MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE

Plan de control operacional Gestión de la Continuidad del Negocio

PROCESO

Gestión Estratégica de Tecnologías de la Información

Versión 1

22/12/2022

MADSIG
Sistema Integrado de Gestión

TABLA DE CONTENIDO

INTRODUCCIÓN

Para el desarrollo de este plan de control operacional se tomaron como base los diferentes aspectos que cubre la Norma ISO 22301 y la Norma ISO 27005, con el fin de establecer una guía para controlar el Sistema de Gestión de la Continuidad del Negocio, enfocando el control de su gestión en:

- La realización y actualización del BIA, temiendo en cuenta la metodología definida.
- La gestión de los riesgos de Continuidad del Negocio en el marco metodológico integral de la Entidad.
- La revisión periódica de la definición de las estrategias de mitigación de contingencias de continuidad del negocio definidas y sus escenarios de riesgo.
- Definición y desarrollo del plan de acción definida para probar las diferentes estrategias de mitigación dentro de una programación anual.
- Evaluación de los indicadores de gestión definidos.

1. OBJETIVO

Definir la estrategia en el Ministerio para planificar, implementar y controlar las acciones y procedimientos necesarios para cumplir con los requisitos de recuperación de los procesos considerados como críticos para el negocio identificados en el BIA, implementando estrategias de mitigación de riesgos asociados y efectuando sus respectivos planes de prueba.

2. PLAN DE CONTROL OPERACIONAL

El Plan de control operacional para controlar el cumplimiento de los requisitos de la continuidad del negocio se enfocan en los siguientes componentes de control:

- BIA (Business Impact Analysis)
- Gestionar los riesgos de continuidad del negocio periódicamente para lograr un nivel de riesgo aceptable (Riesgo residual) frente a escenarios relacionados con eventos disruptivos.
- Control sobre la operación de los diferentes componentes del sistema.
- Manejo adecuado de la documentación de registros de soporte a la gestión de seguridad.

El plan de acción para el desarrollo de estos elementos del plan de control operacional se esquematiza en el siguiente cuadro.

COMPONENTES DEL PLAN	QUE	COMO	CUANDO	QUIEN
BIA	Actualización periódica	Revisión con base en la metodología	Anual – primer trimestre de cada año	Responsable de CN y gestores de procesos
	Actualización por cambios organizacionales (entorno interno o externo)	Revisión y ajuste para los procesos impactados por el cambio	Cuando suceda el cambio	Responsable de CN y gestores de procesos
	Actualización por nuevos productos o servicios del Ministerio	Revisión y ajuste para los procesos impactados por el cambio	Cuando suceda el cambio	Responsable de CN y gestores de procesos
Gestión de riesgos de continuidad del negocio	Actualización en la identificación de riesgos.	Valoración de riesgos con base en la metodología	Definida en la metodología de gestión integral del riesgo en el Ministerio.	Responsable de CN y Riesgos

	Gestión de incidentes de continuidad del negocio	Manejo de incidentes y contingencias de continuidad del negocio.	Cuando se materialice un riesgo de continuidad del negocio	Responsable de CN y gestores de procesos involucrados
Estrategias de Continuidad del Negocio	Validar y actualizar las estrategias de mitigación de riesgos de continuidad del negocio	Probar las estrategias de CN periódicamente y definir estrategias para nuevos riesgos identificados	Plan de acción de pruebas d CN	Responsable de CN y gestores de procesos involucrados
	Definición de plan de pruebas de continuidad del negocio	Desarrollo del plan de pruebas	Programación anual del plan de pruebas	Responsable de CN.
Concientización y capacitación	Definir un programa de capacitación y concientización en continuidad del negocio.	Desarrollar el programa de capacitación y concientización definido.	Plan de capacitación y concientización anual.	Responsable de CN.
Gestión de indicadores de CN	Validar la eficacia del SGCN	Evaluando el resultado de la validación de los indicadores definidos para los diferentes componentes del SGCN	Con base en la periodicidad definida en la batería de indicadores	Responsable de CN.

3. BIA (Business Impact Analysis)

Este componente del plan permite mantener actualizado el análisis de impacto del negocio teniendo en cuenta los contextos externos e internos del Ministerio para poder identificar vulnerabilidades y escenarios de riesgo potenciales, que puedan afectar la operación normal del negocio.

El BIA se debe actualizar periódicamente o en su defecto cuando se presenten cambios en el entorno, para poder mantener la actualización de las funciones y procedimientos considerados como críticos y poder re definir si es necesario los niveles de tolerancia y tiempos de recuperación objetivo, así como los puntos de recuperación requeridos en caso de presentarse un evento disruptivo que afecten los objeticos del negocio.

4. GESTION DE RIESGOS

Este elemento del plan de control operacional, se gestiona bajo la metodología de gestión integral de riesgos del Ministerio y su objetivo es hacer una identificación continua de riesgos, evaluarlos y definir su tratamiento para mantenerlos en un nivel de riesgos residual aceptable.

El plan de control operacional para la gestión de riesgos se basa en la verificación de realización de cada estrategia de mitigación de continuidad del negocio definida y su respectivo plan de prueba definido.

Simultáneamente se debe realizar el ejercicio de identificación de nuevos riesgos de continuidad, teniendo en cuenta los cambios y actualizaciones definidos en el BIA.

- Marco teórico para la gestión de los riesgos de Continuidad del negocio

La gestión adecuada de los incidentes evita que se genere una disrupción en los procesos del negocio y el negocio mismo por ello es importante tener claros los riesgos que puedan estar asociados.

Se define una metodología basada en el modelo PHVA con la finalidad de establecer el proceso de gestión con enfoque en mejora continua y tiene su base en estándares ISO 31000 e ISO 27005, que incluyen además otras guías como:

- NTC ISO/IEC 27001 (Norma técnica Colombiana) para implementación de controles de seguridad acordes con el SGSI.
- MAGERIT para la gestión y análisis de riesgos de los sistemas de información.

- NIST SP/800 Guía desarrollada por el Instituto Nacional de Estándares y Tecnología para la gestión de riesgos de sistemas de tecnología de la información de Estados Unidos.
- NTC 5254 Norma técnica colombiana para la gestión de riesgos adoptada de la norma AS/NZ
- 4360:2004, que es una guía genérica que sirve como fuente de verificación de definiciones y proceso de documentación.

En el Anexo 1 – Cuadros de Riesgos de Continuidad del Negocio se presentan los pasos de la metodología para la gestión de riesgos de continuidad antes de un evento disruptivo, durante la continencia del evento y en la recuperación.

5. ESTRATEGIAS DE CONTINUIDAD DEL NEGOCIO

Este elemento contempla las definiciones de mitigación de los diferentes escenarios de riesgos en donde se diseñan las estrategias para ser probadas y poder validar su efectividad frente a la posible materialización de los riesgos de continuidad del negocio.

Las estrategias de Mitigación propuestas se presentan en el Anexo 2 - Estrategias de Mitigación para los riesgos de Continuidad del Negocio

El control operacional se basa en la ejecución de las pruebas programadas de las estrategias de mitigación en los diferentes escenarios de riesgo. Para el año 2023 se plantean pruebas que se esquematizan en los siguientes planes de acción Anexo 3 – Plan De Acción pruebas de Continuidad del Negocio

6. CONCIENTIZACIÓN Y CAPACITACIÓN

La capacitación y concientización sobre la necesidad de que el Ministerio mantenga el enfoque en sostener la continuidad del negocio es esencial para lograr que las estrategias de mitigación produzcan los resultados y específicamente en la efectividad d ellos planes de mitigación. En la medida de que la participación de los funcionarios y terceros que gestionan los diferentes procesos del negocio es fundamental y sin estos talentos no se pueden lograr las recuperaciones y retorno a la normalidad ante eventos disruptivos.

El plan de control establece un programa de capacitación anual, en donde específicamente se dé inicio al programa de capacitación en el 2023 y propone el siguiente plan:

QUE	COMO	CUANDO	QUIEN
Procedimientos de contingencia en continuidad del Negocio	Seminarios de capacitación	Primer trimestre de 2023	Funcionarios de los diferentes procesos del negocio
Pruebas de procedimientos	Talleres por proceso y procedimientos. Prioridad para procedimientos considerados como críticos, para aumentar su capacidad y madurez en la gestión de eventos disruptivos.	Segundo Trimestre de 2023	Funcionarios de los diferentes procesos del negocio

NOTA: Para la realización de este plan es necesario que los procesos de negocio desarrollen instructivos en detalle para los diferentes procedimientos de estos procesos.

7. GESTION DE INDICADORES DE CONTINUIDAD DEL NEGOCIO

Con base en los requerimientos definidos en la norma ISO 27001 como modelo de buena práctica y en la estructura del SGCN definida, se establecen para medición los siguientes componentes y sus variables de medición:

- Política de continuidad
  - Conocimiento de la política de CN y sus lineamientos
  - Cumplimiento de la política de CN
- Implementación y actualización del SGCN
  - Actualización del BIA
  - Gestión de riesgos de CN - Identificación
  - Definición de estrategias de CN
- Tratamiento de riesgos de CN
  - Gestión de riesgos de CN - Valoración
- Competencia y conciencia
  - Capacidad y madurez del equipo responsable de la implementación del SGCN y la administración de sus incidentes
- Operación

- Cumplimiento del plan de control operacional

Se anexa documento que contiene la batería de indicadores definida.

Anexo 1: Cuadros de Riesgos de Continuidad del Negocio.

- RIESGOS ANTES DE UN EVENTO

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE	IDENTIFICACION DE RIESGOS DE CONTINUIDAD DEL NEGOCIO						
ID	ESCENARIO DE RIESGO/CAUSA	AMENAZA/CAUSA	VALORACION	VULNERABILIDAD	VALORACION	RIESGO CONFIGURADO / DESCRIPCION DEL	NATURALEZA DEL RIESGO
1	Recuperar los canales de comunicación principales	Cambio en las condiciones de la estructura de conectividad al retornar a la normalidad	Media	Protocolo de retorno a la normalidad deficiente	Baja	**Pérdida económica y reputacional debido a imposibilidad de retornar a la normalidad, afectando la disponibilidad de los**	OPERACIONAL
2	Talento humano insuficiente para el retorno a la normalidad	No contar con el talento humano requerido para retornar a la normalidad	Media	Pérdida total o parcial del talento humano	Baja	**Afectación económica y reputacional debido a ausencia parcial o total del talento humano para retornar a la normalidad, afectando el desarrollo de**	OPERACIONAL
3	Recuperar la pérdida o falla de datacenter principal	No poder recuperar los servicios del datacenter Cambio en las condiciones de retorno a la normalidad	Media	Protocolo de retorno a la normalidad deficiente No contar con los recursos suficientes para retornar a la normalidad	Baja	**Pérdida económica y reputacional debido a imposibilidad de retornar a la operación normal del datacenter principal, afectando la**	OPERACIONAL
4	Recursos financieros insuficientes para recuperar la operación normal del Ministerio	No contar con las partidas y apropiaciones presupuestales necesarias	Media	Presupuesto insuficiente	Media	**Afectación económica y/o reputacional debido insuficiencia de recursos para el cumplimiento de las obligaciones misionales de la Entidad**	OPERACIONAL

- RIESGOS DURANTE LA CONTINGENCIA

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE — *IDENTIFICACION DE RIESGOS DE CONTINUIDAD DEL NEGOCIO* — MADSIG Sistema Integrado de Gestión

ID	SCENARIO DE RIESGO/CAUSA	AMENAZA/CAUSA	ON AMENAZA	VULNERABILIDAD	VULNERABILIDAD	RIESGO CONFIGURADO / DESCRIPCION DEL RIESGO	NATURALEZA DEL RIESGO
1	Pérdida de conectividad/comunicaciones con los canales de contingencia implementados	Daño en los canales de comunicaciones Daño en equipos de comunicaciones	Media	No tener infraestructura y servicios de soporte debidamente probados	Baja	**reputacional debido a daño o fallas en la estructura de conectividad de contingencia, afectando la disponibilidad de los servicios y activos de TI**	OPERACIONAL
2	Talento humano insuficiente durante la contingencia	Capacidad limitada del talento humano	Media	Capacidad limitada del talento humano preparado y capacitado para enfrentar la contingencia	Baja	**reputacional debido a ausencia parcial o total del talento humano capacitado en contingencia, afectando el desarrollo de la gestión de los procesos recuperados**	OPERACIONAL
3	Falla o pérdida del datacenter alterno	Fallas o daño en el servicio del datacenter	Media	No tener infraestructura y servicios de soporte debidamente probados	Baja	**reputacional debido a daño o fallas en la estructura de contingencia del datacenter alterno, afectando la disponibilidad de los servicios y activos**	OPERACIONAL

- RIESGOS EN LA RECUPERACIÓN

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE

IDENTIFICACION DE RIESGOS DE CONTINUIDAD DEL NEGOCIO

ID	SCENARIO DE RIESGO/CAUSA	AMENAZA/CAUSA	VALORACION	VULNERABILIDAD	VALORACION	RIESGO CONFIGURADO / DESCRIPCION DEL	NATURALEZA DEL RIESGO
1	Recuperar los canales de comunicación principales	Cambio en las condiciones de la estructura de conectividad al retornar a la normalidad	Media	Protocolo de retorno a la normalidad deficiente	Baja	**Pérdida económica y reputacional debido a imposibilidad de retornar a la normalidad, afectando la disponibilidad de los**	OPERACIONAL
2	Talento humano insuficiente para el retorno a la normalidad	No contar con el talento humano requerido para retornar a la normalidad	Media	Pérdida total o parcial del talento humano	Baja	**Afectación económica y reputacional debido a ausencia parcial o total del talento humano para retornar a la normalidad, afectando el desarrollo de**	OPERACIONAL
3	Recuperar la pérdida o falla de datacenter principal	No poder recuperar los servicios del datacenter Cambio en las condiciones de retorno a la normalidad	Media	Protocolo de retorno a la normalidad deficiente No contar con los recursos suficientes para retornar a la normalidad	Baja	**Pérdida económica y reputacional debido a imposibilidad de retornar a la operación normal del datacenter principal, afectando la**	OPERACIONAL
4	Recursos financieros insuficientes para recuperar la operación normal del Ministerio	No contar con las partidas y apropiaciones presupuestales necesarias	Media	Presupuesto insuficiente	Media	**Afectación económica y/o reputacional debido insuficiencia de recursos para el cumplimiento de las obligaciones misionales de la Entidad**	OPERACIONAL

Anexo 2: Estrategias de mitigación para los riesgos de continuidad del negocio

MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE — **BCP**

	IDENTIFICAION DE RIESGOS DE CONTINUIDAD DEL NEGOCIO									RIESGO RESIDUAL	
ID	ESCENARIO DE RIESGO	AMENAZA	VALORACION AMENAZA	VULNERABILIDAD	VALORACION VULNERABILIDAD	RIESGO CONFIGURADO / DESCRIPCION DEL RIESGO	PROBABILIDAD	IMPACTO	*ESTRATEGIAS DE CONTINUIDAD*	PROBABILIDAD	IMPACTO
1	Perdida de conectividad/comunicación entre la oficina principal y la arquitectura en la nube de AWS	Daño en el canal de cumunicaciones	Media	Infraestructura y servicios de TI alojados en el Datacenter (Aplicacones, Bses de datos, Servidores)	Muy Alta	Pérdida económica y reputacional debido a daño o fallas en la estructura de conectividad con el datacenter, afectando la disponibilidad de los servicios y activos de TI	Moderada/Posible	Mayor	1. DRP 2. Contingencia en el canal de comunicaciones 3. Acceso al Datacenter a travez de VPN Acceso remoto.	Baja/Improbable	Menor
2	Pérdida de conectividad/comunicaciones por daños o fallas en la infraestructura de comunicaciones propia y/o de nuestros proveedores	Daños o fallas en la infraestructura de cominucaciones de proveedores - Caida del servicio de comunicaciones	Media	Servicios de TI en nube publica y privada que dependen de la conectividad para su acceso	Muy Alta	Pérdida económica y reputacional debido a daño o fallas en la estructura de conectividad con el datacenter, afectando la disponibilidad de los servicios y activos de TI	Moderada/Posible	Mayor	1. DRP 2. Contingencia en canales de comunicaciones 3. Acceso al Datacenter a travez de VPN Acceso reomoto.	Muy Baja/Raro	Menor
3	Eventos catastróficos que afecten la infraestructura de las oficinas del Ministerio	Desastres naturales Fallas o daños en la infraestructura física del edificio (incluye facilities) Eventos pólíticos sociales que afecten la zona en donde se ubican las instalaciones del Ministerio	Media	Unico sitio de operación y administración	Alta	Afectación económica y reputacional debido a pérdida parcial o total de las instalaciones físicas de la ADRES ocasionada por desastres naturales o provocados	Moderada/Posible	Mayor	1. Contingencia en canales de comunicaciones 2. Acceso al Datacenter (Servicios de TI) a travez de VPN Acceso reomoto. 3. Teletrabajo 4. Centro alterno de operación	Baja/Improbable	Importante/ Moderado
4	Eventos que afecten la integridad de los funcionarios y colaboradores del Ministerio	Epidemias / Pandemias Accidentes o incidentes que efecten la integridad de lso funcionarios del Ministerio	Media	Roles y responsabilidades con un único responsable	Alta	Afectación económica y reputacional debido a ausencia parcial o total del talento humano asociado a ausencia parcial o total de las instalaciones físicas de la ADRES ocasionada por desastres naturales o provocados	Moderada/Posible	Importante/ Moderado	1. Esquema de roles y responsabilidades contingentes (Activiades con respaldo de responsables definido) 2. Procedimientos actualizados con esquemas de contingencia definidos para los roles y responsabilidades	Baja/Improbable	Menor
5	Amenazas en la web que puedan afectar la integridad, disponibilidad y confidencialidad de los activos de información del Miniaterio	Cibreataques	Alta	Deficiencias en le monitoreo perimetral Incumplimiento de políticas y lineamientos de seguridad de la información y ciberseguridad	Alta	Perdida económica y reputacional debido a indisponibilidad de los servicios de TI ocasionada por ciberataques a los activos tecnológicos y de información de la Entidad.	Alta/Probable	Mayor	1. SOC 2. Preparación de equipos de atención de incidentes de ciberseguridad (BLUE TEAM) 3. Implementar ejercicios de RED TEAM	Moderada/Posible	Importante/ Moderado
6	Daño o falla en el servicioa de AWS	Ciberataques Daño o falla del sercicio en la Nube AWS	Baja	Dependencia del datacenter para la prestación de servicios de TI	Alta	Afectación económica y reputacional debido a capacidad operativa limitada o interrumpida, debido a daño o falla en el datacenter que soporta los servicios de TI de la ADRES	Moderada/Posible	Importante/ Moderado	1. ASL 2. Ejercicios de auditoría y cumplimiento de los ASL	Baja/Improbable	Menor
7	Pérdida de conectividad/comunicaciones con los canales de contingencia implementados	Daña o falla en los canales de contingencia utilizados ante un evento disruptivo o elos canales principales	Baja	No contar con un tercer nivle de contingencia	Alta	Pérdida económica y reputacional debido a daño o fallas en la estructura de conectividad de contingencia, afectando la disponibilidad de los servicios y activos de TI	Moderada/Posible	Importante/ Moderado	1. Implementación de tercer nivel de contingencia 2.ASL que imcluya contingencia de los canales de contingencia	Baja/Improbable	Menor
8	Talento humano insuficiente durante la contingencia	Indicponibilidad del talento humano que soporta la contingencia o evento disruptivo	Media	No contar con un segundo nivel de contingencia en talento humano de respaldo	Media	Afectación económica y reputacional debido a ausencia parcial o total del talento humano capacitado en contingencia, afectando el desarrollo de la gestión de los procesos recuperados	Moderada/Posible	Importante/ Moderado	2. Diseño de procedimientos de contingencia para actividades ccríticas	Baja/Improbable	Menor
9	Falla o pérdida del datacenter alterno	Falla en la ejecución del DRP	Baja	DRP con debilidades e insuficiencias	Media	Pérdida económica y reputacional debido a daño o fallas en la estructura de contingencia del datacenter alterno, afectando la disponibilidad de los servicios y activos de TI	Moderada/Posible	Importante/ Moderado	1. Probar periodicamente el DRP	Baja/Improbable	Menor
10	Recuperar los canales de comunicación principales	Falla en los canales principales - Continua	Baja	Depender d ela infraestructura definida para retorno a la normalidad	Media	Pérdida económica y reputacional debido a imposibilidad de retornar a la normalidad, afectando la disponibilidad de los servicios y activos de TI	Baja/Improbable	Mayor	1. Continuar con canales de contingencia y ampliar su capacidad	Baja/Improbable	Menor
11	Talento humano insuficiente para el retorno a la normalidad	Perdida del Telenfo Humani indefinida	Media	No contar con el Talento Humano suficiente para recuperar todos los servicios	Alta	Afectación económica y reputacional debido a ausencia parcial o total del talento humano para retornar a la normalidad, afectando el desarrollo de la gestión de los procesos	Moderada/Posible	Importante/ Moderado	1. Contratar talento humano requerido 2. Proceso y procedieintos deocuemntados y actualizados	Baja/Improbable	Menor
12	Recuperar la pérdida o falla de datacenter principal	Falla en el datacenter principal - Continua	Baja	Depender d ela infraestructura definida para retorno a la normalidad	Alta	Pérdida económica y reputacional debido a imposibilidad de retornar a la operación normal del datacenter principal, afectando la disponibilidad de los servicios y activos de TI	Baja/Improbable	Mayor	1. Migración de servicios a nube pública	Baja/Improbable	Menor

Anexo 3: Plan de acción pruebas de Continuidad del Negocio

PLAN DE ACCION PRUEBAS ESCENARIOS DE CONTINUIDAD DEL NEGOCIO (Contingencia de continuidad de negocio, respaldo de información en sitio alterno)

MADSIG Sistema Integrado de Gestión — MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE

TIPO DE PREUBA		ACTIVIDADES	SIMULACION				AMBIENTE REAL			
			RESPONSABLE	TIEMPO ESTIMADO	FECHA DE REALIZACION	NIVEL DE CUMPLIMIENTO	RESPONSABLE	TIEMPO ESTIMADO	FECHA DE REALIZACION	NIVEL DE CUMPLIMIENTO
PRUEBA DE ESCRITORIO	LISTA DE CHEQUEO	1. Definición del escenario de riesgo 2. Definición del alcance 2.1 Validación de sitio alterno 3. Definición de participantes 4. Revisión de procedimientos a aplicar 5. Terceros participantes 6. Recursos adicionales requeridos 7. Validación de arquitectura de TI en el DRP 8. Validación de requerimientos de configuración 9. Otros	Continuidad del Negocio	2 Horas	Abril de 2023		Continuidad del Negocio	2 Horas	Segundo semestre de 2023	
	TABLE TOP	1. Validación y actualización de listas de chequeo 2. Definición de roles en la participación de la prueba 3. Validación de procedimientos 4. Definición de riesgos de la prueba 5. Evaluación de riesgos 6. Revisión de cronogramas y ventanas de tiempo 7. Objetivos de la prueba 8. Alcance de la prueba 9. Desarrollo de Minuto gama	Continuidad del Negocio	4 Horas (2 Sesiones de 2 Horas)	Abril de 2023		Continuidad del Negocio	4 Horas (2 Sesiones de 2 Horas)	Segundo semestre de 2023	
	INTERRUPCION TOTAL	1. Seguimiento del esquema de pruebas definido pro la Sociedad (Flujo de la Prueba) 2. Inicio de la prueba 3. Fin de la prueba 4. Informe de la prueba 5. Plan de acción de mejoramiento	TI	1 Día (Horario no hábil)	Abril de 2023		TI	1 Día (Horario no hábil)	Segundo semestre de 2023	
PRUEBA POR COMPONENTE	LISTA DE CHEQUEO	1. Validación del escenario de riesgo 2. Definición del componente a probar 3. Definición de participantes 4. Revisión de procedimientos a aplicar 5. Terceros participantes 6. Recursos adicionales requeridos 7. Validación de arquitectura de TI en el DRP 8. Validación de requerimientos de configuración 9. Otros	Continuidad del Negocio	2 Horas	Abril de 2023		Continuidad del Negocio	1 Día (Horario no hábil)	Segundo semestre de 2023	
	TABLE TOP	1. Validación del componente a probar 2.Validación y actualización de listas de chequeo 3. Definición de roles en la participación de la prueba 4. Validación de procedimientos 5. Definición de riesgos de la prueba 6. Evaluación de riesgos 8. Revisión de cronogramas y ventanas de tiempo 9. Objetivos de la prueba 10. Alcance de la prueba 11. Desarrollo de Minuto gama	Continuidad del Negocio	4 Horas (2 Sesiones de 2 Horas)	Abril de 2023		Continuidad del Negocio	1 Día (Horario no hábil)	Segundo semestre de 2023	
	INTERRUPCION PARCIAL PARA SIMULACION/ INTERRUPCION TOTAL PARA AMBIENTE REAL	1. Seguimiento del esquema de pruebas definido pro la Sociedad (Flujo de la Prueba) 2. Inicio de la prueba 3. Fin de la prueba 4. Informe de la prueba 5. Plan de acción de mejoramiento	TI	1 Día Horario no hábil	Abril de 2023		TI	1 Día (Horario no hábil)	Segundo semestre de 2023	
PRUEBA INTEGRADA	LISTA DE CHEQUEO	1. Validación del escenario de riesgo 2. Validación del alcance 3. Actualización de participantes 4. Revisión de procedimientos a aplicar 5. Terceros participantes 6. Recursos adicionales requeridos 7. Validación de arquitectura de TI en el DRP 8. Validación de requerimientos de configuración 9. Otros	Continuidad del Negocio	4 Horas (2 Sesiones de 2 Horas)	Abril de 2023		Continuidad del Negocio	4 Horas (2 Sesiones de 2 Horas)	Segundo semestre de 2023	
	TABLE TOP	1. Validación y actualización de listas de chequeo 2. Definición de roles en la participación de la prueba 3. Validación de procedimientos 4. Definición de riesgos de la prueba 5. Evaluación de riesgos 6. Revisión de cronogramas y ventanas de tiempo 7. Objetivos de la prueba 8. Alcance de la prueba 9. Desarrollo de Minuto gama	Continuidad del Negocio	2 Horas	Abril de 2023		TI	2 Horas	Segundo semestre de 2023	
	INTERRUPCION PARCIAL PARA SIMULACION/ INTERRUPCION TOTAL PARA AMBIENTE REAL	1. Seguimiento del esquema de pruebas definido pro la Sociedad (Flujo de la Prueba) 2. Inicio de la prueba 2.1 Activación de sitio alterno 3. Fin de la prueba 4. Informe de la prueba 5. Plan de acción de mejoramiento	TI	3 Días	Abril de 2023		TI	1 Día	Segundo semestre de 2023	