el GCN ha sido estandarizado en el año 2019 bajo la norma internacional colombiana NTC-ISO 22301:2019, la cual en la actualidad es una norma certificable y sobre la que se basa gran parte de estas reflexiones.

INTRODUCCIÓN

En los últimos años, los diferentes tipos de entidades a lo largo del territorio nacional han concedido una importancia creciente a la implementación de planes, procedimientos y estructuras que garanticen la continuidad de sus productos y servicios críticos del negocio ante eventualidades de diversas categorías y diferentes niveles de impacto. Estos factores, junto con una legislación cada vez más exigente, (Circulares de la Superintendencia Financiera y el Marco de Referencia de Arquitectura de TI, entre otros) en lo relacionado con la confiabilidad y seguridad en la prestación de estos productos y servicios, hacen necesario en la actualidad, que se cuente con una GCN para así lograr tener una sociedad cada vez más comprometida con la protección del talento humano, con la seguridad de la información (ISO 27001:2022) y nuevas tecnologías profundamente disruptivas al igual que con el incremento de la productividad, la efectividad y la eficiencia.

En un principio los factores de riesgo estaban asociados principalmente a contingencias de carácter natural y tecnológico, las consecuencias derivadas de sucesos como el terrorismo, la inestabilidad política, las pandemias, la pérdida de empleados claves y el ciberterrorismo, han mostrado la necesidad de incorporar nuevas amenazas en el proceso de BCM con el fin de garantizar la continuidad de las operaciones ante un escenario cada vez más dinámico en lo relacionado con el tipo de riesgos al que se está expuesto. De acuerdo con la encuesta anual BCI Horizon Scan, los incidentes generados por ataques cibernéticos poseen en la actualidad (2023) la mayor frecuencia como se puede observar en la Figura No. 1.

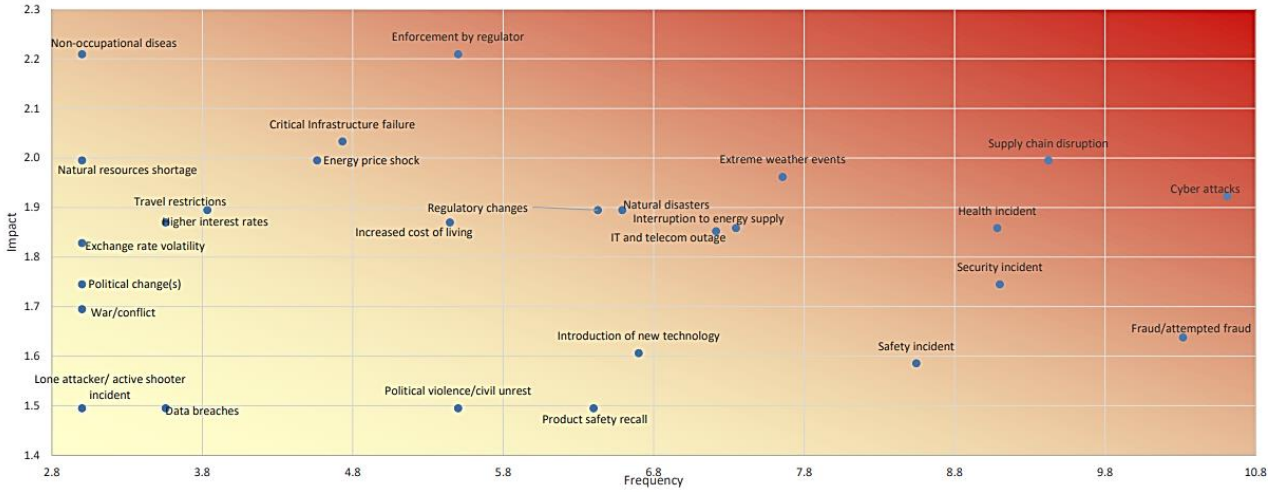

Figura No. 1. Incidentes con mayor frecuencia o impacto.

¿QUÉ ES UN GCN?

La Gestión de la Continuidad del Negocio busca sostener en niveles previamente definidos y aceptados, los productos y servicios críticos del negocio a través de la estructuración de procedimientos e información, los cuales son desarrollados, compilados y mantenidos en preparación para su uso durante y después de una interrupción o desastre, con el fin de proteger los intereses de las partes interesadas, reputación, marcas y actividades generadoras de valor.

La GCN está principalmente relacionado con las siguientes actividades como se muestra a continuación:

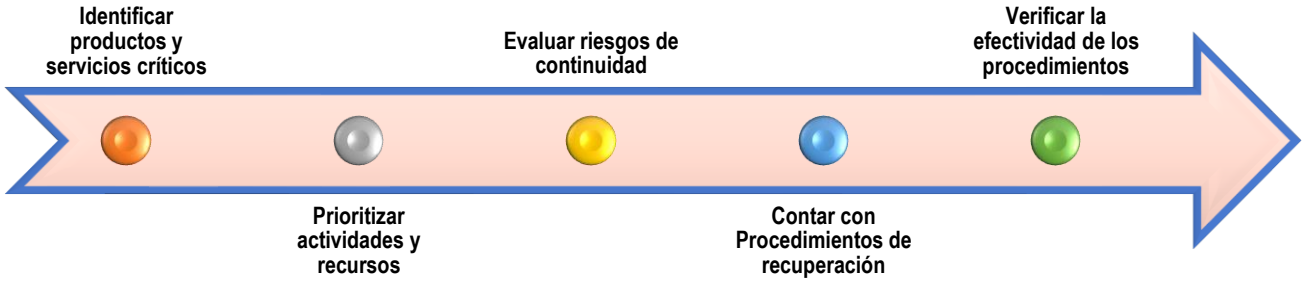

Figura No. 2. Actividades principales en el GCN.

De la anterior figura se desprende que una de las actividades iniciales y principales de un GCN, es la identificación de los productos y servicios críticos de una organización. A través de esta gestión de la continuidad, la organización será capaz de reconocer qué necesita ser protegido: el talento humano, las edificaciones, la tecnología, la información, los proveedores, partes interesadas y la reputación. Con este reconocimiento, se tendrá la habilidad de diseñar las estrategias

óptimas de recuperación cuando una disrupción se presente, y de esta manera, controlar el impacto como consecuencia de la materialización de determinado riesgo. De modo que comprender la organización es una parte fundamental cuando se trata de avanzar en un proyecto GCN. En la siguiente figura, se puede observar los componentes de una organización, resaltando los elementos que deben ser considerados cuando se trata de entender el propósito y la razón de ser de una organización.

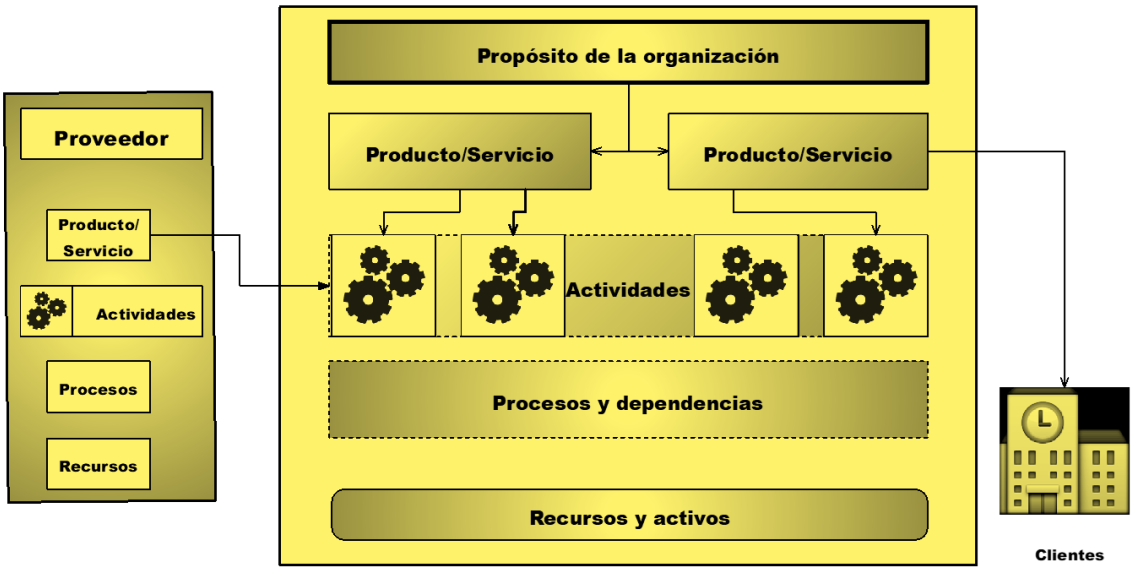

Figura No. 3. Entendiendo la organización.

PLANES ADICIONALES AL GCN

La siguiente figura, se encuentra basada en la publicación especial del NIST, SP800-34, en la cual se observa una versión holística de los diferentes tipos de planes relacionados con la atención de incidentes y emergencias, que se interrelacionan con el GCN, lo complementan y lo apoyan:

Figura No.4. Planes complementarios al GCN.

Del análisis inicial de la anterior figura, se puede observar la eventual conveniencia de que el GCN se complemente con una serie de planes adicionales. Sin embargo, debido a la carencia de definiciones estandarizadas para estos tipos de planes, en algunos casos, el alcance e implementación puede variar entre las diferentes organizaciones.

- **Plan de comunicación de crisis**: Este documento debe describir los procedimientos internos y externos que las organizaciones deben preparar ante un desastre. Este plan debe estar coordinado con los demás planes de la organización para asegurar que sólo comunicados aprobados sean divulgados y que solamente el personal autorizado sea el responsable de responder las diferentes inquietudes y de diseminar los reportes de estado a los empleados y al público en general.

- **Planes de evacuación por edificio**: Estos planes, contienen los procedimientos que deben seguir los ocupantes de una instalación o facilidad en el evento en que una situación se convierta en una amenaza potencial a la salud y a la seguridad del personal, al ambiente o la propiedad. Tales eventos podrían incluir fuego, terremoto, huracán, ataque criminal o una emergencia médica. Estos planes son normalmente desarrollados a nivel de instalación, específicos a la localización geográfica y al diseño estructural de la construcción.

- **Plan de respuesta a ciber incidentes**: Este plan establece procedimientos para responder a los ataques en el ciberespacio contra un sistema de Tecnología Informática (TI) de una organización. Estos procedimientos son diseñados para permitirle al personal de seguridad identificar, mitigar y recuperarse de incidentes de cómputo maliciosos tales como: acceso no autorizado a un sistema o información, negación del servicio, cambios no autorizados a hardware, software, entre otros (entre los ejemplos de elementos que pueden generar incidentes de

seguridad se encuentra: la lógica maliciosa, tales como virus, gusanos, o caballos de Troya). Estos planes normalmente pueden pertenecer al Sistema de Gestión de la Seguridad de la Información (SGSI).

- **Plan de recuperación de desastres (DRP)**: Este plan es conocido como DRP (Disaster Recovery Plan), por sus siglas en inglés y está orientado a responder a eventos importantes, usualmente catastróficos que niegan el acceso a la facilidad normal por un período extendido. Frecuentemente, el DRP se refiere a un plan enfocado en TI diseñado para restaurar la operabilidad del sistema, aplicación o facilidad de cómputo objetivo en un sitio alterno después de una emergencia. El alcance de un DRP puede solaparse con el de un Plan de Contingencia de TI; sin embargo, el DRP es menos amplio en alcance y no cubre interrupciones menores que no requieren reubicación. Dependiendo de las necesidades de la organización, pueden existir varios DRP´s.

- **Planes de contingencias**: Según el NIST, los planes de contingencia representan un amplio espectro de actividades enfocadas a sostener y recuperar servicios críticos de TI para una organización después de una emergencia en un tiempo mínimo. Es posible en algunos casos contar con múltiples planes de contingencia, uno por cada componente, sistema o servicio crítico. Los planes de contingencia son de rápida activación y se puede asumir un RTO (Recovery Time Objective), es decir, el tiempo objetivo de recuperación muy cercano a cero. Planes de contingencia son típicos en los canales de comunicaciones, de tal manera que ante la falla de uno de estos canales, otro, entrará en operación muy rápidamente y en muchos casos de manera automatizada.

METODOLOGÍA

La metodología recomendada en este artículo para el desarrollo del GCN (apoyada en ISO 22301:2019), propone un proceso comprendido desde el inicio del proyecto hasta la definición de la estructura de respuesta ante incidentes. La siguiente figura presenta las fases de la metodología que se procederá a explicar:

1. Inicio del proyecto
2. Definición de la política
3. Compromiso de la presidencia
4. Contexto de la organización
5. Análisis de impacto al negocio (BIA, Business Impact Analysis, por sus siglas del inglés)
6. Gestión de riesgos
7. Estrategias de continuidad y recursos
8. Estructura de respuesta a incidentes
9. Revisión, mantenimiento y mejoras

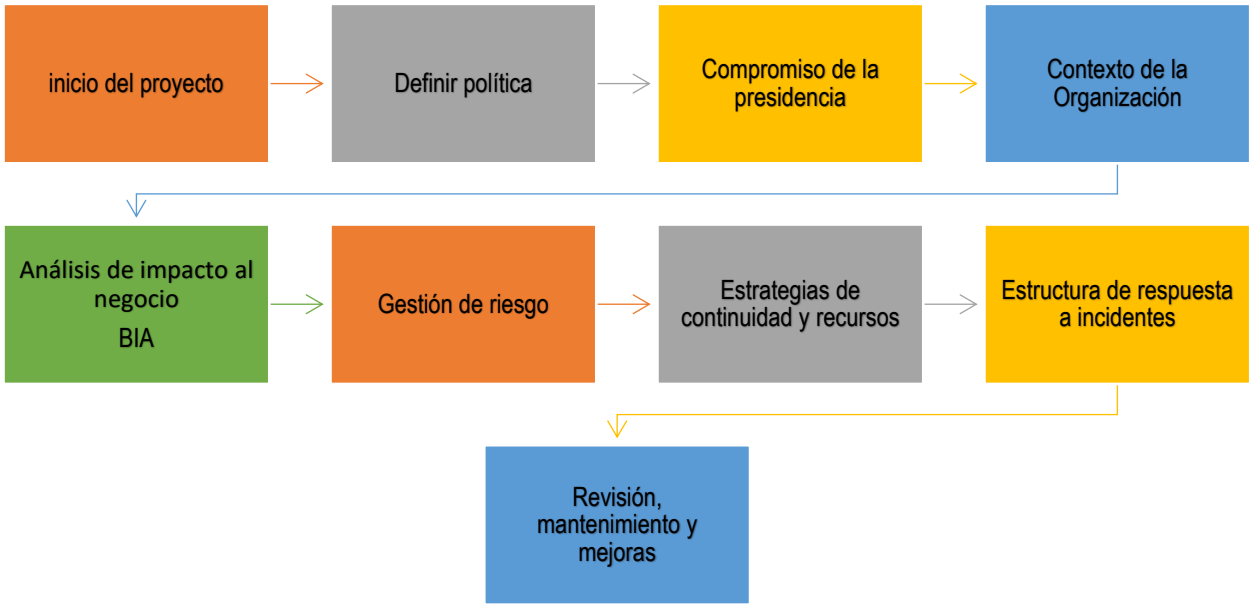

Figura No. 5. Fases de la metodología propuesta.

INICIO DEL PROYECTO

Esta fase se realiza con el propósito de estructurar el proyecto para el GCN, de forma tal que éste se encuentre adecuadamente organizado y controlado durante su ejecución para cumplir los objetivos estipulados. Es fundamental definir el alcance del proyecto, lo cual será luego ajustado con los resultados que se obtengan de la realización del BIA. De igual manera es importante identificar las partes interesadas con el fin de considerar sus requerimientos en todo el desarrollo del GCN.

DEFINIR LA POLÍTICA DE CONTINUIDAD DEL NEGOCIO

Con el fin de garantizar la efectividad y el entendimiento por parte del personal de los requerimientos de continuidad del negocio, el plan debe estar basado y apoyado en una política definida y posteriormente aprobada de manera formal. Entre los elementos principales a los que debe estar orientada esta política se tienen: apropiada a los propósitos de la organización, provea un marco de referencia para establecer los objetivos del negocio, incluya un compromiso para la mejora continua del GCN, debe ser comunicada al interior de la organización, debe estar disponible a las partes interesadas y debe ser revisada a intervalos definidos con el fin de garantizar su relevancia.

COMPROMISO DE LA PRESIDENCIA

Se confirma la aprobación de la política por parte de la alta gerencia de la organización para la realización del proyecto, de la misma forma se debe validar la existencia de los recursos financieros, humanos y logísticos requeridos tanto para la etapa de diseño como para la etapa de implementación del GCN. También la presidencia debe promover la mejora continua de todo el Sistema de la Gestión de la Continuidad del Negocio, BCMS (Business Continuity Management System) y velar porque se logren los objetivos definidos al decidir implementar este sistema.

CONTEXTO DE LA ORGANIZACIÓN

Antes de realizar el análisis de impacto al negocio, BIA, siguiendo las recomendaciones de la norma ISO 22301:2019, la organización debe documentar e identificar los siguientes aspectos:

- Las actividades, funciones, productos, asociaciones y proveedores, además del impacto a incidentes que afecten la continuidad del negocio
- Los enlaces entre la política de continuidad y la gestión de riesgos
- Se debe determinar el apetito al riesgo de la organización y de sus líneas de negocio
- Estimar las expectativas de las partes interesadas
- Analizar el Ambiente regulatorio que rodea a la organización
- Con base en lo anterior se debe actualizar el alcance del BCM o GCN

ANÁLISIS DE IMPACTO AL NEGOCIO BIA

El análisis de impacto al negocio tiene como función principal determinar los productos y servicios críticos de la organización y el impacto relacionado con la no prestación de ellos. Se recomienda realizar tres tipos de BIA, los cuales se explican en la siguiente tabla:

Tipos de BIA	Definición
BIA estratégico	Identifica y prioriza los productos y servicios más urgentes y determina los tiempos de recuperación y el impacto a la disrupción desde un punto de vista estratégico.
BIA táctico	Se determinan los procesos requeridos para la entrega de los productos y servicios críticos y se analizan los impactos por interrupciones.
BIA operacional	Se identifican y se priorizan las actividades en los procesos determinados como críticos y se determinan los recursos requeridos.

Tabla No. 1. Tipos de BIA.

De manera resumida, las principales actividades que se realizan en un BIA son:

- Evaluar el impacto potencial de un incidente disruptivo
- Identificar las actividades que soportan la prestación de los productos y servicios
- Evaluar el impacto sobre el tiempo de no realizar las actividades propias del negocio
- Especificar los tiempos de recuperación

- Identificar dependencias y recursos

En la siguiente figura, se presentan los tiempos determinados como parte del BIA. El MTPD (Maximum Tolerable Period of Disruption, por sus siglas del inglés), o el Máximo Período Tolerable de Disrupción, el cual, en base a las entrevistas que se realicen, ayudan a estimar los tiempos máximos en que un producto o servicio puede estar fuera de su operación normal. El RTO (Recovery Time Objetive, por sus siglas del inglés), es el Tiempo Objetivo de recuperación, el cual debe ser menor que el MTPD, y se aplica tanto para productos, procesos y recursos. Por último, se tiene el RPO, (Recovery Point Objetive, de sus siglas del inglés) Punto Objetivo de Recuperación, el cual determina la máxima información que se puede perder una vez ocurrido un incidente.

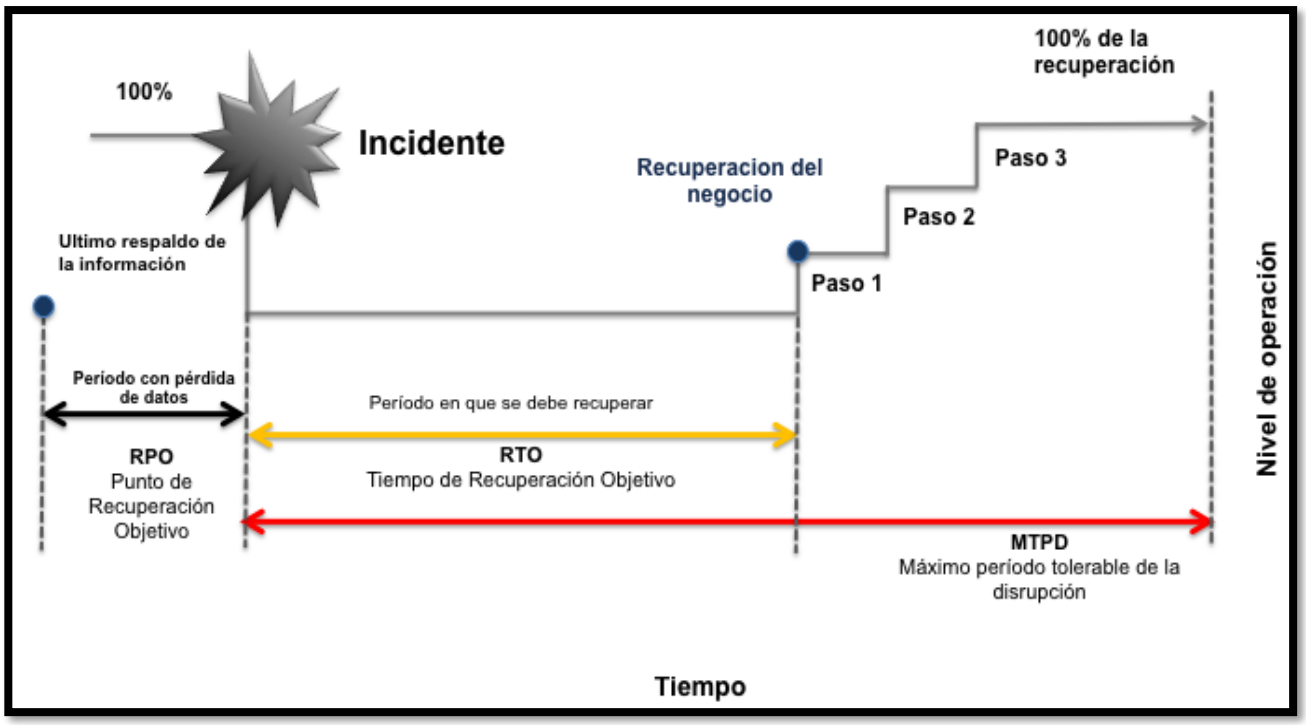

Figura No. 6 Tiempos de recuperación.

GESTIÓN DE RIESGOS

La etapa de gestión de riesgos tiene como objetivo principal establecer, implementar y mantener un proceso de evaluación de riesgos que sistemáticamente identifique, analice y evalúe los riesgos asociados a incidentes disruptivos en la organización. Este proceso puede ser realizado siguiendo las recomendaciones de la ISO 31000:2018, para implementar un sistema de gestión de riesgos.

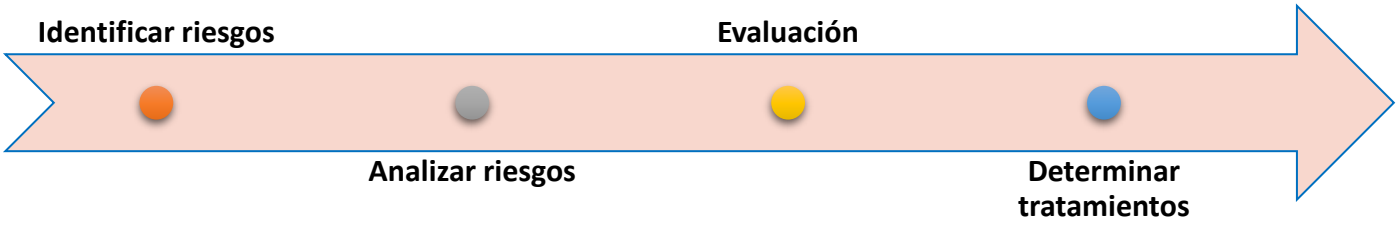

Figura No. 7. Gestión de riesgos.

ESTRATEGIAS DE CONTINUIDAD

La etapa de estrategias de continuidad del negocio tiene como objetivo principal analizar los diferentes esquemas de continuidad operacional según los escenarios de riesgo definidos, de tal forma que cumplan con los requerimientos reflejados por el Análisis de Impacto de Negocio y la Evaluación de Riesgos de Continuidad.

Los recursos según la norma ISO 22301: 2019 que deben de ser considerados son: personas, información, edificios, equipamiento, tecnologías, transporte, finanzas, y proveedores.

ESTRUCTURA DE RESPUESTA A INCIDENTES

La estructura de respuesta a incidentes tiene como función principal la toma de decisiones en caso de que ocurra un desastre que cause la interrupción o disrupción de los productos y servicios críticos de la organización.

Entre las funciones principales, se pueden resaltar las siguientes

- Analizar la situación para responder oportunamente
- Tomar la decisión de activar o no los planes de continuidad (BCP o DRP)
- Iniciar el proceso de notificación a los empleados a través de los diferentes responsables
- Definir un presupuesto estimado para gastos que genere la crisis
- Seguimiento del proceso de recuperación, con relación a los tiempos estimados de recuperación
- Tomar decisiones ante situaciones o imprevistos durante la recuperación de operaciones
- Comunicar a los diferentes comités de la organización las decisiones que se tomen

REVISIÓN, MANTENIMIENTO Y MEJORAS

Llegados a este punto, se ha concluido lo que son las etapas de diseño e implementación. La organización debe implementar un procedimiento para revisar la efectividad del plan de continuidad y recuperación ante desastres. Se deben revisar los procedimientos y planes que se tengan hasta la fecha por medio de ejercicios y pruebas. Con base en los

resultados que se obtengan de estos ejercicios o pruebas, se deben realizar las correcciones pertinentes a los procedimientos, planes o estrategias. La organización debe realizar auditorías internas a intervalos regulares para revisar la conformidad del sistema. (ISO 22301, 9.2). La revisión debe ir de la mano de una supervisión continua de los planes, con el fin de obtener resultados sobre su efectividad y de esta manera proponer un plan de acción para mejorar las debilidades encontradas. Por último, pero no menos importante, se deben identificar las no conformidades, tomar acciones para corregirlas teniendo en cuenta sus causas. La organización continuamente debe mejorar la adecuación y la efectividad del Plan de Continuidad (ISO 22301, 10.2).

OBSERVACIONES FINALES SOBRE EL GCN

De acuerdo con lo anteriormente expresa, se pretende, por un lado, mostrar la importancia de contar con una gestión de la continuidad del negocio, y por el otro, comprender como el estándar ISO 22301 nos da el apoyo para que podamos convocar a nuestra organización a entrar un proceso de continuidad dado que de esta manera garantizamos un futuro confiable de la organización y además logramos hacer una sociedad más segura. La continuidad del negocio se ha comenzado a ver en muchas partes del mundo como un emprendimiento que nace de las directivas con un componente real de tipo estratégico.

Los beneficios de contar con una adecuada GCN son múltiples y beneficiosos para las organizaciones en Colombia y el mundo, debido a las constantes amenazas a las que el país o países están expuestos, existirá una regulación cada vez más estricta y finalmente será un proceso a nivel empresarial el cual será adoptado por la mayoría de las organizaciones con el fin de ser cada vez más confiables, generar mejores productos y ser organizaciones más globalizadas. El uso de la inteligencia artificial y algoritmos de Deep Learning tendrá aplicaciones tantos desde el punto de vista del adversario como de los que protegen la seguridad de la información alojada en bases de datos vectoriales o LLM (Large Language Model), estas tecnologías ofrecen desafíos a la continuidad de las operaciones como era de esperarse. A continuación, se presenta un resumen gráfico acerca de los principales beneficios de contar con estos planes.

Figura No. 8. Beneficios de contar con un GCN..

Glosario de términos

SANS[1]: La continuidad del negocio se refiere a las actividades requeridas para mantener su organización operando durante un periodo de desplazamiento o interrupción de la operación normal.[2]

BCI[3]: La continuidad del negocio es una colección de procedimientos e información que es desarrollada, compilada y mantenida en preparación para el uso en el evento de una emergencia o desastre.

DRI international[4]: La planeación de la continuidad del negocio es el proceso de desarrollar arreglos previos y procedimientos que capaciten a la organización para responder a un evento de tal manera que las funciones críticas del negocio continúen con los niveles planeados de interrupción o cambios esenciales.

NIST[5]: El BCM se enfoca en sostener las funciones de negocio de una organización, durante y después de una interrupción mientras se recupera paralelamente. El BCM se orienta hacia los productos y servicios críticos. Por su parte, el DRP provee procedimientos detallados para facilitar la recuperación de las capacidades en sitio alterno. Normalmente está enfocado en Tecnologías de la Información (en adelante TI) y limitado a interrupciones mayores con efectos a largo plazo. Los planes de contingencia representan un amplio espectro de actividades enfocadas a sostener y recuperar servicios críticos de TI después de una emergencia. Debido a que los planes de contingencia deben ser desarrollados para cada aplicación importante o sistema de soporte, se pueden contar con múltiples planes de contingencia dentro de un BCP.

BRITISH STANDARDS (BSI) & BS 25999: La Gestión de la Continuidad del Negocio (BCM) es un proceso de gestión que identifica amenazas potenciales a la organización y provee una estructura para construir confiabilidad y capacidades para una efectiva respuesta que proteja los intereses de los accionistas, la reputación, la marca y las actividades de creación de valor, también involucra la gestión de la recuperación y continuidad después de un incidente y la gestión de todo el programa por medio de entrenamientos, pruebas, y revisiones para mantener el BCM al día.

[1] SysAdmin, Audit, Network, Security, para mayor información consultar: http://www.sans.org

[2] Traducción del autor del documento.

[3] Business Continuity Institute, http://www.thebci.org/

[4] Disaster Recovery Institute Internacional: https://www.drii.org

[5] National Institute of Standards and Technology, Contingency Planning Guide for Information Technology Systems, NIST Special Publication 800-34.

BIBLIOGRAFÍA

Business Continuity Institute (2019) *Good Practice Guidelines: A guide to global good practice in business continuity*, Business Continuity Institute, Caversham.

Disaster Recovery Institute International (DRII) (2012) *Professional Practices for Business Continuity Practitioners*, DRII, New York.

ISO 22301 (2019) – Societal security – Business continuity management systems – Requirements

ISO 22301 (2019) – Societal security – Business continuity management systems – Guidance

ISO 22301 (2019) – Societal security – Terminology