Implementación de un Plan de Continuidad del Negocio en la Policía Nacional

Ana Catherine Mariño Rincón
Diego Alberto Castro Garzón
Raúl Andrés Guana Olarte
Departamento de Ingeniería de Sistemas y Computación
Universidad de los Andes
Bogotá, Colombia
{ac.marino10, da.castro500, r-guana}@uniandes.edu.co

Resumen

Este artículo propone la implementación del Plan de Continuidad del Negocio para la Policía Nacional. Identificados los procesos de negocio y el modelo operacional, es posible realizar un análisis de impacto del negocio (BIA), en donde se puede determinar tiempo de respuesta para el regreso a la operación y punto de información de restablecimiento. Bajo este contexto, se puede llegar a realizar un análisis de riesgos que permite identificar los procesos que le resultan críticos para la organización, convirtiéndose, en el punto de partida para la realización del plan de continuidad del negocio y determinar las posibles estrategias de recuperación.

Abstract

This article proposes the implementation of the Business Continuity Plan for the National Police. Once the business processes and the operational model have been identified, it is possible to carry out a business impact analysis (BIA), where the response time for the return to operation and the information point of restoration can be determined. Under this context, it is possible to carry out a risk analysis that allows identifying the processes that are critical for the organization, becoming the starting point for the development of the business continuity plan and determining possible recovery strategies.

Índice de Términos – Análisis de Impacto del Negocio, Plan de Recuperación ante Desastres, Riesgos, Amenaza, Vulnerabilidad, Seguridad Digital.

I. CONTEXTO

La Policía Nacional de Colombia creada hace ciento veintinueve años, tiene la misión constitucional de garantizar las condiciones necesarias para el ejercicio de los derechos y libertades públicas, y para asegurar que los habitantes de la nación convivan en paz. Actualmente la integran más de 180.000 hombres y mujeres distribuidos en cuatro oficinas asesoras, un área de supervisión y catorce direcciones de tipo administrativo y operativo.

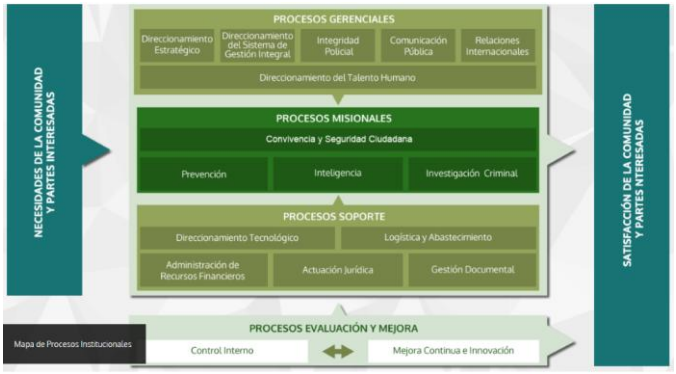


Fig. 1. Mapa de procesos Policía Nacional [1]

El despliegue de las actividades de prevención y control se realiza a nivel nacional a través de la desconcentración de unidades de cada una de las anteriores Direcciones y Oficinas Asesoras, en seccionales y regionales de operación. La Dirección General es la única que se concentra en la Capital y de la que depende el ordenamiento y directrices para el despliegue y cumplimiento de los objetivos trazados para la institución.

Para dar cumplimiento a las expectativas y satisfacer las necesidades del cliente interno y externo de la Institución, se cuenta con procesos definidos y estandarizados en cumplimiento de las políticas de calidad y seguridad de la información.

En este despliegue de unidades y desconcentración de funciones se resalta la importancia de la Oficina de Telemática como eje asesor del Director y de los

comandantes a nivel nacional en materia de toma de decisiones y administración tecnológica, así mismo, es el área encargada de brindar soporte a las aplicaciones de la entidad. Sumado a esto, dentro de las metas trazadas a largo plazo por la Institución, se establece de forma pública que: "Durante los primeros cuatro años, cumpliremos con el Servicio de policía a través de la unidad institucional para responder a los diversos comportamientos generacionales y regionales que impacten en la convivencia, mediante la innovación, el uso de herramientas tecnológicas y la optimización de los recursos"[2]. Es por esto que, "la Oficina de Telemática tiene como misión asesorar y promover el desarrollo tecnológico de la institución en las áreas de informática y telecomunicaciones a través de la investigación, implementación, administración y soporte, con el fin de estandarizar los procedimientos e innovar la infraestructura telemática para apoyar la gestión policial"[3]; así las cosas, resultan de gran relevancia los servicios ofrecidos por esta Oficina, de la cual dependen los sistemas y herramientas tecnológicas en la prestación del Servicio de Policía.

Como medio de análisis de seguimiento y medición, la Oficina de Telemática implementa un control tecnológico que busca analizar el grado de usabilidad de las aplicaciones y equipos de comunicación dispuestos para el servicio, pero no se describe ninguno que se asocie al sostenimiento de la infraestructura de la información.

II. DESCRIPCIÓN DE LA PROPUESTA

A. Descripción del problema

En la actualidad la oficina de Telemática de la Policía Nacional carece de una estrategia integral que responda de manera efectiva al restablecimiento de los servicios tecnológicos frente a fallas mayores, causando eventualmente un impacto a la reputación de la entidad afectando la capacidad operativa para el logro de la misión y objetivos de la institución.

B. Propuesta de solución

La propuesta de solución es implementar un Plan de Continuidad del Negocio de los servicios tecnológicos primarios, soportados por la infraestructura y procesos de administración que presta la Oficina de Telemática de la Policía Nacional. Un plan de continuidad permitirá a la entidad ofrecer una respuesta adecuada en caso de fallas mayores que pongan en peligro la continuidad del negocio con estrategias efectivas que aseguren su recuperación. El plan se construirá en tres etapas: Análisis de impacto del negocio, Definición del plan de recuperación, Consolidación del plan de continuidad del negocio.

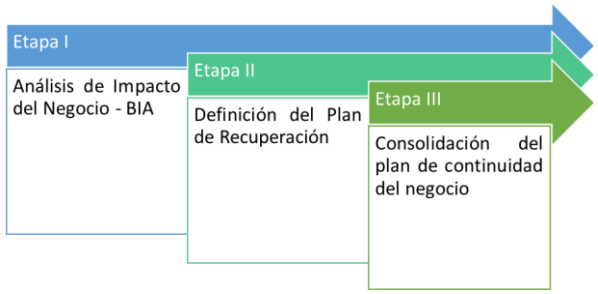


Fig. 2. Formulación del Plan de Gestión de Continuidad del Negocio de la Oficina de Telemática de la Policía Nacional

Etapa I: Elaboración del Análisis de Impacto del Negocio – BIA (Bussiness Impact Analysis). El resultado de esta etapa permitirá identificar con claridad los procesos misionales de la Policía Nacional y analizar el nivel de impacto con relación a la gestión del negocio. Al final de esta etapa se tendrá un documento donde se identifican todas las áreas críticas del negocio, siendo este un instrumento que garantice la medición de la magnitud del impacto operacional de la entidad, al momento de presentarse una interrupción. Este documento contendrá la siguiente información:

1. Identificación y priorización de los procesos críticos en la gestión de la entidad.
2. Identificación de los recursos necesarios para su funcionamiento en condiciones de normalidad.
3. Interrelaciones con otros procesos.
4. Análisis del nivel de impacto.
5. Tiempos de recuperación.

Etapa II. Definición del Plan de Recuperación. Para esta etapa se tendrá un documento en que se determinan las estrategias de continuidad necesarias para reanudar y recuperar las operaciones críticas priorizadas e identificadas. Este contempla la siguiente información:

1. Definición de los procedimientos para la activación de las respuestas.

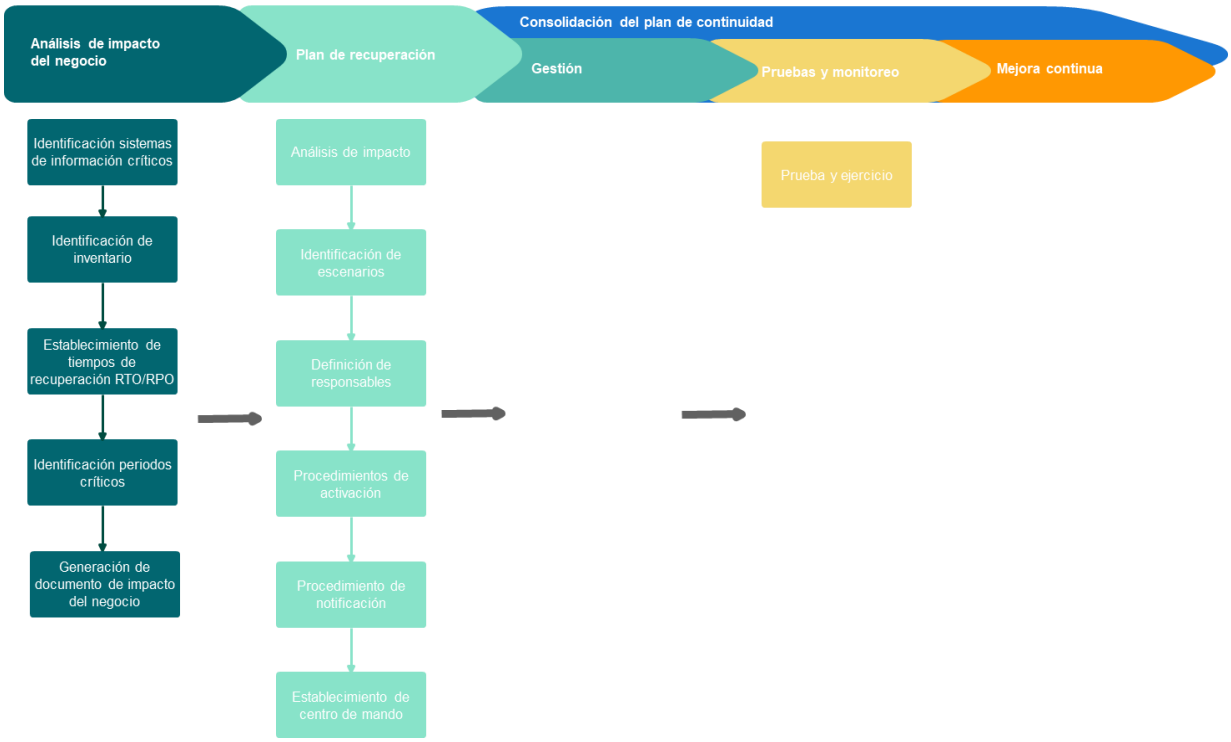


Fig. 4 Arquitectura del estado actual (AS IS) del plan de continuidad del negocio de la Oficina de Telemática de la Policía Nacional

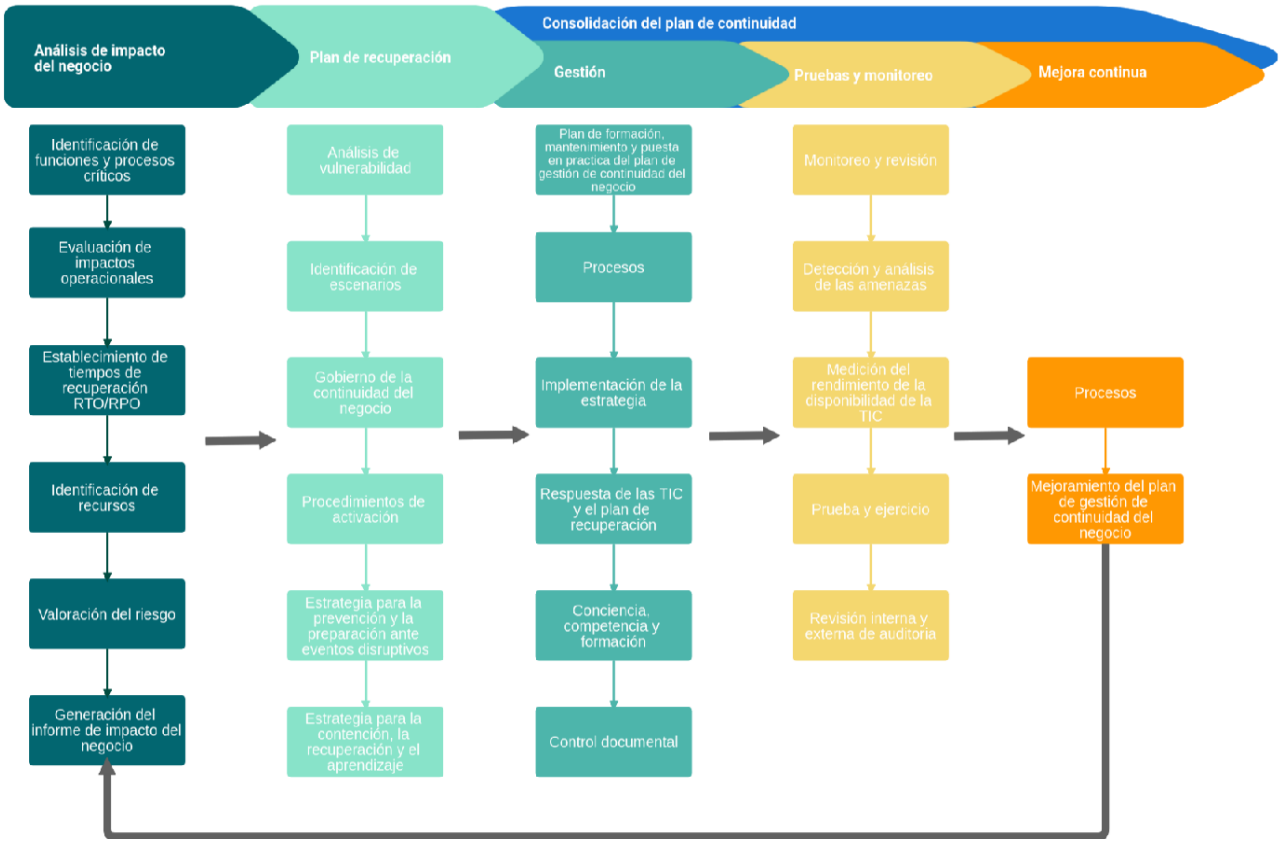


Fig. 3. Arquitectura propuesta para el Plan de Gestión de Continuidad del Negocio de la Oficina de Telemática de la Policía Nacional

2. Definición de los roles y responsabilidades definidos para las personas y los equipos que tienen autoridad durante y después de un incidente.
3. Estrategias para las operaciones críticas.

Etapa III. Consolidación del plan de continuidad del negocio. Es la etapa final que comprende las actividades de divulgación y apropiación al interior de la entidad, con el objetivo de iniciar un proceso de mejora continua y consolidación de esta propuesta de solución, aplicada a las operaciones que desarrolla la Oficina de Telemática de la Policía Nacional. De la ejecución de esta etapa se obtendrían los siguientes resultados:

1. Definición de pruebas de contingencia.
2. Definición del plan de capacitaciones.
3. Definición del plan de seguimiento y evaluación.

La figura Fig. 3 muestra la arquitectura a la cual se desea llegar una vez finalizado el proceso propuesto. En esta se plantean los pasos necesarios para el desarrollo, implementación y mantenimiento del plan de recuperación.

III. SOLUCIÓN

En los siguientes capítulos se presentan los pasos para la creación del plan de recuperación en la Policía Nacional. Para esta etapa de la solución se realiza todo el proceso de análisis de impacto de negocio, luego de esto se plantea el DRP (Disaster Recovery Plan) para el proceso más crítico que resultó de análisis.

A. Análisis de Impacto del Negocio

El objetivo de esta etapa es poder identificar con claridad los procesos misionales de la Policía Nacional y analizar el nivel de impacto con relación a la gestión del negocio A continuación los pasos realizados.

1) Realización de entrevistas

Para realizar una plena identificación y gestión de continuidad en la Policía Nacional de Colombia, es fundamental tener claridad sobre los productos y servicios misionales que ofrece como institución garante de la convivencia y seguridad ciudadana, actividad que se realiza con base en las necesidades y expectativas de las partes interesadas. Además de la identificación de procesos, se deben definir los recursos necesarios para el desarrollo de estos y realizar un análisis al respecto del nivel de impacto que representa la caída de servicios. Con ello, determinar el tiempo objetivo de recuperación (RTO) y el punto de recuperación objetivo (RPO), entre otros.

Para recopilar información necesaria para la construcción del BIA, se realizan entrevistas con los líderes funcionales, técnicos, de cada servicio, aplicación o herramienta tecnológica, con el fin de obtener y documentar la información que permitiera entender las necesidades y el funcionamiento de la organización.

2) Identificación de procesos

Con la información recopilada se diligenció la siguiente tabla, lo que permite listar todos los procesos y sus funciones dentro de la organización:

Nombre del proceso de negocio	Descripción y responsabilidades del proceso

3) Evaluación de impacto

En virtud de los servicios prestados por la Policía Nacional, se cuantifica el impacto causado por cada uno de los procesos al no encontrar la debida disponibilidad, integridad y/o confidencialidad. Esta es hallada en relación con la cantidad de transacciones o usos dejados de prestar. La información recolectada y su calificación se consigna en tabla con los siguientes campos:

Proceso Estratégico	Nombre del proceso de negocio	IMPACTO				
		Ninguno	Bajo	Medio	Alto	Potencial del impacto

Respecto al análisis realizado de impacto por interrupciones del servicio, se logró identificar que, el proceso del Direccionamiento Tecnológico es de vital importancia para la prestación de todos los demás servicios en la Institución. A través de este proceso es que logran dinamizar y realizar los registros y accesos a todos los sistemas y plataforma tecnológica que tiene la Policía Nacional.

La siguiente gráfica representa la cantidad promedio de registros por hora dejados de realizar, al presentarse una indisponibilidad de la plataforma tecnológica.

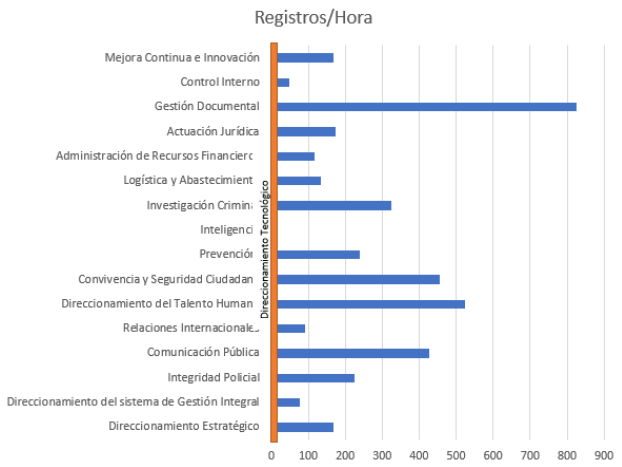


Fig. 5. Registros por hora dejados de realizar

4) Determinación del punto objetivo de recuperación y tiempo objetivo de recuperación

Definidas las frecuencias en que se desarrollan las actividades, fue posible determinar el tiempo máximo en que cada proceso puede tolerar un retraso. Se diligencia esta información en la siguiente tabla

Proceso Estratégico	Nombre del proceso de negocio	RTO

Al igual, identificados los procesos que componen la institución y su tiempo máximo de respuesta, fue posible determinar el trabajo que se desarrolla en forma manual y el punto de antigüedad máximo con la cual se puede recuperar la información. Se consigna la información en la siguiente tabla.

Nombre del proceso de negocio	Procedimiento Manual de Solución	% que se puede hacer manual	RPO

5) Evaluación de Riesgos

Para adelantar el análisis del riesgo se deben considerar los siguientes aspectos: Calificación del riesgo y evaluación del riesgo. El riesgo se debe medir a partir de las siguientes especificaciones:

Nivel	Descriptor	Descripción	Frecuencia
1	Raro	El evento pude ocurrir solo en circunstancias excepcionales	No se ha presentado en los últimos 5 años
2	Improbable	El evento puede ocurrir en algún momento	Al menos de una vez en los últimos 5 años
3	Posible	El evento podría ocurrir en algún momento	Al menos de una vez en los últimos 2 años
4	Probable	El evento probablemente ocurrirá en la mayoría de las circunstancias	Al menos de una vez en el último año
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de una vez al año

Tabla 1. Tabla de Probabilidad

Bajo el criterio de impacto, el riesgo se debe medir a partir de las siguientes especificaciones:

Nivel	Descriptor	Descripción
1	Insignificante	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la entidad
2	Menor	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad
3	Moderado	Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad
4	Mayor	Si el hecho llegara a presentarse, tendía altas consecuencias o efectos sobre la entidad
5	Catastrófico	Si el hecho llegara a presentarse tendría desastrosas consecuencias o efectos sobre la entidad

Tabla 2. Tabla de Impacto

Para determinar el impacto se pueden utilizar distintos aspectos que representan los temas en que suelen impactar la ocurrencia de los riesgos y se asocian con la clasificación del riesgo previamente realizada, y se relaciona con las consecuencias potenciales del riesgo identificado, para este caso en particular se tendrá en cuenta el impacto operacional.

Ahora bien, la Evaluación del Riesgo permite comparar los resultados de la calificación del riesgo, con los criterios definidos para establecer el grado de exposición de la entidad; de esta forma es posible distinguir entre los riesgos aceptables, tolerables, moderados, importantes o inaceptables y fijar las prioridades de las acciones requeridas para su tratamiento.

Para facilitar la calificación y evaluación a los riesgos, a continuación, se presenta una matriz que contempla un análisis cualitativo, para presentar la magnitud de las consecuencias potenciales (impacto) y la posibilidad de ocurrencia (probabilidad). Las categorías relacionadas con el impacto son: insignificante, menor, moderado, mayor y catastrófico. Las categorías relacionadas con la probabilidad son raro, improbable, posible, probable y casi seguro.

Probabilidad	Impacto				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Raro (1)	B	B	M	A	A
Improbable (2)	B	B	M	A	E
Posible (3)	B	M	A	E	E
Probable (4)	M	A	A	E	E
Casi seguro (5)	A	A	E	E	E

B: Zona de riesgo baja: Asumir el riesgo
M: Zona de riesgo moderada: Asumir el riesgo, reducir el riesgo
A: Zona de riesgo Alta: Reducir el riesgo, evitar, compartir o transferir

E: Zona de riesgo extrema: Reducir el riesgo, evitar, compartir o transferir

Tabla 3. Matriz de calificación, evaluación y repuesta a los riesgos

Se caracterizan los riesgos identificados de todos los procesos de gestión de la Policía Nacional en el siguiente formato:

Proceso	Riesgo	Probabilidad	Impacto	Tipo	Evaluación

6) Priorización del proceso con mayor nivel de criticidad

Según la escala de niveles de criticidad, los procesos se categorizan de acuerdo con la función que realizan es considerada de misión crítica, o son funciones necesarias importantes, o si son funciones relevantes para el negocio. De acuerdo con su impacto total en el negocio, obtenido del siguiente interrogante: ¿Si la operación del proceso analizado se interrumpe, se afecta gravemente el logro del objeto, la entrega de los productos y/o la prestación de los servicios de la entidad?

A continuación, se muestra la escala de niveles de criticidad definida para la categorización de los procedimientos críticos:

Nivel		Descripción
A	Función de Misión Crítica	Crítico para el Negocio, la función del negocio no puede realizarse Esta categoría está conformada por los procedimientos de alto impacto para el cumplimiento del objeto, la entrega de los productos y/o la prestación de los servicios de la entidad. Si la operación se interrumpe, se interrumpe el logro del objeto, la entrega de los productos y/o la prestación de los servicios de la entidad y esto afectaría a los clientes externos y la Nación.
B	Funciones Necesarias Importantes	No es crítico para el Negocio, pero la operación es una parte integral del mismo. Esta categoría está conformada por los procedimientos necesarios para el funcionamiento de los procesos de misión crítica. Si estos procesos pierden su continuidad, se ven afectados los recursos de la Organización
C	Funciones relevantes	La operación no es parte integral de la misión crítica del negocio. Esta categoría está conformada por los procedimientos que proveen información relevante para la toma de decisiones, necesarios para la definición estratégica de la corporación; su interrupción afecta en menor medida el cumplimiento del objeto, la entrega de los productos y/o la prestación de los servicios de la entidad y su tiempo de recuperación puede ser mayor.

Tabla 4. Escala de Niveles de Criticidad

Teniendo en cuenta el resultado de la evolución de los riesgos se selecciona el proceso que presenta mayor criticidad, y a este se le plantea el plan de recuperación de desastres, como se muestra en el siguiente capítulo.

B. Plan de Recuperación de Desastres – DRP

El Disaster Recovery Plan – DRP es un proceso compuesto por distintas acciones para recuperar y proteger la infraestructura de TI de una organización en caso de un desastre, es decir, a un evento súbito, imprevisto catastrófico que interrumpe los procesos de negocio lo suficiente como para poner en peligro la supervivencia de la organización.

A continuación se describen los pasos realizados para la elaboración de este plan.

1) Escenario de Continuidad

Con el fin de establecer las medidas de recuperación del proceso priorizado, se realizará un análisis de riesgo identificando posibles causas y consecuencias; los riesgos identificados en la valoración de riesgo son:

Id Riesgo	Descripción del Riesgo
R1	Deficiencias en el hardware y/o en el software Base
R2	Indisponibilidad en las telecomunicaciones
R3	Descarga y/o instalación de software no Corporativo
R4	Acceso no autorizado a los sistemas de información corporativos
R5	Uso indebido o inadecuado de los datos contenidos en las bases de datos corporativas
R6	Sistemas de información desarrollados o adquiridos puestos en producción, que no cumplen con las especificaciones funcionales
R7	Deficiencias en la supervisión de los contratos a cargo del proceso
R8	Extralimitación y abuso de poder
R9	Incumplimiento en el tiempo de entrega para la puesta en producción de los Sistemas de información desarrollados o adquiridos

Tabla 5. Riesgos identificados para el proceso de Direccionamiento Tecnológico

Las consecuencias constituyen los efectos de la ocurrencia de los riesgos sobre los objetivos de la entidad. Se detallan las consecuencias en los casos en que los riesgos se pudieran materializar haciendo uso del siguiente formato.

Identificador de Riesgo	Descripción del Riesgo	Consecuencias / Efectos del Riesgo

2) Escenarios de No Continuidad

Los controles o acciones de respuesta preventivos son el conjunto de medidas que hacen parte de la gestión operativa de la no continuidad que se implementan antes de que se presente un evento disruptivo grave, su finalidad es prevenir o asegurar la no ocurrencia o

minimizar el impacto por la ocurrencia de riesgos que puedan afectar gravemente la continuidad del negocio en la entidad.

Existen diferentes alternativas de recuperación donde la estrategia apropiada es la que tiene un costo para un tiempo aceptable de recuperación que también es razonable con el impacto y la probabilidad de ocurrencia. Las acciones más efectivas serían:

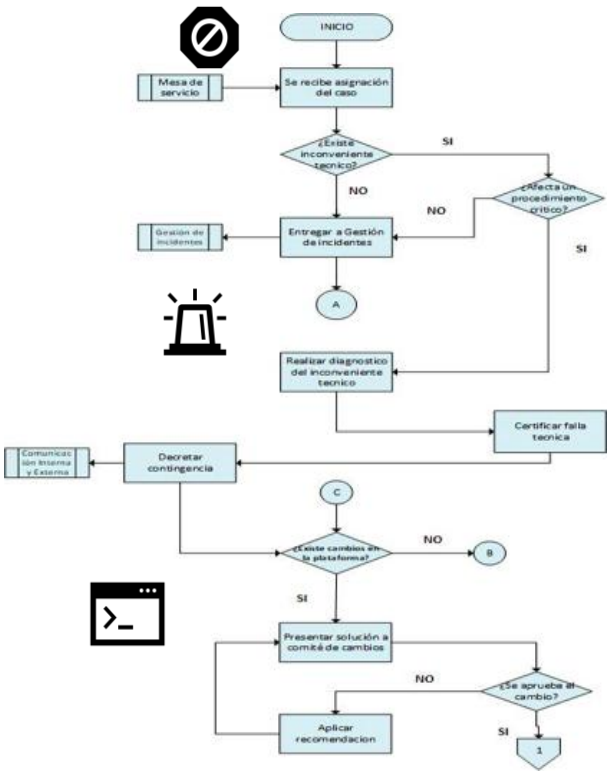


Fig. 6. Flujo de ejecución del DRP

- Eliminar la amenaza completamente.
- Minimizar la probabilidad y el efecto de la ocurrencia.

La selección de una estrategia de recuperación depende de:

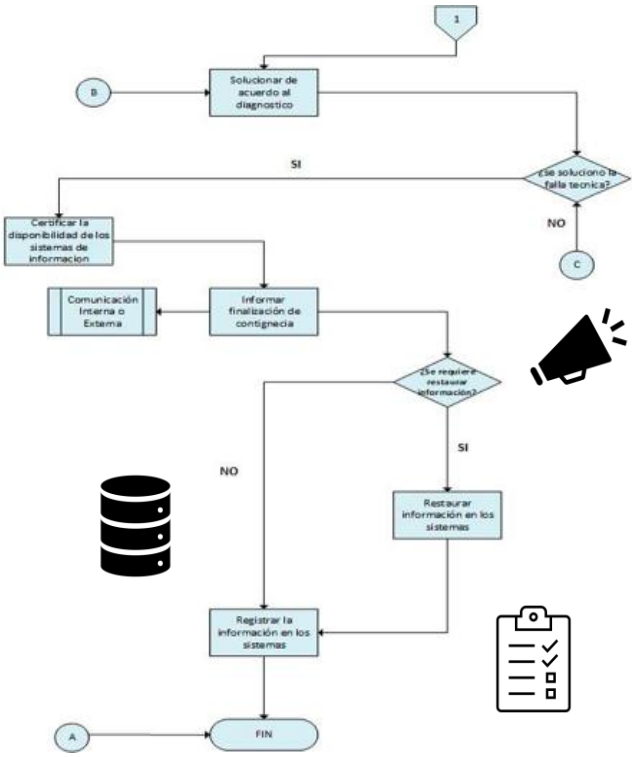
- La criticidad del proceso del negocio y las aplicaciones que soportan los procesos.
- Costo.
- El tiempo requerido para recuperarse.
- Seguridad.

3) Detección y Ejecución del DRP

La figura Fig. **6** muestra el flujo propuesto para la detección y ejecución del DRP.

IV. TRABAJO FUTURO

El mantenimiento del plan de continuidad del negocio es de vital importancia para asegurar la vigencia de lo que se ha recuperado y los procedimientos que rigen la recuperación. Ante los cambios que se produzcan en la



organización, el plan debe ajustarse, integrando el proceso de administración de cambios, con la permanente actualización a partir de pruebas de verificación, adquisición de activos tecnológicos y crecimiento progresivo de la información.

Adicionalmente es necesaria la evaluación periódica de las actividades de recuperación, con el fin de garantizar el funcionamiento de este, y a la vez afianzar el conocimiento y manejo del plan de recuperación, de tal forma en que se presente un incidente real sea manejado de manera correcta.

Por otro lado, las circunstancias actuales han provocado que el sector público acelere sus procesos de transformación digital. El confinamiento ha motivado que

el desarrollo de las labores habituales y la misionalidad se ha tenido que desempeñar desde casa. Por lo tanto, es imperativo que los colaboradores de las entidades del Estado cuenten con las herramientas y servicios basados en tecnologías de la información y las comunicaciones con el propósito de apoyar la gestión de manera remota.

Los efectos de la pandemia conllevan a la proyección en el tiempo de las medidas fijadas para evitar contagios masivos y elevar vertiginosamente el pico de propagación, el trabajo en casa es una de estas medidas y esto obliga a que dichos servicios y herramientas de TI se evalúen y monitoreen de manera permanente toda vez que serán la clave para una adecuada prestación del servicio garantizando el desarrollo de los planes de acción y contingencias soportados en la continuidad del negocio para fortalecer la gestión de las entidades.

Así las cosas, la Policía Nacional debe propender por lo siguiente:

- Trabajar expedientes digitales, con firmas electrónicas y notificaciones electrónicas, los expedientes en papel deben tender a su reducción.
- Potenciar las opciones de teletrabajo.
- Considerar las nuevas formas de información y asistencia a los ciudadanos (atención mediante la web o mediante aplicaciones móviles) impulsando el gobierno digital que es la gran apuesta del gobierno nacional para volver eficiente la administración pública otorgando mas y mejores servicios en línea.
- Utilizar la enorme cantidad de información que disponen las entidades vigiladas por la Agencia, en este sentido propiciar un ecosistema de control basado en las distintas formas de cooperación y colaboración.
- Contar con sistemas de información para hacer más eficiente el control e implementar canales de comunicación más robustos para dinamizar las denuncias y en general el control social, siempre y cuando se despliegue una masiva y efectiva campaña de difusión y publicidad.
- Mejorar la calidad de la información y en ese ámbito es imperativo el mejoramiento de los medios donde circula dicha información, con la implementación de un procedimiento seguro, la modalidad de trabajo en casa resulta desafiante en la medida que el control de acceso y monitoreo sobre el ecosistema digital de la entidad se vuelve más complejo.

V. CONCLUSIONES

- El Análisis de Impacto del Negocio – BIA junto con la Valoración de Riesgos, desarrolla la Etapa I del Plan de Continuidad del Negocio y constituye el diagnóstico inicial para la identificación de los procesos críticos y la consecuente definición de las estrategias de continuidad que debe adoptar la entidad en caso de una No Continuidad.
- El proceso crítico seleccionado de acuerdo con los objetivos del presente trabajo es el de Direccionamiento Tecnológico, columna vertebral de los demás procesos y sobre el cual se cierne toda la atención en tiempos de pandemia.
- El proceso del Direccionamiento Tecnológico, obra como ejecutor de las Políticas y lineamientos de configuración frente a lo que la institución desea proyectar y es el medio para presentar los avances frente a la mejora técnica del servicio de Policía, cumpliendo lo establecido en políticas gubernamentales, siendo éste el proceso que facilita y promueve la adaptación ante nuevos retos de modernización y transformación.
- La planeación es una actividad crítica en las entidades del Estado, mayor aún en las Fuerzas Militares y de Policía que deben propender por plataforma tecnológicas más robustas y seguras. Para ello, es necesario que las entidades tengan en cuenta la dinámica de los diferentes procesos para la continuidad de las operaciones, como el almacenamiento, la protección de datos, la recuperación efectiva de información, entre otros, que sean fuertes, pero a la vez fáciles de incorporar e implementar, asegurando así la confidencialidad, integridad y disponibilidad de la información.

VI. REFERENCIAS

[1] Policía Nacional de Colombia. Organigrama - Policía Nacional. [Online]. https://www.policia.gov.co/organigrama

[2] Policía Nacional de Colombia. (2020, Diciembre) Misión, visión, mega, valores, principios y funciones. [Online]. https://www.policia.gov.co/mision-vision-mega-

principios-valores-funciones

[3] Policía Nacional. (2020, Diciembre) Oficina de Telemática de la Policía Nacional. [Online]. https://www.policia.gov.co/oficinas-asesoras/telematica

[4] Policía Nacional de Colombia. Organigrama Oficina de Telemática de la Policía Nacional. [Online]. https://www.policia.gov.co/oficinas-asesoras/telematica/organigrama

[5] Ministerio de Tecnologías de la Información y las Comunicaciones, "Guía No. 10: Guía para la preparación de las TIC para la continuidad del negocio," 2010.

[6] Ministerio de Tecnologías de la Información y las Comunicaciones, "Guía No 11: Guía para realizar el Análisis de Impacto de Negocios BIA," 2015.

[7] Ministerio de Tecnologías de la Información y las Comunicaciones, "Guía No. 21: Guía para la Gestión y Clasificación de Incidentes de Seguridad de la Información," 2016.

[8] Departamento Administrattivo de la Función Pública, "Guía para la administración del riesgo y el diseño de controles en entidades públicas," Bogotá, 2108.

[9] ISO 22301:2012, *Sistemas de Gestión y Continuidad del Negocio*.

[10] ISO/IEC 27035, *Information Technology. Security Techniques. Information Security incident imanagement*.

[11] A. Yarlequé Gutiérrez, *Diseño de un Plan de Recuperación de Desastres de TI (DRP TI) para el Centro de Cómputo de la sede principal de una entidad educativa superior del sector privado basado en la norma NIST SP 800-34*. Lima: Universidad Peruana de Ciencias Aplicadas(UPC).