



III Seminario Latinoamericano sobre Gestión de Tesorerías Públicas

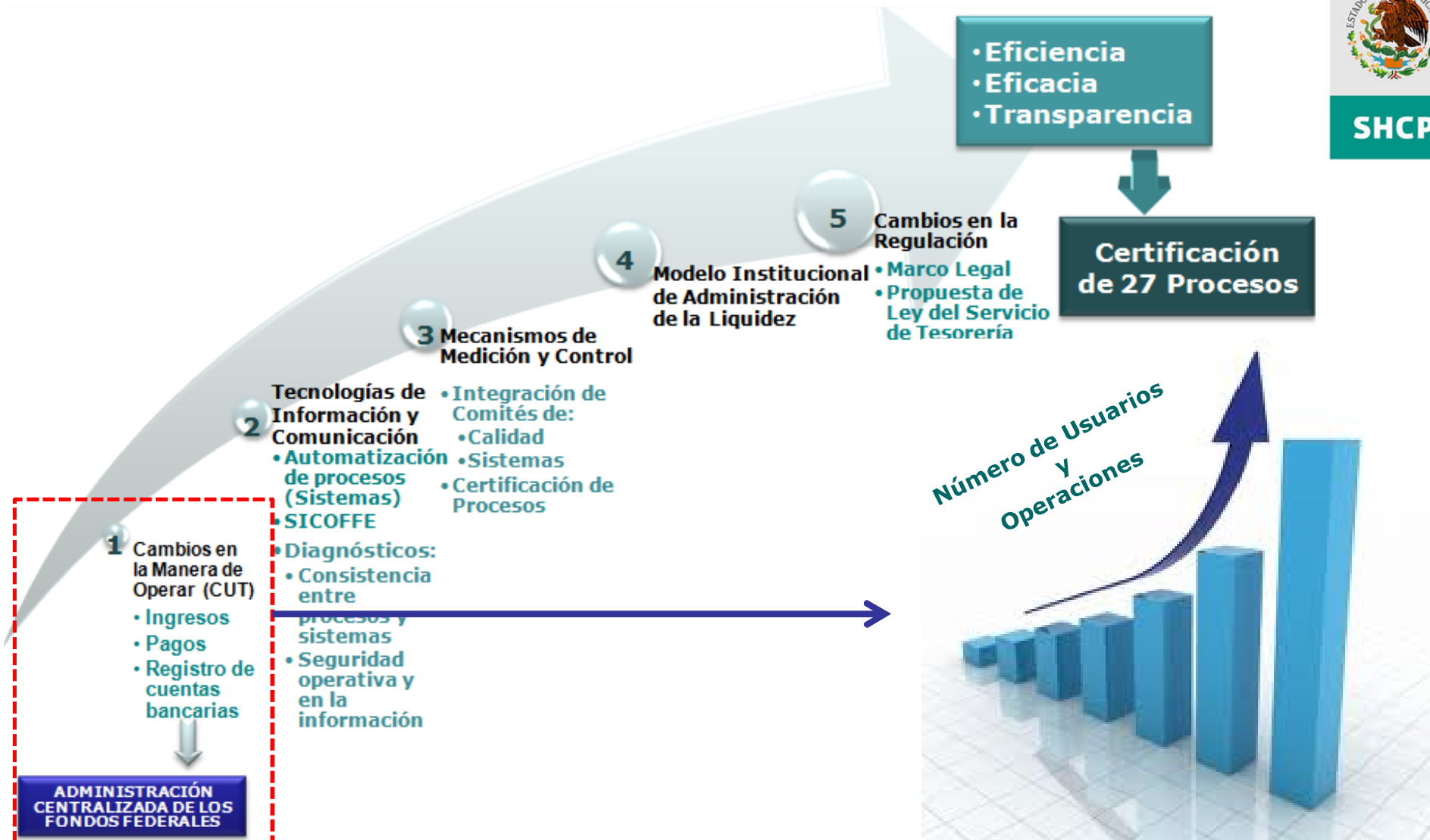
Matriz de Riesgos de Tesorería y Plan de Continuidad

23 de Agosto 2012

Proyecto de Modernización



SHCP



Proyecto de Modernización



**Asegurar y Garantizar
la Continuidad
Operativa**

Situación al cierre del 2007



SHCP

No se contaba con un Plan de Continuidad de la Tesorería.

Se contaba con procesos documentados y la identificación de los sistemas que los soportaban; sin embargo, no se tenía identificada la asociación de los controles con los riesgos.

Ante un evento que no permitiera realizar las operaciones, se llevaban a cabo acciones de forma reactiva.

Se desconocía el universo de riesgos a los que estaba expuesta la Tesorería.

No existía una coordinación entre las áreas externas clave de la Tesorería, como la de Tecnologías de la Información y el Banco Central.

Acciones realizadas por la Tesorería (2008-2009)



SHCP

Se identificó que los eventos recurrentes que afectaban la continuidad de las operaciones se debían a fallas en los sistemas y a situaciones que no permitían el acceso al lugar de trabajo, por lo que la Tesorería llevó a cabo las siguientes acciones:



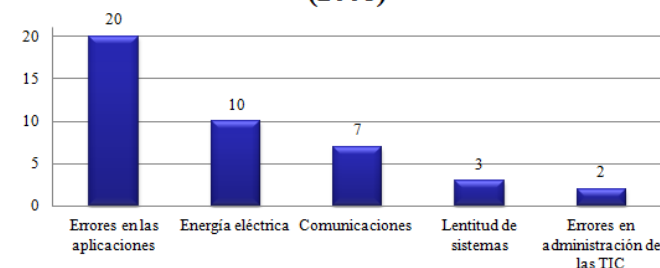
Bitácora de fallas por sistemas y sus causas.



Identificación de las causas de las fallas recurrentes en los sistemas (errores en las aplicaciones, energía eléctrica, comunicaciones, etc.).

Acciones preventivas para atender las fallas identificadas (Plan de mejora y actualización de sistemas, planta eléctrica de emergencia, centro de cómputo con equipos redundantes, etc.).

Causas de las fallas en los sistemas (2008)



Acciones realizadas por la Tesorería (2008-2009)



SHCP

Se identificó que los eventos recurrentes que afectaban la continuidad de las operaciones se debían a fallas en los sistemas y a situaciones que no permitían el acceso al lugar de trabajo, por lo que la Tesorería llevó a cabo las siguientes acciones:



Análisis de acciones que permitieran operar en caso de no tener acceso al lugar de trabajo.



Creación de un sitio alternativo de trabajo que consideró los lugares para el personal crítico y computadoras con los sistemas requeridos.



Acciones realizadas por la Tesorería (2008-2009)



SHCP

Se identificó que los eventos recurrentes que afectaban la continuidad de las operaciones se debían a fallas en los sistemas y a situaciones que no permitían el acceso al lugar de trabajo, por lo que la Tesorería llevó a cabo las siguientes acciones:



Diagnóstico
interno a los
sistemas



- **Identificación de los riesgos tecnológicos** (sistemas desarticulados y obsoletos, ejecución de procesos manuales, vulnerabilidades en la integridad de la información, etc.)
- **Acciones preventivas para mitigar los riesgos identificados** (Planeación del portafolio de proyectos tecnológicos para automatizar procesos manuales y actualizar los sistemas obsoletos, robustecimiento de controles de seguridad, etc).

Acciones realizadas por la Tesorería (2008-2009)



Diagnóstico
interno a los
sistemas



Bitácora de
Fallas de los
sistemas



**Matriz de riesgos tecnológicos
que pueden afectar a la
operación**

La Tesorería:

- Requería conocer TODOS los riesgos a los que estaba expuesta, no sólo los tecnológicos.
- Formalizar las acciones realizadas con la finalidad de garantizar la continuidad operativa, por lo que se consideró que un Plan de Continuidad Operativa era la herramienta idónea.

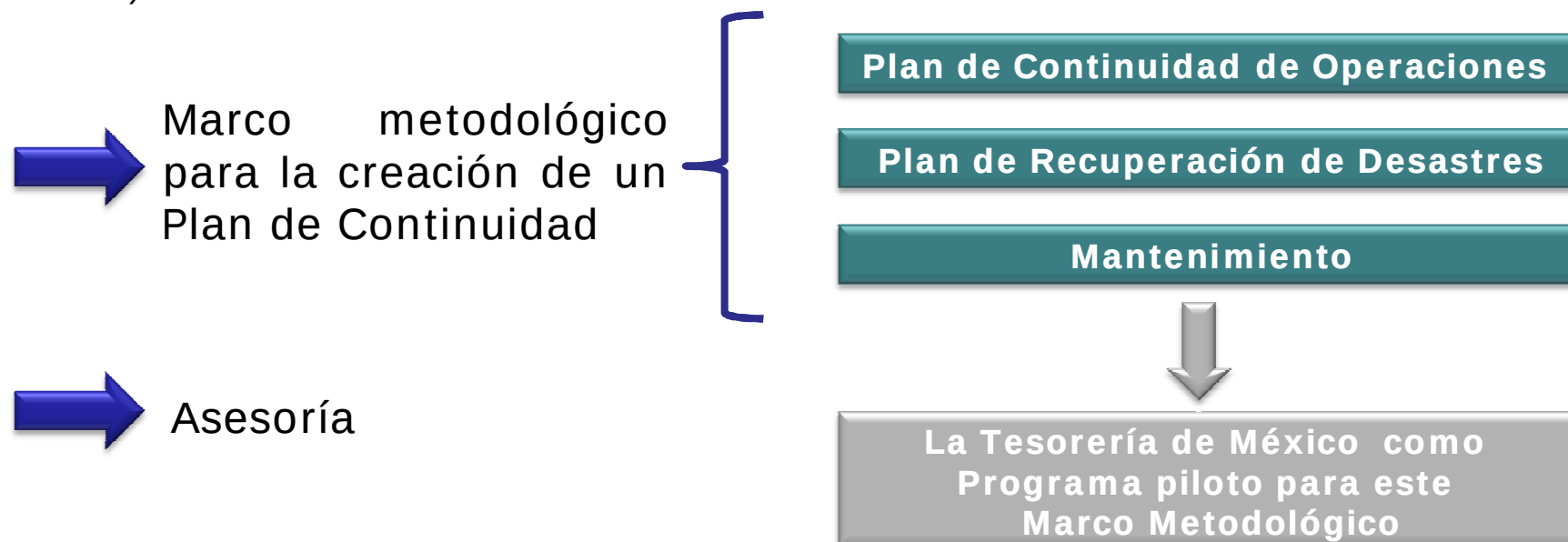


La Tesorería no contaba con un área o con personal especializado en la detección y gestión de riesgos.

Asesoría Técnica (Marco metodológico y Asesoría)



Asistencia técnica por expertos en el tema de continuidad operativa y gestión de riesgos. (Fondo Monetario Internacional -Ian Storkey / Mark Silins-).



Asesoría Técnica (Marco metodológico y Asesoría)

Asesoría y análisis de la situación de la Tesorería con base en el Marco Metodológico



SHCP

Plan de Continuidad de Operaciones

Riesgos Operacionales

Objetivo y Política

Evaluación de Riesgos
y Análisis del Impacto a
las Operaciones

Estrategias de TESOFE
de Mitigación de
Riesgos

Plan de Recuperación de Desastres

Estructura de Manejo
de Incidentes

Centro de Comando

Proceso de
Recuperación

Infraestructura de
recuperación

Conexión con terceros

Capacitación y pruebas

Lista de verificación

Mantenimiento

Actividades para que
forme parte de las
operaciones diarias

Calendario de pruebas

Responsables

Asesoría Técnica (Marco metodológico y Asesoría)

Asesoría y análisis de la situación de la Tesorería con base en el Marco Metodológico



SHCP



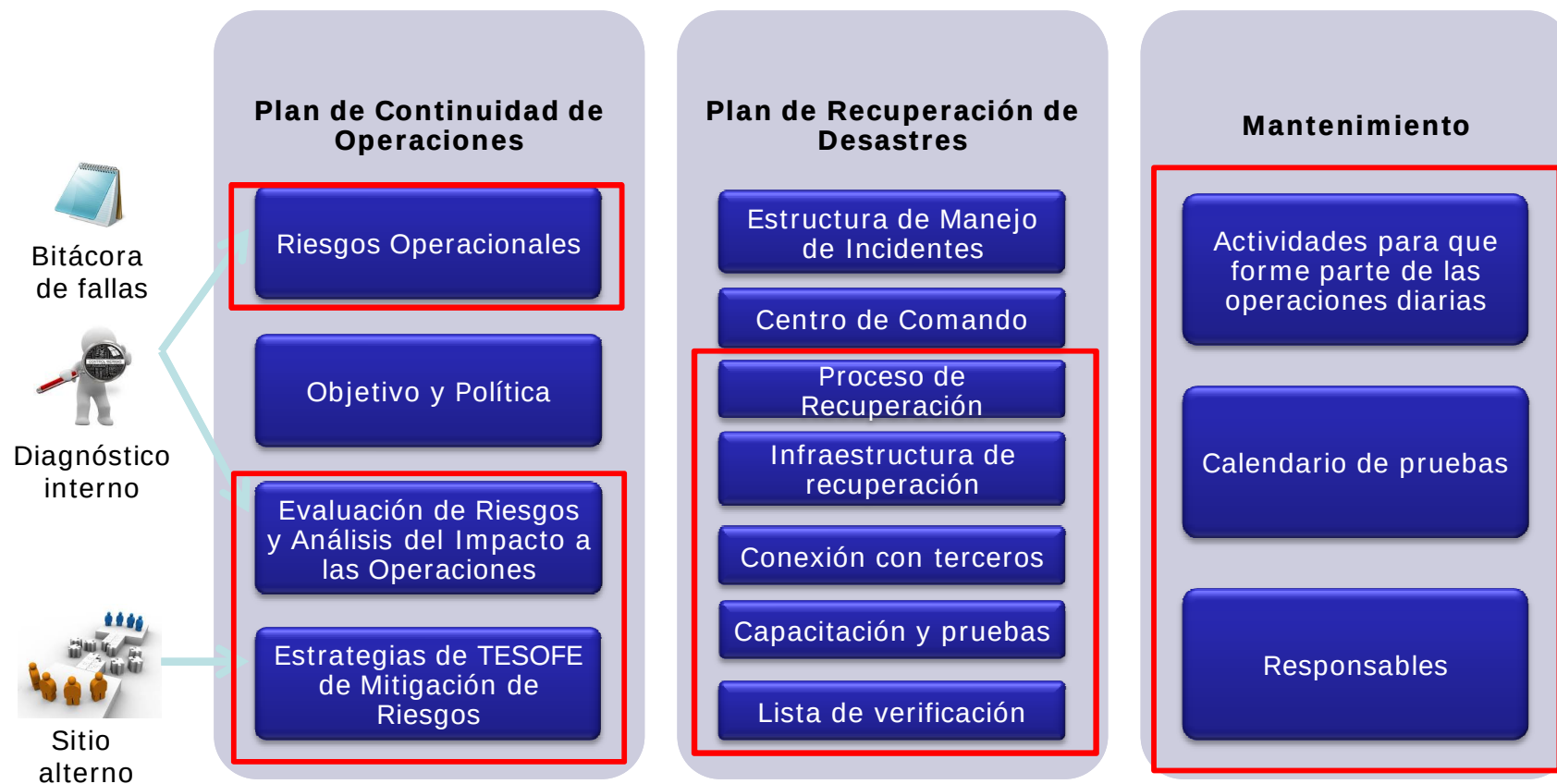
Las acciones realizadas por la Tesorería sirvieron de insumo para el Plan de Continuidad

Asesoría Técnica (Marco metodológico y Asesoría)

Asesoría y análisis de la situación de la Tesorería con base en el Marco Metodológico



SHCP

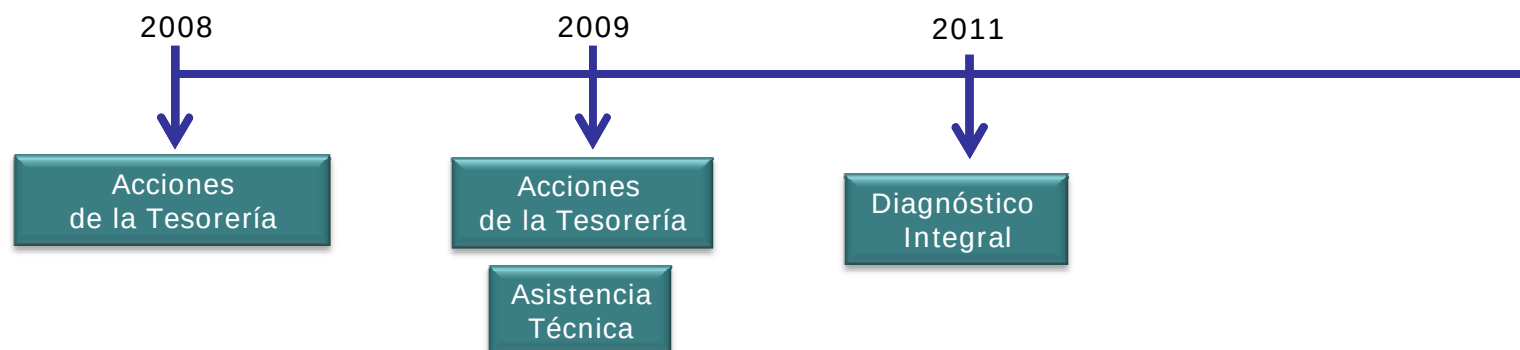


Sin embargo, se requerían realizar acciones adicionales para la identificación, definición, evaluación y análisis en los siguientes rubros.

Diagnóstico Integral



SHCP



Diagnóstico integral, por una empresa consultora especializada, de los procesos, los sistemas, la capacidad de la infraestructura tecnológica para soportar las operaciones y la seguridad de la información. (Banco Mundial)

Diagnóstico Integral



SHCP



Identificación, evaluación y análisis:

- **Escenarios de riesgo**
- **Impacto a los procesos y a los sistemas** por cada riesgo identificado
- **Nivel de vulnerabilidad** basado en la probabilidad de ocurrencia y en el impacto de cada proceso



Definición de:

- **Requerimientos mínimos de operación** por cada proceso (Personal, cantidad de hojas de papel, computadoras, impresoras, sistemas, etc.)
- **Estrategias de continuidad**
- **Matrices de escalación**
- **Plan de respuesta a emergencias** (Prevención, respuesta, regreso al estado normal)
- **Programa de pruebas**

Diagnóstico Integral

Resultados y Plan de Trabajo



La Tesorería, a través del diagnóstico, pudo certificar que:

- El nivel de riesgo operativo es bajo.
- Los riesgos detectados están controlados.

Con la finalidad de robustecer el esquema de seguridad y continuidad operativa y bajo una cultura de mejora continua sobre sus procesos; con base en el Diagnóstico, se elaboró un Plan de Trabajo que consideró, entre otras líneas de acción, las siguientes:

- Conformar un **Comité de Continuidad Operativa** de la TESOFE.
- Contar con un **Modelo de Análisis de Riesgos** y terminar las acciones necesarias para formalizar el **Plan de Continuidad**.
- Elaborar **políticas internas para la seguridad de la información**.

Diagnóstico Integral y su relación con el Marco Metodológico



SHCP



Definición de:

- **Requerimientos mínimos de operación** por cada proceso (Personal, cantidad de hojas de papel, computadoras, impresoras, sistemas, etc.)

• Estrategias de continuidad

- **Matrices de escalación**
- **Plan de respuesta a emergencias** (Prevención, respuesta, regreso)
- **Programa de pruebas**



Identificación, evaluación y análisis:

• Escenarios de riesgo

- **Impacto a los procesos y a los sistemas** por cada riesgo identificado

- **Nivel de vulnerabilidad** basado en la probabilidad de ocurrencia y en el impacto de cada proceso

Plan de Continuidad de Operaciones

Riesgos Operacionales

Objetivo y Política

Evaluación de Riesgos y Análisis del Impacto a las Operaciones

Estrategias de TESOFE de Mitigación de Riesgos

Diagnóstico Integral y su relación con el Marco Metodológico



SHCP



Plan de Recuperación de Desastres

Estructura de Manejo de
Incidentes

Centro de Comando

Proceso de Recuperación

Infraestructura de
recuperación

Conexión con terceros

Capacitación y pruebas

Lista de verificación



Identificación, evaluación y análisis:

- **Escenarios de riesgo**
- **Impacto a los procesos y a los sistemas** por cada riesgo identificado
- **Nivel de vulnerabilidad** basado en la probabilidad de ocurrencia y en el impacto de cada proceso

Definición de:

- **Requerimientos mínimos de operación** por cada proceso (Personal, cantidad de hojas de papel, computadoras, impresoras, sistemas, etc.)
- **Estrategias de continuidad**
- **Matrices de escalación**
- **Plan de respuesta a emergencias** (Prevención, respuesta, regreso)
- **Programa de pruebas**

Diagnóstico Integral y su relación con el Marco Metodológico



SHCP



Mantenimiento

Actividades para que
forme parte de las
operaciones diarias

Calendario de pruebas

Responsables



Identificación, evaluación y análisis:

- **Escenarios de riesgo**
- **Impacto a los procesos y a los sistemas** por cada riesgo identificado
- **Nivel de vulnerabilidad** basado en la probabilidad de ocurrencia y en el impacto de cada proceso

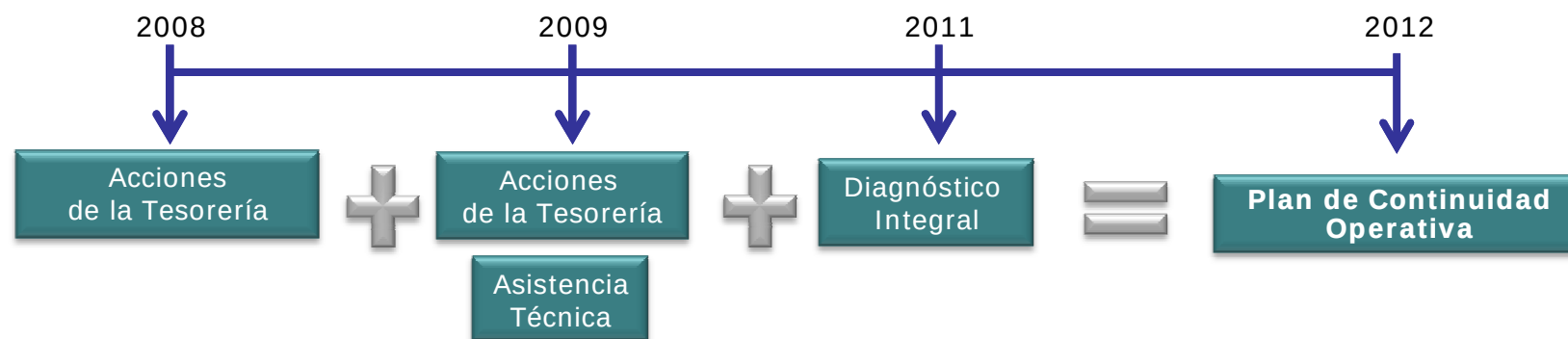
Definición de:

- **Requerimientos mínimos de operación** por cada proceso (Personal, cantidad de hojas de papel, computadoras, impresoras, sistemas, etc.)
- **Estrategias de continuidad**
- **Matrices de escalación**
- **Plan de respuesta a emergencias** (Prevención, respuesta, regreso)
- **Programa de pruebas**

Situación al 2012



SHCP

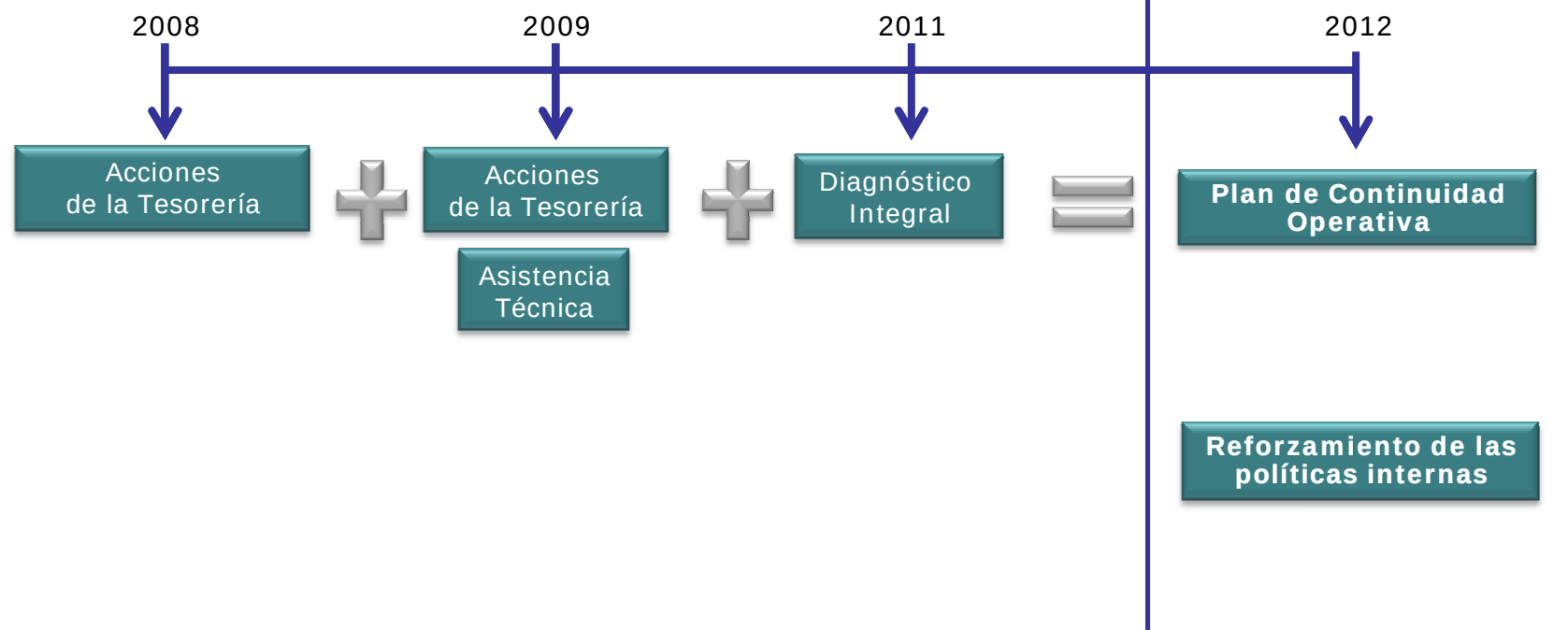


Situación al 2012

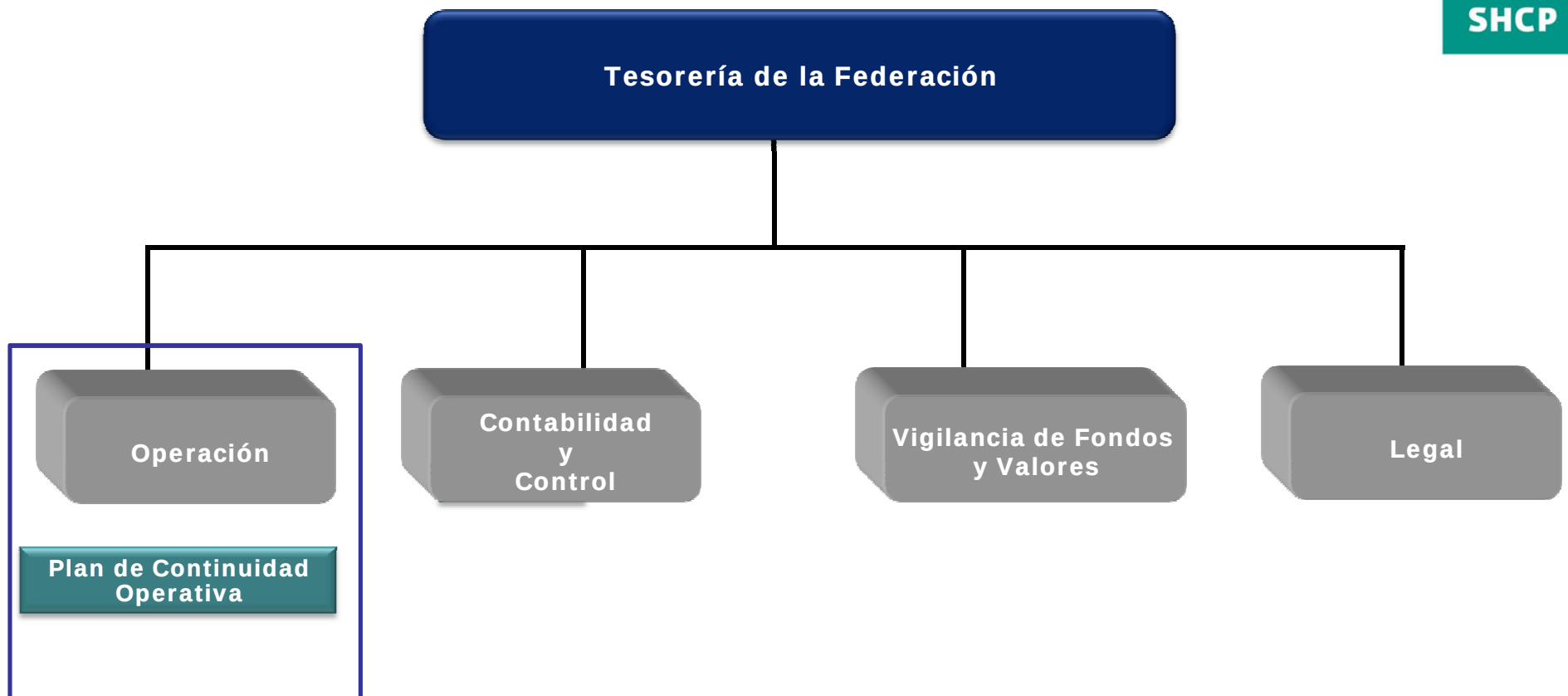
Marco de Continuidad Operativa Institucional



SHCP



Situación al 2012



Aplicación del Plan de Continuidad Operativa



SHCP

Manifestación en las instalaciones de la Tesorería

CRONOGRAMA

Operación Normal

Respuesta a Emergencias

Mantenimiento del PCO

Mantenimiento al Sitio Alterno (Disponibilidad y actualización de la información y de los sistemas)

Evaluación y toma de decisión (Centro de Comando)

- Evaluación (personal que pudo acceder al sitio, tiempo de la manifestación, operaciones pendientes, seguridad del personal)
- Toma de decisión (Activación del plan de contingencia para operar en el sitio alternativo)

Continuidad de Negocio

Activación Plan de Contingencia

- Activación de infraestructura (Acceso al personal, líneas telefónicas, sistemas de cómputo, etc.)
- Operación a Nivel Supervivencia (Realización de actividades críticas y suspensión temporal de las menos críticas en tiempo)
- Escalación (Aseguramiento del correcto funcionamiento)

Recuperación

Revisión de daños y regreso a la operación normal (Centro de Comando)

- Aseguramiento de la seguridad del personal y capacidad de retorno.
- Activación del plan de retorno

Mantenimiento

Tesorera de la Federación
Subtesorero de Operación
Titular de la Coordinación Administrativa
Coordinador de Tecnologías de Información y Comunicación

Siguientes Pasos



- Capacitación del personal en la sensibilización sobre riesgos operativos y fomento de una cultura de continuidad como una actividad del día a día.
- Conformación de la documentación que sirva como guía al personal.
- Contemplar aspectos menos críticos de procesos de negocio que pueden afectar su continuidad.
- Establecimiento de un plan de pruebas exhaustivo al plan de continuidad (plantillas, listas de verificación, responsables, calendario, simulacros).

Siguientes Pasos



- Celebrar un Acuerdo de Nivel de Servicio (SLA, por sus siglas en inglés) con todos los terceros involucrados en el Plan de Continuidad de Operaciones.
- Incluir en el alcance a las demás áreas de la Tesorería.



- Realización de las labores formalmente en el sitio alterno de manera periódica.
- Actualización continua del plan de continuidad.

Conclusiones



SHCP

- La gestión del riesgo, incluyendo el riesgo operativo, es crítica para la integridad de los procesos y sistemas de pago del gobierno y la recaudación de ingresos.
- Se ha incrementado la tendencia entre los tomadores de decisiones de crear comités para la gestión del riesgo , conjuntamente con planes para la continuidad del negocio y la recuperación de desastres.
- El dueño y responsable de un Plan de Continuidad es el negocio y no las áreas de Tecnologías de la Información.
- Un Plan de Continuidad no es un documento estático, requiere de una revisión y actualización continua que garantice la alineación con los cambios en el negocio.

Recomendaciones

- Capitalizar experiencias internacionales.
- Fomentar una cultura de continuidad operativa al interior de la institución.
- Tener documentados los procesos, incluyendo su alineación con los sistemas y todos los activos que requieren para operar (personal, infraestructura y demás insumos).
- Comenzar por un alcance acotado que sólo abarque a los procesos críticos; y, de manera gradual, incorporar a los demás procesos.
- Realizar la matriz de riesgos que incluya cualquier evento que pueda afectar a las operaciones de la Tesorería, desastres naturales, errores humanos, manifestaciones, fallas en los sistemas o en la energía eléctrica, entre otros.



SHCP