ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad en Ingeniería en Electricidad y Computación

Maestría en Seguridad Informática Aplicada

"ANÁLISIS Y DISEÑO DEL PLAN DE CONTINUIDAD DEL NEGOCIO DE UNA ENTIDAD BANCARIA"

EXAMEN DE GRADO (COMPLEXIVO)

Previa a la obtención del grado de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

VANIA MARLENE CENTURIÓN BERMEO

GUAYAQUIL-ECUADOR

AÑO: 2016

AGRADECIMIENTO

Agradezco a mi familia quien ha sido el pilar fundamental y motivación para la culminación de mi maestría.

A mi esposo, mi compañero de vida y apoyo a lo largo del desarrollo de este trabajo.

DEDICATORIA

El presente trabajo lo dedico a mis padres quienes desde pequeña me enseñaron lo importante de esforzarse para alcanzar las metas trazadas, y principalmente han sido el impulso que he necesitado para poder llegar a ser quien soy hoy en día.

TRIBUNAL DE SUSTENTACIÓN

_____

MGS. Lenin Freire

DIRECTOR MSIA

_____

MGS. Lenin Freire

PROFESOR DELEGADO POR LA UNIDAD ACADÉMICA

_____

MGS. Juan Carlos García

PROFESOR DELEGADO POR LA UNIDAD ACADÉMICA

RESUMEN

El requerir la definición de Planes de Continuidad del Negocio para las instituciones del sector financiero surge por la necesidad de brindar la confianza del caso a sus clientes, así como dar cumplimiento a lo dispuesto en el Libro I.- Normas Generales para la aplicación de la Ley General de Instituciones del Sistema Financiero, Titulo X.- De la Gestión y Administración de Riesgos, Capítulo V.- De la Gestión del Riesgo Operativo, Sección IV.- Continuidad del Negocio, artículo 15.

La institución busca que su planeación de la continuidad del negocio le posibilite disminuir el impacto de una interrupción en las actividades críticas del negocio y, principalmente, disminuir el riesgo de ocurrencia de estas interrupciones (posibilidad de que éstas ocurran), protegiendo la operación de los procesos críticos contra los efectos de fallas o desastres significativos.
A través de la metodología de continuidad de negocios a utilizar, se definirá correctamente un proceso de Continuidad del Negocio, alineado con estándares y mejores prácticas de uso mundial.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

BIA: Análisis de Impacto al Negocio

DRII: Disaster Recovery Institute International.

RA: Análisis de Riesgo

RPO: Tiempo que transcurre entre la generación de la última copia de seguridad de la información, almacenada fuera del área afectada, y el tiempo del desastre. Indica la cantidad de información que el Banco está dispuesta a perder sin causar un impacto grave.

RTO: Tiempo que requiere la organización para restablecer la operatividad del subproceso, producto o servicio después de un desastre o una interrupción mayor.

.

ÍNDICE DE FIGURAS

INTRODUCCIÓN

El Plan de Continuidad del Negocio, es un proceso de manejo integrado que identifica el impacto de potenciales amenazas que tiene la entidad y provee un marco de actividades, procedimientos, planes y presupuestos orientados a la construcción de una respuesta sólida y con las capacidades necesarias para que sea efectiva, salvaguardando los intereses de los clientes, reputación, y actividades críticas, conforme a la naturaleza, escala y complejidad de las actividades del Banco.

Implica que en cualquier momento en que se identifiquen las amenazas de interrupción, ocasionada por factores internos o externos tales como atentados de bomba, incendios, inundaciones, terremotos, ataques cibernéticos, interrupción de las comunicaciones, falta de disponibilidad de los sistemas, perdida de datos o cualquier evento sobre los cuales no tiene control la entidad, ésta tenga la habilidad de organizar y priorizar exitosamente los esfuerzos de varios especialistas de diversas áreas para resguardar efectivamente los intereses del Banco y superar eficientemente la pérdida de parte o de toda la capacidad operacional instalada.

El Banco sobre el cuál realizaremos nuestro Plan de continuidad del Negocio es un Banco de baja transaccionabilidad, y que cuenta con una única

agencia ubicada en su Matriz, la cual se encuentra ubicada en la ciudad de Guayaquil.

El desarrollo de este trabajo incluye únicamente el desarrollo de estrategias manuales de continuidad en caso de falla de los sistemas que soportan los procesos críticos.

Vale recalcar que el alcance de este trabajo no incluye el desarrollo del Plan de Recuperación de Desastres de la Institución Bancaria.

CAPÍTULO 1.

GENERALIDADES

1.1. Descripción del problema

En la actualidad, las instituciones del sector financiero se encuentran sujetas al control de la Superintendencia de Bancos, cuya actividad se rige por las normas contenidas en la Ley General de Instituciones del Sistema Financiero y otras leyes y normas complementarias, expedidas por la Junta Bancaria, Superintendencia de Bancos, Banco Central del Ecuador y demás normas aplicables vigentes en el territorio nacional ecuatoriano.

Con el fin de dar cumplimiento a lo dispuesto en el Libro I.- Normas Generales para la aplicación de la Ley General de Instituciones del Sistema Financiero, Titulo X.- De la Gestión y Administración de Riesgos, Capítulo V.- De la Gestión del Riesgo Operativo, Sección IV.- Continuidad del Negocio, artículo 15, que dice textualmente: “Las instituciones controladas deben implementar planes de contingencia y de continuidad, a fin de garantizar su capacidad para operar en forma continua y minimizar las pérdidas en caso de una interrupción severa del negocio”.

Para el efecto, las instituciones del sistema financiero deben establecer un proceso de Administración de la continuidad del negocio, tomando como referencia el estándar ISO 22301 [5] o el que lo sustituya.

1.2. Solución propuesta

La necesidad de la definición de un Plan de Continuidad del Negocio para el Banco surge por la necesidad de brindar la confianza del caso a sus clientes.

Por lo tanto se sugiere desarrollar:

a. Análisis de impacto al Negocio

b. Análisis de riesgos sobre los procesos críticos
c. Elaboración de estrategias de continuidad
d. Gestión de incidentes
e. Comunicación en crisis
f. Responsabilidades de continuidad

Beneficios:

La institución, además de dar cumplimiento a la norma, busca que su planeación de la continuidad del negocio le posibilite disminuir el impacto de una interrupción en las actividades críticas del negocio y, principalmente, disminuir el riesgo de ocurrencia de estas interrupciones (posibilidad de que éstas ocurran), protegiendo la operación de los procesos críticos contra los efectos de fallas o desastres significativos.

Vale recalcar que el alcance de este trabajo no incluye el desarrollo del Plan de Recuperación de Desastres de la Institución Bancaria.

1.3. Descripción de la Metodología

Nuestra solución para cumplir con los objetivos propuestos y las necesidades del Banco, se fundamenta en un modelo evolutivo de la continuidad del negocio con el objetivo de avanzar hacia un estado ideal en el cual la continuidad del negocio se ajuste a las mejores prácticas de la industria y permita optimizar los costos relacionados.

La Metodología de desarrollo propuesta de Planes de Continuidad para la institución financiera, se basa en las mejores prácticas establecidas por el Disaster Recovery Institute (DRI) [1] [2] y el British Standards Institute (BSI) - BS25999 [3], acopladas a las necesidades identificadas en el Banco.

Por lo anterior, la metodología desarrollada incluye las siguientes etapas, tal como muestra la Figura 2.1.:

Figura 2.1 Metodología aplicada al Banco

CAPÍTULO 2.

ANÁLISIS DE CONTINUIDAD

Realizar el análisis de impacto al negocio y el análisis de riesgo a los procesos del Banco, es esencial ya que por este medio se identificaran los procesos críticos para la institución y los recursos necesarios para la operación de los mismos, así como las posibles amenazas que pueden contribuir para realizar un alto de su operación.

2.1. Análisis de la situación actual

Se realizó en análisis de la situación actual con el objetivo de medir el nivel de madurez de la institución con respecto a la continuidad del negocio.

A continuación se detallan los resultados obtenidos:

- La alta gerencia reconoce la importancia de la gestión de la continuidad para el negocio.

- No se cuenta formalmente con una estructura organizacional orientada a mantener el plan de continuidad.

- No se cumplen con los requerimientos regulatorios actuales en relación a la continuidad de negocios.

- En caso de la ocurrencia de un evento de continuidad la institución no se encuentra preparada para mantener la continuidad de sus operaciones.

2.2. Análisis de Impacto al Negocio BIA

El objetivo principal de este análisis de impacto al negocio, es el de proveer a la institución de información esencial, y otros elementos necesarios para identificar las estrategias que podrían minimizar la probabilidad de ocurrencia de eventos que impacten en la capacidad del Banco para operar los procesos que se identifiquen como críticos, en caso de presentarse un evento de interrupción.

El análisis realizado cubre los siguientes aspectos:

- Identificar procesos de negocio críticos: Identificar aquellos procesos de negocio, los cuales en caso de no operar con normalidad, causarían un impacto financiero y reputacional de alto impacto para el Banco.
- Identificar dependencias: Identificar las áreas del Banco que llevan a cabo los procesos críticos.
- Identificar la criticidad de las aplicaciones: Identificar aquellas aplicaciones que soportan los procesos críticos.
- Identificar documentación clave: Identificar la documentación (física o digital) requerida para llevar a cabo los procesos críticos.

2.2.1. Análisis Financiero y Reputacional

Se elaboró el análisis de financiero y operacional con las distintas áreas del banco, en el cual se concluyó que los procesos considerados como críticos son aquellos cumplan con las siguientes premisas:

Impacto Financiero: Procesos que en caso de no poder operar, su impacto financiero causaría pérdidas de 1 millón de dólares, lo cual representa aproximadamente el 15% del patrimonio del Banco.

Impacto Operacional: Procesos que en caso de no poder operar, su impacto operacional causaría inconformidad entre los clientes en un rango de tiempo de 4 horas.

2.2.2. Procesos Críticos

Como resultado del análisis de impacto financiero y operacional, hemos identificado los siguientes procesos con prioridad Alta, los cuales se consideran como procesos críticos:

- Retiro de efectivo (cuenta ahorros)
- Depósito de efectivo (cuenta corriente o ahorros)
- Cambios de cheques
- Depósitos de cheque (cuenta corriente o ahorros)

A Continuación un detalle de los procesos críticos y su descripción, tal como muestra la Figura 2.1:

Nombre del Proceso de Negocio	Descripción Breve
Retiro de efectivo (cuenta ahorros)	Entrega de efectivo al cliente por retiro a cuenta de ahorro por el canal de ventanilla de las agencias y sucursales.
Depósito de efectivo (cuenta corriente o ahorros)	Recepción de efectivo para depósito en cuentas corrientes o de ahorros.
Cambio de cheques	Entrega de efectivo al cliente por pago de cheque por ventanilla del Banco.
Depósitos de cheques (cuenta corriente o ahorros)	Recepción de cheques para depósitos en cuentas corrientes o de ahorros

Figura 2.2 Procesos Críticos y su Descripción

La aplicación identificada como crítica fue la Aplicación CoreBC, la cual es el core bancario desde donde se realizan las diferentes transacciones correspondientes a retiros de efectivo, depósitos de efectivo, cambios de cheques y depósitos de cheques.

Las áreas de las cuales existe dependencia de los procesos críticos son:

- Ventanillas
- Disponibilidad de efectivo.

La información vital de la cual dependen los procesos críticos son:

- Retiro de efectivo (cuenta ahorros)
    - Papeletas de retiro

- Depósito de efectivo (cuenta corriente o ahorros)
    - Papeletas de depósito

- Cambio de cheques
    - Cheques

- Depósitos de cheques (cuenta corriente o ahorros)
    - Cheques
    - Papeletas de depósito

2.2.3. RTO y RPO

El RTO se calculó de acuerdo con la experiencia del usuario y su conocimiento en cuanto a las interrupciones aceptables y no aceptables sobre el proceso. Se documentó el RTO más crítico para el peor escenario que puede presentarse.

Posterior al análisis realizado y en conjunto con las distintas áreas del Banco, se determinó que el tiempo máximo que se podría parar las operaciones es de 4 horas.

El RPO se calculó contemplando lo siguiente:

- Cantidad de trabajo realizado.
- Información es recuperable o no. A menor posibilidad de recuperación el RPO debe ser menor.
- Facilidades para recuperar la información que se pierda del sistema a través de otras fuentes diferentes al backup. A mayor facilidad / número de fuentes alternas de recuperación mayor RPO.
- Tiempo empleado en la recuperación de las transacciones, a mayor tiempo de recuperación menor RPO.

Posterior al análisis realizado y en conjunto con las distintas áreas del Banco, se determinó que el tiempo objetivo de recuperación del Banco es de 10 horas.

2.3. Análisis de Riesgo

En esta etapa se realiza un análisis de posibles amenazas a los procesos identificados como críticos en la etapa anterior.

El análisis de riesgos de no disponibilidad examina las amenazas o posibles eventos que podrían interferir en el funcionamiento normal de los recursos que soportan los procesos críticos del Banco, las vulnerabilidades o debilidades que estos recursos puedan tener.

Como referencia hemos tomado las amenazas que forman parte de la lista de la norma NFPA1600 [4] de amenazas.

A continuación un detalle de las amenazas NFPA que fueron tomadas en cuenta para realizar el análisis de riesgo, tal como muestra la figura 2.3:

Amenaza
(1) a.i - Terremoto-Guayaquil
(1) a.ii - Tsunami – Guayaquil
(1) a.iii - Erupción volcánica-Guayaquil (ceniza)
(1) b.i - Inundaciones-Guayaquil

Amenaza
(1) b.iii ; (2) a.ii - Fuego en las instalaciones y áreas aledañas/Explosiones-Guayaquil
(1) b.vii - Descargas proveniente de tormentas eléctricas-Guayaquil
(1) c.i - Enfermedades, pandemias
(2) a.iv - Colapso del edificio/estructura-Guayaquil
(2) a.ix - Crisis financiera, inflación, colapso del sistema financiero
(2) a.v; (3) d - Falla de la energía eléctrica-Guayaquil
(2) a.x; (3) c - Interrupciones de las comunicaciones
(2) b.ii - Sabotaje (interno y externo)
(2) b.iii - Desorden público o insurrección-Guayaquil
(2) b.viii - Crimen (vandalismo, robo, robo de datos, robo de equipos)-Guayaquil
(2) b.xi - Incumplimiento de seguridad física-Guayaquil
(3) a - Fallas en el centro de cómputo-Principal
(3) a - Fallas en el centro de cómputo-Alterno
(3) a - Fallas en aplicaciones (internas / externas)
(3) b - Falla en los equipos auxiliares de soporte (Token)

Figura 2.3 Amenazas Norma NFPA 1600

A través de reuniones con el personal que interviene en los procesos críticos del Banco, así como las principales gerencias, se realizaron votaciones en la cual se utilizó el criterio y expertise de cada participante, para calificar la probabilidad de ocurrencia y nivel de impacto en caso de que las amenazas detalladas se materialicen.

Dicha calificación fue realizada sobre cada proceso crítico por cada una de las amenazas.

Posterior a la realización del taller, el resultado del análisis final del riesgo residual, muestra que las siguientes amenazas presentan el más alto riesgo residual:

- Incendio
- Terremoto

Incendio: Se recomienda implementación del control mitigante de alarmas de incendios en las instalaciones del Banco, así como un sistema de apagado automático de incendio en las áreas consideradas como sensibles.

Terremoto: Según nos indicó la administración del Banco, la amenaza de terremoto se considera como un riesgo asumido. Las medidas recomendadas para minimizar el impacto en caso de materialización de la amenaza es la implementación de Planes de evacuación y emergencia. De la elaboración de dichos planes se encargará el área de Seguridad Física de la institución Bancaria.

CAPÍTULO 3.

DISEÑO DEL PLAN DE CONTINUIDAD DEL NEGOCIO

La gestión de la continuidad del negocio es la actividad que se lleva a cabo en una organización para asegurar que todos los procesos de negocio críticos estarán disponibles para los clientes de la institución Bancaria.

La gestión de la continuidad no se implanta cuando ocurre un desastre, sino que hace referencia a todas aquellas actividades que se llevan a cabo diariamente para mantener el servicio y facilitar la recuperación.

La base de la gestión de la continuidad son las guías y procedimientos implementados por la organización para gestionar sus recursos y prestar los servicios de negocio.

2.4. Estrategias de Continuidad

En esta fase se realiza el diseño de las estrategias alternas de operación para los procesos seleccionados en la fase de Análisis de Impacto al Negocio (BIA) como procesos críticos.

Las estrategias alternas de operación, responden a escenarios en los cuales, el sistema principal que soporta a las operaciones de la institución no se encuentre en funcionamiento.

Los procesos identificados como críticos y sobre los cuales se realizarán las estrategias alternas de operación son:

- Retiro de efectivo (cuenta ahorros)
- Depósito de efectivo (cuenta corriente o ahorros)
- Cambios de cheques
- Depósitos de cheque (cuenta corriente o ahorros)

A continuación se detallan las estrategias definidas para los procesos críticos:

PROCESO: Retiro de efectivo (cuenta ahorros)

Premisas: Se deberá contar con una base actualizada de saldos de cuentas de los clientes. Dicha base debe ser actualizada diariamente, tres veces al día. Los horarios de cada corte de actualización son 11h00, 14h00 y 17h00.

Responsable: Cajero

- Receptar papeleta de retiro, libreta de ahorros de cliente, cédula de identidad.
- Verificar que la firma de la papeleta sea igual a la de la cédula de identidad del cliente
- Validar si la cuenta tiene saldo, mediante la base de saldos.
- Solicitar aprobación a jefe de sucursal

Responsable: Jefe Sucursal

- Revisar nuevamente si el cliente posee saldo para poder realizar el retiro, mediante la base de saldos.
- Dar aprobación a cajero

Responsable: Cajero

- Entregar efectivo
- Archivar papeleta de retiro y libreta de ahorros.
- Realizar el Cierre y cuadre de las cajas.

PROCESO: Depósito de efectivo y Depósito de Cheque (cuenta corriente o ahorros)

Premisa: Se contará con el formulario de cierre de caja el cual será necesarios para realizar el cierre de caja al final del día.

Responsable: Cajero

- Receptar la doble papeleta de depósito y efectivo/cheque
- Entregar al cliente papeleta sellada como comprobante de depósito.
- Archivar papeleta de depósito adicional como comprobante de ventanilla

Responsable: Cajero y Jefe Sucursal

- Realizar el cierre de operaciones para el control y cuadre correspondiente.

PROCESO: Cambios de cheques

Premisas: Se deberá contar con una base actualizada de saldos de cuentas de los clientes. Dicha base debe ser actualizada diariamente, tres veces al día. Los horarios de cada corte de actualización son 11h00, 14h00 y 17h00.

Responsable: Cajero

- Receptar cheque e identificación del cliente
- Verificar monto del cheque, en la base de saldos.
- Solicitar aprobación a Jefe Sucursal

Responsable: Jefe Sucursal

- Validar saldo de la cuenta nuevamente en la base de saldos
- Dar aprobación a cajero

Responsable: Cajero

- Entregar al cliente el efectivo e identificación
- Archivar cheque como soporte

Responsable: Cajero y Jefe Sucursal

- Realizar el cierre de operaciones para el control y cuadre correspondiente

2.5. Gestión de Incidentes

Fase I: Respuesta ante un evento

Esta fase se activa en caso de presentarse un evento que afecte:

1) Instalaciones físicas: Donde se desarrollan los procesos críticos y que pueda causar daños en las personas. Estas actividades son ejecutadas por el Equipo de Emergencia.

   Sus principales actividades son:

   - Evacuar y reubicar del personal.
   - Entregar del control a las entidades de apoyo locales o nacionales.
   - Asegurar activos.

- Recopilar información de empleados lesionados / fallecidos.
- Valorar la extensión de los daños en la infraestructura y/o activos.
- Valorar el tiempo estimado de reparación de instalaciones y autorización de acceso.
- Comunicar resultado al Equipo de Gestión de Incidentes.

2) Sistemas: Acciones a ejecutar por el Banco para contener la emergencia al presentarse un incidente lógico en los servidores. En esta actividad interviene la Gerencia de Tecnología.

   Realizar la valoración de daños para dimensionar las consecuencias del evento presentado. La valoración debe contener como mínimo:

   - Información de sistemas y procesos afectados.
   - Servicios afectados por la falla lógica.
   - Extensión de los daños en la infraestructura de TI y/o activos.
   - Tiempo estimado de recuperación de las operaciones, procedimientos de restauración de respaldos o infraestructura física.
   - Notificación al Equipo de Gestión de Incidentes de la valoración realizada.

Fase II: Activación de Planes

Evaluación de activación de las Estrategias Manuales de Continuidad o el Plan de Recuperación de TI, según la extensión de los daños y el tiempo estimado de recuperación tanto para un daño físico a las instalaciones y/o daño lógico en los sistemas. En estas actividades interviene el Equipo de Gestión de Incidentes.

La activación de los planes de continuidad va a depender de si el tiempo de recuperación sobrepasa el RTO establecido de 4 horas.

Fase III: Recuperación

En esta fase se activan los procedimientos de continuidad.

Deben ser tomadas en cuenta las siguientes actividades:

- Traslado de personal a sitio de operación alterno e inicio de operaciones en el mismo, en caso de daño en las instalaciones donde se ejecutan los procesos.
- Activación del centro de cómputo alterno, en caso de presentarse un daño a nivel lógico.

- Ejecución de las estrategias manuales de continuidad, en caso de falla de los sistemas, y de no poder activarse el centro de cómputo alterno.
- Monitoreo de las actividades que se están llevando a cabo, en el sitio de operación alterno, y/o en el centro de cómputo alterno.

De igual forma, en esta fase, se deben establecer estrategias de reparación de los daños, mediante las cuales se deben ejecutar las siguientes actividades:

- Validar que la seguridad física del edificio y/o del proceso, sea adecuada para permitir el acceso a los equipos de reparación.
- Coordinar los esfuerzos de recuperación de activos.
- Definir el tiempo estimado de reparación.
- Establecer los requerimientos de compras y/o reparación de instalaciones y equipos.
- Solicitar la aprobación de estrategias de reparación.
- Ejecutar las estrategias (compras y/o reparaciones).

Fase IV: Retorno

En esta fase se establecen procedimientos para hacer el cierre de la operación en contingencia y dar inicio a las actividades de retorno, una vez que han finalizado los procedimientos de reparación del ambiente principal.

Las principales actividades a llevar a cabo son:

- Establecer estrategias de retorno, en la cual deben incluir fecha de retorno, estrategia de movilización de personal, esquema de activación se procesos en el sitio de operación principal.
- Asegurar la disponibilidad de los recursos para el inicio de la operación.
- Verificar la operatividad en ambiente de producción.
- Finalizar operaciones en ambiente de contingencia.
- Evaluar las acciones realizadas durante la continuidad.

2.6. Sitios de Operación alterno

El sitio de operación alterno, es la ubicación física alterna en donde se podrán ejecutar los procesos críticos en caso de daño físico de la instalación principal.

Es recomendable que esta ubicación alterna se encuentre a mínimo a 10 kilómetros de distancia de la ubicación principal.

La ubicación alterna debe de contar con todos los recursos necesarios para que el personal que opera los procesos críticos del negocio pueda ejecutar sus operaciones lo más normalmente posible.

2.7. Comunicación en Crisis

Para establecer un buen plan de comunicación en crisis se deben establecer:

Audiencias: Los comunicados deben estar elaborados y dirigidos según el tipo de audiencia. Los tipos de audiencia pueden ser empleados, familiares de empleados, socios del negocio, entidades gubernamentales, clientes y medios.

Voceros: Según el tipo de audiencia es necesario identificar quienes son las personas más adecuadas para emitir los comunicados.

El perfil sugerido para los voceros es el siguiente:

- Tener un alto cargo directivo.
- Contar con buenas habilidades de comunicación oral.
- Tener conocimiento de los productos y servicios del Banco.
- Tener capacitad para comunicar información técnica o especializada de forma creíble.
- Tener experiencia / recibir entrenamiento en el manejo de medios.
- Ser y mostrarse comprensivo con las audiencias.
- Tener habilidad para comunicarse en forma serena y para mantener la calma ante situaciones conflictivas.

Canales: Se debe identificar cuáles son los canales más indicados para emitir comentarios acerca del evento que se está presentando.

A continuación se detallan algunos canales por los cuales se pueden transmitir los comunicados:

- Conferencias de prensa.
- Correo interno.
- Línea de atención a audiencias.
- Reuniones informativas.
- Publicidad impresa.

- Redes digitales y sociales (twitter, Facebook, entre otros).

Mensajes: Se debe considerar la temática de los mensajes para la elaboración de los mismos, ya que en los mismos se deben incluir lo que ha ocurrido, el porqué, que acciones se está tomando para controlar el evento, y qué efectos tendrá el evento en relación a la institución y sus clientes.

Esquema de notificación de incidentes: Durante la operación normal se pueden presentar incidentes que por su magnitud no activan el plan de continuidad de inmediato, pero que si no son tratados oportunamente, pueden afectar las operaciones y por tanto, hacer necesario la invocación del plan de continuidad.

Por lo anterior, se hace importante el que dichos incidentes sean oportuna y adecuadamente comunicados para mantener el control sobre su administración.

2.8. Roles y Responsabilidades

La gestión de eventos imprevistos que podrían afectar la capacidad operacional de la Entidad, supone un conjunto de acciones antes, durante y después del evento, los cuales deben ser ejecutados por:

Dueños de procesos: Personas que van a ejecutar los procesos considerados como críticos durante un evento de continuidad.

Personal de Continuidad: Este grupo lo integra en Comité de Continuidad del Negocio. Por normativa este comité está integrado por el funcionario responsable de Continuidad del Negocio reporta al Gerente de Riesgos, quien será el Líder del Comité de Continuidad del Negocio, el avance, pendientes y problemas identificados en las actividades concernientes a los Planes de Continuidad del negocio de Banco del Estado.

Equipo de Gestión de Incidentes: Son los encargados de la toma de decisiones en el momento en el que se presente un evento de interrupción mayor. Son los encargados de la activación de los planes de continuidad del negocio, así como son los encargados de tomar la decisión de retorno a la normalidad.

Equipo de Emergencias: Son los encargados de reaccionar en el caso de ocurrencia de un evento que afecta la infraestructura física

donde se llevara cabo los procesos, y además este suceso afecte o atente contra la vida de las personas. De igual forma son los encargados de realizar la evaluación de daños en caso de daño físico. Reportan al Equipo de Gestión de Incidentes.

Gerencia de Tecnología: Es la encargada de la activación del Plan de Recuperación de Desastres de TI. De igual forma son los encargados de realizar la evaluación de daños al ambiente y/o infraestructura tecnológica. Reportan al Equipo de Gestión de Incidentes.

.

CONCLUSIONES Y RECOMENDACIONES

Después del desarrollo anterior se concluye lo siguiente:

1. Las amenazas de cualquier tipo trascienden las fronteras geográficas, lo que significa que los eventos aparentemente no relacionados pueden afectar la capacidad de respuesta de cualquier país, cuidad o localidad, es por esto que debemos estar preparados para la materialización de estas posibles amenazas.

2. La continuidad del negocio permite garantizar la continuidad de las operaciones para disminuir el impacto financiero, credibilidad y reputación de la institución.

3. Mediante la implementación de planes de continuidad se reduce el tiempo en la recuperación de los procesos críticos del negocio en caso de la ocurrencia de un evento mayor de interrupción.

4. Realizar un correcto Análisis de Impacto al negocio (BIA) permite determinar las estrategias con mayor facilidad.

5. Realiza un correcto Análisis de Riesgo (RA) de los temas de continuidad permite crear conciencia de la administración de las vulnerabilidad a las que el negocio es susceptible.

6. Realizar un análisis financiero y reputacional anual permitiría reevaluar los procesos críticos.

7. Para una correcta comunicación en crisis se deben conjugar los siguientes factores: voceros, audiencias, canales y mensajes.

8. Es importante definir los roles y responsabilidades de los actores en continuidad.

Para finalizar se recomienda:

1. Se recomienda a las Instituciones Bancarias la implementación del Sistema de Gestión de Continuidad del Negocio, los cuales contribuyan en mantener la operación de los procesos críticos del negocio en caso de ocurrencia de un evento de interrupción de sus operaciones normales.

2. Realizar análisis de riesgo y amenazas anual.

3. Evaluar mediante el análisis de impacto al negocio (BIA), si hay cambios de procesos y cambios en las actividades críticas.

4. Realizar pruebas de las estrategias anualmente.

5. Es importante definir las actividades antes durante y después de una contingencia.

6. Es importante definir un centro de operaciones alterno.

BIBLIOGRAFÍA

[1] Disaster Recovery Institute International, Disaster Recovery Institute, https://www.drii.org/, Diciembre 2015.

[2] Metodología del DRII, Metodología del DRII para el desarrollo de un BCP, http://skat.ihmc.us/rid=1206379798267_743688316_16094/Metodolog%C3%ADa%20del%20DRII.pdf, Agosto 2015

[3] BSI, Transition Guide, Moving from 25999-2 to ISO 22301, https://www.bsigroup.com/Documents/iso-22301/resources/BSI-BS25999-to-ISO22301-Transition-UK-EN.pdf, Julio 2012

[4] NFPA 1600, NFPA 1600: Standard on Disaster/Emergency Management and Business Continuity/Continuity af Operations Programs, http://www.nfpa.org/assets/files/AboutTheCodes/1600/1600-13-PDF.pdf, Julio 2013

[5] ISO 2012, Internacional Estándar ISO 22301, ISO 220301:2012 First Edition, mayo 2012.