UNIVERSIDAD MARIANO GALVEZ DE GUATEMALA

FACULTAD DE INGENIERIA EN SISTEMAS DE INFORMACIÓN

CENTRO UNIVERSITARIO DE ZACAPA

SEGURIDAD Y AUDITORÍA DE SISTEMAS

ING. MA. JOSÉ VINICIO PEÑA ROMÁN

PLAN DE CONTINUIDAD DE NEGOCIO

Julio Cesar Aguilar Sobalvarro 1190-03-14929

Christopher Imanol Sandoval Urrutia 1190-21-14806

Zacapa, Agosto de 20225

INDICE

Plan de Continuidad de Negocio (BCP) para TechnoBank S.A. 6

Resumen ejecutivo 6

Perfil de TechnoBank S.A.: 6

1. ANÁLISIS DE IMPACTO EN EL NEGOCIO (BIA) - 25% 6

1.1. Metodología del BIA 6

1.2. Identificación de procesos críticos de negocio 7

1.2.1. Procesos de nivel crítico 7

1.2.2. Procesos de nivel alto 7

1.3. Clasificación por niveles de criticidad 7

1.4. Análisis de dependecias tecnológicas y operativas 8

1.4.1. Dependencias tecnológicas críticas 8

1.4.2. Dependencias operativas 8

1.5. Cálculo de pérdidas potenciales 9

1.5.1. Pérdidas financieras directas 9

1.5.2. Impacto reputacional y regulatorio 9

1.6. Determinación de RTO y RPO 10

1.6.1. Matriz de RTO/RPO por proceso 10

1.7. Matriz de criticidad – entregable 11

2. ANÁLISIS DE AMENAZAS Y VULNERABILIDADES - 20% 12

2.1. Metodología de evaluación de riesgos 12

2.2. Inventario de activos críticos 12

2.2.1. Activos de hardware e infraestructura 12

2.2.2. Activos de software y aplicaciones 12

2.2.3. Activos de datos e información 13

2.3. Identificación de amenazas 13
2.3.1. Amenazas naturales 13
2.3.2. Amenazas tecnológicas 13
2.3.3. Amenazas humanas 14
2.4. Evaluación de vulnerabilidades por activo 14
2.4.1. Vulnerabilidades de infraestructura 14
2.4.2. Vulnerabilidades de aplicaciones 15
2.5. Matriz de riesgo (probabilidad × impacto) 15
2.5.1. Escala de evaluación 15
2.6. Priorización de riesgos críticos 16
2.7. Registro de riesgos – entregable 17
3. ESTRATEGIAS DE CONTINUIDAD - 25% 18
3.1. Marco estratégico de continuidad 18
3.2. Estrategias de prevención por proceso crítico 18
3.2.1. Banca móvil - estrategias de prevención 18
3.2.2. Transferencias - estrategias de prevención 18
3.2.3. Préstamos online - estrategias de prevención 19
3.3. Procedimientos de respuesta inmediata 19
3.3.1. Estructura de respuesta 19
3.3.2. Secuencias de respuesta por tipo de incidente 19
3.4. Planes de recuperación y sitios alternos 21
3.4.1. Configuración de sitios de recuperación 21
3.4.2. Personal de respaldo y trabajo remoto 21
3.5. Comunicaciones de crisis 22
3.5.1. Estrategia de comunicación por audiencia 22

3.5.2. Gestión de medios y redes sociales 22
3.6. Proveedores y recursos externos 23
3.6.1. Clasificación de proveedores críticos 23
3.6.2. Acuerdos de Mutual Aid 23
3.7. Manual de procedimientos operativos – entregable 24
4. PLAN DE RECUPERACIÓN DE DESASTRES (DRP) - 20% 25
4.1. Arquitectura de respaldo 25
4.1.1. Diseño de infraestructura de recuperación 25
4.1.2. Estrategia de backup y restore 25
4.2. Procedimientos de Failover/Failback 26
4.2.1. Failover automático 26
4.2.2. Failover manual 27
4.3. Configuración de sitios de recuperación 27
4.3.1. Especificaciones técnicas por sitio 27
4.4. Secuencia de restauración de servicios 28
4.4.1. Priorización de servicios para recuperación 28
4.5. Scripts y comandos automatizados 29
4.5.1. Script de validación Post-Failover 29
4.5.2. Script de sincronización Pre-Failback 33
4.6. Runbooks técnicos detallados – entregable 35
5. PROGRAMA DE PRUEBAS Y MANTENIMIENTO - 10% 36
5.1. Marco de pruebas de continuidad 36
5.2. Cronograma de pruebas 36
5.2.1. Pruebas desktop (Tabletop exercises) 36
5.2.2. Simulacros parciales 37

5.2.3. Ejercicio anual completo 38
5.3. Métricas de efectividad 38
5.3.1. KPIs de desempeño de pruebas 38
5.3.2. Benchmarks y objetivos 39
5.4. Proceso de actualización del plan 39
5.4.1. Ciclo de revisión continua 39
5.4.2. Gestión de cambios en BCP 40
5.5. Programa de capacitación del personal 40
5.5.1. Capacitación por niveles 40
5.5.2. Certificaciones profesionales 41
5.6. Revisiones periódicas 41
5.6.1. Calendario de revisiones 41
5.7. Calendario de actividades con responsables – entregable 43

Plan de Continuidad de Negocio (BCP) para TechnoBank S.A.

Resumen ejecutivo

TechnoBank S.A. es un banco digital de nueva generación que atiende a 500,000 clientes a través de servicios exclusivamente digitales: banca móvil, transferencias electrónicas y préstamos online. La organización opera con una infraestructura distribuida en tres centros de datos con aplicaciones cloud híbridas y un modelo de trabajo donde el 60% de sus 1,200 empleados trabajan de forma remota.

Este Plan de Continuidad de Negocio (BCP) establece las estrategias, procedimientos y recursos necesarios para mantener las operaciones críticas durante interrupciones, asegurando el cumplimiento de los objetivos RTO (Recovery Time Objective) y RPO (Recovery Point Objective) definidos para cada proceso crítico. El plan se fundamenta en los estándares ISO 22301:2019, NIST SP 800-34, COBIT 2019 e ITIL v4.

Perfil de TechnoBank S.A.:

- **Base de clientes:** 500,000 usuarios activos
- **Servicios principales:** Aplicación bancaria móvil, sistema de transferencias P2P/empresariales, motor de préstamos automatizado
- **Infraestructura:** 3 centros de datos (configuración activo-activo-pasivo), arquitectura cloud híbrida
- **Recursos humanos:** 1,200 empleados (720 remotos, 480 presenciales)
- **Volumen operativo:** 2.5 millones de transacciones diarias promedio

1. ANÁLISIS DE IMPACTO EN EL NEGOCIO (BIA) - 25%

1.1.Metodología del BIA

El Análisis de Impacto en el Negocio se realizó siguiendo la metodología establecida en ISO 22301:2019, empleando técnicas cuantitativas y cualitativas para determinar los efectos de interrupciones en los procesos críticos de TechnoBank. La metodología incluyó entrevistas con stakeholders clave, análisis de datos históricos de transacciones, evaluación de dependencias tecnológicas y modelado financiero de pérdidas potenciales.

1.2.Identificación de procesos críticos de negocio

1.2.1. Procesos de nivel crítico

Plataforma de Banca Móvil La aplicación móvil constituye el canal principal de interacción con los clientes, representando el 85% de todas las transacciones. Incluye funcionalidades de consulta de saldos, transferencias, pagos de servicios y gestión de productos. La interrupción de este servicio genera impacto inmediato en la experiencia del cliente y pérdida de ingresos por comisiones.

Sistema de Transferencias y Pagos Motor de procesamiento que maneja transferencias interbancarias, pagos P2P y empresariales. Conecta con las cámaras de compensación nacional e internacional. Su criticidad radica en ser el diferenciador competitivo principal de TechnoBank, con promesa de transferencias instantáneas 24/7.

1.2.2. Procesos de nivel alto

Motor de Aprobación de Préstamos Sistema automatizado de evaluación crediticia que utiliza machine learning y conexiones con burós de crédito. Genera el 40% de los ingresos por intereses de la entidad. Su interrupción afecta la originación de nuevos préstamos pero no compromete los ya desembolsados.

Plataforma de Atención al Cliente Centro de contacto omnicanal que integra chat en vivo, llamadas telefónicas y tickets de soporte. Crítico durante incidentes para mantener comunicación con clientes y gestionar expectativas.

1.3.Clasificación por niveles de criticidad

Proceso	Criticidad	Justificación	%Ingresos Afectados
Banca Móvil	Crítico	Canal principal, 85% transacciones	70%
Transferencias	Crítico	Diferenciador competitivo, disponibilidad 24/7	25%
Préstamos Online	Alto	Fuente primaria ingresos por intereses	40%

Atención Cliente	Alto	Crítico durante crisis, imagen corporativa	N/A
Reportería Regulatoria	Medio	Cumplimiento normativo, no tiempo real	N/A
Operaciones Internas	Bajo	Soporte administrativo, tolerancia alta	N/A

1.4.Análisis de dependecias tecnológicas y operativas

1.4.1. Dependencias tecnológicas críticas

Infraestructura de red y conectividad

- Enlaces de fibra óptica redundantes entre centros de datos
- Conectividad a Internet a través de múltiples ISPs
- Red privada virtual (VPN) para empleados remotos
- **Punto de falla:** Saturación de ancho de banda durante ataques DDoS

Bases de datos transaccionales

- Cluster PostgreSQL en configuración maestro-esclavo
- Replicación síncrona entre DC principal y secundario
- Cache Redis para sesiones de usuario y consultas frecuentes
- **Punto de falla:** Corrupción de índices o falla de sincronización

Servicios cloud híbridos

- AWS para servicios de analytics y machine learning
- Microsoft Azure para backup y disaster recovery
- CDN global para distribución de contenido estático
- **Punto de falla:** Interrupción masiva de proveedores cloud

1.4.2. Dependencias operativas

Personal clave

- 5 arquitectos de sistemas con conocimiento profundo de infraestructura crítica

- 3 especialistas en seguridad certificados para respuesta a incidentes
- 8 ingenieros DevOps con acceso a sistemas de producción
- **Riesgo:** Concentración de conocimiento crítico en pocas personas

Proveedores críticos

- Proveedor principal de conectividad de datos
- Vendor de soluciones de seguridad y monitoreo
- Proveedor de servicios de backup y disaster recovery
- **Riesgo:** Dependencia de terceros para servicios esenciales

1.5.Cálculo de pérdidas potenciales

1.5.1. Pérdidas financieras directas

Pérdida de ingresos por comisiones

- Transacciones perdidas durante interrupción: $35,000/hora
- Comisiones por servicios no prestados: $20,000/hora
- **Total pérdidas operacionales:** $55,000/hora

Costos de recuperación

- Personal especializado en sobretiempo: $8,000/hora
- Servicios de terceros para recuperación: $12,000/hora
- Infraestructura temporal adicional: $5,000/hora
- **Total costos de recuperación:** $25,000/hora

Pérdidas totales directas: $80,000/hora de interrupción

1.5.2. Impacto reputacional y regulatorio

Impacto reputacional Según análisis de casos similares en la industria (TSB Bank 2018, Deutsche Bank 2019), interrupciones prolongadas en servicios bancarios digitales generan:

- Pérdida estimada de clientes: 1.5% por cada 4 horas de inactividad
- Valor de vida promedio del cliente: $1,500

- Pérdida potencial reputacional: $11.25 millones por evento mayor

Impacto regulatorio

- Multas por incumplimiento de disponibilidad: $200,000 - $1,000,000
- Costos de auditorías adicionales: $150,000
- Requerimientos de capital regulatorio adicional: 0.3% del patrimonio

1.6.Determinación de RTO y RPO

La determinación de RTO y RPO se basó en el análisis de impacto financiero, requerimientos regulatorios y expectativas de clientes, considerando el costo de implementar diferentes niveles de recuperación.

1.6.1. Matriz de RTO/RPO por proceso

Proceso	RTO	RPO	Justificación	Inversión Requerida
Banca Móvil	15 min	5 min	Impacto inmediato en clientes, alta frecuencia uso	Alta
Transferencias	30 min	1 min	Compromisos SLA con cámaras compensación	Alta
Préstamos Online	2 horas	15 min	Proceso batch, tolerancia mayor	Media
Atención Cliente	1 hora	30 min	Alternativas manuales disponibles	Media
Reportería Regulatoria	8 horas	4 horas	Ventanas de reporte establecidas	Baja
Operaciones Internas	24 horas	24 horas	Procesos no críticos para clientes	Baja

1.7.Matriz de criticidad – entregable

Proceso	Criticidad	RTO	RPO	Impacto_Financiero_Hora	Dependencias_Principales	Personal_Clave	Tecnologia_Critica	Justificacion_Tecnica
Banca Móvil	Crítico	15 min	5 min	$35,000	API Gateway, Base Datos Principal	Arquitecto Sistemas, DevOps Lead	PostgreSQL, Redis, Load Balancer	85% de transacciones, canal principal clientes
Transferencias	Crítico	30 min	1 min	$30,000	Switch Pagos, Conectividad Externa	Especialista Pagos, Arquitecto	Payment Switch, VPN Bancaria	Diferenciador competitivo, disponibilidad 24/7
Préstamos Online	Alto	2 horas	15 min	$15,000	Motor ML, Burós Crédito	Data Scientist, DevOps	AWS SageMaker, API Externa	40% ingresos por intereses, proceso automatizado
Atención Cliente	Alto	1 hora	30 min	$8,000	CRM, Telefonía IP	Supervisor Call Center	Genesys Cloud, Microsoft Teams	Crítico durante crisis, imagen corporativa
Reportería Regulatoria	Medio	8 horas	4 horas	$5,000	Data Warehouse, ETL	Analista Riesgos	Snowflake, Pentaho	Cumplimiento normativo, ventanas establecidas
Operaciones Internas	Bajo	24 horas	24 horas	$2,000	Office 365, ERP	Administrador TI	SharePoint, SAP	Soporte administrativo, tolerancia alta

2. ANÁLISIS DE AMENAZAS Y VULNERABILIDADES - 20%

2.1.Metodología de evaluación de riesgos

La evaluación de amenazas y vulnerabilidades se realizó utilizando la metodología FAIR (Factor Analysis of Information Risk) combinada con las directrices NIST SP 800-30. El proceso incluyó la identificación sistemática de activos críticos, catalogación de amenazas relevantes por categoría, evaluación de vulnerabilidades específicas y cálculo cuantitativo de riesgo utilizando escalas de probabilidad e impacto de 1 a 5.

2.2.Inventario de activos críticos

2.2.1. Activos de hardware e infraestructura

Centros de datos

- **DC Principal (Zona Norte):** 80 servidores físicos, capacidad 1,600 VMs, valoración $12M
- **DC Secundario (Zona Sur):** 60 servidores físicos, capacidad 1,200 VMs, valoración $9M
- **DC Respaldo (Zona Este):** 40 servidores físicos, cold standby, valoración $6M

Equipamiento de red

- Routers core Cisco ASR9000 series (6 unidades): $800,000
- Firewalls Palo Alto PA-5000 series (10 unidades): $500,000
- Switches de distribución y acceso: $300,000
- Load Balancers F5 Big-IP: $200,000

2.2.2. Activos de software y aplicaciones

Aplicaciones críticas

- Core Banking System (desarrollo interno): $5,000,000
- Mobile Banking App (iOS/Android): $2,000,000
- Payment Processing Engine: $1,500,000
- Customer Relationship Management: $800,000

Licenciamiento de software

- Oracle Database licenses: $600,000/año
- Microsoft Enterprise licenses: $400,000/año
- Security tools y monitoring: $300,000/año

2.2.3. Activos de datos e información

Datos de clientes

- Información personal identificable (PII): 500,000 registros
- Datos financieros y transaccionales: histórico 5 años
- Datos biométricos y autenticación: huella dactilar, facial
- **Valoración estimada:** $200,000,000 (valor de vida del cliente)

Propiedad intelectual

- Algoritmos propietarios de scoring crediticio
- Código fuente de aplicaciones desarrolladas internamente
- Documentación técnica y procedimientos operativos
- **Valoración estimada:** $15,000,000

2.3.Identificación de amenazas

2.3.1. Amenazas naturales

Eventos sísmicos Los tres centros de datos están ubicados en zona de actividad sísmica moderada. Eventos históricos muestran terremotos de magnitud 6.0+ cada 15-20 años. El DC principal se encuentra en zona de mayor riesgo sísmico según estudios geológicos recientes.

Inundaciones El DC secundario está ubicado en zona con riesgo de inundación por desbordamiento del río principal durante temporada de lluvias. Eventos de 2019 y 2021 causaron inundaciones menores en el área circundante.

2.3.2. Amenazas tecnológicas

Ataques de Denegación de Servicio (DDoS) TechnoBank ha experimentado 15 intentos de DDoS en los últimos 12 meses, con 3 eventos que causaron degradación de servicios. Los ataques más significativos alcanzaron 50 Gbps de tráfico malicioso.

Ransomware y malware La industria bancaria experimenta un incremento del 300% en ataques de ransomware según reportes de 2024. TechnoBank ha identificado 8 intentos de infiltración de malware, todos bloqueados por las defensas actuales.

Fallas de hardware Estadísticas internas muestran una tasa de falla de hardware del 12% anual en servidores críticos. Los componentes más propensos a falla son discos duros (35% de fallas) y fuentes de poder (28% de fallas).

2.3.3. Amenazas humanas

Errores operacionales Análisis de incidentes históricos revela que el 60% de las interrupciones menores son causadas por errores humanos: configuraciones incorrectas, eliminación accidental de datos, cambios no autorizados en producción.

Amenazas internas Evaluación de riesgo interno identifica 15 empleados con acceso privilegiado a sistemas críticos. Implementación de controles de segregación de funciones reduce pero no elimina completamente este riesgo.

Ingeniería social y phishing Campañas de concientización revelan que 12% de empleados son susceptibles a ataques de phishing en pruebas controladas, mejorando desde 28% el año anterior.

2.4.Evaluación de vulnerabilidades por activo

2.4.1. Vulnerabilidades de infraestructura

Sistemas de red

- Configuraciones por defecto en equipos no críticos
- Falta de micro-segmentación en algunas VLANs
- Dependencia de un solo proveedor de Internet en DC respaldo
- **Nivel de riesgo:** Medio-Alto

Servidores y sistemas operativos

- Ventanas de parcheo de 30 días para sistemas no críticos
- Sistemas legacy sin soporte extendido del fabricante
- Cuentas de servicio con privilegios excesivos
- **Nivel de riesgo:** Medio

2.4.2. Vulnerabilidades de aplicaciones

Aplicaciones web

- Autenticación multifactor no implementada universalmente
- Validación de entrada insuficiente en algunas APIs
- Logging inconsistente entre aplicaciones
- **Nivel de riesgo:** Medio

Bases de datos

- Cifrado en reposo implementado pero no en todas las comunicaciones internas
- Backups con tiempo de retención variable entre sistemas
- Cuentas de administrador compartidas en sistemas no críticos
- **Nivel de riesgo:** Medio-Alto

2.5.Matriz de riesgo (probabilidad × impacto)

2.5.1. Escala de evaluación

Probabilidad (1-5):

1. Muy Baja (0-5% anual)
2. Baja (6-25% anual)
3. Media (26-50% anual)
4. Alta (51-75% anual)
5. Muy Alta (76-100% anual)

Impacto (1-5):

1. Muy Bajo (<$50,000)

2. Bajo ($50,000-$200,000)
3. Medio ($200,000-$500,000)
4. Alto ($500,000-$1,000,000)
5. Muy Alto (>$1,000,000)

2.6.Priorización de riesgos críticos

Amenaza	Probabilidad	Impacto	Riesgo Total	Prioridad	Estrategia de Mitigación
Ataques DDoS	4	3	12	Alta	CDN, filtrado de tráfico, ISPs múltiples
Fallas Hardware	4	3	12	Alta	Redundancia N+1, monitoreo proactivo
Error Humano	4	2	8	Media	Automatización, capacitación, procedimientos
Ransomware	2	5	10	Alta	EDR, segmentación, backups offline
Eventos Sísmicos	2	4	8	Media	Construcción sismorresistente, distribución geográfica
Amenazas Internas	2	4	8	Media	Controles de acceso, monitoreo, segregación
Inundaciones	2	3	6	Media	Ubicación elevada, sistemas de drenaje
Ingeniería Social	3	2	6	Media	Capacitación, políticas de verificación

2.7.Registro de riesgos – entregable

ID_Riesgo	Amenaza	Activo_Afectado	Probabilidad	Impacto	Nivel_Riesgo	Mitigacion_Actual	Responsable	Estado	Fecha_Evaluacion
R001	Ataques DDoS	Infraestructura Red	4	3	12	CDN Cloudflare, Rate Limiting	CISO	Activo	2025-08-29
R002	Ransomware	Servidores Aplicaciones	2	5	10	Endpoint Detection, Backups	Security Team	Activo	2025-08-29
R003	Fallas Hardware	Servidores Criticos	4	3	12	Redundancia N+1	Infrastructure Team	Activo	2025-08-29
R004	Error Humano	Configuraciones Sistema	4	2	8	Change Management	Operations Team	Activo	2025-08-29
R005	Eventos Sismicos	Centros de Datos	2	4	8	Construccion Sismorresistente	Facilities Team	Activo	2025-08-29
R006	Amenazas Internas	Datos Confidenciales	2	4	8	PAM, Segregacion Funciones	HR + Security	Activo	2025-08-29
R007	Inundaciones	DC Secundario	2	3	6	Ubicacion Elevada	Facilities Team	Activo	2025-08-29
R008	Phishing	Credenciales Usuario	3	2	6	Security Awareness	Security Team	Activo	2025-08-29

3. ESTRATEGIAS DE CONTINUIDAD - 25%

3.1.Marco estratégico de continuidad

Las estrategias de continuidad de TechnoBank se fundamentan en un enfoque de defensa en profundidad que combina prevención proactiva, detección temprana, respuesta rápida y recuperación resiliente. El marco estratégico se estructura en cuatro pilares: Prevención y Protección, Detección y Respuesta, Continuidad Operativa, y Recuperación y Mejora Continua.

3.2.Estrategias de prevención por proceso crítico

3.2.1. Banca móvil - estrategias de prevención

Redundancia de infraestructura

- Load balancers en configuración activo-activo entre DC principal y secundario
- Servidores de aplicación en clusters con capacidad N+2 para absorber fallas múltiples
- Base de datos con replicación síncrona y failover automático en menos de 60 segundos
- CDN global con 15 puntos de presencia para optimizar distribución de contenido

Monitoreo proactivo

- Implementación de APM (Application Performance Monitoring) con New Relic para detectar degradación antes de impacto al usuario
- Alertas automáticas cuando el tiempo de respuesta supera 1.5 segundos o la tasa de error excede 0.1%
- Monitoreo sintético simulando transacciones críticas cada 60 segundos

3.2.2. Transferencias - estrategias de prevención

Conectividad redundante

- Conexiones duales a cada cámara de compensación (ACH, SWIFT) a través de ISPs diferentes

- Enlaces de respaldo satelital para comunicaciones críticas con entidades financieras
- Validación automática de conectividad cada 30 segundos con failover automático

Integridad de transacciones

- Implementación de blockchain interno para audit trail inmutable de transferencias
- Validación criptográfica de cada transacción con firmas digitales HSM
- Reconciliación automática cada 5 minutos con alertas de discrepancias

3.2.3. Préstamos online - estrategias de prevención

Diversificación de proveedores

- Conexiones a 3 burós de crédito diferentes con algoritmo de consensus
- Backup de modelos de machine learning en proveedores cloud alternativos
- Cache local de datos de scoring para operación offline durante 2 horas

3.3.Procedimientos de respuesta inmediata

3.3.1. Estructura de respuesta

Centro de Comando de Incidentes (ICC) El ICC se activa automáticamente ante eventos que superen los umbrales predefinidos. La estructura incluye:

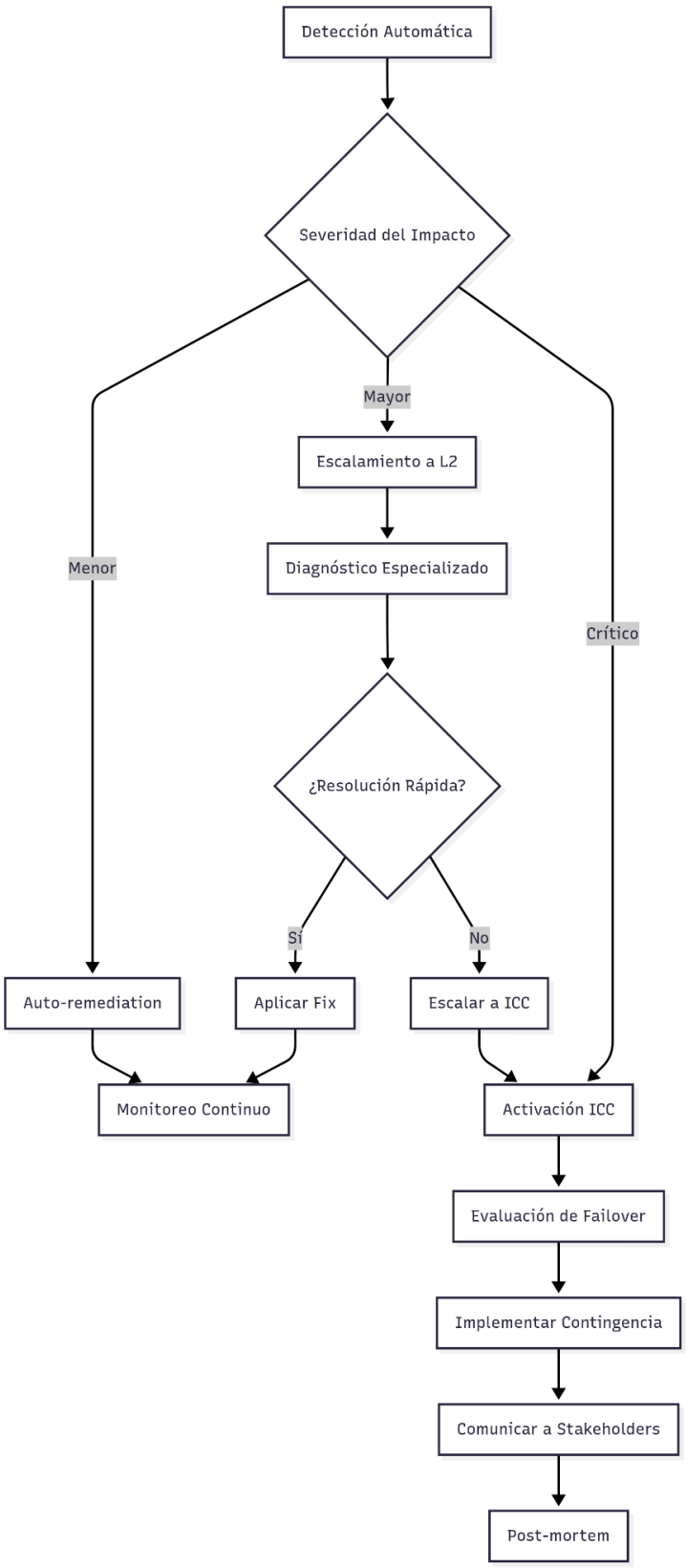
- **Comandante de incidente:** Autoridad para toma de decisiones operativas
- **Oficial técnico:** Coordinación de equipos de ingeniería y operaciones
- **Oficial de comunicaciones:** Gestión de comunicaciones internas y externas
- **Enlace con negocio:** Interface con áreas de negocio afectadas

Criterios de activación:

- Interrupción de servicios críticos por más de 15 minutos
- Degradación de performance superior al 50% por más de 30 minutos
- Compromiso confirmado de seguridad en sistemas críticos
- Eventos con impacto financiero estimado superior a $100,000

3.3.2. Secuencias de respuesta por tipo de incidente

Respuesta a fallas técnicas



Procedimiento para ataques cibernéticos:

1. **Contención (0-15 minutos):** Aislamiento automático de sistemas comprometidos
2. **Evaluación (15-30 minutos):** Análisis de alcance y vectores de ataque
3. **Erradicación (30-120 minutos):** Eliminación de malware y cierre de vectores
4. **Recuperación (2-8 horas):** Restauración gradual de servicios validados
5. **Lecciones Aprendidas (24-48 horas):** Análisis post-incidente y mejoras

3.4.Planes de recuperación y sitios alternos

3.4.1. Configuración de sitios de recuperación

Sitio principal a secundario (Hot Site)

- **RTO:** 15 minutos para servicios críticos
- **Capacidad:** 100% de carga de producción
- **Sincronización:** Datos en tiempo real con lag máximo de 5 segundos
- **Activación:** Automática basada en health checks

Sitio secundario a respaldo (Warm Site)

- **RTO:** 4 horas para activación completa
- **Capacidad:** 60% de carga de producción inicialmente, escalable a 100% en 8 horas
- **Sincronización:** Snapshots cada 15 minutos, backups diarios
- **Activación:** Manual con autorización del comandante de incidente

3.4.2. Personal de respaldo y trabajo remoto

Estrategia de Workforce Resilience TechnoBank mantiene un modelo híbrido que proporciona resiliencia natural:

- 60% del personal ya equipado para trabajo remoto permanente
- 5 oficinas satélite distribuidas geográficamente
- Acuerdos con 8 espacios de coworking para contingencias
- Equipamiento móvil pre-configurado para equipos críticos

Roles críticos y sucesión:

- Cada posición crítica tiene 2 suplentes capacitados y certificados
- Cross-training trimestral entre equipos de diferentes turnos
- Documentación de procedimientos en formato step-by-step para reducir dependencia de personal específico

3.5.Comunicaciones de crisis

3.5.1. Estrategia de comunicación por audiencia

Comunicación con clientes

- **Canales primarios:** Push notifications en app móvil, SMS masivo, email
- **Canales secundarios:** Website banner, redes sociales, call center
- **SLA de comunicación:** Primera comunicación en 15 minutos, actualizaciones cada 30 minutos

Templates de mensajes críticos:

```
INICIAL: "TechnoBank está experimentando dificultades técnicas.
Sus fondos están seguros. Información actualizada en:
[URL]/status"

ACTUALIZACIÓN: "Continuamos trabajando en la resolución.
Estado actual: [servicios disponibles/no disponibles].
Próxima actualización: [hora]"

RESOLUCIÓN: "Servicios restaurados completamente.
Gracias por su paciencia. Detalles del incidente: [URL]"
```

Comunicación regulatoria

- **Superintendencia financiera:** Notificación en 4 horas, reportes cada 4 horas
- **Banco central:** Notificación inmediata para eventos que afecten pagos
- **Otros reguladores:** Según requerimientos específicos por jurisdicción

3.5.2. Gestión de medios y redes sociales

Estrategia de medios

- **Portavoz único:** CEO o persona designada
- **Mensaje clave:** Enfoque en seguridad de fondos, medidas proactivas, transparencia
- **Monitoreo:** Seguimiento de menciones cada 15 minutos durante crisis

Gestión de redes sociales

- Equipo dedicado de 3 especialistas para respuesta en redes sociales
- Tiempo objetivo de respuesta: 15 minutos para queries críticas
- Escalamiento automático para comentarios con alto potencial viral

3.6.Proveedores y recursos externos

3.6.1. Clasificación de proveedores críticos

Tier 1 - Críticos para operación

- **AWS/Microsoft Azure:** Servicios de cloud computing y backup
- **ISPs principales:** Conectividad de datos primaria y backup
- **Proveedores de seguridad:** SOC externo y herramientas de protección
- **SLA requerido:** Respuesta en 15 minutos, disponibilidad 99.95%

Tier 2 - Importantes para continuidad

- **Oracle/PostgreSQL:** Soporte de bases de datos
- **Cisco/F5:** Soporte de equipamiento de red
- **ServiceNow:** Plataforma de gestión de incidentes
- **SLA requerido:** Respuesta en 2 horas, disponibilidad 99.5%

3.6.2. Acuerdos de Mutual Aid

Acuerdos con Instituciones Financieras TechnoBank mantiene acuerdos recíprocos con dos bancos digitales similares:

- Préstamo de espacio de oficinas para hasta 150 empleados por 30 días
- Compartir expertise técnico durante emergencia

- Acceso a infraestructura de red backup en casos extremos
- Comunicación coordinada durante eventos que afecten el sector

3.7.Manual de procedimientos operativos – entregable

Proceso	Estrategia_Prevencion	Respuesta_Inmediata	Plan_Recuperacion	Comunicacion_Crisis	Proveedor_Backup	RTO_Objetivo
Banca Móvil	Load Balancer Redundante, CDN Global	Auto-failover <60s	Sitio Secundario Hot	Push App, SMS	AWS CloudFront	15 min
Transferencias	Conectividad Dual ISP, Blockchain	Validación automática	Switch backup, Manual override	Email institucional	ISP Backup	30 min
Préstamos Online	3 Burós Crédito, Cache local	Modo degradado 2h	Replicación ML Models	Web banner	Azure ML Services	2 horas
Atención Cliente	CRM redundante, IVR backup	Redirección automática	Call center externo	Redes sociales	Genesys Cloud	1 hora
Reportería Regulatoria	Data Warehouse mirror	Proceso batch diferido	Backup site warm	Comunicación regulador	Snowflake DR	8 horas
Operaciones Internas	Office 365 backup	Trabajo remoto total	Oficinas alternas	Comunicación interna	Microsoft 365	24 horas

4. PLAN DE RECUPERACIÓN DE DESASTRES (DRP) - 20%

4.1.Arquitectura de respaldo

4.1.1. Diseño de infraestructura de recuperación

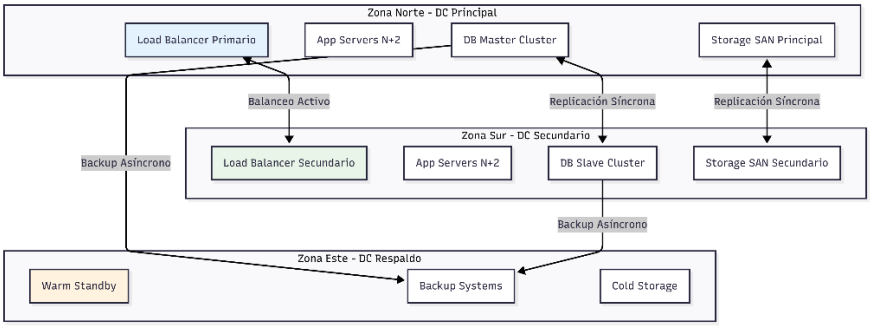
La arquitectura de recuperación de TechnoBank implementa una configuración tri-modal diseñada para maximizar la disponibilidad mientras optimiza los costos operativos. La estrategia se basa en tres niveles de recuperación con diferentes RTO y capacidades.

Configuración Activo-Activo (DC Principal - DC Secundario)

- **Distancia:** 25 km entre sitios, fuera de zona de riesgo común
- **Conectividad:** Enlaces de fibra óptica dedicados a 10 Gbps con backup a 1 Gbps
- **Sincronización:** Replicación síncrona para datos críticos, asíncrona para datos secundarios
- **Balanceo:** Distribución 60/40 de carga entre sitios

Sitio de respaldo (DC terciario)

- **Distancia:** 300 km, diferente región geográfica y sísmica
- **Configuración:** Warm standby con capacidad de activación en 4 horas
- **Sincronización:** Snapshots cada 4 horas, backups completos diarios
- **Capacidad:** 60% de carga inicial, escalable a 100% en 8 horas adicionales



4.1.2. Estrategia de backup y restore

Clasificación de datos por criticidad

Tier 1 - Datos Críticos (RPO: 5 minutos)

- Saldos de cuentas y posiciones financieras
- Transacciones en proceso y pendientes de liquidación
- Datos de autenticación y seguridad
- **Estrategia:** Replicación síncrona + snapshots cada 15 minutos

Tier 2 - Datos Importantes (RPO: 1 hora)

- Histórico transaccional completo
- Información de clientes y perfiles de riesgo
- Configuraciones de sistema y parámetros
- **Estrategia:** Replicación asíncrona + backups incrementales cada hora

Tier 3 - Datos Archivados (RPO: 24 horas)

- Logs históricos y auditoría
- Documentos y reportes generados
- Datos de analytics y BI
- **Estrategia:** Backup completo diario + archivado mensual

Tecnologías de backup implementadas

- **Veeam Backup & Replication**: Plataforma principal para virtualización
- **PostgreSQL Streaming Replication:** Replicación nativa de bases de datos críticas
- **Commvault Complete Data Protection:** Backup enterprise con deduplicación
- **AWS S3 Glacier Deep Archive:** Almacenamiento de largo plazo (7 años retención)

4.2.Procedimientos de Failover/Failback

4.2.1. Failover automático

Criterios de Activación Automática El sistema de monitoreo evalúa múltiples métricas para determinar la necesidad de failover automático:

- **Pérdida de Conectividad:** Falla de ambos enlaces primarios por >3 minutos
- **Degradación Crítica:** Latencia >3 segundos o tasa de error >2% por >5 minutos

- **Falla de Infraestructura:** >60% de servidores críticos inaccesibles
- **Falla de Aplicación:** Core banking system inaccesible por >2 minutos

Secuencia de Failover automático

00:00 - Detección de falla por sistema de monitoreo
00:01 - Validación por sensores múltiples y confirmación automática
00:02 - Inicio de secuencia de failover sin intervención humana
00:03 - Actualización de DNS y redirección de tráfico
00:04 - Activación de servicios en sitio secundario
00:06 - Validación automática de servicios críticos
00:08 - Notificación a equipos operativos y management
00:10 - Inicio de comunicaciones a clientes (si aplicable)

4.2.2. Failover manual

Autoridades para autorizar Failover manual

- **CTO o CTO Adjunto:** Decisiones técnicas de rutina
- **COO:** Impactos operativos significativos
- **CEO:** Situaciones de crisis o alto impacto reputacional
- **Comandante de Incidente:** Durante activación formal de BCP

Proceso de Failover manual controlado

1. **Análisis de impacto (15 minutos):** Evaluación riesgo-beneficio del failover
2. **Preparación (30 minutos):** Sincronización de datos y preparación de sistemas
3. Comunicación previa (15 minutos): Notificación a stakeholders internos
4. **Ejecución por fases (45 minutos):** Migración gradual por grupos de servicios
5. **Validación (30 minutos):** Verificación completa de funcionalidades
6. **Monitoreo intensivo (4 horas):** Supervisión continua post-failover

4.3.Configuración de sitios de recuperación

4.3.1. Especificaciones técnicas por sitio

DC Principal (Zona norte)

- **Capacidad computacional:** 1,600 VMs, 320 TB RAM, 50 PB almacenamiento
- **Conectividad:** 4x10Gbps fibra óptica, 2x1Gbps backup
- **Energía:** 2N UPS (30 min autonomía), 2 generadores diésel (72h combustible)
- **Refrigeración:** Sistema redundante con backup automático
- **Seguridad física:** Biometría, cámaras 24/7, guardias presenciales

DC Secundario (Zona sur)

- **Capacidad computacional:** 1,200 VMs, 240 TB RAM, 40 PB almacenamiento
- **Conectividad:** 2x10Gbps fibra óptica, 2x1Gbps backup
- **Energía:** N+1 UPS (20 min autonomía), 1 generador diésel (48h combustible)
- **Refrigeración:** Sistema con backup manual
- **Seguridad física:** Tarjetas de acceso, cámaras 24/7, guardia horario extendido

DC Respaldo (Zona este)

- **Capacidad computacional:** 800 VMs, 160 TB RAM, 25 PB almacenamiento
- **Conectividad:** 2x1Gbps fibra óptica, 1x1Gbps backup satelital
- **Energía:** N UPS (15 min autonomía), 1 generador portátil (24h combustible)
- **Refrigeración:** Sistema básico sin redundancia
- **Seguridad física:** Acceso con llaves, cámaras básicas, sin guardia permanente

4.4.Secuencia de restauración de servicios

4.4.1. Priorización de servicios para recuperación

Fase 1 - Servicios críticos (0-30 minutos)

1. Infraestructura de red y conectividad
2. Servicios de autenticación y seguridad
3. Base de datos transaccional principal
4. API Gateway y load balancers

Fase 2 - Aplicaciones core (30-60 minutos)

1. Core banking system
2. Motor de transferencias y pagos

3. Aplicación móvil (backend services)
4. Sistema de monitoreo y alertas

Fase 3 - Servicios de soporte (1-4 horas)

1. Motor de aprobación de préstamos
2. CRM y atención al cliente
3. Sistemas de reportería
4. Herramientas administrativas internas

Fase 4 - Servicios complementarios (4-8 horas)

1. Analytics y business intelligence
2. Sistemas de marketing
3. Herramientas de desarrollo
4. Sistemas de backup y archivo

4.5.Scripts y comandos automatizados

4.5.1. Script de validación Post-Failover

```
#!/bin/bash
# Archivo: post_failover_validation.sh
# Propósito: Validar funcionalidad crítica post-failover

LOG_FILE="/var/log/failover_validation.log"
ALERT_EMAIL="ops-team@technobank.com"

log_message() {
   echo "$(date '+%Y-%m-%d %H:%M:%S') - $1" | tee -a $LOG_FILE
}

# Validar conectividad de base de datos
validate_database() {
   log_message "Validando conectividad de base de datos..."
```

```
    DB_STATUS=$(psql -h db-cluster.internal -U monitor -d banking_db -c "SELECT 1" -t)
    if [ "$DB_STATUS" = " 1" ]; then
        log_message "✓ Base de datos accesible"

        # Validar integridad de datos críticos
        ACCOUNT_COUNT=$(psql -h db-cluster.internal -U monitor -d banking_db -c "SELECT COUNT(*) FROM customer_accounts" -t | xargs)
        log_message "✓ Cuentas de clientes disponibles: $ACCOUNT_COUNT"

        return 0
    else
        log_message "✗ ERROR: Base de datos no accesible"
        return 1
    fi
}

# Validar servicios de aplicación
validate_applications() {
    log_message "Validando servicios de aplicación..."

    # Core Banking API
    CORE_STATUS=$(curl -s -o /dev/null -w "%{http_code}" http://core-banking.internal:8080/health)
    if [ "$CORE_STATUS" = "200" ]; then
        log_message "✓ Core Banking API operativo"
    else
        log_message "✗ ERROR: Core Banking API no responde (HTTP $CORE_STATUS)"
```

```
        return 1
    fi

    # Mobile Banking API
    MOBILE_STATUS=$(curl -s -o /dev/null -w "%{http_code}"
https://api.technobank.com/v1/health)
    if [ "$MOBILE_STATUS" = "200" ]; then
        log_message "✓ Mobile Banking API operativo"
    else
        log_message "✗ ERROR: Mobile Banking API no responde (HTTP
$MOBILE_STATUS)"
        return 1
    fi

    return 0
}

# Validar transacciones críticas
validate_transactions() {
    log_message "Validando capacidad transaccional..."

    # Test de consulta de balance
    BALANCE_TEST=$(curl -s -X POST https://api.technobank.com/v1/test/balance \
                -H "Content-Type: application/json" \
                -d '{"account":"TEST123456","auth":"test_token"}')

    if echo $BALANCE_TEST | grep -q "success"; then
        log_message "✓ Consulta de balance funcional"
    else
        log_message "✗ ERROR: Consulta de balance falló"
```

```
        return 1
    fi

    return 0
}

# Función principal
main() {
    log_message "=== INICIANDO VALIDACIÓN POST-FAILOVER ==="

    ERRORS=0

    validate_database || ERRORS=$((ERRORS+1))
    validate_applications || ERRORS=$((ERRORS+1))
    validate_transactions || ERRORS=$((ERRORS+1))

    if [ $ERRORS -eq 0 ]; then
        log_message "=== VALIDACIÓN EXITOSA - TODOS LOS SERVICIOS
OPERATIVOS ==="
        echo "Failover validation successful" | mail -s "TECHNOBANK: Failover
Validation SUCCESS" $ALERT_EMAIL
    else
        log_message "=== VALIDACIÓN FALLIDA - $ERRORS ERRORES
ENCONTRADOS ==="
        echo "Failover validation failed with $ERRORS errors. Check $LOG_FILE for
details." | mail -s "TECHNOBANK: Failover Validation FAILED" $ALERT_EMAIL
        exit 1
    fi
}

main "$@"
```

4.5.2. Script de sincronización Pre-Failback

```
-- Archivo: pre_failback_sync.sql
-- Propósito: Sincronizar datos antes de failback al sitio principal

-- Crear tabla temporal para análisis de brecha
CREATE TEMPORARY TABLE data_gap_analysis AS
SELECT
    'transactions' as table_name,
    COUNT(*) as records_count,
    MAX(created_at) as latest_timestamp,
    SUM(amount) as total_amount
FROM transactions
WHERE created_at > (
    SELECT COALESCE(MAX(sync_timestamp), '2025-01-01'::timestamp)
    FROM sync_log
    WHERE table_name = 'transactions'
);

-- Insertar análisis para otras tablas críticas
INSERT INTO data_gap_analysis
SELECT
    'customer_accounts' as table_name,
    COUNT(*) as records_count,
    MAX(updated_at) as latest_timestamp,
    0 as total_amount
FROM customer_accounts
WHERE updated_at > (
    SELECT COALESCE(MAX(sync_timestamp), '2025-01-01'::timestamp)
    FROM sync_log
    WHERE table_name = 'customer_accounts'
```

```
);

-- Mostrar resumen de datos a sincronizar
SELECT
    table_name,
    records_count,
    latest_timestamp,
    CASE
        WHEN table_name = 'transactions' THEN total_amount::text
        ELSE 'N/A'
    END as financial_impact
FROM data_gap_analysis;

-- Validar integridad pre-sincronización
SELECT
    'VALIDATION' as type,
    COUNT(*) as total_transactions,
    SUM(amount) as total_amount,
    MIN(created_at) as earliest_tx,
    MAX(created_at) as latest_tx
FROM transactions
WHERE DATE(created_at) = CURRENT_DATE;

-- Marcar inicio de proceso de sincronización
INSERT INTO sync_log (table_name, sync_timestamp, status, records_affected)
SELECT
    table_name,
    NOW(),
    'PRE_FAILBACK_STARTED',
    records_count
FROM data_gap_analysis;
```

4.6.Runbooks técnicos detallados – entregable

Sistema	Procedimiento_Backup	Comando_Failover	Tiempo_RTO	Validacion_Post	Rollback_Procedure	Contacto_Soporte
PostgreSQL_DB	pg_basebackup daily + streaming	pg_ctl promote -D /data/postgres	5 min	SELECT COUNT(*) FROM accounts	pg_rewind master	DBA Lead ext.1234
Core_Banking_App	Veeam VM backup 4h	veeam failover --vm core-banking	15 min	curl health endpoint	veeam failback --vm core-banking	DevOps Lead ext.1235
Payment_Switch	rsync config + data	systemctl start payment-switch-backup	10 min	test-payment-transaction.sh	restore config backup	Payments Architect ext.1236
API_Gateway	Kong declarative config	kong start --config failover.yml	2 min	curl /health	kong reload --config primary.yml	Platform Engineer ext.1237
Load_Balancer	F5 UCS backup	f5 failover --device secondary	1 min	f5 health-check --all-pools	f5 failover --device primary	Network Engineer ext.1238
Redis_Cache	redis-cli BGSAVE	redis-server failover.conf	30 sec	redis-cli PING	restore from backup	Database Admin ext.1239

5. PROGRAMA DE PRUEBAS Y MANTENIMIENTO - 10%

5.1.Marco de pruebas de continuidad

El programa de pruebas de TechnoBank sigue la metodología establecida en ISO 22301:2019, implementando un enfoque escalonado que progresa desde pruebas conceptuales hasta ejercicios complejos de simulación total. Los objetivos incluyen validar la efectividad de procedimientos, identificar gaps de capacidad, desarrollar competencias del personal y cumplir requerimientos regulatorios.

5.2.Cronograma de pruebas

5.2.1. Pruebas desktop (Tabletop exercises)

Frecuencia: Mensual por área crítica
Duración: 2-3 horas por sesión
Participantes: 8-12 personas clave por proceso
Metodología: Escenarios hipóticos presentados por facilitador externo certificado

Cronograma anual de pruebas desktop:

Mes	**Área de Focus**	**Escenario Principal**	**Participantes Clave**	**Objetivos Específicos**
Enero	Banca Móvil	Ataque DDoS masivo	CTO, Mobile Team, DevOps	Validar procedimientos de mitigación
Febrero	Transferencias	Falla en cámara de compensación	Head of Payments, Operations	Procedimientos de reconciliación
Marzo	Préstamos	Caída de proveedor de scoring	Head of Credit, Data Scientists	Modelos de backup y decisiones

Abril	Atención Cliente	Sobrecarga por crisis externa	Customer Service Manager	Escalamiento y comunicaciones
Mayo	Infraestructura	Falla total DC principal	Infrastructure Team	Failover y recuperación
Junio	Ciberseguridad	Ransomware avanzado	CISO, Security Team	Contención y erradicación

5.2.2. Simulacros parciales

Frecuencia: Trimestral

Duración: 4-8 horas incluyendo post-mortem

Alcance: Servicios no críticos en horarios de bajo tráfico

Simulacros programados 2025:

Q1 - Simulacro de recuperación de reportería

- **Fecha:** Sábado 15 de marzo, 08:00-14:00
- **Escenario:** Corrupción de data warehouse principal
- **Objetivo:** Validar recuperación desde backup y procedimientos de validación
- **Métricas:** Tiempo de detección, RTO real vs objetivo, integridad de datos

Q2 - Simulacro de migración de load balancer

- **Fecha:** Domingo 15 de junio, 06:00-12:00
- **Escenario:** Falla crítica en load balancer principal
- **Objetivo:** Probar failover manual controlado sin impacto a usuarios
- **Métricas:** Tiempo de conmutación, pérdida de sesiones, estabilidad post-cambio

Q3 - Simulacro de trabajo remoto masivo

- **Fecha:** Viernes 19 de septiembre, 14:00-18:00
- **Escenario:** Evacuación de oficina principal por emergencia
- **Objetivo:** Validar capacidad de operación 100% remota
- **Métricas:** Tiempo de transición, productividad, comunicaciones}

Q4 - Simulacro de recuperación de sitio alterno

- **Fecha:** Sábado 14 de diciembre, 10:00-16:00
- **Escenario:** Activación de DC respaldo (warm site)
- **Objetivo:** Probar recuperación desde sitio terciario
- **Métricas:** Tiempo de activación, capacidad operativa, sincronización de datos

5.2.3. Ejercicio anual completo

Ejercicio 2025: "Scenario Storm"
Fecha: 15-16 de noviembre (fin de semana)
Duración: 48 horas continuas
Alcance: Toda la organización + terceros críticos

Narrativa del ejercicio: TechnoBank enfrenta una tormenta perfecta de eventos simultáneos:

- Ataque cibernético coordinado con múltiples vectores
- Falla de infraestructura en DC principal por evento sísmico
- Crisis de comunicaciones por campaña de desinformación
- Sobrecarga de sistemas por pánico financiero generalizado

Fases del ejercicio:

- **Detección y respuesta (Horas 0-6):** Identificación de múltiples amenazas
- **Gestión de crisis (Horas 6-18):** Coordinación de respuesta integral
- **Recuperación (Horas 18-36):** Implementación de planes de contingencia
- **Normalización (Horas 36-48):** Retorno gradual a operaciones normales

5.3.Métricas de efectividad

5.3.1. KPIs de desempeño de pruebas

Métricas cuantitativas:

- **Tiempo de detección:** Promedio de tiempo desde inicio del evento hasta identificación

- **Tiempo de escalamiento:** Desde detección hasta activación del equipo correcto
- **RTO real vs objetivo:** Comparación de tiempos reales de recuperación vs metas
- **Éxito de procedimientos:** Porcentaje de procedimientos ejecutados correctamente
- **Participación:** Porcentaje de personal clave que participa en ejercicios programados

Métricas cualitativas:

- **Calidad de comunicaciones:** Claridad y oportunidad de mensajes durante crisis
- **Coordinación entre equipos**: Efectividad de interfaces y handoffs
- **Toma de decisiones:** Calidad y velocidad de decisiones bajo presión
- **Liderazgo en crisis:** Efectividad del comando y control durante ejercicios

5.3.2. Benchmarks y objetivos

Métrica	Baseline 2024	Objetivo 2025	Objetivo 2026
Tiempo Detección	8 minutos	5 minutos	3 minutos
Tiempo Escalamiento	15 minutos	10 minutos	7 minutos
RTO Banca Móvil	25 minutos	15 minutos	10 minutos
RTO Transferencias	45 minutos	30 minutos	20 minutos
Éxito Procedimientos	85%	92%	95%
Participación Ejercicios	80%	90%	95%

5.4.Proceso de actualización del plan

5.4.1. Ciclo de revisión continua

Revisión Post-Ejercicio (Inmediata)

- Análisis hot wash dentro de 24 horas del ejercicio
- Identificación de gaps críticos y acciones inmediatas
- Actualización de procedimientos basada en lecciones aprendidas
- Comunicación de cambios a todos los stakeholders relevantes

Revisión trimestral (Sistemática)

- Actualización de contactos y matriz de escalamiento
- Incorporación de cambios en infraestructura y aplicaciones
- Ajuste de RTO/RPO basado en capacidades actuales
- Validación de acuerdos con proveedores críticos

Revisión anual (Estratégica)

- Evaluación completa del landscape de amenazas
- Actualización del Business Impact Analysis (BIA)
- Revisión de estrategias vs cambios del negocio
- Benchmarking con mejores prácticas de la industria

5.4.2. Gestión de cambios en BCP

Proceso de Evaluación de Impacto Todo cambio significativo debe incluir evaluación de impacto en continuidad:

- **Identificación de dependencias:** Servicios y procesos afectados por el cambio
- **Análisis de riesgo:** Nuevos riesgos introducidos o mitigados
- **Actualización documental:** Modificación de runbooks, contactos, procedimientos
- **Validación:** Pruebas específicas para confirmar efectividad post-cambio
- **Comunicación:** Socialización de cambios con equipos afectados

Criterios para revisión obligatoria:

- Cambios en arquitectura de aplicaciones críticas
- Nuevos servicios o productos customer-facing
- Modificaciones en proveedores de servicios tier 1
- Cambios en ubicaciones físicas o estructura organizacional
- Actualizaciones regulatorias que modifiquen requerimientos

5.5.Programa de capacitación del personal

5.5.1. Capacitación por niveles

Nivel 1 - Todos los empleados (Anual)

- **Contenido:** Conceptos básicos de BCP, roles individuales durante crisis
- **Duración:** 2 horas e-learning + 1 hora presencial
- **Evaluación:** Quiz online con 80% mínimo para aprobación
- **Certificación:** Válida por 12 meses

Nivel 2 - Personal clave (Semestral)

- **Contenido:** Procedimientos específicos, herramientas especializadas, coordinación
- **Duración:** 8 horas distribuidas en 2 días
- **Evaluación:** Ejercicio práctico + examen teórico
- **Certificación:** Válida por 6 meses

Nivel 3 - Líderes de crisis (Trimestral)

- **Contenido:** Comando y control, toma de decisiones, gestión de stakeholders
- **Duración:** 16 horas presenciales + ejercicios de simulación
- **Evaluación:** Evaluación 360° durante ejercicios
- **Certificación:** Evaluación continua

5.5.2. Certificaciones profesionales

Programa de certificación externa:

- **CBCP (Certified Business Continuity Professional):** Mínimo 5 personas
- **MBCI Associate/Specialist:** 10 personas en roles clave
- **CISSP con dominio BCP**: 3 personas en seguridad
- **ITIL Expert con BCP focus:** 2 personas en operaciones

5.6.Revisiones periódicas

5.6.1. Calendario de revisiones

Revisión mensual de métricas

- Dashboard de KPIs de continuidad
- Análisis de incidentes del período

- Estado de acciones correctivas pendientes
- Preparación para ejercicios del siguiente mes

Revisión trimestral de efectividad

- Análisis de tendencias de métricas
- Efectividad de mejoras implementadas
- Ajustes a cronograma de pruebas
- Actualización de evaluación de riesgos

Revisión semestral de estrategia

- Alineación con objetivos de negocio
- Evaluación de nuevas amenazas
- Revisión de presupuesto y recursos
- Planificación de ejercicios mayor

Revisión anual integral

- Evaluación completa del programa BCP
- Benchmarking con estándares de industria
- Definición de objetivos para siguiente año
- Presentación a Junta Directiva

5.7.Calendario de actividades con responsables – entregable

Mes	Actividad	Tipo	Responsable	Participantes	Objetivo	Duracion	Entregable	Fecha_Tentativa
Enero	Desktop Banking	Tabletop	BCP Manager	Mobile Team	Validar respuesta DDoS	3h	Informe GAPs	Viernes 24 Enero
Febrero	Backup Restore	Técnica	DBA Lead	Database Team	Probar procedimientos	2h	Tiempo RTO real	Sábado 15 Febrero
Marzo	Simulacro Reportes	Simulacro	Risk Manager	Analytics Team	Recovery parcial	6h	Post-mortem	Sábado 22 Marzo
Abril	Desktop Payments	Tabletop	Payments Head	Operations	Falla compensación	3h	Matriz mejoras	Viernes 25 Abril
Mayo	Security Drill	Simulacro	CISO	Security Team	Respuesta ransomware	4h	Plan remediation	Sábado 17 Mayo
Junio	LB Migration	Técnica	Network Lead	Infrastructure	Failover manual	6h	Runbook actualizado	Domingo 15 Junio
Julio	Desktop Crisis	Tabletop	COO	All Managers	Comunicaciones crisis	3h	Templates actualizados	Viernes 18 Julio
Agosto	DR Test	Técnica	Infrastructure Head	DevOps Team	Activación DC backup	4h	Procedimientos DR	Sábado 16 Agosto
Septiembre	Remote Work	Simulacro	HR Manager	All Staff	Trabajo remoto masivo	4h	Capacidad validada	Viernes 19 Septiembre
Octubre	Desktop Cyber	Tabletop	CISO	Security + IT	APT multicanal	3h	Plan respuesta	Viernes 24 Octubre
Noviembre	Storm Exercise	Completo	CEO	Toda Organización	Crisis integral	48h	BCP actualizado	15-16 Noviembre
Diciembre	Warm Site	Simulacro	CTO	Technical Teams	Recuperación sitio 3	6h	RTO validado	Sábado 14