UNIVERSIDAD DE CHILE
FACULTAD DE CIENCIAS FÍSICAS Y MATEMÁTICAS
DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

METODOLOGÍA DE MEJORA PARA CONTINGENCIAS TECNOLÓGICAS BANCARIAS

TESIS PARA OPTAR AL GRADO DE MAGISTER EN TECNOLOGÍAS DE LA INFORMACIÓN

FRANCISCO JAVIER TORRES TOLEDO

PROFESORA GUÍA:
MARÍA CECILIA BASTARRICA PIÑEYRO

MIEMBROS DE LA COMISIÓN:
HUGO BELTRÁN ALEJOS
ALEJANDRO HEVIA ANGULO
MAURCICIO SOLAR FUENTES

SANTIAGO DE CHILE
2021

Resumen

La banca ha sufrido cambios en los últimos años que la hacen más competitiva, con tecnologías que permiten entregar nuevos productos o la incorporación de nuevos actores en la industria. Las unidades de tecnología dentro de este ambiente multicanal y de alta competencia llevan su foco a servicios 7x24.

La necesidad de contar con alta disponibilidad de los servicios junto con el aumento en requerimientos ligados a contingencias tecnológicas, llevó a la organización a contar con un grupo de contingencia cuyo principal foco es el Plan de Contingencia Tecnológico (PCT).

A finales del 2017, era clara la necesidad de contar con una metodología que permitiera mejorar de forma continua el PCT, por lo que fue planteado a la jefatura el objetivo de contar con una Metodología de Mejora para Contingencias Tecnológicas.

Este proyecto de tesis, aborda las siguientes inquietudes: ¿Cuáles son las fuentes de información que debe considerar la metodología para actualizar el PCT?, ¿Cómo asegurar que los requerimientos asociados a la continuidad tecnológica pasen por el grupo de contingencia?, ¿Cómo hacer partícipe de la metodología al resto de las unidades de tecnología generando sinergia?

Las razones que permiten afirmar que este trabajo logró sus objetivos radica en:

1. La construcción e implementación de una nueva metodología dentro de la Gerencia de Tecnología, acorde a la estrategia de continuidad de negocio del banco.

2. Generación de sinergia con el resto de las unidades de tecnología, para responder a los requerimientos relacionados a contingencias tecnológicas.

3. Incorporar esta metodología dentro de la formalidad del Banco.

Agradecimientos

Rara vez un logro realmente importante, es obra de una sola persona, sacar adelante un título de magister no es la excepción, son tantas las personas a quienes agradecer, alguna que incluso ya no están entre nosotros.

Agradezco a mi madre y mi Tata, quienes velaron y protegieron al ser que hoy soy.

Agradezco a mi esposa Jacqueline Veliz, quien con su amor y dedicación me dio el valor y tiempo necesario para que pudiese dedicarme de lleno en esta empresa. Cada vez que sentía que no se lograría, sus palabras y aliento me levantaban.

Agradezco a mi profesora guía Cecilia Bastarrica, que con paciencia tuvo que descifrar los primeros intentos de escrito hasta llegar al documento que hoy entrego. Su dedicación más allá de su deber y consejos profesionales fueron un faro, fue una fortuna contar con su ayuda.

Agradezco a los profesores Daniel Perovich y Sergio Ochoa, por su preocupación, sus consejos y acompañamiento en este camino. Me han permitido ver el trabajo desde otras perspectivas.

Agradezco a mis hijos, por su comprensión por todos los tiempos perdidos y el sacrificio a nivel familiar que este tipo de empresas implica.

A todos aquellos, que me dijeron alguna vez, “tú puedes Francisco, sigue adelante”, mil gracias, no saben lo importante que fue esas palabras de aliento.

TABLA DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

Capítulo 1: Introducción

El Banco, en adelante nombrado como "el Banco", está presente en Chile desde 1978. Es una institución financiera privada que opera dentro de una industria normada. A nivel local su regulador es la Comisión para Mercado Financiero conocida por su sigla CMF1 y a nivel interno su regulador es el Corporativo de Banco Santander en España.

La visión del Banco es "ser el banco líder y más valorado del país, poniendo al cliente al centro de nuestra razón de ser. Para concretar ese propósito nos basamos en tres conceptos que constituyen nuestra forma de hacer las cosas: Simple, Personal y Fair". Para alcanzar este ideal auto impuesto el Banco cuenta en la actualidad con más de 11.305 colaboradores a lo largo de todo el territorio nacional, distribuidos en 392 sucursales y edificios centrales del Banco.

Apalancando su visión y cercanía con los clientes, es un banco multicanal, que cuenta con un sistema tecnológico con página corporativa, aplicaciones móviles para smartphones, sus propios sistemas de tarjetas, 910 cajeros automáticos y un vox de atención que prestan servicios a aproximadamente 3,5 millones de clientes en Chile actualmente.

1.1 Reguladores de la Industria

El Estado de Chile, identificando a la industria bancaria como un pilar básico de la economía del país, a partir de 1925 crea la Superintendencia de Bancos e Instituciones Financieras de Chile (SBIF), la que a partir de Junio de 2019 pasa a ser la actual Comisión para el Mercado Financiero2. Esta entrega los lineamientos de la industria por medio de Normativas y Circulares, estableciendo los marcos de comportamiento a nivel financiero, operacional y de continuidad del negocio.

1 COMISIÓN PARA EL MERCADO FINANCIERO CONOCIDA CON LA SIGLA CMF, SERVICIO PÚBLICO DESCENTRALIZADO, DE CARÁCTER TÉCNICO, DOTADO DE PERSONALIDAD JURÍDICA Y PATRIMONIO PROPIO, QUE SE RELACIONA CON EL PRESIDENTE DE LA REPÚBLICA A TRAVÉS DEL MINISTERIO DE HACIENDA.

2 LA CMF ADEMÁS DE REGIR A LA INDUSTRIA BANCARIA, TIENE LAS ATRIBUCIONES DE REGULAR A LA INDUSTRIA DE VALORES Y SEGUROS, SUS LABORES LAS DESEMPEÑA DE FORMA INDEPENDIENTE AL GOBIERNO DE TURNO, COMO UN ÓRGANO PROFESIONAL DEL ESTADO DE CHILE.

El Banco además cuenta con un regulador interno a nivel corporativo, quien dictamina por medio de políticas la forma en que deben trabajar y actuar cada una de las filiales alrededor del mundo.

1.2 Organización administrativa del Banco

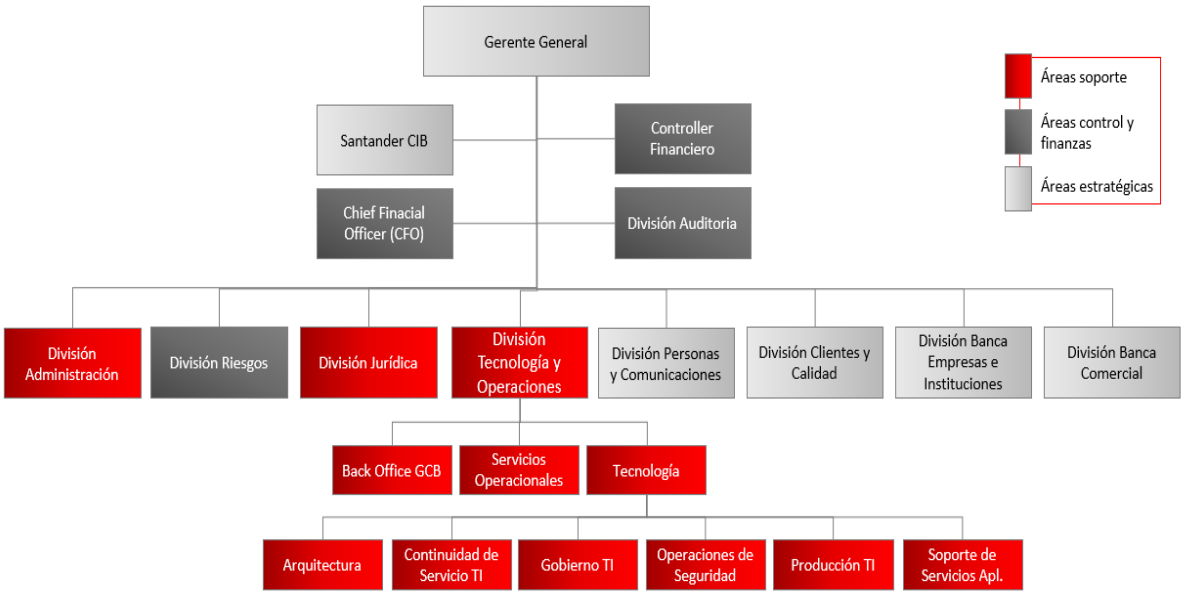


Figura 1. Organigrama administrativo del Banco

El Banco se divide operacionalmente en divisiones que se pueden agrupar en tres áreas: soportes, estratégicas y control/finanzas. Forman parte de las áreas de soporte, la División de Administración, Jurídica y de Tecnología y Operaciones.

La División de Tecnología y Operaciones tiene como principal función apoyar a las operaciones y estrategia del Banco, proporcionando ambientes tecnológicos robustos, seguros, accesibles y estables, para el desarrollo, mantención, mejora y explotación de los aplicativos que utilizan las distintas unidades del Banco.

La Gerencia de Tecnología depende directamente de la División de Tecnología y Operaciones. Adicionalmente es controlada como segunda línea por la gerencia de Riesgo no Financiero y como tercera línea por la Unidad de Auditoria Interna. Su

principal función es administrar el ambiente productivo3 del banco y velar por su correcto funcionamiento de cara a los clientes internos y externos.

Arquitectura es la unidad encargada de realizar análisis funcionales de software, revisión de diseños técnicos, visar pasos a producción, generar capacitaciones sobre nuevas tecnologías, mantención de catálogos tecnológicos, la actualización de conocimientos e impulsar nuevas tecnologías.

Continuidad de Servicio TI es la unidad encargada de realizar seguimiento y clasificación diaria de incidencias, seguimiento semanal en mesa de continuidad de servicio, administración y mantención de sistema de alertas, informes de continuidad, gestión de contingencia tecnológica, coordinación y control de pruebas de contingencia, coordinación de cumplimiento con comités y actualización de planes de contingencia.

Gobierno TI es la unidad encargada de cumplimiento de auditorías, indicadores de gobierno, solicitudes de compra TI, presupuestos de inversión y pago de proveedores.

Operaciones de Seguridad es la unidad encargada de gestión de acceso, parchado y bastionado, detección y gestión de vulnerabilidades, certificados y plataformas de seguridad.

Producción TI es la unidad encargada de gestión de inventario tecnológico, atención a estaciones de trabajo (notebook y PCs), almacenamiento, telecomunicaciones, telefonía, infraestructura tecnológica, Data Center y obsolescencia.

Soporte de Servicios Aplicativos es la unidad encargada del registro de incidencias diarias, gestión de planes de calidad, desarrollo de optimizaciones al sistema, desarrollo de planes de calidad, atención a incidencias Batch y On-line.

[3] A NIVEL DE HARDWARE, ALMACENAMIENTO Y COMUNICACIONES TAMBIÉN PRESTA SERVICIOS A AMBIENTES PREVIOS (HOMOLOGACIÓN, INTEGRACIÓN Y DESARROLLO) QUE SON ADMINISTRADOS POR LA GERENCIA DE BACK OFFICE GCB.

1.3 La Gerencia de Tecnología como apoyo a las operaciones del Banco

Los procesos críticos del Banco, sean productivos o de soporte a la operación, utilizan recursos de infraestructura tecnológicos. La infraestructura tecnológica y su correcto funcionamiento son responsabilidad de la gerencia de Tecnología. Para esta tarea cuenta con monitoreo 7x24 sobre los sistemas y soportes especializados para cada una de las distintas plataformas que el banco posee.

La tabla 1 muestra la gestión directa[4] de la gerencia de Tecnología entregando apoyo al resto de las unidades del banco.

Tabla 1. Gestión y apoyo sobre infraestructura tecnológica

	Gestión	Descripción
1	Atención de incidencias	Mediante la mesa de ayuda se captan eventos de usuarios internos sobre los aplicativos, sistemas o canales, de cualquier unidad de negocio del Banco.
2	Monitoreo de consolas backend	Control sobre el backend de procesos críticos e informes directos para unidades de negocio asociadas.
3	Monitoreo sistemas 7x24	Control de alertas sobre los sistemas y canales que prestan servicios a los procesos del banco y a clientes.
4	Soporte en pasos a producción	Monitoreo y seguimiento en los despliegues en ambiente productivo de los cambios de software y hardware.
5	Asesoramiento de arquitectura	Relacionado a las tecnologías apropiadas para nuevos aplicativos y desarrollos.
6	Asesoramiento de infraestructura tecnológica	Asesoramiento sobre infraestructura tecnológica, sus reglas y exigencias dentro del ambiente de producción para los nuevos desarrollos y aplicativos.
7	Seguimiento y comunicación de incidencias	Contacto y asistencia a unidades de negocio afectadas, entrega de información, solicitud de envío de evidencias de error y solicitud de pruebas.

[4] EXISTE UNA GRAN CANTIDAD DE PROCESOS, ACTIVIDADES Y TAREAS QUE LA GERENCIA DE TECNOLOGÍA DEBE REALIZAR PARA BRINDAR LAS ACTIVIDADES DE GESTIÓN DIRECTA, ENTRE ESTAS ESTÁN LOS PROCESOS DE COMPRA DE HARDWARE, LAS CAPACITACIONES AL PERSONAL, LA ADMINISTRACIÓN DE HERRAMIENTAS DE SOPORTE, GESTIÓN DE PROVEEDORES, ETC.

	Gestión	Descripción
8	Creación de servidores y bases de datos	A solicitud de unidades de desarrollo de software, se crea la infraestructura tecnológica aprobada.
9	Incorporación en sistemas de respaldo	Para servidores nuevos, se configura las políticas de respaldo según requerimiento y necesidades de la unidad de negocio.
10	Enlaces y conectividad	Habilitación de conexión de nuevas sucursales y plantas administrativas.
11	Habilitación de enlaces con terceros	Conexión con proveedores que requieren las distintas unidades de negocio para sus operaciones.
12	Respuesta experta ante requerimiento de grandes clientes	Evaluaciones relacionadas a tecnología y cualquier otro requerimiento de cumplimiento que necesiten clientes claves "exigido por sus propias normativas de cumplimiento".
13	Soporte en prueba de PCN[5]	Desde la habilitación de sitios de trabajo alternativos a la creación de estaciones de trabajo virtual, dependiendo de las necesidades de cada unidad de negocio.

Los múltiples servicios que proporciona la gerencia de Tecnología al resto de la organización y los clientes del Banco, hace que esta gerencia sea el soporte clave de las operaciones bancarias. Toda transacción se realiza y queda registrada en los sistemas tecnológicos de información: trasferencias entre clientes, entre bancos, con banco central; pagos de IVA, de patentes, de nóminas; liquidación de documentos, usos de tarjetas bancarias, etc. Si los sistemas tecnológicos de información dejasen de prestar servicios por cualquier falla en un tiempo prolongado, el impacto económico, legal y de imagen serian críticos para la subsistencia de la organización.

La continuidad del Banco está ligada directamente a la continuidad de los servicios brindados por la gerencia de Tecnología, por tal motivo el Plan de Contingencia Tecnológica es vital. Mantener un Plan de Contingencia Tecnológica actualizado resulta un enorme desafío, ya que no existe un proceso formal o metodología que permita su mejora continua.

[5] PCN Ó "PLANES DE CONTINUIDAD DE NEGOCIO", SE REFIERE A UN CONJUNTO DE ACTIVIDADES Y ESTRATEGIAS QUE DEFINE LA UNIDAD PARA ENFRENTAR ESCENARIOS QUE PONGAN EN RIESGO SU NORMAL OPERACIÓN.

1.4 Problema

La gerencia de Tecnología tiene la obligación de mantener un Plan de Contingencia Tecnológica[6] actualizado. Sin embargo, actualmente no existe formalmente un proceso o metodología para facilitar esta actividad, lo que incrementa el grado de dificultad si se consideran los constantes cambios tecnológicos y el foco del personal en la atención de incidencias y la operación diaria (ver figura 4).

La gestión sobre la actualización del PCT es realizada por el grupo de contingencia compuesto por 2 personas, una vez al año, basado en:

1. Los resultados obtenidos en las pruebas de contingencia (4 anuales).

2. La consulta a los jefes de unidades de tecnología, sobre cambios en los documentos complementarios del PCT o en las secciones del PCT donde sus unidades tienen participación.

Profundizando lo anterior,

1. El aporte obtenido de la ejecución de cada prueba es escaso, dado que no existe un proceso que:

    a. Capture los problemas en el ejercicio,
    b. Genere las correcciones sobre los eventos detectados,
    c. De seguimiento a la implementación de las soluciones, y
    d. Actualice el PCT según los resultados obtenidos con las soluciones incorporadas en producción.

[6] PLAN QUE PROCURA LA RECUPERACIÓN DE LOS SERVICIOS EN EL MENOR TIEMPO Y CON EL MENOR IMPACTO A LA ORGANIZACIÓN.

En este tipo de pruebas participan unas 60 personas solo de tecnología (cualquiera de ellos puede identificar un punto de mejora o una incidencia). Esto hace que sea muy complejo lograr robustecer el plan, debido a que los problemas quedan y son resueltos solo por la unidad (ver figura 4). Cada colaborador puede (dentro de sus actividades) identificar, gestionar y solucionar problemas que se le presenten en la ejecución del plan, poniendo énfasis en la recuperación y no en el registro de las acciones correctivas.

Mientras se ejecuta el plan, las actividades normales son pasadas a un segundo plano, lo que implica una acumulación de trabajo pendiente para todos los colaboradores, quienes vuelven a las actividades normales una vez normalizados los servicios, sin dejar registros y evidencias a disposición del grupo de contingencia, impidiendo la retroalimentación y el mantenimiento del plan.

Sumado a lo anterior, las jefaturas de cada unidad realizan las correcciones necesarias a sus sistemas según los eventos detectados (en pruebas y contingencia reales) con una mirada en sus actividades normales, no llegando la información de forma directa al plan de contingencia tecnológica, generando una diferencia entre las actividades y sistemas corregidos en producción y el plan de contingencia tecnológica.

2. Las unidades de tecnología implementan mejoras a nivel de continuidad, derivadas de requerimientos de comités, que no eran informadas al grupo de contingencia y no quedaban reflejadas en el PCT. al momento de la actualización.

3. Existen comités formales al interior del Banco, que realizan requerimientos directamente a las unidades de tecnología. Parte de estos requerimientos modifican aspectos considerados dentro del PCT pero, como el grupo de contingencia no forma parte de los comités, estas modificaciones quedan en el PCT sólo si el jefe de la unidad de tecnología lo considera al momento de la actualización.

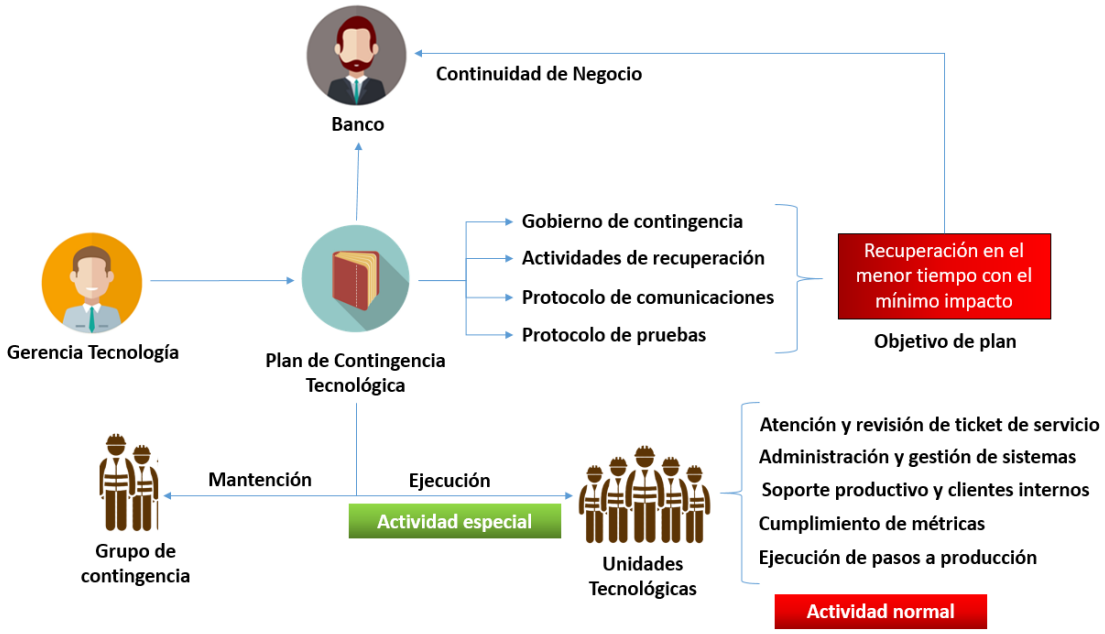


Figura 2. Componentes del Plan de Contingencia Tecnológica.

La figura 2 muestra la dicotomía que existía en relación al PCT, siendo visto por las unidades de tecnología como una actividad especial que debían cumplir, sin percibir un beneficio para ellos versus sus actividades normales que son medidas y por las que son evaluados. Sin embargo, para el resto de la organización el rol del PCT es fundamental a nivel de Continuidad del Negocio.

Adicional a lo anteriormente expuesto, tanto en pruebas como en incidencias reales, se presentan situaciones que, pudiendo encontrar una solución definitiva, no son atendidas al no recaer su responsabilidad directa en una unidad de tecnología específica.

Los problemas para llegar a contar con una metodología adecuada son los siguientes:

1. No existe una metodología clara para abordar el mantenimiento del Plan de Contingencia Tecnológica.

2. Existen factores culturales que impiden generar sinergia entre los colaboradores que ejecutan las actividades y los que están encargados de mantener actualizado el plan.

3. No existe participación del grupo de contingencia en las instancias de discusión sobre continuidad.

1.5 Objetivos

A fines de 2017 el grupo de contingencia comenzó a trabajar sobre una metodología que permitiese responder a necesidades relacionadas a contingencias tecnológicas. Se esperaba que estas respuestas (en forma de soluciones) generasen actualizaciones y mejoras al PCT.

Para contar con una metodología en forma rápida, se determinó crearla escalable, vale decir, partir con una metodología inicial (básica pero funcional), que fuese incorporando nuevos elementos producto de la retroalimentación, hasta llegar finalmente a contar con una Metodología de Mejora para Contingencias Tecnológicas (MMCT) robusta y lista para el proceso de formalización del Banco.

1.5.1 Objetivo general

Crear una metodología que apoye la resolución de contingencias tecnológicas que sea escalable y robusta.

1.5.2 Objetivos específicos

- Definir la metodología existente en la actualidad.
- Evaluar la efectividad de esta metodología.
- Diseñar una nueva metodología que identifique carencias y proponga soluciones a estas.

- Aplicar la nueva metodología para comprobar que efectivamente las mejoras implementadas cumplen con:

    - Disminución de tiempos de ejecución en los elementos sujetos de mejora.

    - Cumplimiento de revisiones de la organización (Auditorías y reguladores internos).

1.6 Estructura de la tesis

En los siguientes capítulos de esta tesis se detallará la construcción y comprobación de la MMCT, específicamente:

El capítulo 2 muestra en qué consiste el PCT y el grupo encargado de su mantenimiento.

El capítulo 3 detalla la estrategia con que se implementó la solución.

El capítulo 4 detalla las etapas donde se evaluó el comportamiento de la MMCT, sus resultados y la formalización de la MMCT en el Banco.

Finalmente, en el capítulo 5 se exponen las conclusiones de todo el trabajo.

Capítulo 2: Antecedentes

2.1 Continuidad de Servicios TI y de las operaciones como apoyo al negocio

Como ya se explicó en el capítulo anterior, la gerencia de Tecnología y sus unidades técnicas están enfocadas en ser un apoyo a las operaciones del Banco, por medio de todas sus plataformas de servicio (Web, Móvil, Sucursales, etc.). Prestar estos servicios a un alto nivel requiere asegurar la disponibilidad, accesibilidad y la continuidad de los servicios tecnológicos; por tal motivo Tecnología cuenta con la unidad de Continuidad de Servicios TI.

Continuidad de Servicios TI hace seguimiento a las incidencias dentro de la operación tecnológica, categorizándolas según impacto, asistiendo a las unidades técnicas en los planes de acción, coordinando con el resto de la organización cuando las soluciones lo requieren y colaborando con sus herramientas de monitoreo sobre comportamiento de aplicaciones y canales.

La figura 2 muestra una incidencia producto de una falla en la infraestructura tecnológica. En este ejemplo la falla impacta a nivel aplicativo, perdiendo disponibilidad en las funcionalidades, afectando tanto a los usuarios internos del Banco como a los clientes. Si la cantidad de clientes y usuarios afectados llega a umbrales establecidos como críticos, estamos hablando de una incidencia mayor con carácter de contingencia. Existen otros factores que determinan una contingencia tecnológica. Estos factores están relacionados a cantidad de servidores y aplicativos afectados, criticidad de aplicativos, fecha o día de la afectación (ejemplo fin de mes o quincena con pago de IVA), unidades de negocio afectadas, origen del evento (hardware, comunicaciones, etc), entre otros.

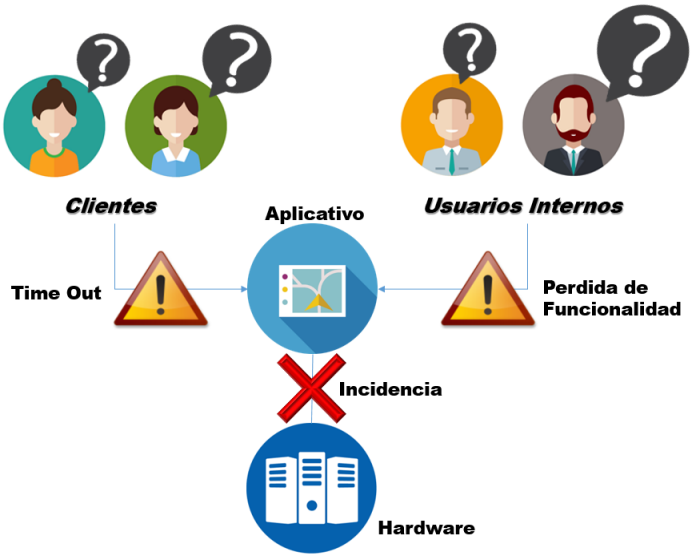


Figura 3. Impacto de incidencia producto de falla en infraestructura tecnológica.

2.2 Contingencia tecnológica

Una contingencia tecnológica implica un potencial impacto a la operación normal del Banco y a la accesibilidad de los clientes a sus cuentas y productos bancarios. La materialización de los impactos producto de una contingencia tecnológica podría significar al Banco perdidas a nivel de imagen, financieras, problemas legales por incumplimientos de servicios y contratos (dependiendo de la prolongación de la contingencia). Vista como una incidencia mayor, la contingencia tecnológica constituye uno de los focos centrales de la continuidad del negocio de la organización, ya que afectaría a las funciones de apoyo a las operaciones del Banco, teniendo el potencial de afectar a sus clientes, productos y negocios.

2.3 Regulaciones sobre la continuidad del negocio

Uno de los aspectos de interés para la CMF es la continuidad del negocio de la industria bancaria. En la tabla 2, se describen los capítulos relacionados a continuidad de negocio, que son normados por la CMF y exigidos por Riesgos no Financieros (RNF) y los auditores del Banco. Existen otros capítulos referentes a otros temas como operaciones con moneda extranjera, blanqueo de capitales, etc. que no aplican a este trabajo.

Tabla 2. Normativas de Continuidad del Negocio

Capítulo	Normativa	Puntos de interés
Capítulo 1-13	Clasificación de gestión y solvencia	Principios de Basilea. Categorías para la gestión y solvencia de los bancos. Duración de la clasificación tras la evaluación de la organización. Niveles de gestión, considerando debilidades en relación a controles internos, seguridad de sus redes y capacidad para enfrentar escenarios de contingencia Proceso de evaluación sobre la continuidad de negocio de bancos.
Capítulo 20-7	Externalización de servicios	Riesgos que se asumen con motivo de externalización de servicios. Condiciones que deben cumplirse en la externalización de servicios. Continuidad del negocio, frente a interrupción de servicios, contar con planes de continuidad del proveedor.
Capítulo 20-8	Información de incidentes operacionales	Relación de riesgo operacional tecnológico con procesos del negocio de las instituciones dentro de la industria. Comunicación de incidentes operacionales a regulador. Tipo de información y tiempos de envío. Información a clientes o usuarios, cuando afecta a la calidad o continuidad de los servicios. Información a la industria, cuando se trata de incidentes asociados a ciberseguridad.
Capítulo 20-9	Gestión de la continuidad del negocio	Conjunto de lineamientos y buenas prácticas que deben ser consideradas por las entidades en la gestión de los riesgos de continuidad del negocio. Estrategia de administración de la continuidad del negocio. Sistema de gestión de riesgos que afectan a la continuidad del negocio. Una estructura de alto nivel para administrar crisis, con atribuciones técnicas y del negocio, para controlar cualquier interrupción de alto impacto. Políticas aprobadas por el Directorio y revisadas anualmente. Toda innovación debe contar con la evaluación de riesgo de continuidad del negocio. Metodologías formales de evaluación de impacto del negocio (BIA), que considere los criterios necesarios para identificación de los procesos de mayor criticidad y determinar los tiempos de recuperación objetiva (RTO). Considerar como mínimo los escenarios de contingencia de falta total o parcial de los sistemas tecnológicos; ataques maliciosos que afecten la ciberseguridad; ausencia de personal crítico; la imposibilidad de acceder y/o utilizar las instalaciones físicas y la falta de provisión de los servicios críticos contratados a proveedores.

Capítulo	Normativa	Puntos de interés
		Someter a pruebas los planes de contingencia operativos y de recuperación ante desastres que soportan los procesos críticos en todos los escenarios previstos. Realizar pruebas, al menos con periodicidad anual, al plan de recuperación de desastres (DRP) que simulen la indisponibilidad de sus sitios de procesamiento, tanto durante la ejecución de los procesos online, como durante la ejecución de los procesos batch. Plan de comunicaciones en contingencia. Capacitaciones a personal sobre continuidad del negocio y su rol en ella. Auditorias independientes a la continuidad del negocio. Entrega niveles y estándar mínimos para los sitios de procesamiento de datos.

Las normativas expuestas, dejan claro que, ante la evaluación del regulador, la evolución de la tecnología dentro de la industria financiera abre una relación entre el riesgo operacional tecnológico y la continuidad del negocio, y por esto, establece deberes y lineamientos específicos a cumplir.

2.4 Contingencia tecnológica y continuidad del negocio relacionadas

La figura 4, muestra lo que hasta ahora hemos establecido:

Figura 4. Relación entre la continuidad del negocio, los procesos críticos y la infraestructura tecnológica.

Desde arriba hacia abajo, la figura muestra al cliente como prioridad para el Banco y la CMF, asegurando el acceso y disposición de sus productos y activos, por medio de la correcta operación de los procesos críticos y el correcto establecimiento de normas oficiales para cada aspecto de las operaciones bancarias.

Desde abajo hacia arriba, la figura representa a la gerencia de Tecnología y sus unidades técnicas, prestando servicios de apoyo al resto de la organización y sus procesos críticos, por medio de la infraestructura tecnológica.

De izquierda a derecha, muestra la cadena de continuidad de negocio, donde los procesos críticos cuentan entre sus recursos con aplicativos y canales que son soportados por la infraestructura tecnológica.

De derecha a izquierda, muestra como el regulador, tras su evaluación sobre la penetración de la tecnología en la industria, establece en sus normativas de continuidad de negocio, obligaciones y lineamientos específicos a la tecnología y establece la existencia de escenarios de contingencia tecnológica.

Toda la industria bancaria está obligada a considerar dentro de la Continuidad de Negocio las Contingencias Tecnológicas, esto implica la existencia de un elemento fundamental para este tipo de incidencias, el **Plan de Contingencia Tecnológica**.

2.5 Plan de Contingencia Tecnológica

Como ya se estableció, la gerencia de Tecnología cuenta con una unidad de Continuidad de Servicios TI que se encarga de la evaluación de las incidencias, siendo además la responsable de la mantención de Plan de Contingencia Tecnológica.

El Plan de Contingencia Tecnológica establece las acciones definidas de recuperación ante escenarios de contingencia y los responsables de llevar a cabo cada acción de detección, notificación y recuperación de desastres[7].

[7] CUANDO SE HABLA DE DESASTRES, NOS REFERIMOS A LOS EVENTOS INTERNAS O EXTERNAS QUE GENERAN UNA CONTINGENCIA TECNOLÓGICA.

Según la ISO 223018, el Plan de Contingencia Tecnológica debe contar con los siguientes elementos.

- Definición de las situaciones críticas.
- Asignación de responsabilidades.
- Acciones de respuesta.
- Mantenimiento del plan.
- Características de los tiempos de recuperación.

Según la CMF, el Plan de Contingencia Tecnológica debe ser actualizado como mínimo una vez al año. La mantención de este plan es llevada por el grupo de contingencia, compuesto por dos colaboradores, miembros de la Unidad de Continuidad de Servicios TI. El grupo de contingencia, debe realizar dentro de sus labores más importantes:

- Actualizar el Plan de Contingencia Tecnológica.
- Proponer y gestionar la aprobación del calendario de pruebas de contingencia tecnológicas anuales.
- Coordinar las pruebas de contingencia tecnológicas.
- Colaborar con las unidades de tecnología ante requerimientos relacionados a Contingencia Tecnológica.
- Asistir a la gerencia de Tecnología en comités y mesas de trabajo relacionadas a continuidad de negocio.

[8] LA ISO 22301 ES LA NORMA DE CARÁCTER INTERNACIONAL DE GESTIÓN DE CONTINUIDAD DE NEGOCIO.

Capítulo 3: Solución

Para llevar a cabo esta solución el grupo de contingencia decidió abordar el problema en fases sucesivas (figura 5), con el objetivo de sacar un producto funcional desde la primera etapa y que este fuese mejorando en cada fase, hasta alcanzar una metodología adecuada a la cultura y necesidades de la organización.

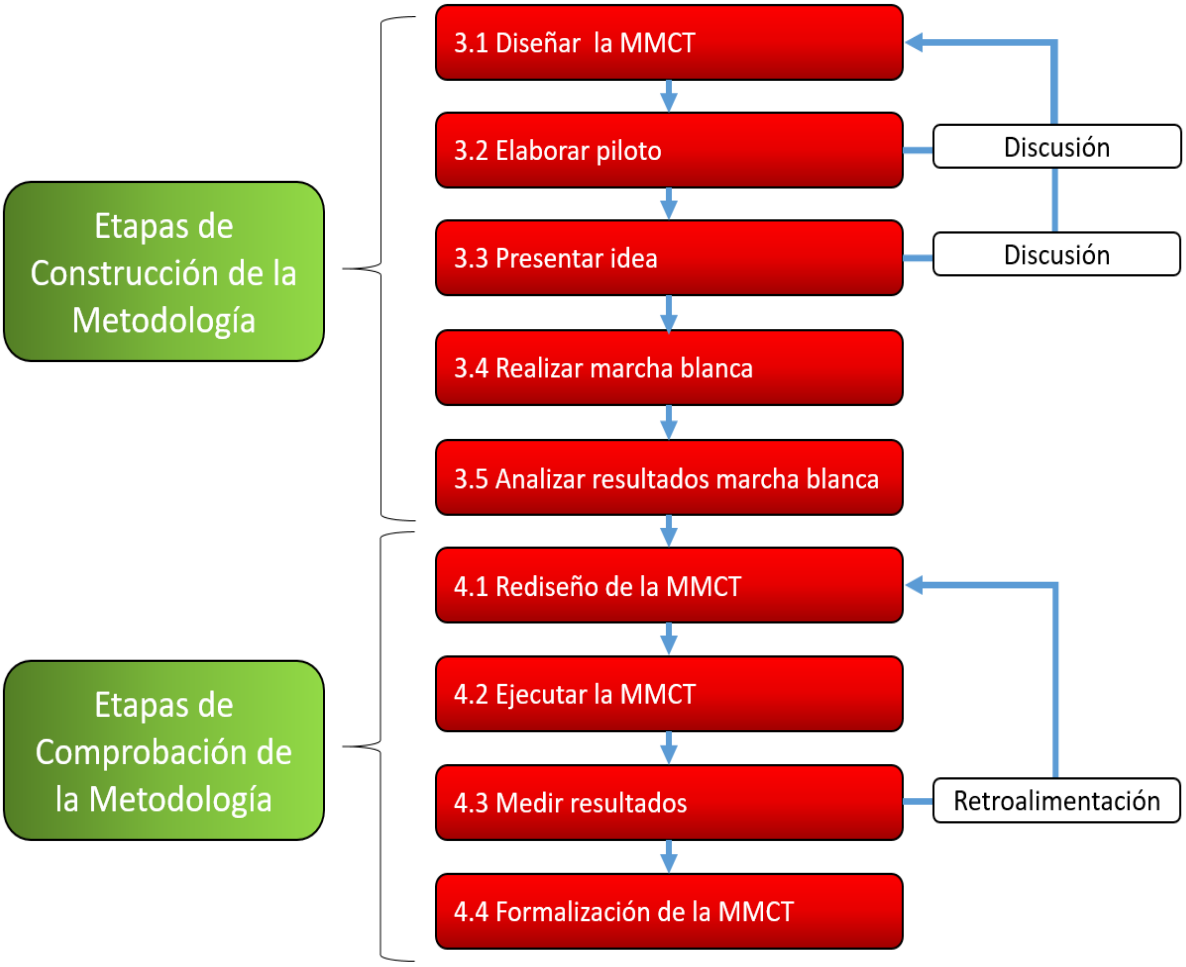


Figura 5. Plan de aplicación de la solución.

3.1 Diseñar la Metodología

Dado que el Plan de Contingencia Tecnológica (PCT) forma parte del sistema de gestión de continuidad de negocio del Banco y que su enfoque principal es la recuperación de la infraestructura tecnológica administrada por la Gerencia de Tecnología, la actualización del PCT depende tanto de los requerimientos relacionados a continuidad de negocio como a los cambios tecnológicos implementados.

El objetivo prioritario de la etapa de diseño de la MMCT fue la identificación de las fuentes de información, e incluye las instancias de captura de los requerimientos y cambios que se relacionen a la continuidad del negocio, constituyéndose como el input de la MMCT.

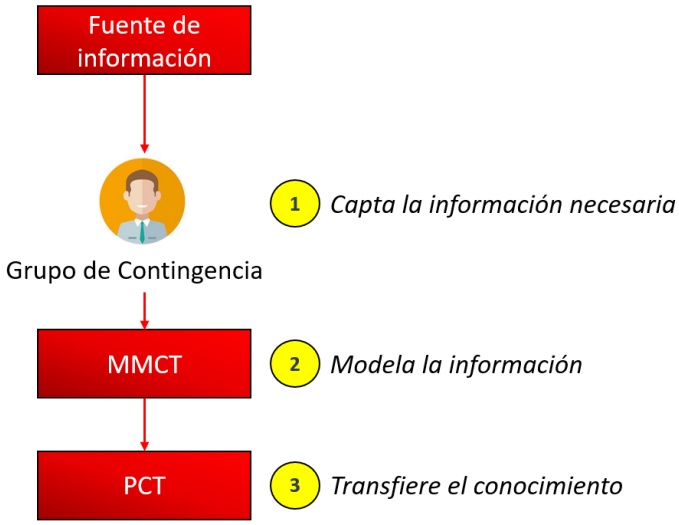


Figura 6. Esquema básico de la MMCT inicial.

La figura 6 muestra los tres pasos iniciales de la MMCT, asegurando en primera instancia contar con la información, para luego ser modelada por el grupo de contingencia dentro de la MMCT obteniendo como output una transferencia concreta de conocimiento al Plan de Contingencia Tecnológica.

3.1.1 Plan de etapa de diseño de la MMCT

Los pasos para lograr un diseño funcional de la MMCT están descritos en la tabla 3.

Tabla 3. Plan de primera etapa de la solución

Objetivos	Acciones
Encontrar los elementos necesarios a considerar dentro de la MMCT.	A. Identificar las fuentes de información al interior de la organización donde se discuten temas relacionados a contingencia y continuidad de negocio.
Contar con una MMCT inicial que responda a los puntos de mejora no atendidos.	B. Articular los elementos de la metodología en un flujograma que finalice en la implementación de las mejoras. C. Articular una estrategia que permita la adopción de la metodología dentro de la Organización.

3.1.2 Ejecución del plan de etapa de diseño de la MMCT

A. Identificar las fuentes de información. Se abordó en dos fases, la primera de ellas una reunión interna del grupo de contingencia y la segunda por medio de entrevistas para determinar la información relevante y sus fuentes.

   Fase 1, Reunión interna del grupo de contingencia: Basado en la experiencia, se determinó cuáles son las fuentes de información a utilizar en la MMCT:

1. Las pruebas de contingencia tecnológicas.

2. Los eventos de contingencia real.

3. Las auditorías sobre tecnología y continuidad del negocio.

Fase 2, Entrevistas a ingenieros: Enfocada en los colaboradores que estuvieron a cargo del Plan de Contingencia Tecnológica en el pasado, quienes señalaron como fuentes de información al Comité de Continuidad de Negocio.

B. Además de las fuentes de información otro elemento para la MMCT es la alineación normativa (cobertura del requerimiento desde el punto de vista normativo). En el anexo A se incluye un par de ejemplos sobre este punto.

Las normativas del regulador local a considerar son las relacionadas a continuidad de negocio, plasmadas en los capítulos 20-7, “externalización de servicios”, y el capítulo 20-9, “gestión de la continuidad del negocio".

Otro elemento a considerar son los roles y funciones dentro de la MMCT. Como roles y funciones es establecieron los siguientes:

- **Analista:** Miembro del grupo de contingencia encargado de procesar la información obtenida desde las fuentes y realizar el ejercicio de alineación con las normativas, para realizar una adecuada propuesta de solución.

- **Presentador:** Miembro del grupo de contingencia encargado de asistir a comités y reuniones para obtener información relacionada a continuidad de negocio y realizar la presentación de las propuestas de solución al aprobador.

- **Aprobador:** Rol asociado al Gerente de Tecnología, cuya principal función era la revisión y aprobación de las propuestas de solución.

Los elementos definidos se articularían en un flujo de cuatro etapas, tal como lo muestra la figura 7.

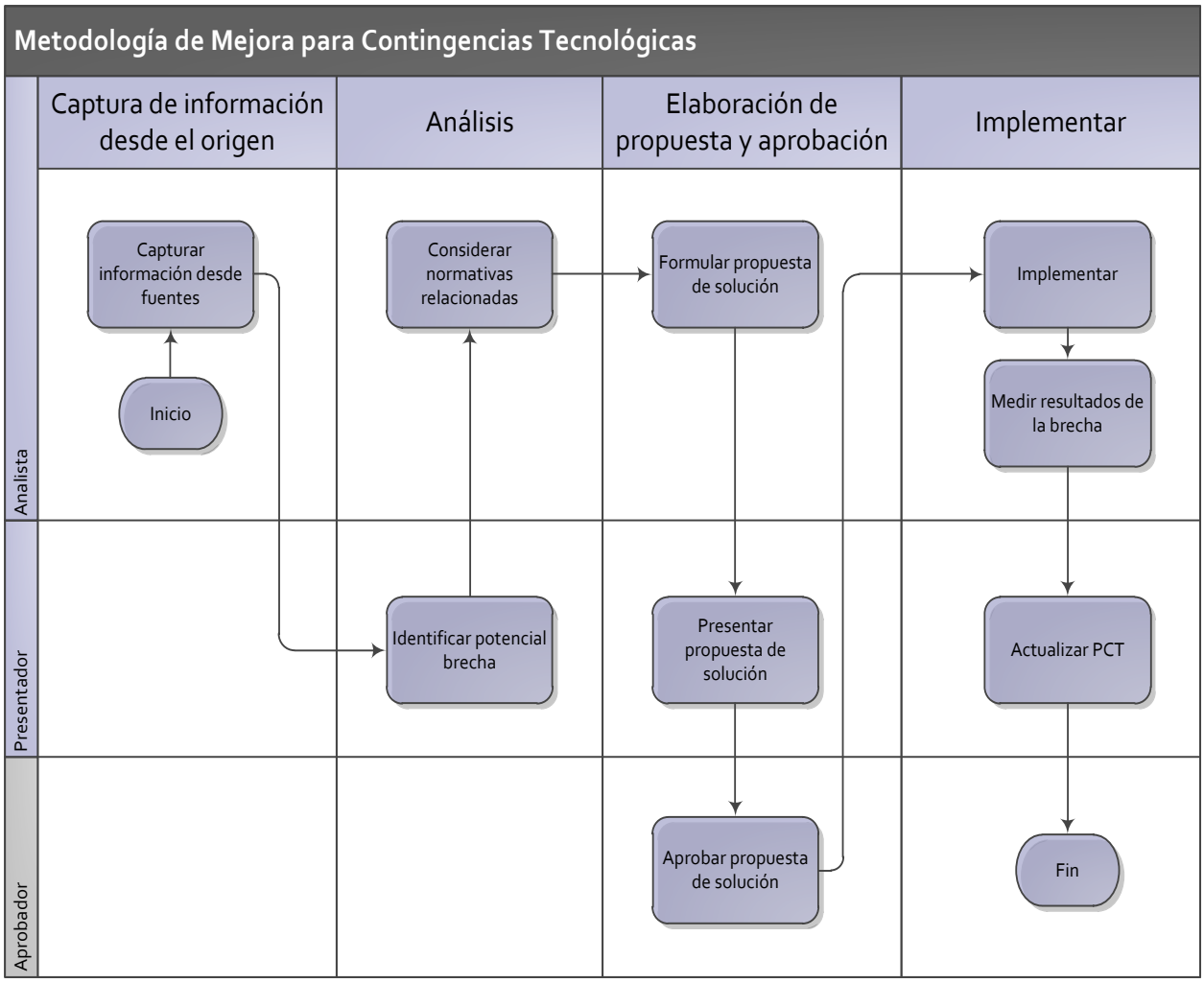


Figura 7. Flujo de la MMCT inicial.

La figura 7 muestra la relación de los elementos definidos en el flujo de la MMCT inicial. La profundización las actividades y acciones a realizar en cada paso son descritas con más detalle en el apartado 4.2.

C. Para que la MMCT pudiese ser adoptada por la organización, debía contar con el apoyo de un partnership que tuviese influencia al interior de la Gerencia de Tecnología y fuese importante fuera de la unidad, por lo tanto, el colaborador idóneo era el gerente de tecnología. Para presentar al gerente de tecnología la MMCT, era necesario contar con un ejemplo concreto de su utilidad aplicada, considerando para esto que lo óptimo era tener una MMCT inicial (escalable) que fuese rápidamente implementada como una POC[9].

   Se decidió en la reunión interna, llevar a cabo la prueba de concepto con solo los siguientes elementos:

   - **Elemento 1:** Fuentes de información.
   - **Elemento 2:** Alineación a las normativas.
   - **Elemento 3:** Roles y funciones dentro de la MMCT.

Finalmente, el grupo de contingencia para esta fase, esperaba que, tras la presentación de los resultados de la POC al gerente de tecnología, sería el mismo gerente quien facilitaría al grupo de contingencia el ingreso como invitado a los comités y mesas identificadas como fuentes de información. Permitiendo al grupo de contingencia probar y pulir la MMCT inicial, haciéndola evolucionar hasta alcanzar el grado de madurez necesario para oficializarla como una herramienta formal del PCT.

[9] POC ES UNA PRUEBA DE CONCEPTO, A MENUDO RESUMIDA O INCOMPLETA REALIZADA CON EL PROPÓSITO DE VERIFICAR QUE EL CONCEPTO O TEORÍA EN CUESTIÓN ES SUSCEPTIBLE DE SER EXPLOTADA DE UNA MANERA ÚTIL.

3.2 Elaborar piloto

Contar con una prueba de concepto previo a la presentación de la MMCT permitiría al grupo de contingencia evidenciar concretamente el potencial de ésta.

3.2.1 Plan de etapa de elaboración de piloto

Tabla 4. Plan de segunda etapa de la solución

Objetivos	Acciones
Identificar en la realidad aspectos no considerados en la fase teórica.	A. Seleccionar la oportunidad de mejora óptima para ser parte del piloto. B. Aplicar la MMCT inicial dentro de una oportunidad de mejora previamente identificada.
Contar con resultados objetivos sobre la utilidad de la MMCT.	
Asociar el uso de la MMCT con elementos concretos para el crecimiento del PCT.	

3.2.2 Ejecución del plan de etapa de elaboración de piloto

A. Seleccionar la oportunidad de mejora óptima para el desarrollo de la prueba de concepto, implicó al grupo de contingencia establecer las siguientes condiciones:

   a. El origen de la mejora debería estar relacionado a alguna de las fuentes de información a las que el grupo de contingencia ya tuviese acceso, reforzando la necesidad de contar con la información de primera mano.

   b. La responsabilidad sobre la brecha detectada no debiera estar directamente asociada a una unidad en particular, evidenciando la utilidad de la MMCT al permitir abordar este tipo de casos.

La oportunidad de mejora que cumplía con ambas condiciones estaba relacionada con el laboratorio de certificación de pruebas de contingencia Mainframe[10].

B. La aplicación de la MMCT inicial sobre el laboratorio de certificación se desarrolló ejecutando cada uno de los pasos establecidos en el flujograma:

Capturar información desde la fuente: Actividad desarrollada durante la ejecución de ambas pruebas de contingencia Mainframe (una de las fuentes de información establecidas). En dichas pruebas los usuarios certificadores se quejaron sobre el laboratorio de certificación, el que consistía en la habilitación de un espacio físico, con estaciones de trabajo (PC) que eran direccionados al Mainframe de Contingencia[11].

Identificar potencial brecha: Se analiza la información captada desde la fuente, en este caso basándose en la evidencia dejada por los usuarios certificadores durante la prueba y los hechos observados por el grupo de contingencia. Los hechos corresponden a los siguientes:

a. Algunos usuarios señalan que no tienen acceso desde la estación de trabajo a sus aplicativos.

b. Dada la limitada cantidad de PC para certificación (10 equipos), se establecen turnos de media hora, para permitir que todos los usuarios certifiquen (30 usuarios). Algunos de los usuarios no llegan en el horario programado y otros se exceden en el tiempo de certificación, generando

[10] PRUEBAS DE CONTINGENCIA MAINFRAME, SON LAS PRUEBAS EXIGIDAS POR EL REGULADOR SOBRE LOS SISTEMAS HOST DEL BANCO, SE REALIZAN TANTO PARA EL BATCH COMO PARA LOS SERVICIOS ON-LINE. COMO TODA PRUEBA TIENE CUATRO PARTES, SIMULACIÓN DE INDISPONIBILIDAD, RECUPERACIÓN DE LOS SISTEMAS, CERTIFICACIONES Y NORMALIZACIÓN DE LOS SISTEMAS

[11] MAINFRAME DE CONTINGENCIA CORRESPONDE A UN TERCER DATA CENTER QUE ERA LEVANTADO DE FORMA LOCAL SI SE PERDÍA CONEXIÓN CON LOS DATA CENTER HOST DE ESPAÑA.

colas y descontento en usuarios de turnos siguientes, llegando a sobrepasar en hasta dos horas y media el tiempo programado.

c. El lugar utilizado para realizar las certificaciones es el laboratorio de certificación técnica de ambientes previos (dependiente de otra gerencia). Las estaciones de trabajo del laboratorio están direccionadas a homologación, lo que implica que para cada prueba se debe:

   - Configurar y re-direccionar cada estación de trabajo al Mainframe de Contingencia.

   - Cambiar los perfiles de cada estación de trabajo incorporando los aplicativos a certificar.

   Realizar todos estos preparativos implica reservar el laboratorio de certificación durante un periodo mínimo de tres días (plazo que puede extenderse hasta en una semana), quedando no disponible para sus funciones originales.

d. Los soportes utilizados para realizar las configuraciones al laboratorio eran ingenieros de nivel 1 y no los soportes de End User, debido a que las configuraciones a realizar no eran estándar y requerían de coordinación con telecomunicaciones y plataformas medias. Esto implicaba la utilización de un ingeniero durante media jornada laboral para realizar labores técnicas, además de la asistencia durante el transcurso de las certificaciones.

   La brecha entre el esfuerzo realizado y el resultado obtenido se resume en la figura 8, donde se muestra la utilización de recursos calificados para una actividad excepcional.

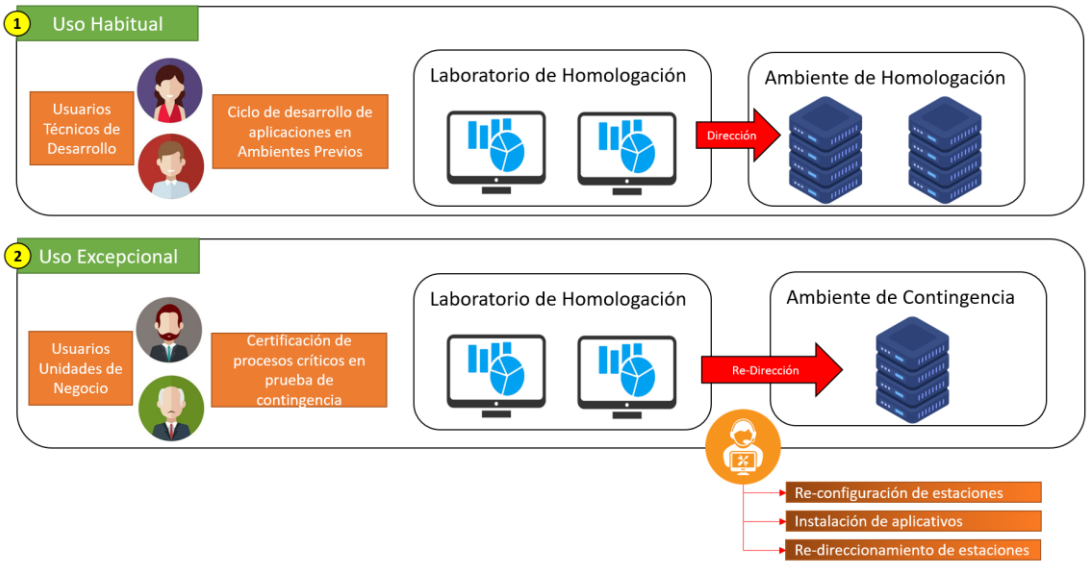


Figura 8. Uso excepcional de laboratorio de homologación.

La figura 8 muestra el uso habitual y excepcional que se daba en el laboratorio de homologación:

- Uso habitual del laboratorio: está enfocado en el desarrollo de nuevos aplicativos en ambiente de homologación. Ubicado en dependencias del Banco que cuenta con estaciones de trabajo direccionadas a este ambiente.

- Uso excepcional del laboratorio: está enfocado en la ejecución de las certificaciones usuarias necesarias durante las pruebas de contingencia Mainframe. Para dicha certificación se requería de parte de los soportes técnicos re-direccionar las estaciones de trabajo al ambiente de contingencia, reconfigurar las estaciones y adicionarles aplicaciones para certificar.

El problema no recaía directamente en una sola unidad, en este caso tratándose de una actividad excepcional se generaban las siguientes situaciones:

- La unidad End-User no era responsable al no tratarse de equipos asignados a usuarios.

- La unidad de Mainframe no era responsable al no tratarse de infraestructura Host.

- Los responsables del laboratorio de ambientes previos no eran responsables al no ser ellos parte de la prueba de contingencia Mainframe y no poseer los conocimientos técnicos.

Considerar normativas relacionadas: La normativa en el capítulo 20-9 en el título "Elementos generales de gestión", establece que las pruebas de contingencia deben realizarse de forma anual probando los procesos críticos definidos por las unidades de negocio. Dado lo anterior, la única forma de evidenciar que estos procesos fueron probados dentro de la prueba de contingencia, era que las unidades de negocio pudieran evidenciar la certificación de dichos procesos, por lo tanto no contar con las condiciones necesarias para la certificación, implicaban un expuesto normativo.

Formular propuesta de solución: Debido a que la necesidad concreta es contar con una **configuración correcta de las estaciones**[12] (no siendo factible realizar esta labor con anticipación), la alternativa óptima es contar con escritorios remotos previamente configurados. Los escritorios remotos debían contar con:

- Un servidor de contingencia donde montar los escritorios remotos, para asegurar su disponibilidad en cualquier dependencia del Banco, que cuente con red banco.

- Crear los perfiles y configuraciones cargadas previamente, para cada tipo de escritorio remoto.

[12] ESTA CONFIGURACIÓN IMPLICA QUE CADA ESTACIÓN APUNTE AL HOST DE CONTINGENCIA, ADEMÁS DE CONTAR CON LOS APLICATIVOS, OFIMÁTICA Y CANALES NECESARIOS PARA REALIZAR LAS CERTIFICACIONES USUARIAS.

Implementar[13]**:** Para la implementación se ejecutaron los siguientes pasos:

- Autorización de mesa de arquitectura: Donde se presenta la solución técnica y las razones por las que se necesita su implementación, obteniendo la aprobación técnica de la solución.

- Autorización de despliegue por la mesa de cambios tecnológicos: Se valida el cumplimiento de las exigencias a nivel de respaldos y aprobación de arquitectura, entre otros requisitos, obteniendo la aprobación de la implementación y la asignación de tareas a los grupos de soporte necesarios.

- Asignación de soporte VMware y Wintel: Para la creación del servidor de contingencia.

- Solicitud de colaboración al grupo de soporte al usuario final: Para obtener los perfiles genéricos acordes a las unidades certificadoras.

- Solicitud de colaboración a técnico de segundo nivel: Para instalar los perfiles en el servidor, configurarlos y realizar clones (obteniendo un grupo de estaciones remotas completamente funcionales).

- Capacitación a los usuarios: Para el uso de los escritorios remotos.

[13] EN EL PILOTO NO SE CONSIDERÓ LA APROBACIÓN NI PRESENTACIÓN ESTABLECIDOS EN EL FLUJO, DEBIDO A QUE ESTO SE REALIZARÍA EN LA FASE DE PRESENTACIÓN DE LA IDEA.

La implementación de las estaciones de trabajo remota tomó dos meses, dentro de los cuales el 80% del tiempo fue utilizado para la creación del servidor de contingencia. Pese al tiempo de implementación, para las pruebas de contingencia de 2018 ya se contaba con el laboratorio virtual operativo y los usuarios capacitados:

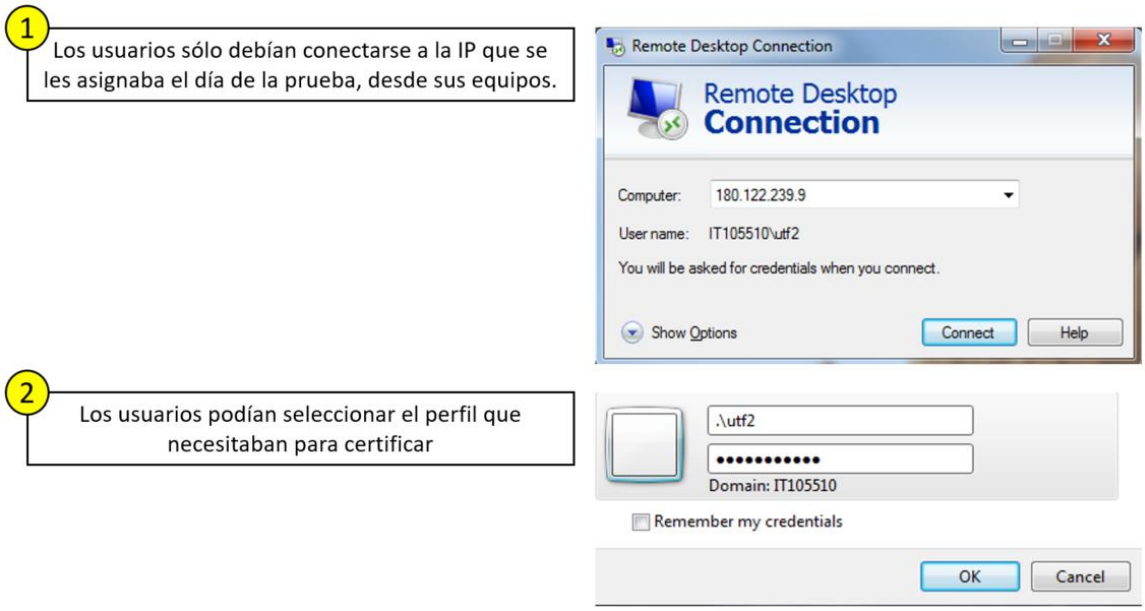


Figura 9. Conexión a escritorio remoto y selección de perfil.

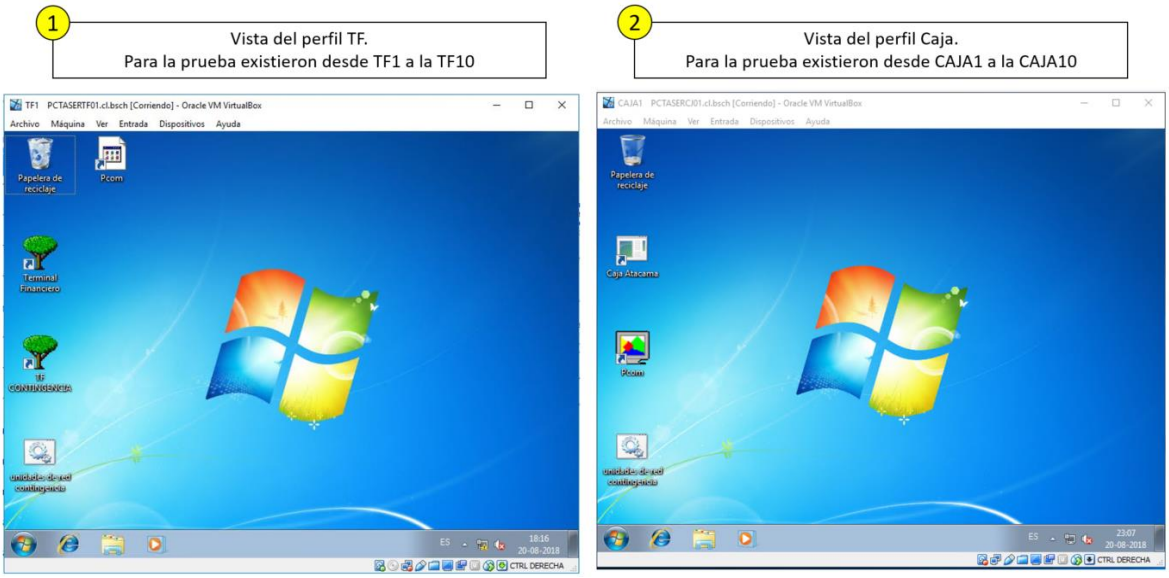


Figura 10. Perfiles de prueba correspondientes al laboratorio remoto.

Medir resultados versus brecha: En las pruebas de contingencia Mainframe del año 2018 se obtuvieron los resultados esperados, los que se tradujeron en:

- En relación al tiempo de configuración de las estaciones, este se redujo de forma significativa, pasando de 4 horas antes de la mejora a 30 minutos en el laboratorio virtual.

- El tipo de soporte para la configuración, cambió de necesitar un ingeniero antes de la mejora a solo un soporte técnico, cuyas funciones se limitaban a actualizar los parches de las estaciones remotas y la revisión de servicios.

- El uso de estaciones remotas permitió aumentar la cantidad de certificaciones simultáneas, disminuyendo el tiempo de certificación, pasando de cinco horas a dos horas y media.

- Se pasó de 10 estaciones físicas a una base de 20 estaciones remotas con la posibilidad de aumentar al doble si se requería. Las unidades de negocio tenían la posibilidad de aumentar la cantidad de usuarios certificadores, reduciendo la carga laboral por cada usuario.

- El uso del servidor permitió la conectividad desde otras dependencias del banco, liberando el Laboratorio de Homologación.

- En ambas pruebas de contingencia no se presentaron problemas de acceso a las aplicaciones, eliminando los reclamos de las unidades por este concepto.

Actualizar PCT: Se realiza la inclusión del laboratorio de certificación virtual en PCT.

3.2.3 Discusión de etapa de elaboración de piloto

La implementación de la propuesta de solución dejó las siguientes enseñanzas al grupo de contingencia:

- La participación en procesos que no son habituales para el grupo (proceso de alta y baja de hardware) implica adquirir conocimiento que otros integrantes de la gerencia de Tecnología ya poseen y desarrollan de forma cotidiana. Integrar a estos colaboradores dentro de la MMCT permitiría disminuir los tiempos de implementación.

- El laboratorio virtual para la primera prueba de contingencia Mainframe estaba montado en un servidor. Para asegurar una alta disponibilidad se creó un clon y se aumentó la RAM de ambos a 32 GB. Si en el diseño de la solución hubiese participado un colaborador familiarizado con la operación, esta mejora hubiese sido considerada desde el inicio.

Modificación de la MMCT: Se debe incluir e involucrar dentro de la MMCT a otras unidades de la gerencia con roles y funciones definidas. Estos nuevos roles y funciones deben generar sinergia y amplificar el abanico de potenciales soluciones.

Finalmente, la prueba conceptual tuvo resultados satisfactorios, mitigando todos los inconvenientes que generaba el laboratorio de certificación. Los resultados del piloto permitirán fortalecer la presentación a la Gerencia de Tecnología e identificar nuevos elementos para la MMCT (roles y funciones de personal asociado). En relación al PCT, el laboratorio virtual fortaleció el capítulo de pruebas de contingencia, detallando los requerimientos y puntos a certificar en pruebas Mainframe y agilizando sus pruebas anuales.

3.3 Presentar idea

La presentación a la gerencia tenía una importancia vital de cara a la implementación de la MMCT, generando acercamiento al sponsor más importante "Gerente de Tecnología". Si para el gerente esta herramienta tenía utilidad potencial, el grupo de contingencia contaría con el impulso para continuar con el resto de las fases.

3.3.1 Plan de etapa de presentación de idea

Tabla 5. Plan de tercera etapa de la solución

Objetivos	Acciones
Mitigar la resistencia al cambio, al momento de incorporar la MMCT.	A. Presentar la MMCT inicial y los resultados del piloto. B. Conseguir el apoyo de la Gerencia de Tecnología.
Identificar la unidad adecuada dentro de Gerencia de Tecnología para implementar la marcha blanca.	

3.3.2 Ejecución del plan de etapa de presentación de idea

A. A través de su jefatura directa, el grupo de contingencia consigue agendar reunión con el Gerente de Tecnología. La presentación contaba con:

   a. Un análisis sobre la situación actual y las dificultades de obtener información para la actualización del PCT.

   b. El impulso que generaría a la gerencia contar con una Metodología de Mejora para las Contingencias Tecnológicas, detallando aspectos como:

- Según las buenas prácticas establecidas dentro de los estándares internacionales, la ISO 22301 para la continuidad del negocio, recomienda contar con un instrumento para la actualización del plan de contingencia.

- Las auditorías internas y externas exigen demostrar cómo se abordan los problemas dentro de las pruebas de tecnología y las incidencias reales.

- Al contar con una metodología proactiva que maneje las oportunidades y enfrente las brechas encontradas al interior de la gerencia de Tecnología, se evita que sean otros departamentos (primera y segunda línea de control), quienes establezcan la forma de abordar estos aspectos, empoderando a Tecnología al interior de la Organización.

c. Mostrar la MMCT inicial como un producto funcional y escalable, que cada vez que se ejecute será afinada hasta llegar al punto óptimo de madurez de la MMCT.

d. Ejemplificar la validez funcional de la MMCT presentando el resultado del piloto en el laboratorio de certificación virtual. Dentro de sus beneficios se destacó:

- Aumento en la capacidad de certificaciones simultáneas y disminución de tiempo de la prueba.

- Eliminación de errores de acceso y falta de aplicativos para certificación.

- Disminución en el tiempo de configuración y reducción de uso de horas hombre.

- Liberación del laboratorio de homologación de cara a la ejecución de las pruebas.

e. Como propuestas de marcha blanca, se listaron una cantidad de aspectos de mejora donde la MMCT podría colaborar con algunas unidades particulares de la gerencia.

f. Expresar los requerimientos para continuar con la implementación de la MMCT.

- Contar con autorización de la Gerencia para que un representante del grupo de contingencia sea parte del comité de continuidad de negocio y la mesa de riesgo tecnológico. Importantes fuentes de información para la MMCT.

- Contar con reuniones mensuales con el Gerente de Tecnología para ver aspectos relacionados a contingencia. Mantener el foco sobre contingencia a alto nivel y aprobación de propuestas de solución generadas por la MMCT.

B. A la reunión asistieron por invitación del gerente de Tecnología, representantes de las unidades de Gobierno, Producción, Operaciones de Producción y Operaciones de Seguridad, además del grupo de Contingencia y el Jefe de Continuidad de Servicios TI.

Al finalizar la presentación, los representantes de cada unidad invitada entregaron sus apreciaciones, para concluir con el gerente de Tecnología aceptando la realización de reuniones mensuales con el grupo de contingencia y autorizando su participación. Esto último implicó la gestión del gerente de Tecnología con el gerente de Riesgos no Financieros para incluir como invitado especial al representante del grupo de contingencia en el comité de Continuidad de Negocio y la mesa de Riesgo Tecnológico.

3.3.3 Discusión de etapa de presentación de idea

El gerente de Tecnología tras la finalización de la presentación dio la palabra a los invitados, quienes centraron su atención en tres focos:

- La solución propuesta como piloto: Dentro de los comentarios se expresó que años atrás se había planteado una solución de laboratorio de certificación y que no prosperó. Fue ese comentario el que mostró al gerente el potencial de la MMCT.

- Las potenciales unidades donde realizar la marcha blanca: Los comentarios expresados apuntaban a no centrar una marcha blanca en una unidad en particular, sino que realizar una marcha blanca más general y enfocada en incidencias reales.

- La solicitud de participación en comités: Las advertencias sobre el re-trabajo que implica la participación en comités y la necesidad de presentar una y otra vez lo mismo en distintas instancias, fue uno de los comentarios más frecuentes.

Aprendizaje concreto: Con el nuevo conocimiento se debe reformular la estrategia de adopción de la MMCT, aprovechando que:

- Para los representantes de las unidades la participación en los comités implica un re-trabajo.

- Para la gerencia la presencia en dichos comités es vital.

Adicionalmente, no fue factible la identificación de una unidad para el inicio de la marcha blanca, por lo que es necesario definir otra forma de partida de la siguiente fase.

3.4 Realizar marcha blanca

La marcha blanca inició con una mejora dentro de la MMCT incorporando los elementos detectados en la fase del piloto y ajustándose a la nueva estrategia de adopción de la MMCT (basada en los input entregados en la fase de presentación de la idea).

3.4.1 Plan de marcha blanca

Tabla 6. Plan de cuarta etapa de la solución

Objetivos	Acciones
Pasar de una MMCT inicial a una MMCT establecida con sus nuevos elementos.	A. Rediseño de flujo de la MMCT incorporando elementos nuevos.
Identificar el aporte de las nuevas fuentes de información a la MMCT.	B. Participación en comités como fuentes de información. C. Ejecución de la MMCT actualizada.

3.4.2 Ejecución del plan de marcha blanca

A. Los nuevos elementos a incorporar en la MMCT fueron los integrantes de otras unidades de la gerencia (figura 11) con roles y funciones definidas.

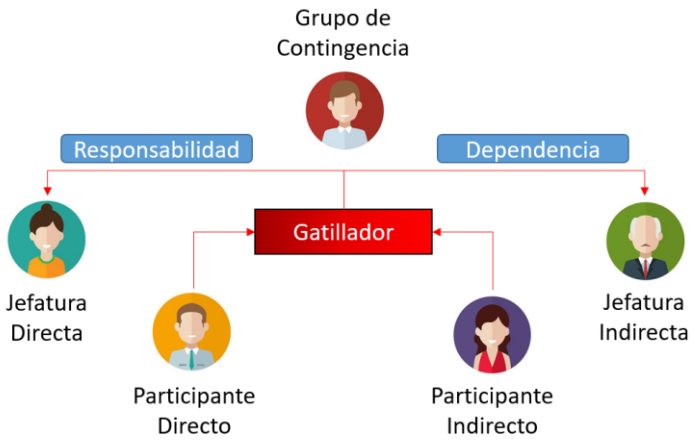


Figura 11. Nuevos roles dentro de la MMCT.

Tal como muestra la figura 11, los roles están definidos según la relación que tenga la unidad con el "gatillador" u origen de la necesidad de mejora:

a. La unidad que tenga responsabilidad operacional sobre este, tendrá un rol directo sobre el diseño de la solución.

b. La unidad que tenga algún grado de dependencia tendrá un rol indirecto (colaborativo).

c. El grupo de contingencia toma un rol contextualizador frente a la regulación asociada y de facilitador (coordinando las reuniones, colaborando con la formalización de la propuesta y dando seguimiento a la implementación). En los casos en que la responsabilidad operacional no quede claramente dentro de una sola unidad, el grupo de contingencia tomará el rol de participante directo y las otras unidades involucradas serán participantes indirectos.

La incorporación de los nuevos roles, implica una modificación de dos etapas de la MMCT inicial (“Análisis” y “Elaboración de propuesta y aprobación”), dejando el flujo tal como lo muestra la figura 12.

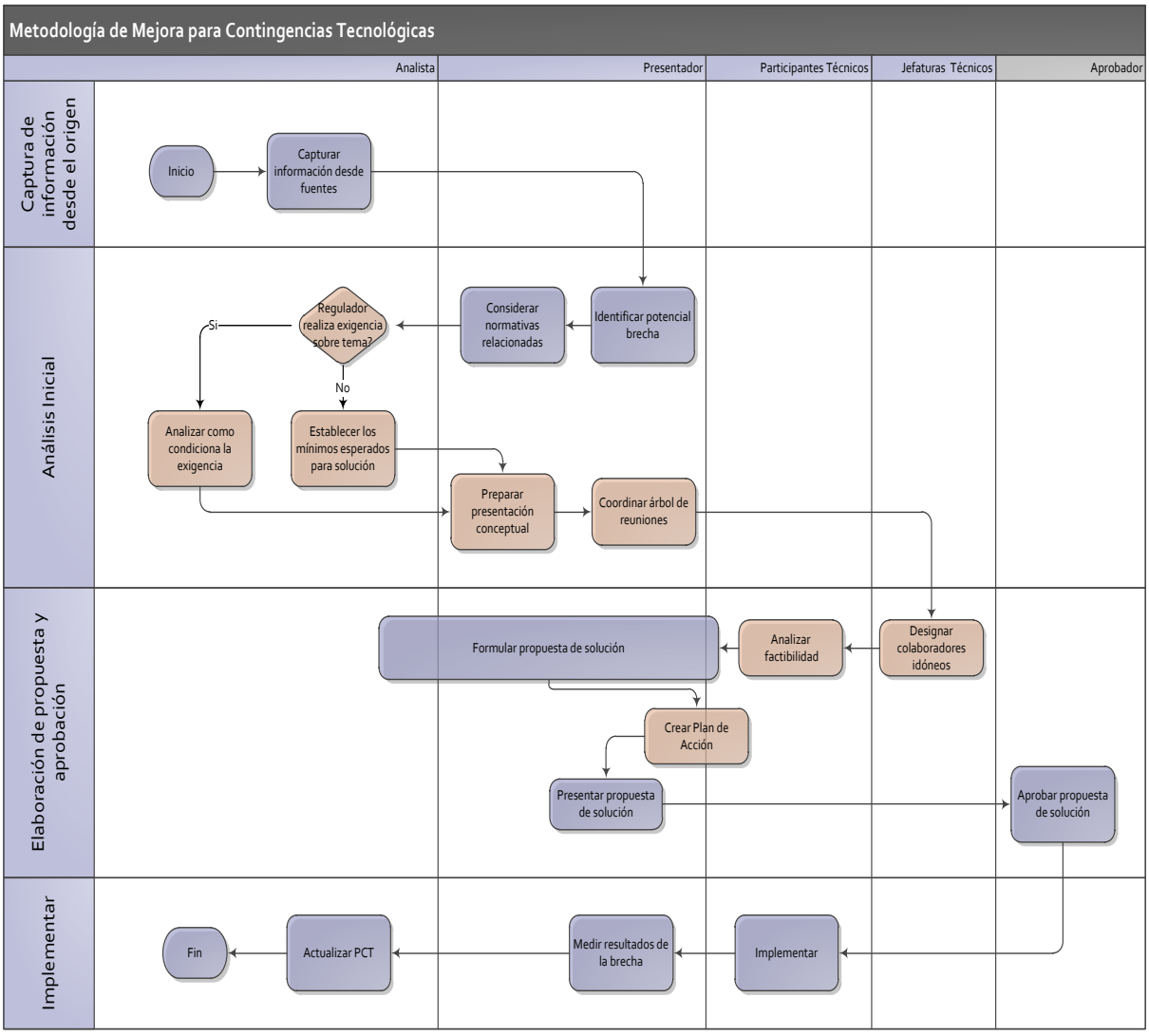


Figura 12. Flujo de la MMCT modificado.

Las modificaciones en el flujo son mostradas en la figura 12 con recuadros de color ocre.

La etapa de análisis no sólo buscaba la alineación de la propuesta de mejora con el marco regulatorio, sino además:

- Es la instancia donde el grupo de contingencia prepara las presentaciones de contexto para las jefaturas y posteriores mesas de trabajo.

- Es la instancia donde se generan las preguntas y desafíos que se expondrán a las unidades técnicas.

La etapa de elaboración de propuesta incorpora la elección de los colaboradores idóneos, además de un análisis de factibilidad para responder con los requisitos y finalmente la creación del plan de acción.

B. Para el inicio de la marcha blanca el grupo de contingencia esperó a participar en los primeros comités de Continuidad de Negocio y mesas de Riesgo Tecnológico.

Comité de Continuidad de Negocio: Sesiona una vez al mes y es constituido por representantes de cada división (ver apartado 1.2) los que tienen un carácter de miembros permanentes, además de los invitados con carácter de miembros esporádicos, cuya función es presentar informan o explican algún aspecto de interés para la sesión en particular. Este comité realiza seguimiento y toma decisión a todas las iniciativas relacionadas a continuidad de negocio.

Mesa de Riesgo Tecnológico: Sesiona cada quince días y es la antesala del comité de riesgo tecnológico. Cuenta con miembros permanentes relacionados a Ciberseguridad, tecnología y riesgo.

A partir de esta instancia, el grupo de contingencia captura de primera mano los requerimientos asociados a contingencia desde los comités. Aprovechando estas nuevas fuentes para el inicio de la marcha blanca de la MMCT.

C. En la marcha blanca de la MMCT se respondió al requerimiento sobre la creación de un Plan de Contingencia Ciberseguridad (respond[14]), solicitado en el Comité de Continuidad de Negocio al Gerente de Tecnología.

En los siguientes párrafos se describe la creación del Plan de Contingencia Ciberseguridad mediante los pasos del nuevo flujograma de la MMCT.

Captura de información desde la fuente: En este caso, la fuente de información fue el Comité de Continuidad de Negocio y el requerimiento era contar con un Plan de Contingencia de Ciberseguridad, pidiendo a la Gerencia de Tecnología que evaluara cuánto tiempo requería para entregar el documento.

Identificación de potencial brecha: El requerimiento apuntaba al potencial escenario donde las herramientas de Ciberseguridad de detección y prevención fueran sobrepasadas, por lo tanto, el Plan de Contingencia Ciberseguridad debía contener sólo la respuesta a un ataque directo a la infraestructura tecnológica del banco. Por lo tanto, las unidades que debían involucrarse como colaboradores eran:

- Operaciones de Seguridad (OS): Por tratarse de la unidad de respuesta a ciberataques.

[14] RESPOND PROVIENE DEL CONCEPTO DE LAS CINCO FUNCIONES DE CIBERSEGURIDAD (IDENTIFY, PROTECT, DETECT, RESPOND Y RECOVER), LOS CUALES EN EL BANCO SON CONCENTRADOS EN TRES PROTECT, DETECT Y RESPOND, DONDE LAS DOS PRIMERAS SON ORQUESTADAS MEDIANTE HERRAMIENTAS DE CIBERSEGURIDAD Y LA SEGUNDA POR MEDIO DE LA ESTRATEGIA DE RECUPERACIÓN ANTE CIBER-ATAQUES QUE HOY SE ENCUENTRA EN EL PCC.

- Operaciones de Producción (OP): Por tratarse de la unidad encargada de la operatividad de los sistemas tecnológicos y el monitoreo.

- Riesgo Tecnológico Operacional (RTO): Unidad externa a la Gerencia de Tecnología, responsable de todo riesgo tecnológico que pueda afectar las operaciones del Banco.

Consideración de normativas relacionadas: La normativa en el capítulo 20-9 en el título "Elementos generales de gestión", establece que las entidades deben considerar dentro de los escenarios de contingencia, los ataques maliciosos que afecten la Ciberseguridad, lo que implica que debe contar con un gobierno de contingencia articulado para poder responder al momento de la materialización de la amenaza.

Preparación de presentación conceptual: Se sostuvieran previamente reuniones informales con miembros de las tres unidades involucradas, con el objetivo de captar sus posturas e intereses sobre este tema.

Las reuniones previas mostraron que ante un escenario de contingencia de ciberseguridad no existía coordinación en las actividades ni acuerdos previos entre los grupos, dado lo anterior el foco de la presentación debía ser "el trabajo en equipos coordinados".

Coordinación de árbol de reuniones: El grupo de contingencia estableció:

- Una reunión inicial con los jefes de cada unidad.

- Ocho reuniones de trabajo con los colaboradores (con posibilidad de aumentar hasta doce si los participantes consideraban que esto era necesario).

- Dos reuniones de revisión del documento final con los participantes.

- Una reunión para aprobación del Gerente Tecnología.

- Finalmente, la presentación del documento final de PCC en Comité de Continuidad de Negocio por parte del grupo de contingencia con asistencia de RTO Respond.

Designación de colaboradores idóneos: Tras la presentación a las jefaturas de cada unidad, se solicitó identificar a los participantes para las reuniones de trabajo. Dada la importancia del Plan, Operaciones de Seguridad y RTO Respond designaron a los jefes de dichas unidades, Operaciones de Producción designó a uno de sus más experimentados representantes. El grupo de contingencia consideró incorporar en las reuniones de trabajo a miembros de Riesgos no Financieros por ser los responsables del comité y segunda línea de revisión.

Análisis de factibilidad: En la primera reunión de trabajo, los representantes de cada unidad describieron las acciones que realiza su propia unidad frente al escenario de contingencia atribuible a un ciberataque, pudiendo identificar dos patrones a mejorar, estos se expresan en las siguientes imágenes.

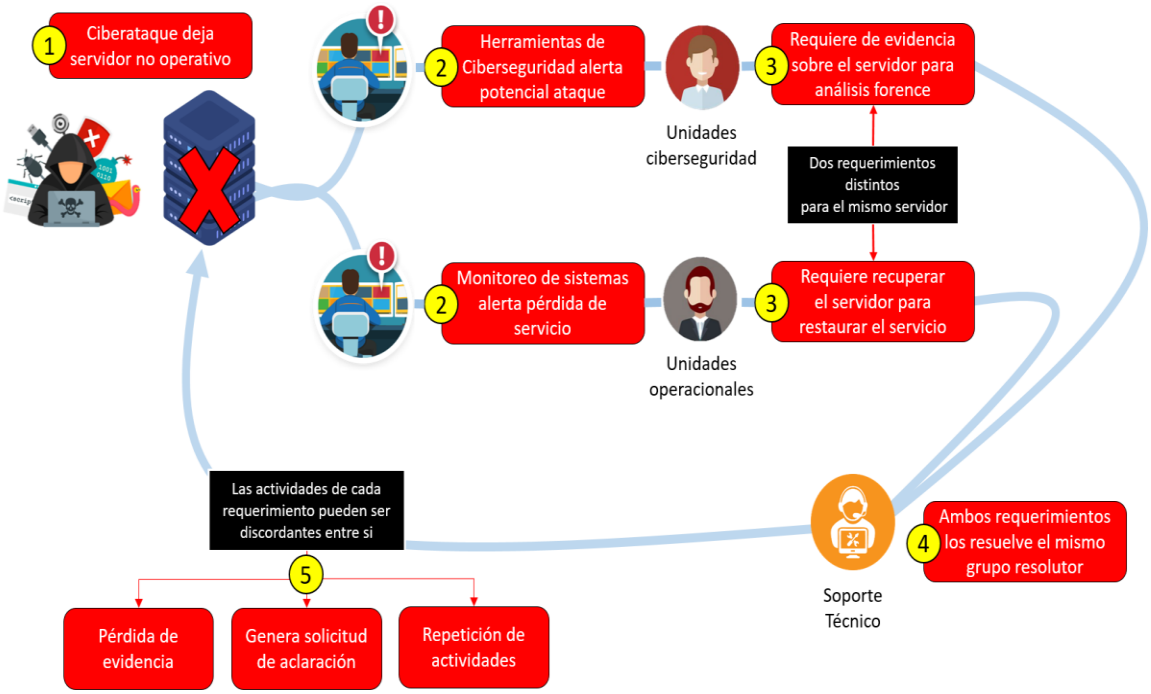


Figura 13. Dicotomía entre la acción y la información.

La figura 13 muestra, como un ciberataque genera alertas tanto en los softwares de ciber-vigilancia como en los softwares de monitoreo operacional. Esto activa a dos unidades del Banco cuyos objetivos son complementarios pero distintos. Riesgo Tecnológico Operacional necesita de evidencia para entender que hace el código malicioso y como detenerlo, mientras que Operaciones de Producción está enfocado en recuperar los servicios en el menor tiempo posible. Hasta antes de tomar este requerimiento con la MMCT, ambos grupos no se coordinaban ante este escenario, lo que podría generar aumentos de tiempo en recuperación e incluso pérdida de información para ciber-análisis (análisis forense) en una misma situación (pérdida de infraestructura).

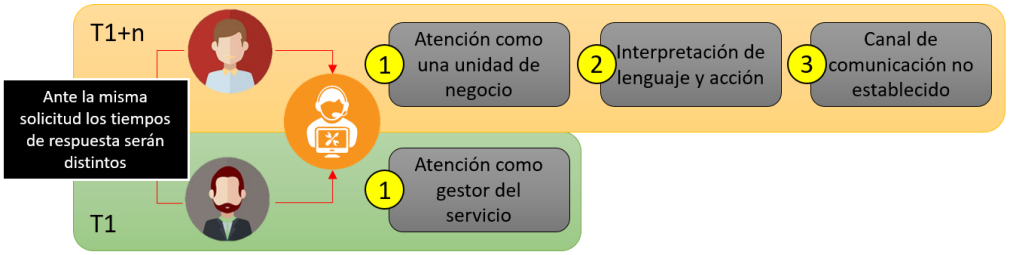


Figura 14. Diferencia de tiempos para la misma actividad.

La figura 14 muestra como la misma solicitud de actividad tomó distintos tiempos si la solicita el gestor de servicio u otra unidad, lo que podría impactar en los tiempos de reacción ante un ciberataque.

Formulación de propuesta de solución: La mesa de trabajo en la segunda reunión estableció que el foco del primer Plan de Contingencia de Ciberseguridad es ***la coordinación y gobierno en este tipo de escenarios***, estableciendo la conformación de **una tríada** conformada por representantes de las tres unidades (RTO – OS – OP).

Para lograr cada acuerdo y cerrarlo, se estableció que en las siguientes mesas de trabajo a falta de un representante de alguna de estas tres unidades se suspendería la reunión y se reagendaba.

Creación de Plan de Acción: En las siguientes sesiones de la mesa de trabajo se acordaron los siguientes puntos:

- Ámbito de acción del PCC[15].
- Escenarios de Ciberseguridad.
- Estrategia general de respuesta.
- Flujos de activación de la tríada.

[15] PCC - ESTA SIGLA CORRESPONDE A PLAN DE CONTINGENCIA DE CIBERSEGURIDAD, UN COMPLEMENTO AL PLAN DE CONTINGENCIA TECNOLÓGICA.

- Umbrales de activación.

- Declaración de “actividades tipo” dependiendo del tipo de ataque.

- Notificaciones (internas y externas) y responsables.

- Gobierno en Contingencia.

- Custodia y actualización del documento.

Presentación de propuesta de solución: Para la presentación de la propuesta y dados los tiempos acotados para cumplir con el requerimiento, el grupo de contingencia redactó el PCC incorporando los acuerdos del punto anterior, generando un documento de 42 páginas revisado por los representantes de las tres unidades.

Aprobación de propuesta de solución: El documento fue presentado al Gerente de Tecnología (CIO[16]) y al Gerente de Riesgo Tecnológico Operacional (CISO[17]) para su aprobación, siendo aprobado y quedando con carácter de Confidencial no distribuible.

[16] CIO SIGLA EN INGLÉS PARA CHIEF INFORMATION OFFICER, CORRESPONDIENTE AL RESPONSABLE DE LOS SISTEMAS DE TECNOLOGÍA DE LA INFORMACIÓN, ROL A CARGO DEL GERENTE DE GTI.

[17] CISO SIGLA EN INGLÉS PARA CHIEF INFORMATION SECURITY OFFICER, CORRESPONDIENTE AL DIRECTOR DE SEGURIDAD DE LA INFORMACIÓN, ROL A CARGO DEL GERENTE DE RTO.

Implementación: Finalmente el documento fue presentado por el grupo de contingencia en el Comité de Continuidad de Negocio y a solicitud de RNF[18] también fue presentado en el Comité de Riesgo Tecnológico, dándose por aprobado e implementado sin observaciones.

Medición de resultados de la brecha: A la fecha el PCC ha sido activado cumpliendo con las expectativas. Los acuerdos que en él se establecieron permiten la disminución de los tiempos de respuesta y las unidades cuentan con la información necesaria para actuar frente a este escenario.

Actualización de PCT: El PCC en una primera instancia fue considerado como un capítulo adicional del PCT, sin embargo, dado que cuenta con escenarios de contingencia distintos y que la conformación de su gobierno también lo es, se convirtió en un Plan adicional con sus propias fechas de revisión y actualización.

3.5 Analizar resultados de marcha blanca

Durante el período de la marcha blanca, además del requerimiento sobre la creación del PCC, a través de la MMCT se respondió otro requerimiento originado por pre-auditoria interna "formalización del gobierno en contingencias del PCT". Esta segunda solución de la marcha blanca implicó la creación de la Mesa de Contingencia GTI con sus roles y funciones específicas. Para más detalles ver anexo B.

[18] RNF corresponde a Riesgos no Financieros unidad de segunda línea, vale decir, controlador interno de toda operación no financiera.

3.5.1 Plan de análisis de resultados de marcha blanca

Tabla 7. Plan de la quinta etapa de la solución

Objetivos	Acciones
Identificar las tareas relevantes para el PCT en la ejecución de la MMCT.	A. Análisis de resultados basado en entrevistas a participantes de marcha blanca y reuniones internas.
Identificar problemas en la ejecución de la MMCT.	

3.5.2 Ejecución del plan de análisis de resultados de marcha blanca

A. Basado en las entrevistas realizadas a los participantes (18 personas) de la creación e implementación de las soluciones de la marcha blanca se obtuvieron los siguientes resultados:

   a. Sobre las fuentes de información: El 83% de los participantes hizo notar que dado lo diversas de las fuentes y lo variado de la información inicial, existe un riesgo de pérdida de información. Se determinó contar con check lists estandarizados que aseguren una base para la posterior toma de decisiones.

   b. Sobre las reuniones de trabajo: El 67% de los entrevistados señalaron que las reuniones perdían su foco una vez presentado el requerimiento y se gastaba una cantidad de tiempo importante en re-dirigir la discusión sobre el tema central (los colaboradores tendían a quedarse en detalles o alternativas que no respondían al requerimiento). Se determinó contar con una asociación directa entre requerimiento y los conceptos de continuidad, centrando la discusión en requerimientos y normativas asociadas.

   c. Sobre el traspaso de conocimiento desde la solución implementada al PCT: Tanto la gerencia de tecnología como la jefatura de Continuidad de Servicios TI señalaron que existe un riesgo en hacer la evaluación del aporte al PCT cuando la solución ya está implementada, esta evaluación

debería hacerse en pasos anteriores. Se determinó anticipar la evaluación dentro de la MMCT.

Otro punto surgió del análisis en reunión interna:

a. Sobre la cantidad de los requerimientos tomados en la MMCT que sólo llegaban a la presentación a las jefaturas y eran cerrados (50% de los casos), por tratarse de aspectos ya considerados dentro de la operación diaria. Se determinó incorporar dentro del análisis de la brecha, elementos que evitaran la duplicidad de trabajo sobre requerimientos.

b. Sobre el flujograma, en especial en lo relacionado al trabajo con los colaboradores, no era representativo de todas las acciones que eran necesarias desarrollar para obtener una propuesta de solución. Por lo tanto, fue necesario actualizar este flujograma.

Uno de los aspectos a destacar de la MMCT en la marcha blanca es que, en ambas soluciones entregadas, el gerente de Tecnología pudo responder a los requerimientos, sin que le dejasen observaciones.

Otro aspecto a destacar es que efectivamente sumar a colaboradores técnicos implicó una disminución en el número de iteraciones para dar cada paso en la etapa de implementación de las soluciones.

Capítulo 4: Evaluación de la MMCT

4.1 Rediseño de MMCT

El rediseño de la MMCT, se basó en todos los puntos obtenidos en el análisis de resultados de la marcha blanca.

4.1.1 Plan de rediseño de MMCT

Tabla 8. Plan de etapa de evaluación de la MMCT

Objetivos	Acciones
Incorporar elementos que respondan a los problemas identificados en la marcha blanca de la MMCT.	A. Rediseño de la MMCT final. B. Redacción de documento formal.
Incorporar métricas de evaluación y comparación entre distintas soluciones que genere la MMCT.	

4.1.2 Ejecución del plan de rediseño de la MMCT

A. Los elementos incorporados en la MMCT corresponden a los encontrados en la siguiente tabla.

Tabla 9. Elementos nuevos a incorporar en la MMCT.

N°	Problema Identificado	Elemento incorporado
1	Diversidad de fuentes de información, con riesgo de no levantamiento de datos relevantes	Inclusión de check list estandarizados según la fuente.
2	Duplicidad de trabajo	Separación de problemas operacionales versus problemas de contingencia
3	Pérdida de foco en los colaboradores	Clasificación de requerimientos dentro de conceptos de continuidad
4	Actividades realizadas no reflejadas en flujo actual	Adecuación del flujo incorporando todas las actividades que se realizan dentro de la MMCT
5	Identificación de impacto en PCT tardía	Perspectivas de Contribución

A continuación, se describirá en qué consisten concretamente cada uno de los elementos.

1. **Check list estandarizados según fuente de información:** Check list inicial sobre los datos mínimos a recopilar para ejecutar la MMCT. Para seleccionar estos, se consideró la factibilidad de obtención y su importancia para la contextualización del requerimiento que la MMCT debía solucionar. En el anexo C aparecen los cuatro check.

2. **Separación de problemas operacionales versus problemas de contingencia: Incluido como parte del análisis de la brecha,** se estableció a modo de declaración cuáles serían para la MMCT aspectos relacionados a la operación y que por consiguiente quedarían fuera de la MMCT. En el anexo D aparecen estos aspectos.

3. **Clasificación de requerimientos dentro de conceptos de continuidad:** Dado el gran número resultante de conceptos de continuidad, se listaron y agruparon (en ocho conjuntos), asociándolos a los capítulos de la normativa y las políticas corporativas vigentes. Esta clasificación cumple una doble funcionalidad, primero acelerar el trabajo de alineamiento normativo de la metodología y segundo asociar el requerimiento o problema a un ámbito específico.

En el anexo E aparece la tabla de conceptos vigente.

4. **Flujo modificado:** El flujo incluido en el anexo F, corresponde a todas las actividades que se deben desarrollar al momento de ejecutar la MMCT.

5. **Perspectivas de Contribución:** Utilizando un concepto proveniente del cuadro de mando integral[19], se desarrollaron cuatro perspectivas[20] que según el grupo de contingencia contribuyen en asegurar que se cumpla con el objetivo del PCT. Cualquier propuesta de solución obtenida de la ejecución de la MMCT antes de pasar por el proceso de aprobación, es tomada por el grupo de contingencia quienes ponderarán su contribución en cada una de las perspectivas, incluso pudiendo comparar el grado de contribución entre propuestas de soluciones, permitiendo medir la real contribución al PCT. En el anexo G aparecen las definiciones de cada perspectiva, mientras que en el anexo H que corresponde al documento de la MMCT aparece su forma de cálculo.

[19] CUADRO DE MANDO INTEGRAL ES UN MODELO DE GESTIÓN QUE TRADUCE LA ESTRATEGIA EN **OBJETIVOS** RELACIONADOS ENTRE SÍ, MEDIDOS A TRAVÉS DE **INDICADORES** Y LIGADOS A UNOS **PLANES DE ACCIÓN** QUE PERMITEN ALINEAR EL COMPORTAMIENTO DE LOS MIEMBROS DE LA ORGANIZACIÓN CON LA ESTRATEGIA DE LA EMPRESA. SUS AUTORES, ROBERT KAPLAN Y DAVID NORTON.

[20] LAS PERSPECTIVAS FORMAN PARTE DEL MODELO DEL CUADRO DE MANDO INTEGRAL. SON LAS BASES QUE FUNDAMENTAN EL OBJETIVO, CADA ACCIÓN REALIZADA DEBE ESTAR ASOCIADA A AL MENOS UNA DE ELLAS, PARA CONTRIBUIR A ALCANZAR EL OBJETIVO ESTABLECIDO.

La evaluación de los resultados permitió identificar una métrica clara entre las soluciones proporcionadas por la MMCT, asociada a la reducción del tiempo de respuesta, factor esencial en una contingencia.

Tabla 10. Comparación de tiempos de respuesta.

Situación Previa	Solución Implementada
Preparación de laboratorio de homologación 4 horas	Preparación de laboratorio virtual 30 minutos
Coordinación entre las partes antes de PCC Aproximadamente entre 30 a 40 minutos[21]	Coordinación entre las partes con PCC Entre 3 a 15 minutos[22]

Adicional a esta métrica, cada requerimiento tiene un objetivo particular a cumplir. Además, dentro de la evaluación de la solución propuesta debe existir una forma de medirlo. En los casos anteriores sería tal como muestra la tabla 10.

Tabla 11. Evaluación de cumplimiento.

Solución entregada por la MMCT	Requerimiento inicial	Evaluación de solución Implementada
Laboratorio virtual de certificaciones	Contar con estaciones de trabajo que permitan realizar certificar usuaria, eliminando el margen de error en la configuración de dichas estaciones.	Número de errores de configuración igual a 0 Número de aplicaciones a certificar no instaladas 0 Número de estaciones de trabajo mal direccionadas al host de contingencia igual a 0
Plan de Contingencia de Ciberseguridad (PCC)	Contar con un documento formal que explicite el Plan de Contingencia para escenarios de Ciberseguridad	PCC redactado y aprobado por Gerencia. PCC formalizado en Comité de Continuidad de Negocio.

[21] DATO OBTENIDO EN ENTREVISTAS PREVIAS A LAS PARTES.

[22] MEDIDO EN PRUEBAS DE CONTINGENCIA CIBERSEGURIDAD.

B. La redacción del documento llevó aproximadamente tres meses, donde fue incluido:

a. Desarrollo de un draft base de la MMCT.

b. Creación del flujograma.

c. Revisión cruzada entre el flujograma y las fases del documento.

d. Obtención del documento final.

El documento final se puede ver en el anexo H.

4.2 Ejecutar la MMCT

La Mesa de Riesgo Tecnológico entrega un requerimiento relacionado a recuperación de respaldos. A solicitud del Gerente de Tecnología este debe ser abordado con la MMCT.

La recuperación de respaldos es un proceso formal del Banco y tiene como objetivo proporcionar a la unidad de negocio que lo requiera, su información particular contenida en un sistema de respaldos en un momento puntal del tiempo. Este proceso cuenta con infraestructura tecnológica dedicada para esta función y operadores que realizan sus funciones basadas en procedimientos específicos de recuperación.

4.2.1 Plan de ejecución de la MMCT

Tabla 12. Plan de ejecución de la MMCT

Objetivos	Acciones
Validación de la efectividad de la MMCT, para ingresarla en el proceso formal de publicaciones del Banco.	A. Ejecución de la MMCT en caso práctico

4.2.2 Ejecución del plan

A. La recuperación de respaldos forma parte importante dentro del Plan de Contingencia Tecnológica, entregando alternativas para la continuidad de servicios ante la pérdida de datos e infraestructura tecnológica.

   El requerimiento relacionado a recuperación de respaldos solicitado por la Mesa de Riesgo Tecnológico, brindó la oportunidad para afinar el nuevo flujo de la MMCT, el cual se ejecutó entre octubre 2019 a julio de 2020 con los siguientes resultados:

a. **Captura de información**, basado en los datos obtenidos desde la fuente de información "Mesa de Riesgo Tecnológico" y plasmado en el check list correspondiente (ver la siguiente tabla).

Tabla 13. Captura de información desde la fuente.

ID	Consideraciones	
01	Contexto del requerimiento	
	Mesa de Riesgo Tecnológico presenta los nuevos indicadores solicitados por el Corporativo, los cuales tiene carácter de obligatorios para todos los países y su implementación debe ser inmediata. Dentro de los indicadores se incluye uno relacionado al control de calendario de recuperación[23], sobre los respaldos de componente asociados a aplicativos críticos. La métrica se calcula de forma mensual, entregando la medición sobre los últimos seis meses vencidos. Cálculo de la métrica: V_1 = Total de componentes relacionados a aplicativos críticos calendarizados. V_2= Componentes relacionados a aplicativos críticos efectivamente recuperados. $\left(\frac{\sum_{n=1}^{6} \frac{V_2 * 100}{V_1}}{6}\right)$	
02	Objetivo o resultado esperado del requerimiento	
	Obtención de un porcentaje igual o superior a 95% (verde). Entre 95% y 85% (amarillo). Inferior a 85% insuficiente (rojo).	
03	GTI es gestor de las acciones o soporte	Gestor y Responsable del indicador.
04	Plazos de entrega	Entrega de observaciones un mes posterior el requerimiento. Cumplimiento del indicador; el quinto día hábil del mes que corresponda a la entrega trimestral.
05	Plataforma tecnológica involucrada	
	Plataformas Medias – Sistema de Respaldos	
06	Personal de GTI que se encuentre trabajando en tema	
	Ingeniería – Soportes de Respaldos – Soportes de Motores de Datos – Operadores	
07	Unidad solicitante	Corporativo

[23] El calendario de recuperación se deriva del antiguo calendario de fiabilidad. Este controlaba la calidad de los medios (cintas magnéticas) donde se guardan los respaldos. Tras el paso de cintas a discos, este control sufrió un reenfoque apuntando a la calidad del proceso de recuperación.

b. **Identificación de la brecha**, paso establecido para separar una mejora de la operación diaria con los temas asociados a contingencia y continuidad de servicios TI.

Tabla 14. Identificación de brecha en tres hitos.

Hitos	Resultado
Completitud de la información	Se realiza una reunión con los responsables de centralizar las métricas de Chile, para entender la dinámica de entrega y las evidencias que se solicitarían para evidenciar los resultados.
Verificación de relación del requerimiento con MMCT	Debido a que la criticidad aplicativa dentro del banco puede ser establecida por los conceptos de: Disponibilidad (contingencia) Integridad (operacional / contingencia) Confidencialidad (operacional) Se solicitó aclaración al Corporativo.
Hallazgo u oportunidad	Dado que es un requerimiento formal se clasifica en la MMCT como una **Oportunidad de Mejora**.

Como resultado de este punto, se clarificó que la recuperación de respaldos calendarizados está asociada a aplicativos críticos por disponibilidad, especificando que:

- Los archivos de evidencia sobre la recuperación deberían ser custodiados por la gerencia.

- La entrega de la métrica debía ser acompañada por el listado de servidores recuperados (con una descripción del resultado del proceso).

c. **Clasificación de la información**, enfocada en encontrar el marco normativo relacionado al requerimiento, por medio de los conceptos de continuidad.

Tabla 15. Clasificación de la información.

Hitos	Resultado				
Asociación a conceptos de continuidad	Concepto de Continuidad		Grupo		Documento
	Medios de respaldo y recuperación		Respaldo de Datos		Capítulo 20-9 CMF Política gestión de la producción Política Plan Contingencia Tecnológica
	Políticas de negocio para los respaldos		Respaldo de Datos		Política Ciberseguridad D6 Política Plan Contingencia Tecnológica
	Políticas técnicas para los respaldos		Respaldo de Datos Respaldo de Configuraciones		Política gestión de la producción Política Ciberseguridad A3 Política Ciberseguridad D6 Política Plan Contingencia Tecnológica
	Procedimientos de respaldo y calendario de respaldos		Respaldo de Datos Respaldo de Configuraciones		Capítulo 1-7 CMF Capítulo 20-9 CMF Política gestión de la producción Política Ciberseguridad A3 Política Plan Contingencia Tecnológica
Bases de la clasificación	Exigencia Normativa	Responsable	Hallazgo u Oportunidad	Tiempo de respuesta	Orden de Prioridad
	Alta	Gerente Tecnología	Oportunidad	Próxima sesión de comité	No Aplica

El requerimiento es de alta exigencia tanto a nivel del regulador local como del corporativo, teniendo un marco normativo claro con exigencias a nivel del proceso, control y resultado esperados. La normativa exige a la entidad que cuente con infraestructura y procedimientos de respaldo que permitan recuperar los datos, software básico y aplicativos, ante una contingencia o corrupción de la información de acuerdo con los RPO[24] y RTO[25] establecidos.

La base de clasificación es útil cuando se cuenta con más de un requerimiento, permitiendo priorizar los esfuerzos. En este caso no fue necesario definir el orden de prioridad.

[24] RPO (Recovery Point Objective) es la cantidad máxima de pérdida de datos definida por la entidad.

[25] RTO (Recovery Time Objective) es el periodo máximo de tiempo establecido entre la disrupción y la recuperación de los servicios tecnológicos.

d. **Formulación de propuesta de solución**, core de la MMCT fuertemente enfocada en el desarrollo colaborativo.

Tabla 16. Formulación de la propuesta.

Hitos	Resultado		
Árbol de Reuniones de Trabajo	Reunión Contextual	Reuniones de Trabajo	Reunión de compromiso
	Enfocado con la jefatura de ingeniería, dado que es el gestor de todos los soportes asociados. Se adicionó a jefatura de operaciones, dado que es la unidad que solicita las recuperaciones ante una contingencia. Se adicionó a jefatura de Gobierno, dado que es la encargada en cumplimientos auditables.	Se estableció una reunión inicial de recolección de información sobre el actual calendario de recuperación y el proceso de recuperación. Tras la primera reunión se establecieron cuatro reuniones de trabajo para acordar un proceso de creación de calendario y trabajar sobre el requerimiento. Se estableció una reunión de entrega de instrucciones a soportes y reuniones mensuales de seguimiento.	Se realizaron dos reuniones de compromiso, la primera con las jefaturas de los participantes. La segunda fue con el Gerente de Tecnología.
	Como resultado, ingeniería designó a un participante directo, mientras que las otras unidades designaron a los participantes indirectos.	El resultado de las reuniones de trabajo se describe en los párrafos posteriores a esta tabla.	Ver resultado en presentación de contribución, que es el último punto de esta tabla.
Determinación de tipos de soluciones	La solución establecida fue de tipo documental, dado que requirió la creación de un procedimiento de confección del calendario de recuperaciones y establecimiento de los criterios de revisión sobre los respaldos. Posteriormente, se adicionó infraestructura tecnológica a la solución, dado que en reuniones de seguimiento se detectó la falta de restore de Oracle para recuperaciones.		

Hitos	Resultado			
Evaluación de impacto sobre el PCT[26]	Gobierno de Contingencia	Estructura y Control	Formación y Crecimiento	Monitoreo y Control
	1	4	2	5
Presentación de contribución	Se aprueba la creación del procedimiento de confección de calendario de recuperación. Se aprueba las reuniones de seguimiento y solución propuesta. Agregando la petición de la gerencia que el grupo de contingencia fuese el dueño del control de la métrica y ampliar el uso de la MMCT en otros aspectos relacionados a respaldos.			

Reunión Inicial: La información recopilada en esta reunión sirvió para concluir que:

Tabla 17. Situación inicial y esperada del proceso.

Situación Inicial	Situación esperada
El calendario de recuperación cuenta con 53% de cobertura de aplicativos críticos, dado que su foco anterior era sobre requerimiento de auditoria.	Cobertura de Aplicativos Críticos sobre un 95%
La unidad de soporte responsable de realizar las recuperaciones es la misma unidad que define que servidores deben ser recuperados.	Separación de funciones
No existe control, solo se revisa la evidencia si un auditor la solicita y cuando esto ocurre es solo para un grupo acotado de servidores. Nombres de los archivos no concuerda con resultado al interior de ellos (no está normado).	Control del proceso y revisión de evidencias de recuperación

Para ver más detalle de cada uno de esto puntos ver anexo I.

[26] La evaluación de impacto de la solución sobre el PCT, es calculada como el promedio obtenido de las evaluaciones individuales de cada participante en el desarrollo de la solución. La nota que se puede asignar a cada una de las cuatro perspectivas va de 1 a 7, siendo 7 la más alta contribución y 1 una baja contribución a la perspectiva.

Reuniones de trabajo sobre el calendario: Para cumplir con la cobertura del requerimiento y realizar una correcta separación de funciones, se acordó que:

- El calendario de recuperaciones 2020 y los sucesivos sería confeccionado por banco[27] y entregado al soporte de recuperación para su ejecución. Para su creación se establecería un procedimiento formal asegurando que siempre cubriese componentes de aplicativos críticos (como era exigido en el requerimiento).

- Se aumentaría la cantidad de servidores a recuperar en al menos un 100%, necesario para asegurar la cobertura que el calendario 2019 no tenía.

Reuniones de trabajo sobre requerimiento: Tras obtener un calendario adecuado al requerimiento, era necesario establecer acuerdos con las unidades que forman parte del proceso de recuperación, para asegurar que las exigencias que planteaba el requerimiento fuesen cubiertas en la ejecución del proceso. Por tales motivos se establecieron controles y seguimientos, tal como muestra la siguiente tabla:

Tabla 18. Acuerdos de control y seguimiento.

Acuerdo	Descripción
Reuniones de seguimiento mensuales	Reuniones entre el responsable banco del servicio, el proveedor que proporciona el servicio de recuperación y el grupo de contingencia. Con foco en el cumplimiento de las recuperaciones establecidas para el mes, el resultado de dichas recuperaciones y observaciones de cualquiera de las partes sobre el proceso de recuperación.
Entrega programada de evidencias	El soporte sería responsable de entregar de forma mensual los archivos con las evidencias de ejecución de cada recuperación.
Disponibilidad de evidencias	El grupo de contingencia recepcionaría los archivos y disponibilizaría un repositorio para que las unidades de Banco pudiesen tener acceso a las

[27] LAS UNIDADES DEL BANCO QUE PARTICIPARÍAN EN LA CREACIÓN SON CONTINUIDAD DE SERVICIO TI (INCLUYENDO LOS SERVIDORES DE APLICATIVOS CRÍTICOS), GOBIERNO TI (INCLUYENDO LOS SERVIDORES EXIGIDOS POR AUDITORIA), OPERACIONES DE PRODUCCIÓN (INCLUYENDO LOS SERVIDORES CON MAYOR TASA DE INCIDENCIAS), TÉCNICA DE SISTEMAS REALIZANDO LAS REVISIONES Y CONTROLES TÉCNICOS A QUE EL CALENDARIO REQUIERA.

	evidencias.
Control sobre los resultados de las recuperaciones	Banco revisaría las evidencias proporcionadas por el soporte considerando[28]: La correcta búsqueda en catálogo[29]. La correcta ejecución de la recuperación. La obtención de evidencia de un elemento respaldado. La correcta tipificación del ejercicio por parte del operador.
Cálculo y entrega de la métrica	Serán de responsabilidad del grupo de contingencia.

Más detalles en anexo I.

Reuniones de compromiso: Tal como establece la MMCT, correspondía realizar una reunión de compromiso donde los jefes de unidad toman conocimiento formal de los acuerdos y pueden dejar sus observaciones frente al trabajo expuesto, presentándoles los siguientes acuerdos:

- Aumento del número de servidores a recuperar, pasando de 15 a 38 servidores por mes.

- Aumento de la cobertura de aplicativos críticos para la plataforma Midrange pasando del 53% al 100%.

Aprobación por parte del gerente de Tecnología, de la solución en su conjunto, solicitando que los resultados de las recuperaciones fuesen presentados en la reunión mensual que sostiene el gerente con el grupo de contingencia.

[28] PARTE DE ESTE CONTROL INCLUÍA LAS CORRECCIONES DEL PROCESO DE RESPALDOS, EN LOS CASOS EN QUE EL SERVIDOR NO EXISTÍA DENTRO DEL CATÁLOGO DE RESPALDOS, SE REALIZARÍA INCLUSIÓN AL SISTEMA DE RESPALDOS Y SE CONSIDERARÍA COMO RECUPERACIÓN FALLIDA PARA LA MÉTRICA.

[29] OTRO DE LOS CONTROLES ERA SOBRE LA CONSTANCIA EN EL PROCESO DE RESPALDOS, POR MEDIO DE LA BÚSQUEDA DEL CATÁLOGO SE IDENTIFICABAN EN LAS EVIDENCIAS POTENCIALES LAGUNAS DE RESPALDO, VALE DECIR, PERIODOS DONDE EL PROCESO DE RESPALDOS NO CORRIÓ.

Reunión de entrega de requerimiento: Se entrega el calendario 2020 a los soportes y las acciones a realizar según los controles definidos.

e. Seguimiento de la implementación

Primera reunión de seguimiento: Se detectaron las siguientes desviaciones:

- Los soportes no realizaban las acciones acordadas según controles establecidos, entregando una métrica del mes de enero de 41% (insuficiente).

- Los archivos entregados incluyen notas redactadas por los operadores, cuyo mensaje no es clarificador.

- Se generó un backlog de recuperaciones calendarizadas, por el aumento de recuperaciones solicitadas en calendario.

Segunda reunión de seguimiento: Los resultados fueron los siguientes:

- Métrica conjunta entre enero y febrero de 59% (insuficiente).

- Las notas de los operadores disminuyen en cantidad y mejoran en claridad.

- Backlog de recuperaciones calendarizadas aumenta en relación al mes anterior.

Se determina:

- Reuniones de seguimiento semanal para realizar las correcciones dentro del mismo mes.

- Volver a realizar las recuperaciones de los meses anteriores.

- Estandarización de notas y acciones a realizar por parte de los operadores (ver tabla 19).

Tabla 19. Problemas detectados en la implementación.

Tipos de Issues	Descripción	Resolución
Servidor no incluido en sistema de respaldos	Servidor que no aparece en el catálogo del sistema de respaldos.	Nota del Operador debe indicar: "Servidor no forma parte de sistema de respaldos". Técnica de Sistemas realiza análisis del servidor identificando: Aplica respaldo, se genera ticket de alta para sistema de respaldos. En métrica se marca como recuperación fallida. Es parte de un cluster, se debe indicar su nombre y ser recuperada. En métrica se considerará el resultado del segundo servidor. Es appliance, no aplica en calendario de recuperación, sistema de respaldos fuera de alcance. Se saca de la métrica.
Fecha de solicitud de recuperación anterior a la existencia de respaldo	Servidor incorporado posteriormente al sistema de respaldos.	Nota del Operador debe indicar: "Servidor con fecha de respaldo posterior a la solicitada". Se recupera la fecha más antigua que aparece en el catálogo. En métrica se considerará el resultado de esta nueva fecha.
Fecha de solicitud posterior a la última existente	Servidor eliminado del sistema de respaldos.	Nota del Operador debe indicar: "Servidor con fecha de respaldo anterior a la solicitada". Se recupera la última fecha en catálogo. En métrica se considerará el resultado de esta nueva fecha. Adicionalmente, el representante de soportes debe entregar ticket donde se solicita la eliminación del servidor del catálogo.
Servidor con laguna de respaldos	Servidor en catálogo con fechas anteriores y posteriores a la solicitada en calendario.	Nota de Operador debe indicar: "Servidor en catálogo con fechas de respaldos posteriores y anteriores a la solicitada". Se recupera la fecha en catalogo más cercana a la solicitada. En métrica se considerará el resultado de esta nueva fecha. Adicionalmente el representante de soportes debe indicar en próxima reunión las fechas que contemplan esta laguna y la causa que la originaron.

Reunión de seguimiento semanal: Durante los siguientes tres meses, los esfuerzos se enfocaron en corregir las desviaciones en acciones y notas de los operadores.

Los resultados obtenidos en la repetición del ejercicio para los meses de enero y febrero fueron satisfactorios, cumpliendo con métricas de 100% para enero y 94,9% para febrero. En el mes de marzo, se identificaron dos tipos adicionales de Issues, mencionados en la tabla 9.

Tabla 20. Segunda tabla de problemas detectados en la implementación.

Tipos de Issues	Descripción	Resolución
Falla de medios	Respaldos en cinta magnética con error al momento de recuperar respaldo	Nota de Operador debe indicar: “Falla de medio”. Error en cinta no tiene opción de reparación. En métrica se considerará como restauración fallida.
Falta de infraestructura tecnológica	Operadores no cuentan con los restore necesarios	Nota de Operador debe indicar: “No cuenta con infraestructura tecnológica”. En reunión de seguimiento se realiza un plan de acción para contar con infraestructura necesaria. En métrica no se considera servidor hasta finalizar plan.

4.3 Medir resultados

El calendario de recuperación fue la primera ejecución de la MMCT final. En este apartado se verán los resultados de su ejecución.

4.3.1 Plan para medir resultados

Tabla 21. Plan para medir resultados

Objetivos	Acciones
Comprobación de la efectividad de la MMCT en un caso concreto	A. Ejecución de la MMCT en caso práctico.

4.3.2 Ejecución del plan

A. Los resultados del calendario de recuperación tras la implementación de la solución derivada de la MMCT, fueron los siguientes:

Tabla 22. Resultados por mes.

Mes calendarizado	Recuperación exitosa
Enero 2020	100%
Febrero 2020	94,9%
Marzo 2020	81,3%
Abril 2020	100%
Mayo 2020	100%
Junio 2020	97,4%
Julio 2020	100%
Agosto 2020	91,4%
Septiembre 2020	100%
Octubre 2020	97,7%

Los resultados favorables, permitieron entregar en el mes de octubre de 2020 por primera vez la métrica, tanto en comités como a nivel corporativo con un 98,1% (compuesto por los porcentajes promediados de los meses entre abril y septiembre), quedando en el rango de métrica satisfactoria. Las variaciones observadas en la tabla se deben principalmente a dos factores, el primero de ellos es la falla de medios en donde se conservan los respaldos (Disco o Cinta Magnética), el segundo factor es la no existencia del servidor solicitado en el proceso de respaldos (esto se corrige incluyéndolo en el sistema), pero para la medición queda registrado como una falla, pues el respaldo no existía al momento de ser solicitado.

Sobre la actualización del PCT, la incorporación del calendario de respaldos fue ingresada en la actualización del 31 de diciembre de 2019, correspondiente a la versión 3.

En la etapa final de la MMCT que permite el ciclo de mejora continua, tras la implementación de cada solución, los resultados obtenidos son agrupados y presentados en la reunión mensual con el Gerente de Tecnología. Se debe considerar además la cobertura del requerimiento original, los siguientes aspectos:

Figura 15. Aspectos considerados en la retroalimentación.

La solución sobre el calendario de recuperación entregó los siguientes resultados:

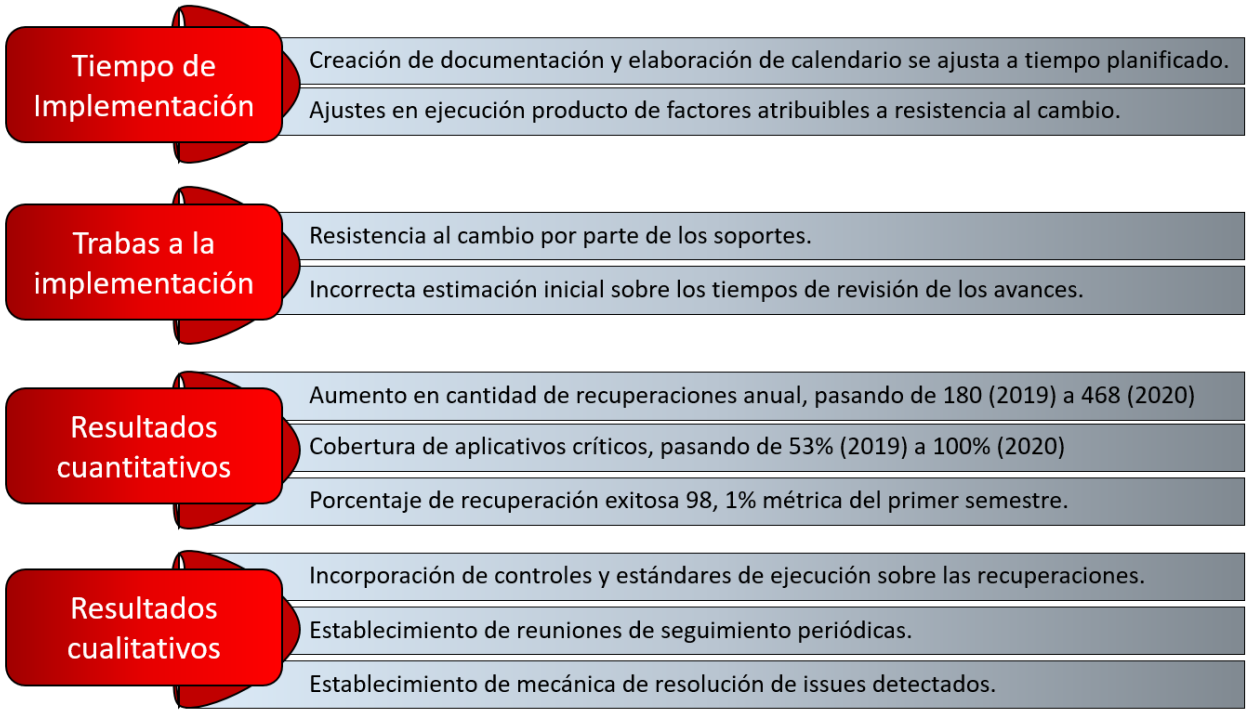


Figura 16. Aspectos considerados en la retroalimentación para la solución particular.

La figura 16 muestra los resultados tras la implementación de la solución para el calendario de recuperación. Los resultados no sólo permitieron responder a la métrica de forma satisfactoria, situándose por sobre el 95% establecido a nivel Corporativo, sino que además potenciaron el PCT desde **el trabajo preventivo** ante la necesidad de recuperación de servicios basada en respaldos.

Contar con controles sobre los respaldos, unido a la sensibilización de los operadores sobre las necesidades de la organización, debe ser visto como **construcción de sinergia**, lo que toma tiempo pues implica romper con paradigmas.

Los resultados de esta solución por medio de la MMCT, fueron tan contundentes que el Gerente de Tecnología solicitó su uso para abordar los siguientes puntos relacionados:

- Métrica sobre porcentaje de recuperaciones fallidas en solicitudes reales de unidades de negocio.

- Control sobre respaldos de bases de datos productivas.

- Estatus de infraestructura tecnológica de respaldos versus estándares esperados.

Tras medir los resultados del mes de Julio de 2020 (100% de recuperaciones calendarizas exitosa), el grupo de contingencia logró el objetivo propuesto de la ejecución de la MMCT pudiendo dar inicio al proceso de formalización de documental.

4.4 Formalización de la MMCT

El proceso de formalización documental debe cumplir etapas de revisión establecidas por la organización para alcanzar la publicación oficial.

4.4.1 Plan de formalización de la MMCT

Tabla 23. Plan de formalización de la MMCT

Objetivos	Acciones
Contar con una Metodología reconocida por los órganos formales del Banco	A. Ejecución del proceso de formalización documental.

4.4.2 Ejecución del plan

A. La siguiente imagen muestra las etapas de formalización por las que pasó la MMCT antes de ser formalmente aceptada dentro de la Organización.

B.

Figura 17. Etapas de formalización de la MMCT dentro de la Organización.

Presentación a Gerencia: Instancia formal de presentación de la MMCT y sus resultados al Gerente de Tecnología, para la aprobación.

La presentación mostró la MMCT dividida en cinco etapas (tal como muestra la imagen), tomando como ejemplo la solución sobre "métrica sobre calendario de recuperaciones".

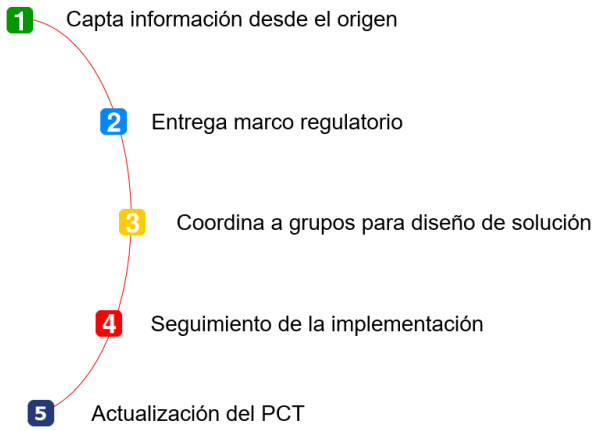


Figura 18. Etapas de la Metodología.

Esta presentación fue revisada en dos reuniones, en las cuales el grupo de contingencia respondió preguntas y profundizó algunos temas de acuerdo con la solicitud del gerente.

Finalizada la presentación, el Gerente de Tecnología entrego su aprobación, mostrándose satisfecho por el trabajo realizado y solicitó generar un documento resumido de la MMCT, que permitiera a los ejecutivos poder interiorizarse sobre el tema con mayor facilidad.

Revisión del documento: La revisión del documento fue en dos fases, la primera con el Jefe de Continuidad de Servicios TI y la segunda con el Gerente de Tecnología.

La primera revisión fue en sesión remota, donde se hizo lectura íntegra al documento, tras esta revisión se realizaron modificaciones de forma y cambio al nombre del concepto "Fuentes de Información" por "Gatilladores de Información".

La segunda revisión implicó el envío del documento al gerente de Tecnología, incluyendo los cambios incorporados de la primera revisión.

Aprobación: Tras la revisión exhaustiva del documento, el Gerente de Tecnología envía su aprobación formal sin observaciones. La MMCT ya aprobada es incluida en la versión 4 del PCT como anexo C y referenciada en el punto 1.9 de "Actualización del PCT", formando parte integral Plan de Contingencia Tecnológica de Banco Santander.

Ratificación institucional: Con la aprobación formal del Gerente de Tecnología, el grupo de contingencia solicita a la unidad de Gestión de Servicios TI, la publicación oficial del documento.

Esta publicación requiere de una ratificación de aprobación por parte del Gerente de Tecnología, ante la consulta de la unidad de Normas y Procedimientos, la que fue entregada el 23 de septiembre de 2020. Con esto, se generó la circular N°8.582 para toda la organización, indicando que la MMCT está publicada en el Portal de Normas e impacta a las unidades de T&O[30].

jueves 24/09/2020 11:46

Normas y Procedimientos

PUBLICACION CIRCULAR N° 8.582 PROCEDIMIENTO DE MEJORA PARA CONTINGENCIAS TECNOLOGICAS (MN070E-2)

Para

CIRCULAR N°8.582 PROCEDIMIENTO DE MEJORA PARA CONTINGENCIAS TECNOLOGICAS (MN070E-2)

Comunicamos que se ha realizado una nueva publicación en el Portal de Normas y Procedimientos de la Intranet, cuyo contenido les solicitamos tomar conocimiento y/o difundir entre el personal de su dependencia, según corresponda.

RESPONSABLE

Gerencia de Tecnología – Área Continuidad de Servicios TI – [redacted]

ÁREAS IMPACTADAS

Todas las Unidades de T&O

OBJETIVOS DEL DOCUMENTO

Tiene por objeto informar la publicación del Documento Metodología de Mejora para Contingencias Tecnológicas en el Portal de Normas.

IMPACTO / IMPLICANCIA

CONSULTAS

[redacted]

ANTIGUO FUNCIONAMIENTO	NUEVO FUNCIONAMIENTO
N/A	*Primera versión del Documento*

Ruta de Publicación: Intranet/Normas y Procedimientos/ Tipo de documentos/Procedimientos

Figura 19. Publicación de Circular sobre la MMCT.

Publicación oficial: Además de la publicación en el Portal de Normas el documento se publica en el Catálogo de Servicios como parte de la Base de Conocimientos del Banco, finalizando con esto el proceso de formalización de la MMCT.

[30] DIVISIÓN DE TECNOLOGÍA Y OPERACIONES

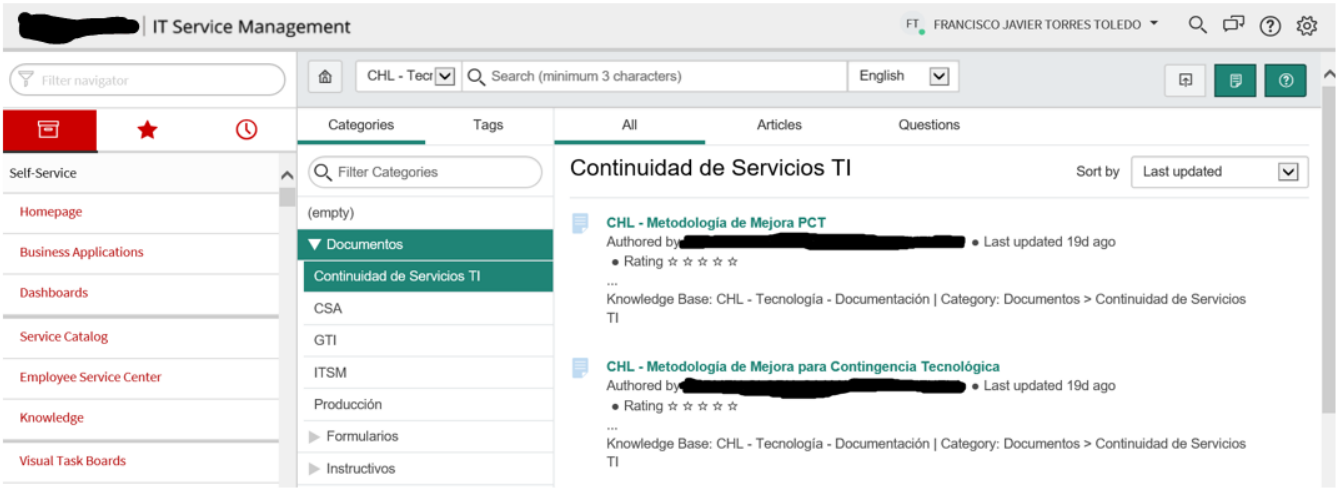


Figura 20. Publicación de MMCT en Catálogo de Servicios.

Capítulo 5: Conclusión

La Gerencia de Tecnología es la responsable al interior del Banco de contar con un Plan de Contingencia Tecnológica correctamente actualizado. Por motivos expuestos en este documento, la actualización del PCT contaba con múltiples problemas en su ejecución, por la falta de acceso a fuentes de información y paradigmas culturales. Todo el trabajo de mejora, adopción y desarrollo de la MMCT que permitía subsanar los problemas, se abordó en este documento de tesis.

Existía una desconexión entre los requerimientos de contingencia, las soluciones brindadas para responderlos y el conocimiento incorporado en el PCT. El grupo de contingencia encargado de las actualizaciones estaba fuera del flujo de información establecido para los requerimientos y solicitudes.

Dada la necesidad de contar con una metodología funcional en el menor tiempo posible, se optó por el desarrollo escalable y que fuese mejorando por medio de la retroalimentación que entregaría cada solución implementada. La primera versión de la MMCT era extremadamente básica; pese a esto permitió al grupo de contingencia ejercitar un flujo de mejora y terminar con un problema que llevaba años.

La segunda versión de la MMCT, se enfocó en subsanar la más grande limitación de la versión inicial, la falta de acceso a las fuentes de información y ampliar la participación en la MMCT a todos los integrantes de la Gerencia de Tecnología en el desarrollo de las soluciones.

La tercera versión de la MMCT (actual), producto de la retroalimentación, fue enriquecida con elementos que generaban sinergia con los colaboradores de otras unidades y mejoró la forma de medición de resultados. La contribución real de las propuestas de soluciones medida con las perspectivas y el ciclo de mejora continua, aseguran un crecimiento del PCT en cada ejecución de la MMCT.

Dado la forma elegida para desarrollar la MMCT, cada requerimiento la desafía, generando en cada ejecución de la MMCT una respuesta al requerimiento y una retroalimentación al flujo. Lo anterior, también genera un riesgo a considerar, pues

ante ejecuciones paralelas es factible que la retroalimentación baje su calidad y la MMCT deje de evolucionar acorde al ambiente y contexto bancario.

La contribución real de la MMCT a la Organización no sólo se puede medir por la buena respuesta a requerimientos concretos (con resultados medidos), sino que además se ve reflejada por la presencia que ha tenido el grupo de contingencia, que para el Gerente de Tecnología en su conjunto son una poderosa forma de respuesta preventiva en relación a los riesgos de ciberataques (dado el contexto de la industria nacional), focalizando hoy sus esfuerzos en respaldos y recuperación.

Glosario

Análisis de impacto de negocio o BIA: Comprende el análisis de actividades o procesos y el efecto que una disrupción del negocio pudiera tener sobre ellos.

Análisis de riesgo o RIA: Comprende la identificación, evaluación y valoración de los riesgos de los procesos, centrados en aquellos riesgos que podrían afectar a la continuidad del negocio.

Continuidad el negocio: Se refiere a la capacidad de la organización para continuar la entrega de productos o servicios en los niveles aceptables de operación, previamente definidos, tras un incidente.

Escenario de Contingencia: La descripción de las circunstancias, condiciones o acontecimientos adversos que pueden representar la peor situación del entorno en un momento futuro del tiempo. Corresponde a un ejercicio de evaluación y análisis personal (a la institución, organización o unidad), considerando las posibilidades dada la realidad de la organización, por enfrentar a una situación que impida al entorno analizado funcionar de forma normal.

Gestión de la continuidad del negocio: Se entiende como un proceso de administración, que incluye las políticas, normas y procedimientos necesarios para garantizar que los productos o servicios entregados por las instituciones bancarias se puedan mantener o recuperar de manera oportuna en el caso de una interrupción.
Incidente(s): Interrupción o reducción en la calidad del servicio o cualquier acontecimiento que podría afectar negativamente el servicio.

ISO 22301: Norma de carácter internacional de gestión de continuidad de negocio.

Plan de contingencia operativo: Se refiere a los procedimientos orientados a recuperar las operaciones ante la ocurrencia de fallas producto de la materialización de alguno de los escenarios de contingencia definidos por el banco. Son complementarios, en lo que corresponde, al Plan de recuperación ante desastres.

Plan de recuperación ante desastres (DRP): Procedimientos diseñados para dar respuesta ante una pérdida parcial o total de los recursos computacionales e instalaciones físicas que las soportan.

Proveedor(es) de servicios: entidad relacionada o no a la institución contratante, que preste servicios o provea bienes y/o instalaciones a ésta.

Proceso de gestión de incidentes: conjunto de actividades orientadas a restaurar la operación normal del servicio a la brevedad y a mantener al mínimo el impacto adverso en la operación normal.

Punto Objetivo de recuperación (RPO): Máxima pérdida de datos aceptada por la entidad. Sitio o centro principal (producción): Infraestructura física donde se centralizan los recursos informáticos para proveer la tecnología necesaria para la operativa diaria.

Sitio o centro de contingencia: Centro de procesamiento que debe contar con los recursos necesarios, para asegurar la recuperación tecnológica de los sistemas en el tiempo estimado por la entidad.

Tiempo de recuperación objetivo o RTO: Periodo de tiempo después de un incidente en que la provisión tecnológica de los productos, servicios o actividad debe reanudarse; o los recursos deben ser recuperados.

Bibliografía

[1] Creación de SBIF
https://www.sbif.cl/sbifweb/servlet/ConozcaSBIF?indice=7.5.1.1&idContenido=525

[2] Reemplazo de SBIF por CMF
http://www.cmfchile.cl/portal/principal/605/w3-article-23902.html

[3] Normativas CMF
http://www.cmfchile.cl/institucional/legislacion_normativa/normativa.php

[4] Capítulo 1-13
http://www.cmfchile.cl/portal/principal/605/w3-article-28811.html

[5] Capítulo 20-7
http://www.sbif.cl/sbifweb3/internet/archivos/norma_119_1.pdf

[6] Capítulo 20-8
https://www.sbif.cl/sbifweb3/internet/archivos/norma_10696_1.pdf

[7] Capítulo 20-9
https://www.sbif.cl/sbifweb3/internet/archivos/norma_11364_1.pdf

[8] ISO 22301 Requisitos
https://www.iso.org/standard/75106.html

[9] Cuadro de Mando Integral
https://cmigestion.es/cuadro-de-mando-integral/

[10] Kaplan y Norton
https://www.isotools.org/2015/07/25/norton-y-kaplan-dos-referentes-para-un-modelo-unico-gestion-estrategia/

[11] Perspectivas del Cuadro de Mando Integral
https://gestion.pensemos.com/perspectivas-del-cuadro-de-mando-integral-que-son-y-para-que-sirven

Anexos

Anexo A: Ejemplos de alineación normativa

1. Si dentro de una prueba de contingencia, la unidad responsable de un sistema detectara un problema técnico sobre una configuración particular, subsanaría la configuración errónea dentro del sistema. La MMCT de cara a la normativa, exigiría un mayor nivel de profundidad, llevándonos a una propuesta de mejora como un plan de revisión sobre los sistemas con configuraciones similares y que tras este análisis se contemple la calendarización de las correcciones.

2. Si un comité solicita una modificación en el manejo de un tipo de respaldo de datos, la unidad responsable de la Gerencia de Tecnología, realizará un análisis de factibilidad técnica sobre el requerimiento y según eso propondrá una forma de resolver el requerimiento. La MMCT de cara a la normativa, contrastaría el requerimiento con lo exigido dentro del marco regulatorio, entregando argumentos claros de como “acoger/no acoger” la modificación y presentar una alternativa distinta si aplica.

Anexo B: Mesa de Contingencia GTI

Esta fue la segunda solución entregada en la etapa de marcha blanca. Respondía al requerimiento de una pre-auditoria interna sobre un ítem particular gobierno de contingencia.

Por medio en entrevistas dentro del marco de la MMCT, se trabajó con los jefes de unidades de la Gerencia de Tecnología. Ellos explicaron cómo se organizaban ante una incidencia y las labores que se realizaban, esto se alineo con los procesos de

gestión de crisis que tiene establecido el banco y fue formalizado directamente dentro del PCT donde se incorporaron los siguientes apartados:

- Se generó en el PCT un apartado completo “Gobierno de Contingencia”.

- Se creo la Mesa de Contingencia GTI estableciendo formalmente sus funciones principales.

- Se establecieron roles y responsabilidades.

- Se formalizaron las Mesas Técnicas y sus participantes.

Ambas mesas fueron probadas en las pruebas de Contingencia FIT para dejar evidencia de su uso en los informes. Tras esto se realizó la auditoria y pasar por revisión tanto el PCT como los informes de prueba, el hiten de gobierno de contingencia, cumplió la auditoría sin observaciones.

Anexo C: Ckeck List sobre fuentes de información

Tabla 24: Check de captura de información de sesiones.

ID	Consideraciones
01	Contexto del requerimiento
02	Objetivo o resultado esperado del requerimiento
03	GTI es gestor de las acciones o soporte
04	Plazos de entrega
05	Plataforma tecnológica involucrada
06	Personal de GTI que se encuentre trabajando en tema
07	Unidad solicitante

Tabla 25: Check de captura de información de cambios documentales.

ID	Consideraciones
01	Señala sistemas o plataformas particulares
02	Entrega parámetros a cumplir (cuantitativos o cualitativos)
03	Solicita o incorpora controles particulares
04	Es de carácter reiterativo/cíclico/procedural
05	Establece tiempos de implementación
06	Exige aprobaciones particulares, escalamientos o divulgación de algún tipo
07	Se trata de un deber o recomendación

Tabla 26: Check de captura de información en prueba de contingencia.

ID	Consideraciones
01	Horario de ocurrencia
02	Tiempo de duración
03	Identificar servicio/canal/aplicativo afectado
04	Identificar unidad de negocio/proceso/funcionalidad afectada
05	Identificar servidores/software/componentes involucrados
06	Existe evidencia física del error (captura de pantalla, imagen de consola, alerta de monitoreo, etc.)
07	Identificar usuario, soporte o tipo de cliente que identifica evento
08	Identificar impacto real ocasionado
09	Identificar grupo, soporte o unidad que solucionó evento

Tabla 27: Check de captura de información en activaciones reales de PCT

ID	Consideraciones
01	Identificar banda horaria de ocurrencia
02	Identificar tiempo de duración
03	Identificar servicio/canal/aplicativo afectado
04	Identificar unidad de negocio/proceso/funcionalidad afectada
05	Identificar servidores/software/componentes involucrados
06	Descripción de la estrategia de recuperación
07	Planificación de la estrategia de normalización
08	Identificar origen del desastre y afectación al banco
09	Identificar grupo, soporte o unidad(es) involucrada(s)

Anexo D: Descarte de aspectos relacionados a la operación

- Los requerimientos de comité que estén relacionados al plan de sistemas, no forman parte de esta metodología.

- Los requerimientos de comité que estén relacionados a la operación diaria de cualquier aspecto de la infraestructura tecnológica no forman parte de esta metodología, salvo en los casos expresamente relacionados a la continuidad del servicio TI.

- Los lineamientos documentales deben ser considerados dentro de la MMCT, con una mirada de continuidad del servicio TI.

- Durante una prueba de contingencia, todo aspecto relacionado a una falla de hardware no forma parte de esta metodología[31].

- Cualquier punto que ya esté siendo tratado dentro del plan de sistemas no forma parte de esta metodología. Salvo la expresa solicitud del Gerente de Tecnología.

[31] SALVO QUE LA FALLA SE PRODUZCA TRAS UN CORTE ABRUPTO O ACTIVIDAD DE RECUPERACIÓN.

Anexo E: Tabla de conceptos de continuidad

Tabla 28: Conceptos de continuidad.

Concepto de continuidad	Grupo	Documento
Acceso a clientes	Servicios tecnológicos	Capítulo 1-7 CMF Política gestión de la producción
Acceso a CPD en contingencia	Accesos y permisos	Capítulo 20-7 CMF Política Ciberseguridad A3
Acceso a máquinas	Accesos y permisos	Capítulo 1-7 /Capítulo 20-7 CMF Política Ciberseguridad A3 Política Plan Contingencia Tecnológica
Actas de contingencia	Gobierno y coordinación	Capítulo 20-8 CMF Política gestión de la producción
Activación de colaboradores y soportes	Notificación y activación	Capítulo 20-9 CMF Política gestión de la producción Política Plan Contingencia Tecnológica
Alertas y configuración de monitoreo	Detección y escalamiento	Capítulo 1-7 /Capítulo 20-8 CMF Política gestión de la producción Política Plan Contingencia Tecnológica
Análisis técnico	Servicios tecnológicos Canales y comunicación	Política gestión de la producción Política Plan Contingencia Tecnológica
Arquitectura de redes	Canales y comunicación	Capítulo 1-7 / Capítulo 20-9 CMF Política Ciberseguridad A3 Política Plan Contingencia Tecnológica
Arquitectura de sistemas	Servicios tecnológicos	Capítulo 1-13 CMF (Ciber)A3 Capítulo 20-9 CMF Política gestión de la producción Política Plan Contingencia Tecnológica
Arquitectura VPN	Canales y comunicación	Capítulo 1-7 CMF Política Ciberseguridad A3

Concepto de continuidad	Grupo	Documento
Auditorías internas y externas	Gobierno y coordinación	Capítulo 1-7 / Capítulo 1-13 CMF Capítulo 1-15 / Capítulo 19-2 CMF Capítulo 20-7 / Capítulo 20-9 CMF Política gestión de la producción
Automatización	Servicios tecnológicos	Capítulo 20-9 CMF
Bastionado y parchados (vulnerabilidades)	Servicios tecnológicos	Capítulo 20-8 CMF
Cadena lógica de recuperación de sistemas (procesos, tareas y protocolos para distintas plataformas)	Servicios tecnológicos / Canales y comunicación	Capítulo 20-9 CMF Política gestión de la producción Política Plan Contingencia Tecnológica
Campañas a clientes	Respaldo de Datos	Capítulo 20-9 CMF
Cantidad de años de custodia y eliminación	Respaldo de Datos	Capítulo 1-10 CMF Política Plan Contingencia Tecnológica
Capacitación continuidad de negocio	Gobierno y coordinación	Capítulo 1-13 / Capítulo 20-9 CMF Política gestión de la producción Política Plan Contingencia Tecnológica
Certificación de CPD	Servicios tecnológicos	Capítulo 20-9 CMF Política gestión de la producción Política Plan Contingencia Tecnológica
Cloud computing	Servicios tecnológicos	Capítulo 20-7 CMF Política Ciberseguridad D6 Política Plan Contingencia Tecnológica
Cluster, granjas, repetidores y distribuidores de carga	Servicios tecnológicos / Canales y comunicación	Capítulo 1-7 CMF Capítulo 20-9 CMF Política Ciberseguridad A3
Condiciones y cambio de condiciones de negocio	Respaldo de Datos	Capítulo 1-7 CMF Capítulo 20-9 CMF
Configuración de aplicaciones, versión, licencias y certificados	Servicios tecnológicos	Política Ciberseguridad A3
Configuración de firewall y switch	Canales y comunicación	Capítulo 1-7 CMF Capítulo 20-9 CMF Política Ciberseguridad A3

Concepto de continuidad	Grupo	Documento
Contratos, acuerdos y anexos de contrato	Respaldo de Datos	Capítulo 20-9 CMF
Datos personales de clientes	Respaldo de Datos	Capítulo 20-8 CMF Política Ciberseguridad D6
Definición de estrategia de recuperación	Gobierno y coordinación	Capítulo 1-13/Capítulo 20-8 CMF Capítulo 20-9 CMF Política gestión de la producción Política Plan Contingencia Tecnológica
Distribuciones y configuración de movimiento equipos virtuales	Servicios tecnológicos	Capítulo 20-9 CMF
Establecimiento de mesas de contingencia	Gobierno y coordinación	Capítulo 1-13 CMF Política gestión de la producción Política Plan Contingencia Tecnológica
Evaluación de escenarios y riesgos	Gobiernos y coordinación	Capítulo 1-13/ Capítulo 20-7 CMF Capítulo 20-9 CMF Política gestión de la producción Política Ciberseguridad A3 Política Plan Contingencia Tecnológica
Existencia, uso y disponibilidad de PCT	Gobierno y coordinación	Capítulo 20-9 CMF Política gestión de la producción Política Ciberseguridad A3
Fechas y montos transaccionales	Respaldo de Datos	Capítulo 1-7 CMF Política Ciberseguridad D6
Front end para clientes y usuarios	Canales y comunicación	Capítulo 1-7 /Capítulo 20-9 CMF
Funciones y roles de mesas de contingencia	Gobierno y coordinación	Capítulo 1-13 /Capítulo 20-9 CMF Política gestión de la producción Política Plan Contingencia Tecnológica
Gestión de incidencias	Detección y escalamiento	Capítulo 1-13/Capítulo 20-7 CMF Capítulo 20-8 CMF Política gestión de la producción
Grupos de acceso en contingencia	Accesos y permisos	Política Ciberseguridad A3

Concepto de continuidad	Grupo	Documento
Grupos de acceso y atributos	Accesos y permisos	Política Ciberseguridad A3
Informes y reportes	Gobierno y coordinación	Capítulo 20-8 /Capítulo 20-9 CMF Política gestión de la producción
Medios de respaldo y recuperación	Respaldo de Datos Respaldo de Configuraciones	Capítulo 20-9 CMF Política gestión de la producción Política Plan Contingencia Tecnológica
Notificación a clientes	Notificación y activación	Capítulo 20-8 /Capítulo 20-9 CMF
Notificación a CMF	Notificación y activación	Capítulo 20-8 /Capítulo 20-9 CMF
Notificación a la organización	Notificación y activación	Capítulo 20-9 CMF Política gestión de la producción Política Plan Contingencia Tecnológica
Notificaciones a monitoreo	Detección y escalamiento	Capítulo 20-9 CMF Política gestión de la producción Política Plan Contingencia Tecnológica
Número de copias de configuración	Respaldo de Configuraciones	Política gestión de la producción Política Plan Contingencia Tecnológica
Políticas de acceso a máquinas	Servicios tecnológicos	
Políticas de negocio para los respaldos	Respaldo de Datos	Política Ciberseguridad D6 Política Plan Contingencia Tecnológica
Políticas de VPN	Canales y comunicación	
Políticas técnicas para los respaldos	Respaldo de Datos Respaldo de Configuraciones	Política gestión de la producción Política Ciberseguridad A3 Política Ciberseguridad D6 Política Plan Contingencia Tecnológica
Procedimientos de respaldo y calendario de respaldos	Respaldo de Datos Respaldo de Configuraciones	Capítulo 1-7 CMF Capítulo 20-9 CMF Política gestión de la producción Política Ciberseguridad A3 Política Plan Contingencia Tecnológica
Promociones a clientes	Respaldo de Datos	Capítulo 1-10 CMF

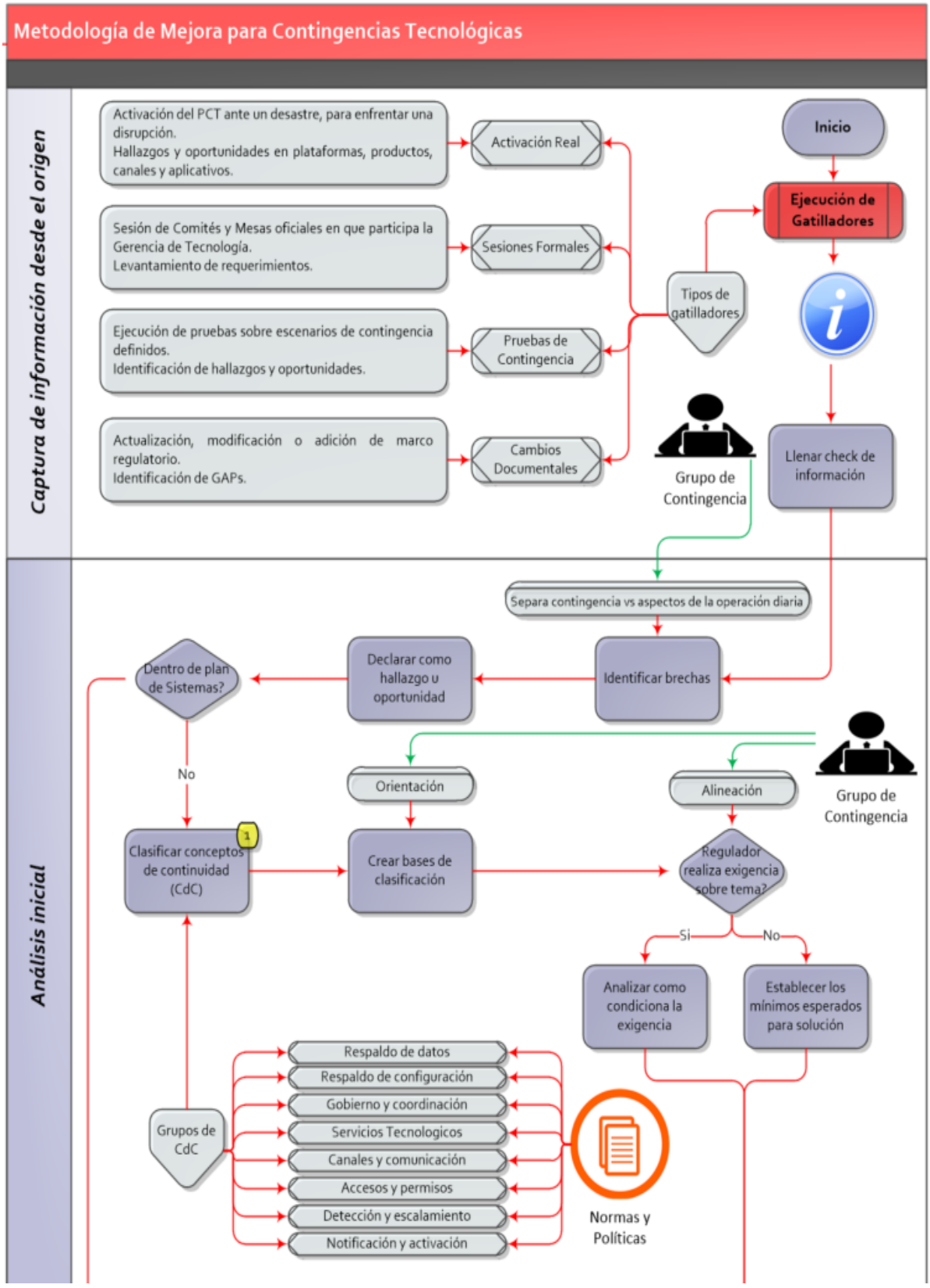
Concepto de continuidad	Grupo	Documento
Proveedores de servicios críticos	Gobierno y coordinación	Capítulo 20-7 CMF Política Ciberseguridad D6 Política Plan Contingencia Tecnológica
Pruebas de contingencia y ejercicios	Gobierno y coordinación	Capítulo 1-13 /Capítulo 20-7 CMF Capítulo 20-9 CMF Política gestión de la producción Política Plan Contingencia Tecnológica
Puerta trasera y condiciones de uso en contingencia	Accesos y permisos	Capítulo 1-7 CMF
Puertos abiertos y conexiones	Respaldo de Configuraciones	Capítulo 20-9 CMF
Recuperación aplicativa	Servicios tecnológicos Canales y comunicación	Capítulo 20-9 CMF Política Ciberseguridad D6 Política Plan Contingencia Tecnológica
Recuperación con versiones obsoletas/ decomisadas	Respaldo de Datos Respaldo de Configuraciones	Capítulo 20-9 CMF
Recuperación de batch y reinicio de mallas	Servicios tecnológicos	Capítulo 20-9 CMF
Recuperación de centrales telefónicas	Canales y comunicación	Capítulo 20-9 CMF
Recuperación de sistemas de servicio (ex. VMware, ciberark, etc.)	Accesos y permisos	Capítulo 20-9 CMF Política Ciberseguridad A3 Política Plan Contingencia Tecnológica
Recursos de CPD (energía, refrigeración y mantenimiento)	Servicios tecnológicos	Capítulo 20-9 CMF Política Plan Contingencia Tecnológica
Redes externas	Canales y comunicación	Capítulo 1-7 / Capítulo 20-7 (end to end) /Capítulo 20-9 CMF
Redes internacionales	Canales y comunicación	Capítulo 1-7 /Capítulo 20-7 CMF (end to end) /Capítulo 20-9 CMF
Redes internas (sucursales y edificios centrales)	Canales y comunicación	Capítulo 1-7/ Capítulo 20-9 CMF Política Ciberseguridad A3
Reporte a comités de crisis	Gobierno y coordinación	Capítulo 20-8 CMF

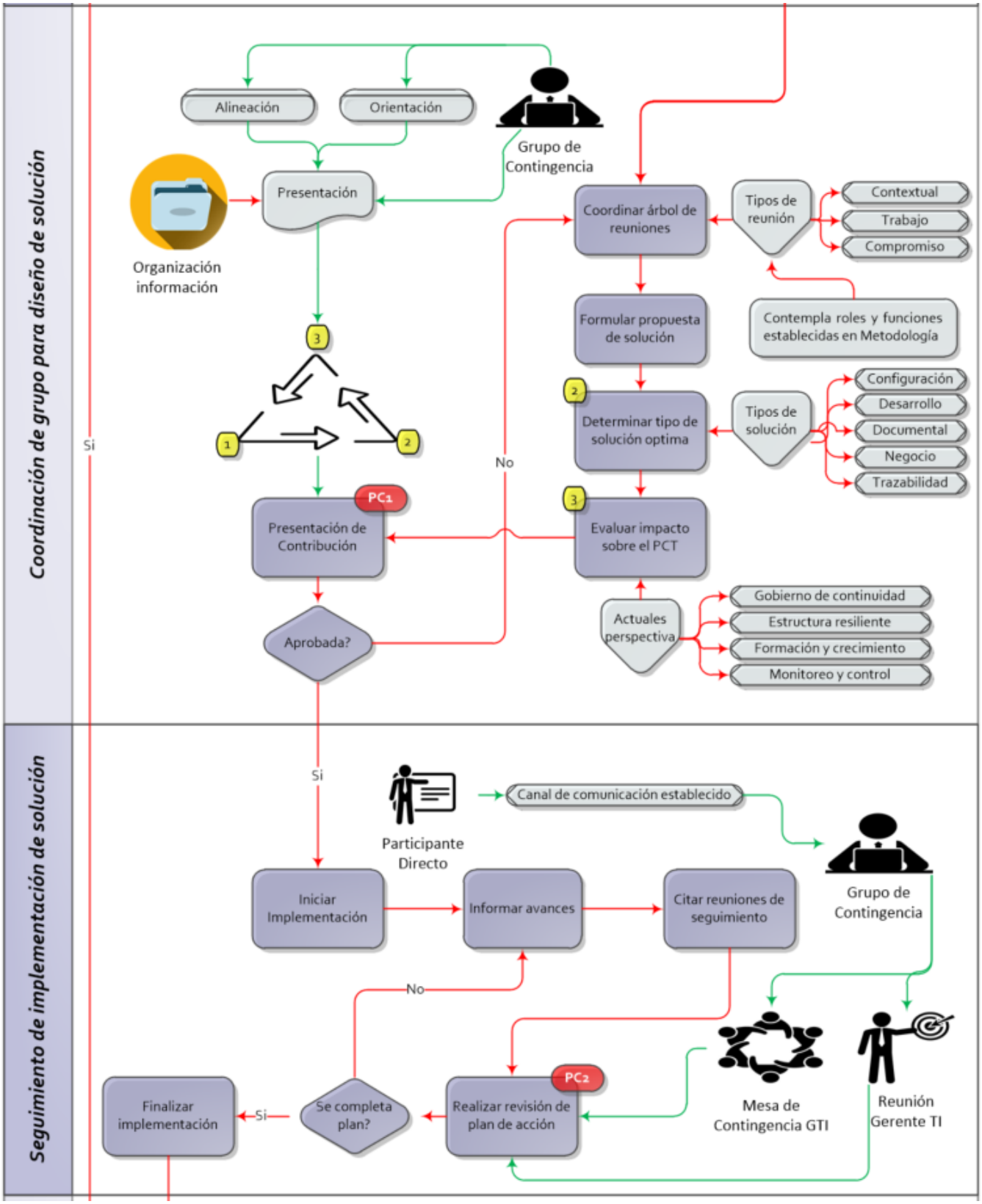
Concepto de continuidad	Grupo	Documento
		Política gestión de la producción Política Plan Contingencia Tecnológica
Repuestos, bodega y cambio de hardware	Accesos y permisos	
Reuniones y estrategia de normalización	Gobierno y coordinación	Capítulo 1-13 / Capítulo 20-9 CMF Política gestión de la producción
RTO & RPO – además de planes de detección y corrección para cumplimiento de niveles esperados	Servicios tecnológicos	Capítulo 1-7 / Capítulo 20-9 CMF Política gestión de la producción Política Ciberseguridad A3 Política Plan Contingencia Tecnológica
Segmentación y aislamiento de redes	Canales y comunicación	Capítulo 1-7 CMF Política Ciberseguridad A3 Política Plan Contingencia Tecnológica
Segunda copia y almacenamiento en CPD	Servicios tecnológicos	Capítulo 20-9 CMF Política Plan Contingencia Tecnológica
Sistema de respaldos	Respaldo de Datos Respaldo de Configuraciones	Capítulo 20-9 CMF Política gestión de la producción Política Ciberseguridad A3 Política Plan Contingencia Tecnológica
Sistema operativo y software base	Respaldo de Configuraciones	Capítulo 20-9 CMF Política gestión de la producción Política Ciberseguridad D6 Política Plan Contingencia Tecnológica
Sistemas de almacenamiento	Servicios tecnológicos	Capítulo 20-9 CMF Política Plan Contingencia Tecnológica
Tamaño de disco y particiones	Respaldo de Configuraciones	Capítulo 20-9 CMF Política gestión de la producción
Tipo de contingencia de sistemas (alta disponibilidad)	Servicios tecnológicos	Capítulo 1-7 CMF (Downtime) Capítulo 20-9 CMF Política Plan Contingencia Tecnológica

Concepto de continuidad	Grupo	Documento
Trazabilidad aplicativo crítico servidor	Gobierno y coordinación	Política gestión de la producción Política Plan Contingencia Tecnológica
Umbrales y ventanas para alertas	Detección y escalamiento	Capítulo 20-7 / Capítulo 20-9 CMF Política gestión de la producción

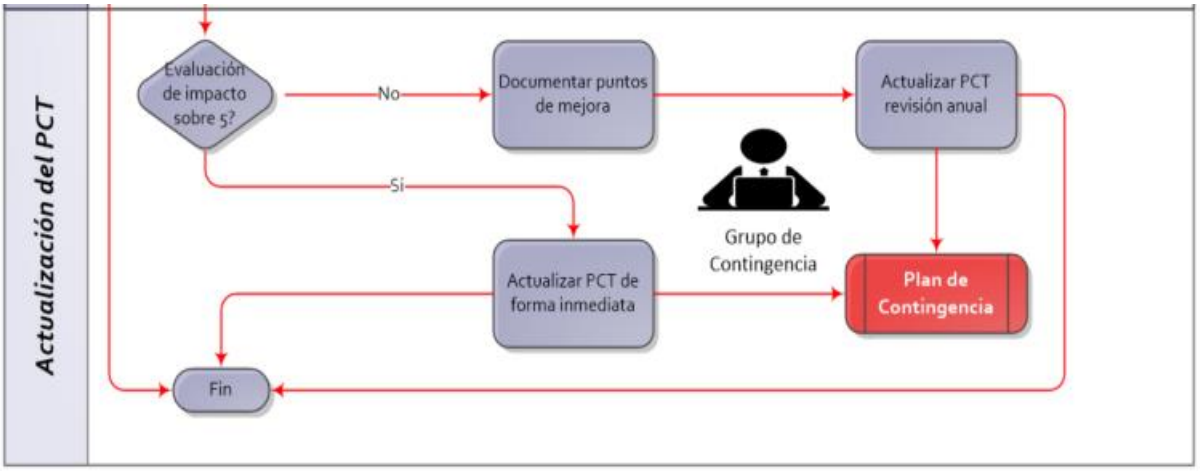
Anexo F: Flujo final de la MMCT

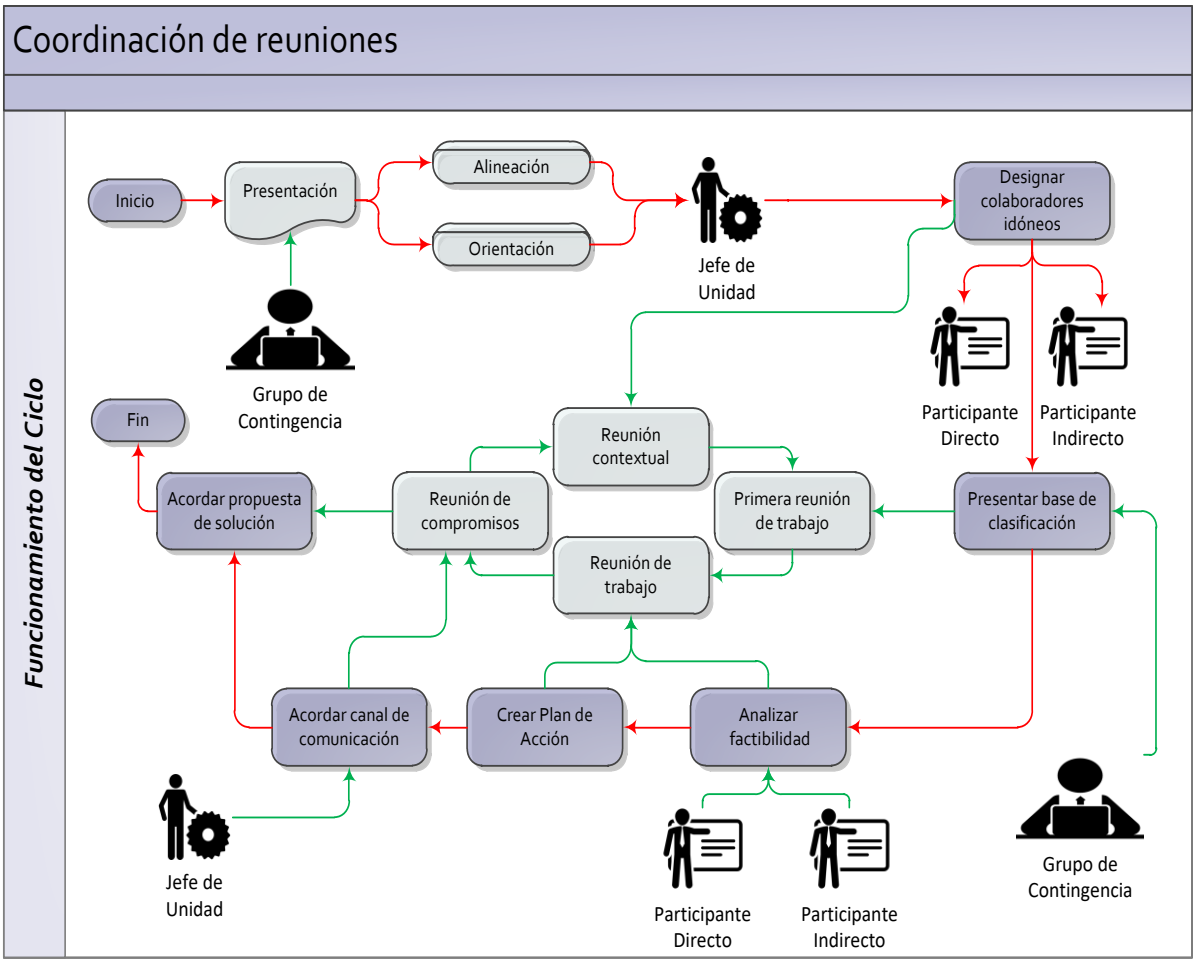
El flujo contempla las cinco fases de la MMCT, además de una profundización sobre las acciones de coordinación de reuniones.


Metodología de Mejora para Contingencias Tecnológicas
Captura de información desde el origen
Activación del PCT ante un desastre, para enfrentar una disrupción.
Hallazgos y oportunidades en plataformas, productos, canales y aplicativos.
Activación Real
Sesión de Comités y Mesas oficiales en que participa la Gerencia de Tecnología.
Levantamiento de requerimientos.
Sesiones Formales
Ejecución de pruebas sobre escenarios de contingencia definidos.
Identificación de hallazgos y oportunidades.
Pruebas de Contingencia
Actualización, modificación o adición de marco regulatorio.
Identificación de GAPs.
Cambios Documentales
Tipos de gatilladores
Inicio
Ejecución de Gatilladores
Grupo de Contingencia
Llenar check de información
Análisis inicial
Separa contingencia vs aspectos de la operación diaria
Identificar brechas
Declarar como hallazgo u oportunidad
Dentro de plan de Sistemas?
No
Clasificar conceptos de continuidad (CdC)
Orientación
Crear bases de clasificación
Alineación
Grupo de Contingencia
Regulador realiza exigencia sobre tema?
Si
No
Analizar como condiciona la exigencia
Establecer los mínimos esperados para solución
Grupos de CdC
Respaldo de datos
Respaldo de configuración
Gobierno y coordinación
Servicios Tecnologicos
Canales y comunicación
Accesos y permisos
Detección y escalamiento
Notificación y activación
Normas y Políticas


Coordinación de grupo para diseño de solución
Alineación
Orientación
Grupo de Contingencia
Presentación
Organización información
Coordinar árbol de reuniones
Tipos de reunión
Contextual
Trabajo
Compromiso
Formular propuesta de solución
Contempla roles y funciones establecidas en Metodología
Determinar tipo de solución optima
Tipos de solución
Configuración
Desarrollo
Documental
Negocio
Trazabilidad
Evaluar impacto sobre el PCT
Actuales perspectiva
Gobierno de continuidad
Estructura resiliente
Formación y crecimiento
Monitoreo y control
PC1
Presentación de Contribución
Aprobada?
Si
No
Seguimiento de implementación de solución
Participante Directo
Canal de comunicación establecido
Grupo de Contingencia
Iniciar Implementación
Informar avances
Citar reuniones de seguimiento
Mesa de Contingencia GTI
Reunión Gerente TI
PC2
Realizar revisión de plan de acción
Se completa plan?
Finalizar implementación

}


Actualización del PCT
Evaluación de impacto sobre 5?
No
Si
Documentar puntos de mejora
Actualizar PCT revisión anual
Grupo de Contingencia
Actualizar PCT de forma inmediata
Plan de Contingencia
Fin


Coordinación de reuniones
Funcionamiento del Ciclo
Inicio
Presentación
Alineación
Orientación
Jefe de Unidad
Designar colaboradores idóneos
Grupo de Contingencia
Participante Directo
Participante Indirecto
Fin
Reunión contextual
Acordar propuesta de solución
Reunión de compromisos
Primera reunión de trabajo
Presentar base de clasificación
Reunión de trabajo
Acordar canal de comunicación
Crear Plan de Acción
Analizar factibilidad
Jefe de Unidad
Participante Directo
Participante Indirecto
Grupo de Contingencia

Anexo G: Perspectivas de contribución al PCT

Las perspectivas vigentes son:

Gobierno de contingencia: Relacionado a todos los aspectos de administración y control en el momento de existir una contingencia real, incluyendo los protocolos de comunicación, las funciones y roles en contingencia.

Estructura resiliente: Relacionado a todos los aspectos técnicos antes y durante una contingencia, para una recuperación rápida y la disminución de los impactos al enfrentar un desastre externo o interno.

Formación y crecimiento: Relacionado a todos los aspectos formativos previos a una contingencia, que contribuyen a que los colaboradores y soportes cuenten con una cultura de continuidad del negocio y su rol en la recuperación.

Monitoreo y control: Relacionado a la detección anticipada de anomalías dentro del comportamiento de la infraestructura tecnológica, los procesos y servicios entregados por GTI al resto de la organización.

La forma de cálculo esta detallado en el anexo F, en la sección correspondiente a las perspectivas.

Anexo H: Documento final MMCT

https://drive.google.com/file/d/1XSFMD1rp0-8_UssQpMWSW8d_UWhoLTEy/view?usp=drivesdk

Anexo I: Detalle de reuniones desarrolladas en ejecución de MMCT

Reunión Inicial: La información recopilada en esta reunión sirvió para concluir que:

- Frente a la métrica no existía cobertura. Los servidores que participaban en el calendario de recuperación eran seleccionados bajo un solo criterio "Cumplimiento de Auditoria", recuperando un total de 15 servidores mensualmente. El listado de servidores no tenía variación y era muy acotado, además el porcentaje de aplicativos críticos que cubría el calendario completo era de un 53%.

- No existía separación de funciones. El calendario de recuperación era hecho por los soportes encargados de realizar posteriormente la recuperación y aprobado por el gestor del servicio banco. El calendario no reflejaba las actuales necesidades de la gerencia.

- No existía control del proceso. El proceso de revisión de evidencias de recuperación, consistía en el envío de los archivos por parte de los soportes y la revisión por parte de auditoria (sólo si el servidor era seleccionado como parte de una auditoria).

- El nombre de los archivos inducia a error. Los archivos eran nombrados con el nombre del servidor seguido de "100%" y en ocasiones la palabra "Justificado", vale decir, si el servidor se llamaba PEPE su archivo se podía llamar PEPE100% o PEPEJUSTIFICADO100%.

Al ser revisada una muestra de dichos archivos se observó:

a. Archivos que en su interior indicaban que la fecha solicitada no existía para ese servidor, se nombraban como Justificado.

b. Archivos que indicaban que el servidor no formaba parte del catálogo, se nombraban como Justificado.

c. Archivos correctamente evidenciados mostrando evidencia sobre la consulta en catálogo, evidencia del proceso de recuperación del respaldo y evidencia sobre los componentes recuperados que podían ser datos o componentes de configuración.

Reuniones de trabajo sobre el calendario: Con el objetivo de mejorar el calendario y que fuera acorde al requerimiento, se estableció:

- El calendario sería entregado por banco a soporte.

- Se crearía un procedimiento para la conformación del calendario.

- La creación del calendario se realizaría por las unidades de:

  - Continuidad de Servicio TI, incluyendo los servidores de aplicativos críticos.

  - Gobierno TI, incluyendo los servidores exigidos por auditorias.

  - Operaciones de Producción, incluyendo los servidores de interés por incidencias.

  - Técnica de Sistemas, revisando la coherencia del listado y eliminando duplicidad por Rac o Cluster.

- Se aumentaría la cantidad de servidores a recuperar en al menos un 100%.

Reuniones de trabajo sobre requerimiento: Se estableció en estas reuniones:

- Seguimiento mensual sobre el calendario de recuperación entre Técnica de Sistemas, el grupo de contingencia y representante de soportes. Se materializaría en reuniones mensuales con soportes para revisión del calendario y resultados de la métrica.

- Entrega de los archivos de evidencia de forma mensual.

- Alojamiento de los archivos de evidencia en un canal vía Teams con acceso a los cuatro grupos del banco que participan en la conformación del calendario.

- Revisión de primera entrega. Los controles serán realizados por parte del grupo de contingencia y el gestor del servicio, posteriormente esta labor seria realizada sólo por el gestor de servicio.

- El cálculo de la métrica y la entrega de los resultados serán parte de Continuidad de Servicios TI.

- Control de cobertura. Cualquier servidor dentro del parque productivo podría integrar el calendario, en caso de no existir dentro del catálogo, se realizaría inclusión al sistema de respaldos y se consideraría como recuperación fallida para la métrica.

- Control de lagunas de respaldo. Se establece dentro del calendario fechas aleatorias de recuperación que se encuentran dentro de los últimos seis años. Los operadores procederán de la siguiente forma:

- Si servidor fue subido al sistema de respaldos en una fecha posterior, debía indicar la primera fecha de respaldo y recuperar dicha fecha.

- Si servidor no cuenta con respaldo en fecha solicitada, pero tiene fechas anteriores de recuperación, debe traer la fecha más cercana e indicar la cantidad de meses de la laguna.