Unidad para las Víctimas

Metodología de Continuidad de Negocio u Operación

Seguridad de la Información

2025

Oficina de Tecnologías de la Información

Tabla de contenido

1. INTRODUCCION

Existen eventos o catástrofes naturales que pueden desencadenar una serie de afectaciones directas o indirectas como daños en infraestructura física, infraestructura TI; riesgo en la integridad de las personas; perdida en datos y sistemas de información; interrupciones en la ejecución de las actividades en los procesos de la Entidad. La Metodología de Continuidad del Negocio permite establecer una serie de acciones antes, durante y después de las interrupciones causadas por eventos o catástrofes; logrando de esta manera definir un marco de acciones para minimizar los tiempos de inactividad en la ejecución de la misión de la Entidad y, así mismo, en una mejor sostenibilidad en los procesos y aplicaciones.

Este documento describe las fases de la Metodología de Continuidad del Negocio en la Unidad para la Atención y Reparación Integral a las Victimas (UARIV), proporcionando una guía secuencial de cómo reaccionar a causa de una posible materialización de un evento o catástrofe; por medio del manejo de las estrategias de respuesta de cada uno de los escenarios de amenaza, planes de crisis, planes de comunicaciones entre otras actividades para el establecimiento de la continuidad del negocio en la Entidad.

2. OBJETIVO

Definir, coordinar y ejecutar el Plan de Continuidad del Negocio en la UARIV, estableciendo un marco conceptual orientado a soportar, reactivar y/o recuperar los procesos críticos en caso de que ocurra un evento o catástrofe.

La metodología de Continuidad de Negocio se diseña como guía para los diecinueve (19) procesos que se encuentran definidos en el mapa de procesos de la UARIV aplicando buenas prácticas ITIL 4, el marco de referencia normativo ISO 22301:2019 y la Guía No. 10 para la preparación de las Tecnologías de la información y las Comunicaciones para la continuidad del negocio de MinTIC. Ésta es de obligatorio cumplimiento para todos los funcionarios, contratistas y proveedores de la entidad.

3. DEFINICIONES

Amenaza: Se entiende como cualquier causa potencial de un incidente no deseado, que puede provocar daños graves a un sistema de información, redes, instalaciones o a la Entidad. Fuente: (NTC-ISO/IEC:27000, 2018)

Análisis de Impacto en el Negocio: Business Impact Analysis (BIA) Es el proceso de análisis de actividades identificando el efecto que podría tener sobre ellas la interrupción de su gestión y desarrollo normal. Fuente: ISO 22301-2019.

Análisis de Riesgo: Proceso que permite comprender la naturaleza del riesgo y establecer el nivel de riesgo. Fuente: ISO 22301-2019.

Business Continuity Plan (BCP): Business Continuity Plan (BCP) o Plan de Continuidad de Negocio, el BCP se enfoca en sostener las funciones de negocio de una organización, durante

y después de una interrupción mientras se recupera paralelamente. El BCP se orienta hacia los procesos de negocio. Fuente: ISO 22301-2019.

Chief Información Security Officer (CISO): De acuerdo con (INCIBE, 2016): "Es el director de seguridad de la información". Esencialmente corresponde al rol o perfil que es desempeñado a nivel ejecutivo y que como objetivo principal es engranar la seguridad de la información con los objetivos estratégico de la Entidad. Fuente: ISO 22301-2019.

Continuidad del Negocio: Capacidad de la Entidad para continuar desarrollando y entregando los servicios en un nivel aceptable predefinido, luego de un incidente. Fuente: ISO 22301-2019.

Crisis: Situación grave que sucede de forma imprevisible, poniendo en peligro el desarrollo de las actividades o procesos de una Entidad y que puede dejar gravemente afectado el funcionamiento de esta. Fuente: ISO 22301-2019.

Disponibilidad: Comprende la capacidad de los usuarios para acceder, utilizar o dar tratamiento a la información autorizada por la Entidad, en una ubicación determinada y en un formato correcto. Fuente: (NTC-ISO/IEC:27000, 2018).

DRP (Disaster Recovery Plan / Plan de Recuperación de Desastre): El DRP suministra los 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. Fuente: ISO 22301-2019.

Evento: Distingue los aspectos o alteración de un conjunto particular de situaciones (Accidentes, incidentes y circunstancias peligrosas). Fuente: (NTC-ISO:31000, 2018).

Evento Catastrófico: Aquellas situaciones con la capacidad de interrumpir la continuidad de las actividades del negocio generando impactos críticos, daños mayores y/o no recuperables para la Entidad. Fuente: ISO 22301-2019.

GAP de madurez: El Gap de Madurez es el instrumento que se utiliza para realizar un diagnóstico del modelo de seguridad y privacidad de la información, cuyo objetivo es identificar el estado actual de la Entidad respecto a la adopción de los controles de seguridad. Fuente: ISO/IEC 27001-2022.

Incidente: Situación que puede ser o podría dar lugar a una interrupción, pérdidas, emergencias o crisis. Fuente: ISO/IEC TR 18044-2024.

Infraestructura: Sistemas, equipos y servicios necesarios para la operación de una Entidad. Fuente: ISO/IEC 27001-2022.

Malware: Se define como virus informático. Se utilizan a menudo como sinónimos, pero un virus es técnicamente un tipo particular de malware. Específicamente, un virus es un código malicioso que oculta software legítimo para dañar y distribuir copias de sí mismo. Fuente: ISO/IEC 27001-2022.

MSPI (Modelo de seguridad y privacidad de la información): Parte de la gestión general para el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejora de la continuidad del negocio. Fuente: (International Organization for Standardization ISO/IEC 27001-2022.

Plan de Continuidad del Negocio: Procedimiento, protocolo o instrumento que guía a la Entidad para reaccionar ante incidentes naturales y/o de factor humano, que lleven a la interrupción directa de la operación o servicios de la UNIDAD PARA LAS VICTIMAS, identificando los niveles mínimos en los cuales la Entidad pueda garantizar la continuidad de la operación. Fuente ISO/IEC 27001-2022.

Plan de Respuesta a Incidentes: El plan incluye procedimientos documentados y lineamientos para la definición de la criticidad de los incidentes, los procesos de presentación de informes y escalado, y los procedimientos de recuperación. Fuente: ISO/IEC TR 18044-2024.

Ransomware: Tipo de código malicioso que cifra la información y solicita pago por rescate de esta. Secuestro de información. Fuente: ISO/IEC 27001-2022.

Respuesta a Incidentes: La respuesta de una entidad a un desastre u otro evento significativo que pueda afectar de manera significativa a la entidad, su gente, o su capacidad de funcionar de manera productiva. Una respuesta a incidentes puede incluir la evacuación de una instalación, iniciando un plan de recuperación de desastres (DRP), la realización de la evaluación de daños y otras medidas necesarias para llevar una entidad a un estado más estable. Fuente: ISO/IEC TR 18044-2024.

Riesgo: Posibilidad de que una amenaza, aproveche o explote una vulnerabilidad para causar una pérdida o daño en un activo de información. Esto suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.
(NTC-ISO/IEC:27001, 2022).

RPO (Recovery Point Objective / Punto de Recuperación Objetivo): Establece los niveles de tolerancia que la Entidad puede tener sobre la pérdida de información en el evento del desastre, así mismo, tener el punto de referencia en el cual la información debe ser restaurada para poner en funcionamiento o habilitar dicha actividad. Fuente: ISO 22301-2019.

RTO (Recovery Time Objective / Tiempo de Recuperación Objetivo): Comprende los Periodos de tiempo que debe transcurrir entre el incidente y la recuperación de la operación. Fuente: ISO 22301-2029.

Seguridad Perimetral: Se define como el perímetro imaginario o línea, que separa una Entidad (sus computadoras, servidores, etc.) de otras redes (generalmente el internet) (NTC-ISO/IEC:27002, 2022).

4. Desarrollo

4.1 MÉTODO

Para el diseño del Plan de Continuidad del Negocio se establecen 3 etapas generales Antes, Durante y Después de las interrupciones causadas por eventos o catástrofes. Las etapas ofrecen una guía utilizando fases secuenciales; las cuales se encuentran articuladas para disminuir los tiempos e impactos desfavorables por la no continuidad en los procesos.

ANTES	DURANTE	DESPUES
•Esta etapa da inicio a la prevención con actividades que van encaminadas a la identificación de los recursos necesarios, antes de ocurra un evento traumático o catastrófico, que interrumpa la gestión y normal funcionamiento de los procesos de la entidad.	•Esta etapa ocurre en el momento del evento traumático o catastrófico, donde se activan los mecanismos según la situación, emergencia, escenario o amenaza, que permite tomar decisiones para dar inicio a la activación de plan de continuidad.	•Esta etapa se basa en la ejecución de procedimientos para el restablecimiento, restauración o recuperación del normal funcionamiento y estado de los procesos, salvaguardando la integridad de las personas y así aplicar las actividades de mejora, mantenimiento, revisión y gestión del cambio.

a) Actividades iniciales para la Metodología de Continuidad de Negocio

En el marco del diagnóstico del GAP[1] de madurez del MSPI, se evidenció que no había políticas, procedimientos, lineamientos o controles respecto a continuidad del negocio, adicionalmente por recomendación de control interno, se establen planes de acción dentro del plan de mejoramiento de la Oficina de Tecnología de la información (OTI). Una vez se realizó este diagnóstico, se determinó:

- Crear un plan de trabajo por lo cual, desde la Oficina de tecnologías de la información, se realizaría este proyecto en cabeza de seguridad de la información.
- Establecer e implantar una política transversal de continuidad del negocio, sin que esta política impida poder trabajar paralelamente en los demás temas relacionados con la continuidad del negocio.
- Crear un formato de gestión BIA (Análisis de impacto del negocio), en el cual nos permita consolidar todos los datos de los procesos con sus lideres de los diferentes dominios de la OTI y datos de contacto, posteriormente nos enfocamos en obtener las entradas y salidas de las actividades, activos o riesgos críticos en donde se logrará identificar los impactos operacionales, financieros, legales y reputacionales por cada

[1] Brecha o distancia entre el estado actual y el deseado.

actividad y poder valorarla según su afectación en tiempos críticos de recuperación a través de los RTO Y RPO.

- Identificar las entradas y salidas de las actividades críticas, con parámetros necesarios para su correcto entendimiento como son: Proveedores – Grupos de Interés – Medios de recepción – Periodicidad de la actividad.
- Identificar los impactos de operación, reputación, financiero y legal de cada una de las actividades críticas en los procesos de la OTI y la valoración total de todos los impactos.
- Identificar los periodos de tiempo con más volumen de trabajo de cada una de las actividades críticas.
- Identificar los tiempos de recuperación como el RPO - Punto de Recuperación Objetivo Y RTO- Tiempo de Recuperación Objetivo.
- Obtener la descripción de los recursos de recuperación mínimos (personal de respaldo, requerimientos físicos, hardware, software, aplicaciones, documentos vitales, puesto de trabajo) que requieren los funcionarios y contratistas para ejercer sus actividades después de una interrupción en sus actividades por causa de un evento o catástrofe natural.
- Identificar las actividades alternas requeridas para mantener la continuidad de los procesos, se Identificaron los proveedores y matrices de comunicación requeridos para restablecer y garantizar la continuidad del negocio.

b) Principios de la Metodología de Continuidad de Negocio

Para el plan de implementación, el modelo de gestión propuesto se basa en el modelo denominado ciclo PHVA (Planificar, Hacer, Verificar y Actuar), a través del cual se coordinan las actividades para realizar periódicamente el Análisis de Impacto de Negocio – BIA identificando la criticidad de los aspectos relacionados a la prestación de productos o servicios críticos de la entidad:

- Asegurar la continuidad del componente de seguridad de la información ante la ocurrencia de eventos no previstos a través de un Plan de Continuidad de Negocio y un Plan de Recuperación de Desastres de la entidad, basado en recuperación tecnológica inicialmente.
- Establecer y ejecutar un plan de pruebas periódico del plan de Continuidad de Negocio que permita evaluar los niveles de recuperación que requiere la entidad, así como los requerimientos de seguridad, funciones, responsabilidades relacionadas con el plan.
- Asignar roles y responsabilidades detallados en el Plan de Continuidad del Negocio a personal idóneo para la atención de los incidentes de Continuidad del Negocio.
- Incluir la concientización y sensibilización de la información con respecto al uso y apropiación de los temas de Continuidad del Negocio de tal forma que los funcionarios, contratistas y proveedores reaccionen de manera eficiente ante un incidente que comprometa su seguridad y el desarrollo de sus actividades en los procesos o la prestación de sus servicios.
- Gestionar el manejo de la crisis o contingencia y los mecanismos de comunicación apropiados durante el estado de contingencia, en caso de presentarse un incidente significativo que conlleve una interrupción de los servicios.
- Disponer de planes de continuidad en caso de que sus actividades afecten el Cumplimiento de la misionalidad de la entidad y probarlos regularmente.

- Todas las personas de la entidad tales como funcionarios, contratistas y proveedores, deben reaccionar de manera eficiente ante un incidente natural y/o de origen humano que comprometa su seguridad y el desarrollo de sus actividades en los procesos o la prestación de sus servicios.

No.	Fases del ciclo PHVA	Actividades
1	Planear	Se identifica el alcance, objetivos, políticas, escenarios de riesgos, roles y responsabilidades, BIA y recursos.
2	Hacer	Se implementa el Plan de Continuidad del Negocio para la entidad, la Política de Continuidad del Negocio y el BIA.
3	Hacer	Se evalúan y se miden los resultados de la implementación, a fin de verificar que se haya logrado la mejora esperada.
4	Actuar	Se adoptan mejoras correctivas y/o preventivas en función de los resultados de la fase anterior (3-Monitorear) para lograr la mejora continua.

Tabla 1. *Fases del ciclo PHVA en la continuidad de negocio.* ***Fuente:*** *elaboración propia.*

c) Escenarios y fases que hacen parte del Plan de Continuidad de Negocio.

Para la definición de los escenarios y fases, es necesario tener en cuenta los siguientes recursos que soportan la operación de la Entidad:

Ilustración 1. *Escenarios y fases del Plan de Continuidad de Negocio.* ***Fuente:*** *elaboración propia.*

Adicionalmente, es necesario indicar que, los mencionados recursos pueden ser afectados por amenazas o impactos listados en la ilustración No. 2, para lo cual es necesario diseñar el Plan de Continuidad de Negocio (BCP por sus siglas en inglés).

Ilustración 2. *Tipos de escenarios de interrupción.* ***Fuente:*** *elaboración propia.*

Ejemplos de escenarios para consideración en la construcción del plan de continuidad del negocio de la UARIV:

"Escenario No.1: (Alteración Orden Público)
"Escenario No.2: (Desastre Natural / Incendio / Terremoto / Inundaciones)
"Escenario No.3: (Fallas de la UPS y Planta Eléctrica del Data Center)
"Escenario No.4: (Ataques Informáticos / Malware / Ransomware)

4.1.1 Fase de Roles y Responsabilidades

Ilustración 3. *Antes – Roles y Responsabilidades.* ***Fuente:*** *elaboración propia.*

Corresponde a la primera fase del Plan de Continuidad del Negocio, en la cual se define la estructura organizacional que apoyará el diseño y ejecución las actividades para la toma de decisiones al interior de la Entidad, para el manejo de crisis o contingencia y llevar a cabo el plan de comunicaciones a los grupos o personas autorizadas para activar el BCP.

En la etapa del antes se definen los roles y responsabilidades de la Gestión de Continuidad de Negocio, pero estos desarrollan sus actividades en todas las etapas antes, durante y después. En el Modelo de Gobierno de la Gestión de Continuidad de Negocio se establecen las responsabilidades preventivas, de respuesta y recuperación desplegadas a continuación.

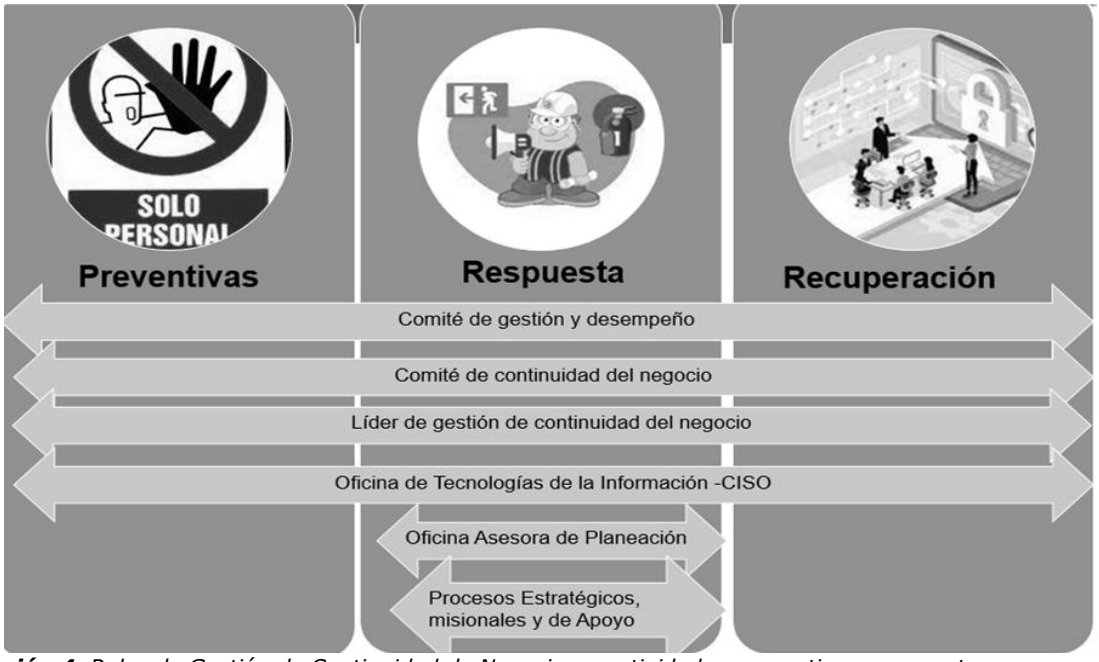

Ilustración 4. *Roles de Gestión de Continuidad de Negocio en actividades preventivas, respuesta y recuperación.*
Fuente: *elaboración propia.*

Alineación entre la estructura organizacional del Gestión de Continuidad de Negocio y la estructura organizacional de continuidad del negocio a alto nivel el cual será gestionado y administrado por la OTI.

Se relacionan a gran escala cada uno de los roles:

- **Comité de Gestión y de Desempeño:** Este comité está compuesto por aquellos responsables a nivel de financiación y gobernabilidad de la continuidad del negocio y las políticas de seguridad de la información las cuales están conformadas por las personas responsables de ofrecer una orientación estratégica y eficaz, asegurando que esta sea la más adecuada para la Unidad. Tomando decisiones importantes que tengan relación a la continuidad del negocio u operación, planeación de la continuidad y recuperación estratégica.

- **Líder de Gestión de Continuidad del Negocio o quien haga sus veces:** Persona líder que administra el Plan de Continuidad del Negocio y coordina la respuesta y recuperación de una eventual crisis junto a su Equipo designado para la Gestión de

Continuidad del Negocio en apoyo con el Comité de Gestión Institucional y de Desempeño.

- **Oficina De Tecnologías de la Información (OTI):** Este grupo o subproceso hace parte de la estructura definida por la Entidad para afrontar cualquier situación o evento catastrófico. Su rol principal es gestionar y brindar apoyo al Líder de Gestión de Continuidad del Negocio (definido o designado por la Dirección General) y al Comité de Gestión Institucional y de Desempeño con las tareas establecidas para la evaluación, activación y supervisión de las actividades de recuperación relacionadas con los servicios de Tecnología de la Información (TI) y trabajar en conjunto con el Equipo designado para la Gestión de Continuidad del Negocio en la implementación y pruebas, teniendo en cuenta los diferentes escenarios y estrategias que se definan en el Plan de Continuidad del Negocio y en el Plan de Recuperación de Desastres.

- **Oficial de Seguridad de la Información o quien haga sus veces:** Este rol apoya al Coordinador de Gestión de Continuidad del Negocio, Comité Gestión Institucional y de Desempeño y al Equipo designado para la Gestión de Continuidad del Negocio, en lo relacionado a la normatividad y requerimientos legales que están alineados a los controles del MSPI.

- **Oficina Asesora de Planeación:** Equipo que tiene la responsabilidad de ser el ente orquestador de las actividades que se desarrollan dentro de la Gestión de Continuidad del Negocio. Es responsable por de la articulación de estrategias de continuidad del negocio dentro de la Entidad, planes de continuidad del negocio, respuesta a emergencias, manejo de crisis, recuperación de tecnología y mantenimiento de la Gestión de Continuidad de Negocio.

- **Equipo De Manejo De Crisis:** Este equipo está conformado por representantes de las diferentes áreas de la Entidad, los cuales cuentan con la experiencia y autoridad para manejar los efectos de un incidente que interrumpa el normal funcionamiento de los procesos críticos de la Entidad. Por lo general lo conforman la Dirección General, Comunicaciones y procesos Misionales de la Entidad junto con la OTI.

- **Líder de Proceso:** Es el líder frente a su respectivo proceso en lo relacionado a la Continuidad del negocio, debe participar en el desarrollo, implementación y administración del plan de continuidad desarrollado para su respectivo proceso. Todo equipo debe poseer las competencias apropiadas para actuar en las actividades de respuesta para el manejo de la crisis, por la materialización de un evento o catástrofe natural que interrumpa las actividades en los procesos en los servicios TI y pueda generar afectaciones a las personas como, por ejemplo; infraestructura física y los datos e información.

La norma ISO 22301:2019 *recomienda para el control de las competencias de los roles y responsabilidades, tener toda la documentación de soportes como evidencia de la educación, formación y experiencia del manejo y gestión de la continuidad del negocio.*

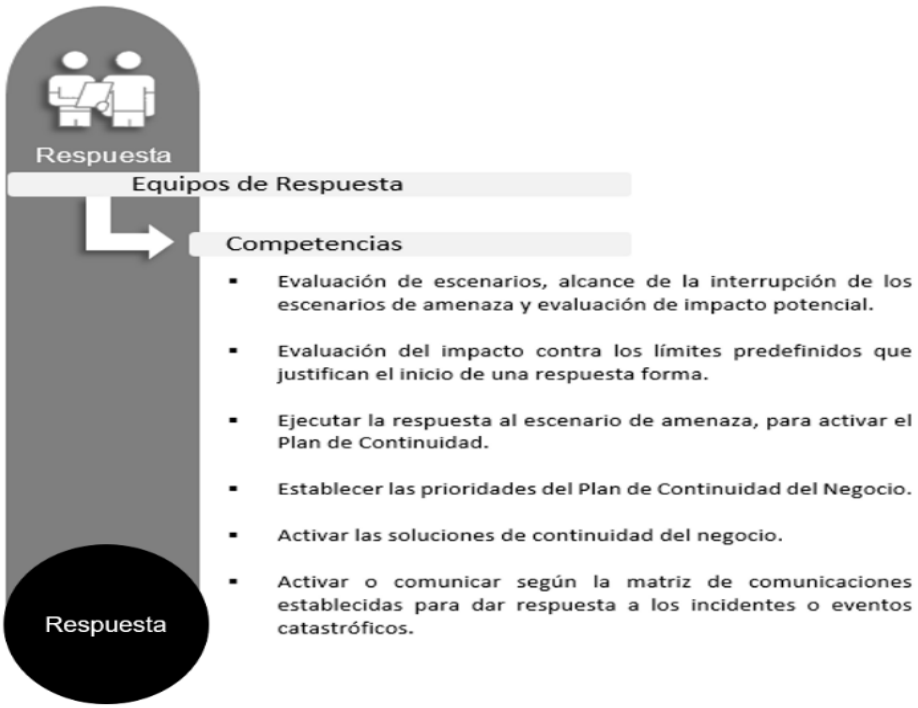

Ilustración 5. *Competencias de los equipos de respuesta para el manejo de crisis o Continuidad.* ***Fuente:*** *elaboración propia.*

En las matrices de riesgo de procesos, datos e información, servicios TI e infraestructura física se contemplan los mismos escenarios de peligro o de amenaza ocasionados por un evento o catástrofe natural; de esta manera todos los equipos de respuesta deben encontrarse alineados y articulados con el fin de proporcionar respuestas acertadas al momento de activar un plan de crisis y continuidad.

4.1.2 Fase de Análisis de Impacto al Negocio (BIA)

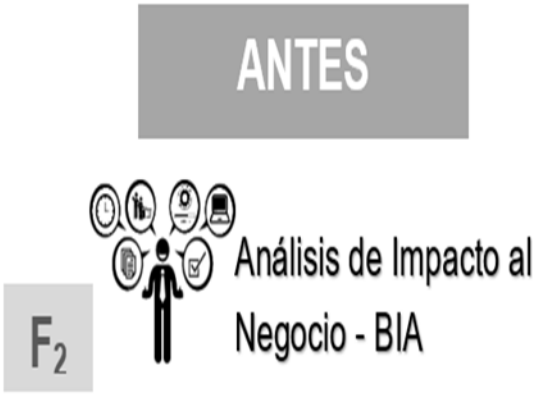

Ilustración 6. *Antes – Análisis de Impacto al Negocio BIA.* ***Fuente:*** *elaboración propia.*

Esta fase 2 corresponde al levantamiento de información sobre los recursos y requisitos de manera particular a las necesidades propias de los procesos al momento de presentarse un

evento o catástrofe natural, cada proceso realiza previamente la identificación de los recursos de recuperación esenciales para respaldar la continuidad de negocio, así como el talento humano de respaldo, recursos físicos, tecnológicos, mobiliario, documentos vitales, suministro eléctrico entre otros; para reducir los impactos de los eventos y abordar las demás fases del Plan de Continuidad del Negocio.

Los recursos de recuperación de los diecinueve (19) procesos deben ser identificados en el levantamiento del Análisis de Impacto al Negocio en los grupos internos, Una vez se finalice el análisis de impacto para la OTI, se debe proceder con el restante de procesos de la entidad para la elaboración del documento consolidado (Consolidado BIA General) el cual contiene la información específica por proceso, direcciones, subdirecciones, lideres, entre otros.

A continuación, se describen cada uno de los aspectos que estructuran el Análisis de Impacto al Negocio realizado en la UARIV:

Datos del proceso:

- Reconocimiento del mapa de procesos de la UARIV, para la identificación de cada uno de los procesos misionales, estratégicos y de apoyo.
- Recolección de la información suministrada por cada proceso.

Entradas y Salidas de Impacto:

- Identificación de las actividades críticas en los procesos.
- Identificación de los activos o actividades necesarias para la ejecución y desarrollo de las actividades críticas en cada uno de los procesos.
- Identificación de las entradas de las actividades críticas, con parámetros necesarios para su correcto entendimiento como son (Proveedores, Grupos de Interés, Medios de recepción y Periodicidad de la actividad).
- Identificación de las salidas de las actividades críticas con parámetros necesarios para su correcto entendimiento como son (Proveedores, Grupos de Interés, Medios de recepción y Periodicidad de la actividad).
- Identificación de los Impactos de Operación, Reputación, Financiero y Legal de cada una de las actividades críticas en los procesos.
- Valoración total del Impacto por la NO ejecución de las actividades críticas.
- Identificación de los periodos de tiempo con más volumen de trabajo de cada una de las actividades críticas.
- Reconocimiento del historial de interrupciones por eventos que han alterado la continuidad de las actividades en los procesos en los últimos 3 años.

Tiempos Críticos:

- **Identificación del RPO:** Se refiere a la pérdida admisible o pérdida máxima de datos generada por un incidente. Este indicador hace referencia al intervalo máximo de tiempo en el que potencialmente se podría perder información, el cual está asociado al momento de la ocurrencia de la falla y la última copia de seguridad o respaldo de los datos.

- **Identificación del RTO:** Se refiere al tiempo máximo en el cual se debe reanudar nuevamente la operación después de una interrupción total o parcial por causa de un evento crítico o catástrofe natural.

Recursos de Recuperación:

- Descripción de los recursos de recuperación mínimos necesarios para operar en contingencia luego de una interrupción total o parcial del proceso por causa de un evento o catástrofe natural. Estos recursos incluyen: talento humano, elementos tecnológicos, recursos físicos, documentos vitales, entre otros.

Actividades Alternas:

- Después de la interrupción de un proceso por causa de un evento crítico o catástrofe natural, es necesario identificar actividades o procedimientos alternos que permitan el logro de los objetivos del proceso dentro de un ambiente de contingencia.

Proveedores:

- Listado de los proveedores catalogados como esenciales en los procesos críticos, los cuales son requeridos para recuperar la operación en un ambiente de contingencia.

Matriz de Comunicaciones:

- Descripción de los mecanismos de comunicación (canales - interlocutores) a seguir en caso de presentarse un evento crítico o catástrofe natural.

Es conveniente realizar el Análisis de Impacto con una periodicidad planificada en la Entidad, para asegurar que la información de recuperación corresponda a las necesidades que los procesos requieren ante una crisis por un evento catastrófico.

4.1.3 Fase de escenarios

Ilustración 7. *Durante – Escenarios de amenaza.* ***Fuente:*** *elaboración propia.*

Una vez se tienen reconocidas las fases 1 y 2 las cuales son vitales para el logro de la fase 3, se encuentra la identificación de los escenarios críticos, mayores o moderados de los procesos identificados a través de los escenarios catastróficos, desastres, emergencias entre otros, son identificados en la Ley 1523 de 2012 (política nacional de gestión del riesgo de desastres) y otras normas que la modifiquen o complementen, presentando que el origen puede ser de

factores externos o internos, afectando el adecuado funcionamiento de los procesos, infraestructura TI, servicios TI, infraestructura física, datos e información y grupos de interés y de valor. Estos escenarios también se encuentran alineados a la Guía No. 10 para la preparación de las TIC para la continuidad del negocio (MinTIC, 2010) y Guía No. 11 para realizar el Análisis de Impacto de Negocios BIA (MinTIC, 2015). Adicionalmente se deberá revisar las diferentes políticas y procedimientos que se tengan en la entidad para determinar su activación o ejecución.

4.1.4 Fase de Estrategias

Ilustración 8. *Durante – Estrategias de continuidad del Negocio.* ***Fuente:*** *elaboración propia.*

Una vez se tienen reconocidas las fases 1, 2 y 3 las cuales son vitales para el logro de la fase 4, se encuentra la identificación de las estrategias de recuperación y solución para cada uno de los escenarios de amenazas que pueden llegar afectar la continuidad de las actividades en la entidad para los 19 procesos.

Al realizar la activación de la estrategia se revisan cuáles componentes (Talento Humano, procesos, infraestructura tecnológica, infraestructura física y datos e Información) se deben asegurar según el escenario de amenaza; con el fin de mitigar los impactos por la interrupción de los escenarios y mitigar la probabilidad de ocurrencia; reduciendo los tiempos de recuperación por medio de la identificación temprana de los recursos de recuperación en el BIA.

Nota: No todos escenarios afectan todos los componentes.

Escenarios De Contingencia Tecnológica:

- Imposibilidad de Acceso a la Infraestructura Tecnológica.
- Imposibilidad de Acceso a los recursos informáticos.
- Acceso no autorizado a las instalaciones.
- Acceso no autorizado a los sistemas de Información.
- Desastres Naturales.
- Fallos de Personal Clave.
- Fallos de Hardware o Software.

4.1.5 Fase del Plan de Crisis o contingencia

Ilustración 9. *Durante – Plan de Crisis o contingencia.* ***Fuente:*** *elaboración propia.*

Una vez se tienen reconocidas las fases 1, 2, 3 y 4 las cuales son vitales para el logro de la fase 5, se describe la hoja de ruta y protocolos para el manejo de crisis o contingencia y acciones para la comunicación de emergencia.

Por medio del Plan de continuidad del negocio la entidad se prepara anticipadamente a los eventos catastróficos y permite manejar de forma clara los pasos generales de cómo reaccionar de manera asertiva y en el menor tiempo posible; con el fin de reducir las afectaciones negativas.

Pasos generarles del Plan de Crisis o Contingencia:

No.	Listado
1.	Evaluación del escenario de crisis o contingencia y determinación de la magnitud de la situación respecto al nivel de amenaza y alerta.
2.	Ejecución del diagnóstico por medio de criterios para identificar una crisis o contingencia, midiendo las afectaciones e impactos a las personas o Talento Humano, infraestructura física, infraestructura tecnológica, procesos y datos o información.
3.	Activación del manejo de crisis o contingencia, según el escenario del evento o catástrofe a través de la OTI.
4.	Activación y ejecución de los recursos, protocolos, planes para el manejo de crisis o contingencia, según la estrategia por el escenario del evento o catástrofe.
5.	Activación del manejo de las comunicaciones durante una crisis o contingencia, (Si aplica a los proveedores para que activen sus propios planes de crisis).

No.	Listado
6.	Ejecución de acciones, procedimientos y planes para regresar a la normalidad analizando las condiciones de las personas o Talento Humano, infraestructura física, infraestructura tecnológica, procesos y datos o información para retornar a la normalidad y así determinar la finalización de la crisis o contingencia.
7.	Evaluación para el mejoramiento continuo del manejo de crisis y contingencia; recopilando las lecciones aprendidas de la aplicación de cada una de las estrategias según el evento o catástrofe presentado.

Tabla 2. *Pasos generarles del Plan de Crisis o Contingencia.* ***Fuente:*** *elaboración propia.*

Todas las crisis o contingencia tienen unas características comunes independientemente de su nivel de importancia, tipo y complejidad; estas poseen tres fases, las cuales se presentan a continuación:

Ilustración 10. *Fases de la crisis contingencia y sus actividades.* ***Fuente:*** *elaboración propia.*

Fase	Descripción de la Actividad	Manejo por Parte de la Unidad Para Las Victimas
Ignición	Se crea la sala de crisis o contingencia conformada por el comité, el cual se reúne para evaluar la situación, en los primeros síntomas del evento o catástrofe, evaluando el impacto negativo en la Entidad.	La Unidad Para Las Victimas ha identificado una serie de escenarios críticos; donde se ha establecido los diferentes eventos tanto internos como externos que pueden afectar a la entidad, de forma negativa e imposibilitarlo en el alcance de sus objetivos; acompañado del Análisis de impacto al negocio donde se

Fase	Descripción de la Actividad	Manejo por Parte de la Unidad Para Las Victimas
	El comité a lo largo de la crisis o contingencia es de vital importancia por la toma de decisiones que permiten pasar a las siguientes fases hasta llegar al final de la crisis. El comité de crisis o contingencia reconoce la crisis según los escenarios evaluando a quienes afecta y la magnitud de la situación por medio de los criterios para identificar una crisis, con los cuales busca apoyar en la cuantificación y cualificación del daño, para una mejor toma de decisiones a la hora de gestionar y contener este tipo de situaciones.	encuentra la identificación de los procesos críticos, recursos de recuperación, tiempos de recuperación entre otros numerales que ayudan en la toma de decisiones por la valoración de los impactos ocasionados en una crisis. Adicionalmente la entidad tiene establecido dentro de su Política Integral para la Administración del Riesgo, realizar monitoreo y seguimiento a los riesgos de manera individual y así contar con una lista de escenarios críticos vigente en todo momento.
Expansión	Acciones que permiten controlar la crisis o contingencia, Son las acciones concretas que el comité debe tomar de forma rápida para evitar la expansión del impacto negativo de la situación de crisis o contingencia y que están encaminadas a neutralizar la causa de la situación de crisis, asegurando en todo momento que se actúe sobre la causa raíz y así resolver el problema de fondo. • Manejo de comunicaciones: Son las acciones de comunicación entre las partes involucradas para poder gestionar eficazmente la situación, transmitiendo o intercambiando información que permita controlar y contrarrestar la crisis presentada.	Paralelamente a las acciones que decida llevar a cabo el comité de crisis o contingencia para el manejo de dichas situaciones, la entidad cuenta con algunos planes de respuesta/contingencia que apoyan a la gestión de las acciones del comité o contingencia Gestión Administrativa: • Atención de Emergencias que prepara a la Entidad en el establecimiento de acciones para afrontar dichas situaciones. • Política o lineamiento de teletrabajo o trabajo en casa, para que los funcionarios

Fase	Descripción de la Actividad	Manejo por Parte de la Unidad Para Las Victimas
		puedan seguir desempeñando sus funciones en la modalidad virtual**.** Gestión de la Información: • Política de seguridad y privacidad de la información • Política de gestión de Incidentes • Política de Seguridad de Protección y Respaldo de Información • Plan de recuperación de desastres tecnológicos en articulación con la Gestión de Continuidad de Negocio. • Política de Seguridad para la Gestión de Contraseñas • Política Buen Uso de Correo Institucional • Política Sobre el Uso de Equipos de Cómputo y Acceso a la Red. • Política Sobre el Uso de Equipos de Cómputo y Acceso a la Red. • Política de Seguridad para la Gestión de Riesgos • Política de Seguridad Física y el Entorno • Política de Seguridad Actualizaciones de Software • Política de Seguridad Relación con Proveedores

Fase	Descripción de la Actividad	Manejo por Parte de la Unidad Para Las Victimas
		En cuanto al manejo de las comunicaciones a través del proceso de estrategia de Comunicaciones se debe tener en cuenta: • Instructivo Portal Web, para la publicación de contenidos en la misma • Instructivo Redes Sociales, para el manejo de las comunicaciones en dichos canales conocidos como redes sociales • Manual de Comunicación Interna y Externa para la divulgación de información a los diferentes grupos de valor de la entidad.
Declinación	Cuando la crisis o la contingencia se reduce y se realizan todas las actividades para el retorno a la normalidad, esta fase analiza todas las condiciones para decidir cuando la Entidad volverá a trabajar bajo normalidad y recuperar la continuidad del negocio en los procesos de la mano con la operación y servicios.	Acciones para retornar a la normalidad las cuales son consultadas por el comité de crisis o continuidad según los escenarios, la entidad cuenta con recomendaciones de retorno que apoyan a la gestión de las acciones: • Instructivo de Gestión de Incidentes Mayores, para retornar los servicios TIC. • Plan de Emergencias • Política de seguridad y salud en el trabajo.

Tabla 3. *Actividades del manejo de crisis o contingencia.* ***Fuente:*** *elaboración propia.*

4.1.6 Fase del Plan de Comunicaciones

Ilustración 11. *Durante – Plan de Comunicaciones.* ***Fuente:*** *elaboración propia.*

Una vez se tienen reconocidas las fases 1, 2, 3, 4 y 5 las cuales son vitales para el logro de la fase 6, donde se describen las actividades de comunicación hacia el Talento Humano seleccionado según el evento o catástrofe natural; con el fin de mantenerlos informados de cómo actuar ante el desastre para salvaguardar la vida y después para que se encuentren enterados de las estrategias adoptadas por la entidad, con el fin de restablecer la continuidad.

Una comunicación a tiempo y especifica de protocolos de desastre y recuperación del negocio; brinda seguridad y confianza en la entidad y a los grupos de interés y de valor; reflejando alineación entre todos los respondientes ante una crisis y llegar de esta manera al logro de los objetivos a corto, mediano y largo plazo del Plan de continuidad del negocio.

En la comunicación al público objetivo se deben tener en cuenta los siguientes elementos:

Elemento	Descripción
Hechos	Contiene la información propia que se quiere transmitir, la cual puede incluir, las personas o grupo afectado, el lugar, la fecha y las circunstancias que describen la afectación.
Impacto	Descripción del impacto que tendrá en la Entidad.
Acciones de contención	Descripción de las acciones realizados o por realizar para evitar la expansión de la situación de crisis.
Alcance Zonal	Describe el alcance que tendrá en la Entidad, si es local en una sola dirección, regional o a nivel nacional.
Tipo de Crisis	Describe el tipo de crisis de acuerdo con el tipo de escenario de crisis presentado: sismo, inundación, incendio, terrorismo, etc.

Tabla 4. *Elementos que se deben comunicar.* ***Fuente:*** *elaboración propia.*

Para ejecutar las actividades de comunicaciones en el manejo de crisis se debe tener en cuenta quienes serían los voceros autorizados y que deberán comunicar en una crisis o contingencia, con esto se debe aplicar procedimientos o actividades de forma eficiente y efectiva respetando los lineamientos ya establecidos.

Ilustración 12. *Actividades del Plan de Comunicaciones.* ***Fuente:*** *elaboración propia*

La Fase 1 y 6 identifican los equipos de respuesta y el manejo de crisis o contingencia; estas 2 fases deben encontrarse alineadas y articuladas, con el fin de proporcionar respuestas acertadas al momento de ejecutar las comunicaciones.

4.1.7 Fase de Manejo de Incidente y Recuperación

Ilustración 13. *Manejo de Incidentes y Recuperación.* ***Fuente:*** *elaboración propia.*

Una vez se tienen reconocidas las fases 1, 2, 3, 4, 5, 6 las cuales son vitales para el logro de la fase 7, se describe la información específica a recuperar según un evento o catástrofe natural; permitiendo restablecer aspectos de continuidad de la operación mediante la reanudación de los sistemas e infraestructura TI que ayudan a la Entidad a soportar las actividades críticas dentro de los procesos.

Los lineamientos de aplicación para esta fase son propios de cada entorno a recuperar; ya sea los sistemas de información, infraestructura tecnológica y todo lo relacionado con TI. En relación con incidentes ocasionados por la afectación de las tecnologías de la información en

la Entidad se establece el Plan de Recuperación de Desastres – DRP (Disaster Recovery Plan) para la infraestructura tecnológica que soporta los servicios.

Para el logro de los objetivos el DRP se alinea con el BCP a través del levantamiento de Análisis de Información al Negocio, con el fin de asegurar el cumplimiento de las necesidades desde los procesos; así como los tiempos de recuperación, disponibilidad de los activos de información críticos y sistemas de información entre otros servicios TI.

A continuación, se listan algunos de los puntos de manejo de incidente y recuperación para tener en cuenta para el manejo de los incidentes y recuperación de los servicios TI.

No.	Listado
1.	Comunicar y activar el personal de respaldo en cada rol y responsabilidad de la ejecución las actividades críticas de los servicios TI.
2.	Comunicar y activar si es necesario la continuidad con los proveedores que soporten los servicios TI.
3.	Activar o gestionar si es necesario una sede alterna con las condiciones mínimas para que se pueda operar de forma segura los servicios TI.
4.	Activar o gestionar si es necesario plataformas virtuales o remotas alternas con las condiciones de seguridad de la información para que se pueda desarrollar las actividades críticas de los procesos y así mismo garantizar la disponibilidad inmediata en caso de no contar con los equipos propios de la sede u oficina principal.
5.	Garantizar el cumplimiento de las políticas de backup, con el fin de restablecer la información y así mismo que se encuentre disponible para el personal que lo requiera en cualquier proceso o servicio.
6.	Tener claro y disponible de forma digital los procedimientos que sean necesarios para el desarrollo de las actividades de los servicios TI desde operación.
7.	Tener disponible de forma digital y actualizado el inventario de los equipos y bienes de cada uno de los procesos.
8.	Todo el personal debe estar al tanto de cómo actuar y proceder según la señalización indicada en caso de un evento o catástrofe natural.
9.	Activar si es necesario las pólizas que haya lugar para el restablecimiento de servicios TI.

Tabla 5. *Puntos de manejo de incidente y recuperación.* ***Fuente:*** *elaboración propia.*

4.1.8 Fase de Pruebas y Revisión

Ilustración 14. *Después – Pruebas y Revisión.* ***Fuente:*** *elaboración propia.*

Una vez se tienen reconocidas las fases 1, 2, 3, 4,5, 6 y 7 las cuales son vitales para el logro de la fase 8, donde se realiza revisión de las fases del Plan de Continuidad del Negocio identificando que se debe mejorar, actualizar o cambiar por medio de la aplicación de pruebas con el fin de validar la gestión y efectividad para garantizar el cumplimiento de los objetivos.

Para la ejecución y desarrollo de las pruebas se inicia la simulación de escenarios de eventos y catástrofes a corto y largo plazo, donde se debe activar el Plan de Continuidad ya creado y realizar el paso a paso documentando resultados de cada una de las fases, para tomar las decisiones según el cumplimiento de efectividad y eficacia de los procedimientos del Plan.

Se recomienda la realización periódica de los Planes de Pruebas, teniendo en cuenta lo siguiente:

No.	Listado
1.	Mantener la información actualizada de los Planes de Continuidad.
2.	Revisar si los objetivos son consistentes con la continuidad del negocio.
3.	Evaluar y actualizar si es necesario la efectividad de los tiempos de recuperación establecidos en el Plan de Continuidad, verificando la disponibilidad requerida por los procesos y servicios.
4.	Evaluar la efectividad e idoneidad de los roles y responsabilidades definidas para la activación de los Planes de Continuidad y así mismo la certidumbre de las actividades diseñadas para la continuidad.
5.	Revisar y validar si se cumplen los objetivos de las estrategias de continuidad planteadas para los escenarios de amenaza.
6.	Evaluar la capacidad de respuesta de los grupos de interés y de valor implicados en el Plan de Continuidad, así mismo con las pruebas se busca concientizar sobre los impactos que pueden tener para la Entidad la materialización de un evento o catástrofe.
7.	Evaluar la capacidad de respuesta de los proveedores al momento de activar sus propios planes de continuidad que aseguren la disponibilidad de los servicios contratados para el cumplimiento de las actividades en los procesos de la Entidad.

8.	Evaluar la correcta ejecución del Plan de crisis y continuidad, identificando si las fases ignición, expansión y declinación si se están cumpliendo.

Tabla 6. *Objetivos de la fase de pruebas y revisión.* ***Fuente:*** *elaboración propia.*

4.1.9 Fase del Plan de Gestión Del Cambio

Ilustración 15. *Después - Plan de Gestión del Cambio.* ***Fuente:*** *elaboración propia.*

Una vez se tienen reconocidas las fases 1, 2, 3, 4, 5, 6, 7 y 8 las cuales son vitales para el logro de la fase 9, el Plan de Gestión del Cambio es vital para la adaptación de todos los cambios necesarios para llevar a cabo el Plan de Continuidad del Negocio a la Entidad.

Para lograr el cumplimiento de los objetivos del Plan de Continuidad se deben realizar modificaciones, implementaciones, adaptaciones, diseñar nuevos procedimientos, ajustar los existentes entre otras oportunidades de mejora que lleven a la transformación y aplicación de los lineamientos de Continuidad en la Entidad.

Con el fin de llevar esta tarea a cabo se deben utilizar las buenas prácticas de gestión del cambio organizacional, con el fin de asegurar en la Entidad las modificaciones o mantenimientos necesarios para implementar el Plan de Continuidad; para esto se debe utilizar la gestión del aspecto/factor humano entre otras.

4.1.10Fase del Plan de Capacitación

Ilustración 16. *Después – Plan de Capacitación.* ***Fuente:*** *elaboración propia.*

Una vez se tienen reconocidas las fases 1, 2, 3, 4, 5, 6, 7, 8 y 9 las cuales son vitales para el logro de la fase 10, el Plan de Capacitación hace parte del Plan de Gestión del Cambio con el fin de realizar actividades enfocadas a la capacitación y concientización de los funcionarios con

el objetivo de hacerlos parte del cambio logrando que se apropien de cómo actuar en una situación de evento o catástrofe natural.

Esta orientación deberá ser tanto técnica como especializada para realizar las actividades propias de cada rol o responsabilidad asignada para diseñar y desarrollar el Plan de Continuidad del Negocio, resaltando la importancia de los funcionarios, contratistas y proveedores los cuales son pieza clave para este cambio en la Entidad.

5. DOCUMENTOS DE REFERENCIA

Tipo	**Otra. ¿Cuál?**	**No.**	**Año**	**Expedida por**	**Título de la Norma (Por medio del cual se regula)**
Otra normatividad	Estándar Internacional	22301	2019	International Organization for Standardization	ISO 22301 2019 Requerimientos para la implementación de sistemas de gestión de continuidad de negocio. Seguridad y resiliencia.
Otra normatividad	Modelo de Seguridad		2010	MinTIC	Modelo de Seguridad y Privacidad de la Información "Para que las Entidades públicas incorporen la seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y, en general, en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos."
Otra normatividad	Guía	10	2010	MinTIC	MINTIC – Guía no. 10 Para la preparación de las TIC para la continuidad del negocio.
Otra normatividad	Guía	11	2015	MinTIC	MINTIC – Guía no. 11 Para realizar el Análisis de Impacto de Negocios BIA
Otra normatividad	Estándar Internacional	27001	2022	International Organization for Standardization	Modelo De Seguridad Y Privacidad De La Información (MSPI) – Requisitos. Norma internacional de Seguridad de la Información que pretende asegurar la confidencialidad, integridad y disponibilidad de la información de una organización y de los sistemas y aplicaciones que la tratan.

6. ANEXOS

No aplica.

7. CONTROL DE CAMBIOS

Versión	Fecha	Descripción de la modificación
1.0	24/04/2025	Creación del documento Metodología de Continuidad de Negocio u Operación