Objetivo:

Analizar e identificar las actividades y procesos críticos de la Empresa, para establecer los riesgos, escenarios, componentes, controles y acciones que le permitan, continuar realizando sus operaciones cuando sea afectado por contingencias mayores

Alcance:

Aplica a cada uno de los procesos de EAAB en el escenario de continuidad, incluyendo servicios que realizan terceros en el marco de los objetivos de cada proceso; inicia con el análisis de impacto de no contar con los servicios de cada proceso (BIA) y finaliza con el mantenimiento del plan y gestión de los riesgos de continuidad de la Empresa.

Términos y definiciones:

1 **ANALISIS DE IMPACTO DE NEGOCIO**(EN INGLÉS BUSINESS IMPACT ANALYSIS- BIA): Actividad por medio de la cual la Empresa analiza cada uno de los impactos de manera cualitativa (financieros y no financieros), sus efectos y pérdidas que pueda sufrir la organización provocados por un incidente o evento imprevisto que interrumpa la continuidad de la operación. Los resultados del BIA se utilizan para apoyar la toma de decisiones concernientes a la solución y la estrategia del Plan de Continuidad del Negocio.

2 **CRISIS**: Ocurrencia de un evento que amenaza las operaciones, el personal, las partes interesadas, la reputación, la confianza, la estrategia y objetivos de la Empresa.

3 **ELEMENTO VITAL**: Conjunto de cosas que un proceso y/o Dirección consideran importantes para mantener y recuperar los servicios que presta a la Organización. Ejemplo: Documentos como pólizas, contratos, convenios; elementos de trabajo con terceros, como Tokens, certificados, usuarios, contactos, enlaces; Contactos críticos para manejo de una situación de contingencia como prensa, redes sociales, servicios en la nube, servicios en sitio; elementos como portátiles, configuraciones, impresoras, sellos, formas continuas etc. En general todo aquello que se considere crítico en una recuperación y se hallan tomado las provisiones para tener copia en un evento de interrupción mayor.

4 **ESCENARIOS DE RECUPERACIÓN**: Contingencias o eventos mayores incluidas dentro del Plan de Continuidad de EAAB.

5 **GESTIÓN DE CONTINUIDAD DEL NEGOCIO** (EN INGLÉS – BUSINESS CONTINUITY MANAGEMENT- BCM): Es el proceso de negocio responsable de gestionar el riesgo de interrupción que tiene un alto impacto en la continuidad del negocio de sus procesos.. BCM protege los intereses de la organización, la reputación, la marca, la ciudadanía y las actividades que aportan valor al negocio. Los procesos de BCM incluyen reducir el riesgo a un nivel aceptable y planificar el restablecimiento de los procesos de negocio ante una situación de interrupción. BCM establece los objetivos, el ámbito y los requerimientos para una Gestión de la Continuidad de los Procesos (Ref. Itil V4.0).

6 **GESTIÓN DE CRISIS**(EN INGLÉS CRISIS MANAGEMENT): Proceso mediante el cual una organización administra el impacto causado por un evento o incidente a la continuidad de las operaciones de la organización hasta que esté bajo control y deje de afectar la organización. El Plan de Manejo de Crisis se activa como parte del proceso de gestión de crisis.

7 **IMPACTO**: El costo para la empresa de un incidente , que puede ser medido en términos cualitativos o cuantitativos -p.ej., pérdida operativa, pérdida de reputación, implicaciones legales, etc.

8 **INCIDENTE**: Cualquier evento que puede estar o puede adelantar la interrupción o la crisis de la Empresa.

9 **PÉRDIDA**: Consecuencia negativa que puede ser financiera, como pérdida de efectivo, o no financiera como pérdida de información o de reputación.

10 **PLAN DE MANEJO DE CRISIS** (EN INGLÉS -CRISIS MANAGEMENT PLAN): Plan de acción claramente definido y documentado para su uso en el momento de una crisis. Este plan cubre normalmente las personas clave, los recursos, servicios y acciones necesarias para implementar y administrar el proceso de gestión de crisis

11 **PLAN DE MANTENIMIENTO**: Es el proceso de administrar y mantener actualizados los planes de Continuidad de la organización para que cuando se requiera, su utilización sea segura y efectiva.

12 **PLAN DE PRUEBAS**: Es un programa de trabajo diseñado para planear y ejecutar las pruebas del plan de continuidad, los roles de las personas, los sistemas de información y los procesos

13 **PLAN GENERAL DE CONTINUIDAD DE LA EAAB:** Entiéndase por "plan general de continuidad de la Empresa" las actividades y documentación incluidos en el proceso de continuidad de la Empresa, con responsables, agendas y prioridades establecidas en planes por Procesos de Negocio.

14 **PLAN DE CONTINUIDAD DE NEGOCIO (EN INGLÉS - BUSINESS CONTINUITY PLAN – BCP):** Plan que define los pasos que se requieren para el restablecimiento de los procesos de negocio después de una interrupción. El plan también identifica los disparadores para la Invocación, las personas involucradas, las comunicaciones, entre otros.

15 **PLAN DE RECUPERACIÓN DE DESASTRES (EN INGLÉS - DISASTER RECOVERY PLAN - DRP):** Describe cómo el área de TI enfrenta posibles desastres mayores que afecten su área de tecnología de la información. Planes direccionados para hacer frente a ocurrencias de desastre no deseados en la infraestructura de TI y para el que es necesario un gran esfuerzo para restaurar el nivel de rendimiento original de los sistemas o servicios provistos a la organización. Tradicionalmente el término se ha utilizado para referirse a la planificación para la recuperación de sistemas informáticos en lugar de procesos de negocio y usualmente se dimensionan para realizarse en instalaciones físicas diferentes al centro de procesamiento principal y/o en la nube. El plan también define los pasos necesarios para recuperar uno o más servicios de TI orientados a los procesos de negocio, además identificará los disparadores de la Invocación del plan y las personas que han de ser involucradas, las comunicaciones necesarias, entre otros.

16 **PRUEBA**: Actividad en la cual se hace seguimiento a una parte o partes de un plan de continuidad de negocios, para asegurar que el plan contiene la información y los procedimientos adecuados deseables como resultado final. Una prueba difiere de un simulacro en que la prueba ocurre en un sitio alterno mientras que el ejercicio normalmente es un ejercicio completo.

17 **PUNTO OBJETIVO DE RECUPERACIÓN** (EN INGLÉS RECOVERY POINT OBJECTIVE RPO): Es el punto en el tiempo para el cual los datos deben estar restaurados luego de un evento o incidente que interrumpa la operación normal del negocio. También se conoce como la máxima cantidad admisible de pérdida de datos luego del backup que antecede al evento de interrupción.
Esta sigla hace referencia a "punto objetivo de recuperación "dado por su nombre en ingles "recovery point objective", el cual es definido por el plan de continuidad del negocio.

18 **REGISTRO VITALES**: Son los registros impresos o almacenados en medio magnético considerados como esenciales para la continuación del negocio luego de un evento o incidente de interrupción.

19 **RESPALDO O BACKUP**: Proceso mediante el cual los datos contenidos en un medio electrónico o impreso, son copiados en otro medio de tal forma que queden disponibles y puedan utilizarse en el caso en que los datos originales sean destruidos, extraviados o dañados.

20 **SIMULACRO**: Ejecución anunciada o no anunciada de un plan de Continuidad de Negocio con el objetivo de verificar la operación del plan en una situación real y así implementar o identificar necesidades de complementarlo y de ajustar controles para que permanezca vigente.

21 **TIEMPO DE INACTIVIDAD MÁXIMO TOLERABLE** (EN INGLÉS MAXIMUN TOLERABLE PERIOD OF DISRUPTION- MTPD): Este tiempo representa el periodo máximo de tiempo de inactividad que puede tolerar la organización, ante la ausencia o indisponibilidad de una función particular del negocio. Este tiempo de inactividad está compuesto por dos elementos, el tiempo de recuperación del sistema y el tiempo de recuperación del trabajo, entonces se podría expresar como MTPD = RTO + WRT.

22 **TIEMPO OBJETIVO DE RECUPERACIÓN** (EN INGLÉS RECOVERY TIME OBJECTIVE - RTO): Es el dato esencial del BIA que identifica el tiempo en el cual las Actividades de Misión Críticas y/o sus dependencias deben estar recuperadas luego de un evento que interrumpa la operación normal del negocio.

23 **TIEMPO DE RECUPERACIÓN** (EN INGLÉS WORK RECOVERY TIME WRT): Es el tiempo disponible para recuperar datos perdidos una vez que los sistemas están reparados dentro del MTPD.

24 **VEEDOR**: Persona asignada con un rol específico, para cada simulacro, prueba o evento real de un evento mayor de interrupción, con la responsabilidad de verificar el nivel de alistamiento que tiene la Empresa para afrontar esta situaciones, documentado las lecciones aprendidas de cada ejercicio.

Políticas de Operación:

1 Cada proceso de negocio debe disponer de un plan de continuidad de negocio, su análisis de impacto "BIA", su socialización así como, un programa periódico de simulacros y pruebas.

2 Dentro del plan general de continuidad de EAAB deben estar incluidas las acciones con sus componentes para cada proceso, priorizadas por el nivel de importancia de cada proceso generado dado por el BIA.

3 El plan de tratamiento de los riesgos de continuidad de EAAB debe incluir la secuencia de acciones que llevan al riesgo a niveles aceptables, estandarizados y difundidos, de acuerdo con la definido en el Procedimiento MPEE0301Administración de Riesgos y Oportunidades.

4 Cuando la Empresa o un proceso se encuentre en la modalidad de contingencia, los niveles de seguridad y privacidad de la información de sus servicios no se deben ver disminuidos.

5 Cuando la Entidad incorpore nuevos servicios o soluciones de negocio, se debe actualizar el respectivo BIA, desarrollar los planes de continuidad de negocio y de tecnología de la información, integrados a los Institucionales.

6 Se debe preservar un histórico documentado de las actualizaciones y/o modificaciones de cada plan de continuidad mediante un manejo de versiones aprobadas en la herramienta definida por la Empresa.

7 El plan de continuidad debe estar articulado con la Gestión de Crisis de la Empresa en la herramienta definida.

8 Cada Simulacro, prueba o incidente de contingencia debe contar con un veedor, que debe tener definido y escrito su papel.

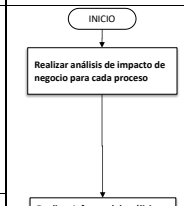
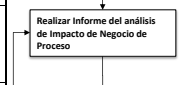
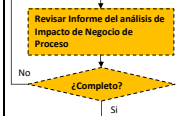
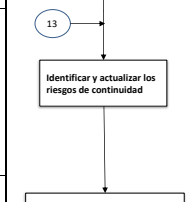
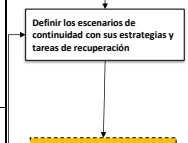
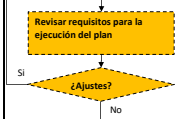
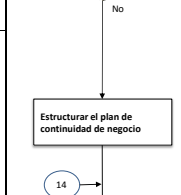
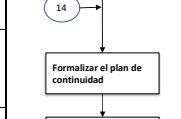
9 Cada proceso de negocio como primera línea de defensa, debe hacer un seguimiento a su plan de continuidad y al plan periódico de pruebas. El líder de Continuidad de negocio, como segunda línea de defensa, hará seguimiento al cumplimiento de cada proceso con su plan de continuidad.

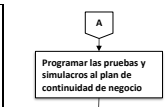
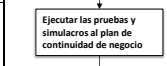
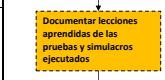
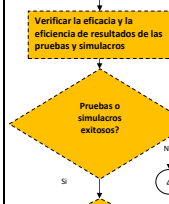
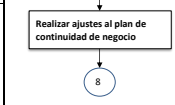
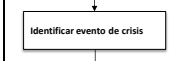
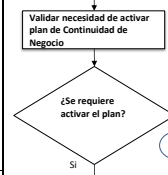
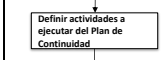
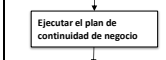
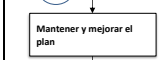
Documentos de soporte

CÓDIGO	NOMBRE	Actividades	ENTIDAD
MPFT0217I01	Instructivo BIA	1	EAAB-ESP
MPFT0217F01	Análisis de Impacto de Negocio Por Proceso	1	EAAB-ESP
MPFT0217F02	Servicios críticos del Proceso	1	EAAB-ESP
MPFT0217F03	Descripción detallada de actividades por servicio	1	EAAB-ESP
MPFT0217F04	Roles y Responsabilidades en modalidad de contingencia	1	EAAB-ESP
MPFT0217F05	Matriz RACI de responsabilidades	1	EAAB-ESP
MPFT0217F06	Contactos Internos	1	EAAB-ESP

MPFT0217F07	Registros Vitales	1	EAAB-ESP
MPFT0217F08	Elementos requeridos en Contingencia	1	EAAB-ESP
MPFT0217F09	Contactos de Proveedores	1	EAAB-ESP
MPFT0217F10	Escenarios y Estrategias de Recuperación	5,6	EAAB-ESP
MPFT0217F11	Plan de Continuidad de negocio EAAB-ESP	7, 8	EAAB-ESP
MPFT0217F12	Matriz de Audiencias, Mensajes y Canales del Plan de Continuidad	9	EAAB-ESP
MPFT0217F13	Eventos Pruebas Simulacros Crisis de Continuidad de Negocio	11, 12	EAAB-ESP
MPEE0301P	Administración de Riesgos y Oportunidades	4,21	EAAB-ESP
MPEE0301F01	Matriz de Riesgos	4,21	EAAB-ESP
MPFD0801F06	Acta de comité	8	EAAB-ESP
MPFD0801F08	Informe	2 y 3	EAAB-ESP
MPFD0801F09	Certificación	8	EAAB-ESP
MPEE0109F01	Plan De Acción Y Cronograma	9, 10	EAAB-ESP
MPEH0502P	Inducción	9	EAAB-ESP
MPEH0503P	Reinducción	9	EAAB-ESP

Actividades

#	Nombre de la actividad	Descripción	Registro	Responsable
1		Elabora/actualiza el Análisis de Impacto de Negocio del proceso en el formato MPFT0217F01 siguiendo el instructivo MPFT0217I01 "Desarrollo del BIA de cada Proceso" y posteriormente realiza el diligenciamiento del conjunto de formatos de Plan de Continuidad relacionados con: 1. Inventario completo de los Servicios críticos del proceso en el formato MPFT0217F02. 2. Descripción detallada de actividades por servicio en el formato MPFT0217F03. 3. Roles y Responsabilidades en modelidad de Contingencia en el formato MPFT0217F04. 4. Matriz RACI responsabilidades en contingencia en el formato MPFT0217F05. 5. Contactos Internos en el formato MPFT0217F06. 6. Registros Vitales en el formato MPFT0217F07. 7. Elementos requeridos en contingencia en el formato MPFT0217F08. 8. Contactos de Proveedores en el formato MPFT0217F09. Ver y aplicar Políticas Operacionales número 1 y 5.	MPFT0217F01 "Análisis de Impacto de Negocio por Proceso" elaborado MPFT0217F02 "Servicios críticos del proceso" MPFT0217F03 "Descripción detallada de actividades por servicio" MPFT0217F04 "Roles y Responsabilidades" MPFT0217F05 "Matriz RACI responsabilidades" MPFT0217F06 "Contactos Internos" MPFT0217F07 "Registros Vitales" MPFT0217F08 "Elementos requeridos en contingencia" MPFT0217F09 "Contactos de Proveedores" diligenciados	Líder del proceso Jefes de Oficina Nivel 06 Jefes de oficina Nivel 08 Director Nivel 08 Facilitador de cada área
2		Con la información diligenciada en la encuesta BIA se genera el informe con el detalle de las funciones y procesos críticos del negocio, así como la información básica de los recursos requeridos y los tiempos de recuperación para que la empresa pueda poner en funcionamiento los servicios y por ende la continuidad del negocio, teniendo en cuenta la Política Operacional número 2.	MPFD0801F08 "Informe" del análisis de Impacto de Negocio de Proceso elaborado.	Coordinador de Seguridad de la Información Dirección de Servicios informáticos Profesional Especializado nivel 20
3		Se revisa el informe frente a la información diligenciada en los formatos MPFT0217F02 al MPFT0217F09 "Conjunto de Formatos Plan de Continuidad" y a la encuesta BIA de Archer, con el fin de validar la coherencia entre los diferentes instrumentos y que el informe contenga la información requerida para activar la continuidad del negocio cuando se requiera. En caso en que no se esté completo, se remite mediante correo electrónico al coordinador de Seguridad de la Información para que realicen los respectivos ajustes.	IMPFD0801F08 "Informe" del análisis de Impacto de Negocio de Proceso aprobado Correo electrónico	Líder del proceso Jefes de Oficina Nivel 06 Jefes de oficina Nivel 08 Director Nivel 08 Facilitador de cada área
4		Con el acompañamiento de la Dirección de Servicios Informáticos revisa los riesgos identificados del proceso y valida si pueden ser categorizados como riesgos de continuidad realizando la actualización. En caso en que no apliquen los riesgos actuales, se realiza la revisión de diferentes variables como el entorno físico, tecnológico y organizacional, eventos de indisponibilidad de los servicios informáticos que soporta los procesos de negocio y se ejecutan las etapas de identificación, análisis, valoración y manejo de los riesgos de continuidad aplicables al proceso; en esta identificación se debe incluir el análisis de amenazas a las que se expone cada proceso a escala EAAB-ESP, así como las vulnerabilidades que existen y los planes de mejora (Ver Política Operacional número 3) para controlarlos efectivamente con base en lo definido en el procedimiento MPEE0301P Análisis de Riesgos y Oportunidades.	Matriz de Riesgos MPEE0301F01 del Proceso actualizada	Líder del proceso Jefes de Oficina Nivel 06 Jefes de oficina Nivel 08 Director Nivel 08 Facilitador de cada área
5		De acuerdo con los resultados de la valoración de los procesos en el análisis BIA y la identificación de riesgos de continuidad, se procede a definir los escenarios con sus estrategias de recuperación que permitan afrontar, desarrollar y proveer continuidad a las funciones de la Empresa junto con sus tareas de recuperación, en caso de interrupciones mayores (representadas en escenarios), diligenciando el formato MPFT0217F10 "Escenarios y Estrategias de Recuperación" y teniendo en cuenta la Política Operacional número 4. **Nota:** Los escenarios, con las estrategias y tareas de recuperación se formulan de manera general para la empresa.	MPFT0217F10 "Escenarios y Estrategias de Recuperación" totalmente diligenciadas.	Coordinador de Seguridad de la Información Dirección de Servicios informáticos Profesional Especializado nivel 20
6		Realiza la revisión general de las estrategias de continuidad diseñadas y valida que las tareas de recuperación definidas para la estrategia tengan relación con los eventos de interrupción seleccionados En caso de requerir ajustes, se realiza la redefinición y formalización de las estrategias de continuidad.	MPFT0217F10 "Estrategias de Recuperación" totalmente diligenciadas.	Coordinador de Seguridad de la Información Dirección de Servicios informáticos Profesional Especializado nivel 20
7		Con base en los objetivos establecidos en el BIA y sus resultados, se estructura el plan de continuidad de negocio de la Empresa, donde para cada proceso se incluyen en el formato MPFT0217F11 "Plan de Continuidad de negocio EAAB-ESP": a) Las estrategias seleccionadas b) Los servicios críticos del área c) La descripción detallada de cada servicio d) Los roles y responsabilidades en contingencia e) Matriz RACI de responsabilidades en contingencia f) Contacto internos g) Registros vitales del proceso h) Los elementos requeridos en contingencia y contactos de proveedores. Aplicar Política Operacional número 6.	MPFT0217F11 "Plan de Continuidad de la Empresa" estructurado y diligenciado .	Coordinador de Seguridad de la Información Dirección de Servicios informáticos Profesional Especializado nivel 20
8		Presenta el plan de continuidad al Comité Corporativo de la Empresa para su adopción y formalización en cada uno de los Procesos.	MPFT0217F11 "Plan de Continuidad de negocio EAAB-ESP" formalizado MPFD0801F06 "Acta de comité" MPFD0801F09 "Certificación"	Comité Corporativo Líder de cada proceso Jefes de Oficina Nivel 06 Jefes de oficina Nivel 08 Director Nivel 08
9		El coordinador de Seguridad de la Información desarrolla/actualiza la matriz de audiencias, mensajes y canales del Plan de Continuidad de la Empresa a Impactados e Involucrados en el formato MPFT0217F12 junto con el plan de socialización en el formato MPEE0109F01 teniendo en cuenta la madurez que lleve la organización en sus procesos y las lecciones aprendidas de eventos de continuidad. Este plan debe ejecutarse, ser certificable y continuo en el tiempo y también incluirse en la inducción a funcionarios y contratistas atendiendo lo definido en el procedimiento MPEH0502P de Inducción y MPEH0503P de Reinducción	Matriz de Audiencias, Mensajes y Canales del plan de continuidad diligenciada en el formato MPFT0217F12 con su Programa de socialización en el formato MPEE0109F01 Plan De Acción Y Cronograma.	Coordinador de Seguridad de la Información Dirección de Servicios informáticos Profesional Especializado nivel 20

10		Programa las pruebas y simulacros de los planes de continuidad de negocio en conjunto con los servicios de Tecnología de la Información.	Programa de pruebas diligenciado en el formato MPEE0109F01 "Plan De Acción Y Cronograma" y registrado en Archer	Coordinador de Seguridad de la Información Dirección de Servicios informáticos Profesional Especializado nivel 20
11		Ejecuta las pruebas y simulacros del plan de continuidad de negocio, siguiendo lo definido. Aplicar Política Operacional número 8.	MPFT0217F13 Eventos de pruebas, simulacros crisis del Plan de Continuidad de Negocio	Líderes de proceso Jefes de Oficina Nivel 06 Jefes de oficina Nivel 08 Director Nivel 08 Facilitador de cada área
12		El veedor del plan debe documentar el desarrollo de las pruebas y simulacros realizadas, los resultados del evento, las lecciones aprendidas y los riesgos que se materializan, lo anterior como insumo para la formulación de planes de mejora.	MPFT0217F13 Resultados de la pruebas y simulacros de crisis en Archer.	Veedor
13		Verifica los resultados de las pruebas y simulacros del Plan de Continuidad de EAAB con el fin de validar que el plan formulado da respuesta a los eventos en crisis a los que se puede enfrentar, el cual debe contener: •Riesgos de interrupción identificados y tratados adecuadamente. •Documentación completa y actualizada •Responsabilidades asignadas y entrenadas. •Aprobaciones •Cumplimiento de los requerimientos de negocio •Efectividad de los resultados •Situaciones no controladas durante la prueba •Acciones de mejoramiento •Manejo de eventos e incidentes. •Lecciones aprendidas. •Efectividad del Veedor En caso en que las pruebas o simulacros no fueron exitosos se informan mediante correo electrónico las observaciones y el resultado de la prueba para que se valore nuevamente el riesgo y se formulen planes de mejora. Cuando se identifican cambios en el plan de continuidad de negocio formulado inicialmente, se informan los ajustes mediante correo electrónico a los procesos implicados. Aplicar Política Operacional número 9.	Registro en Archer del análisis de eficacia y eficiencia de los resultados de las pruebas y simulacros de crisis. Correo electrónico	Coordinador de Seguridad de la Información Dirección de Servicios informáticos Profesional Especializado nivel 20
14		Realizar los cambios al plan de continuidad de negocio del proceso formulado inicialmente de acuerdo con las observaciones recibidas producto de las pruebas, simulacros, cambios realizados	Registro en Archer de los planes actualizados.	Líderes de proceso Jefes de Oficina Nivel 06 Jefes de oficina Nivel 08 Director Nivel 08 Facilitador de cada área
15		Cada vez que el proceso identifica un evento de crisis informa a la mesa de servicio mediante correo electrónico para que informe al Comité de Crisis, y validen si se requiere activar el plan de continuidad de negocio, detallando la situación.	Correo electrónico	Líderes de proceso Jefes de Oficina Nivel 06 Jefes de oficina Nivel 08 Director Nivel 08 Facilitador de cada área
16		Analizan el evento de crisis teniendo en cuenta el alcance y el impacto del evento y establecen si se requiere activar o no el plan de continuidad de negocio. Ver Política Operacional número 7. La decisión se informa mediante correo electrónico al Líder de Continuidad de Negocio y al Líder del proceso que identificó el evento de crisis	Correo electrónico	Comité de Crisis
17		El líder junto con el grupo designado para el manejo de crisis de continuidad de negocio analiza el evento presentado y selecciona del Plan de Continuidad el conjunto de actividades a ejecutar. Considerar la Política Operacional número 4.	Planes de Continuidad de Negocio seleccionados para el manejo de crisis	Líder de Continuidad de negocio junto con el grupo de Manejo de Crisis de Continuidad de Negocio
18		Cada vez que se presente un evento se activa el plan de continuidad de negocio del proceso estructurado y adoptado por la empresa y se ejecutan las actividades definidas.	Reporte de ejecución de actividades ejecutadas del Plan de Continuidad	Grupo de Manejo de Crisis de Continuidad de Negocio
19		El veedor del plan debe documentar los resultados del evento, las lecciones aprendidas y los riesgos que se materializan, lo anterior como insumo para la formulación de planes de mejora. En caso en que se identifiquen cambios en el plan de continuidad de negocio formulado inicialmente, se informan los ajustes mediante correo electrónico al líder de Continuidad de Negocio de EAAB. Aplicar Políticas Operacionales número 8 y 9.	Correo electrónico Documento de Lecciones Aprendidas.	Veedor
20		Actualiza el plan respectivo para que éste refleje los diferentes cambios que se van dando con el tiempo en la estructura del negocio, los cambios Tecnológicos, proyectos y todos aquellos elementos que lo mantienen alineado a las necesidades de negocio. Aplicar Política Operacional número 9.	Plan de continuidad del Procesos debidamente actualizado	Líderes de proceso Jefes de Oficina Nivel 06 Jefes de oficina Nivel 08 Director Nivel 08 Facilitador de cada área
21		Periódicamente, una vez al año como mínimo, actualiza los riesgos de continuidad acorde con los resultados de las pruebas, las situaciones reales, la actualización/desarrollo y ejecución de los planes de mejora, y los cambios realizados y realiza su gestión de acuerdo con lo definido en el procedimiento MPEE0301P Administración de riesgos y oportunidades. Aplicar Política Operacional número 9.	Matriz de Riesgos MPEE0301F01 del Proceso actualizada con los riesgos de continuidad	Líderes de proceso Jefes de Oficina Nivel 06 Jefes de oficina Nivel 08 Director Nivel 08 Facilitador de cada área

Control de cambios

FECHA	DESCRIPCIÓN Y JUSTIFICACIÓN DEL CAMBIO	VERSIÓN
22/01/2024	Se ajusta la estructura del documento de acuerdo con el nuevo formato de Procedimiento. Se eliminan las políticas de operación 5,8,10 y 11. Se incluyen las políticas de operación 7, 8 y 9 Se ajusta la redacción de todas las actividades del procedimiento, detallando las acciones que se realizan, los formatos utilizados y puntos de control	3

Control de revisión y aprobación

Elaboración	Revisión	Aprobación
IVAN ERNESTO GUERRA MATIZ Dirección Servicios de Informática Gerencia de Tecnología	ALVARO PINZON MORALES Dirección Servicios de Informática Gerencia de Tecnología	ADRIANA DEL PILAR GUERRA MARTINEZ Directora Servicios de Informática Gerencia de Tecnología
16/01/2024	16/01/2024	22/01/2024