MAESTRÍA EN GERENCIA DE SISTEMAS
Y TECNOLOGÍAS DE LA INFORMACIÓN

MODELO DE GESTIÓN DE CONTINUIDAD DE INFRAESTRUCTURA TECNOLÓGICA PARA LA OPERACIÓN DE SERVICIOS DE TI EN EMPRESAS FINANCIERAS SOBRE LA BASE DE LAS NORMAS ISO 22301 E ISO 27001. APLICACIÓN A UN CASO DE ESTUDIO

Trabajo de Titulación presentado en conformidad a los requisitos establecidos para optar por el título de Magíster en gerencia de sistemas y tecnologías de la información

Profesor guía
Mgs. Carlos Estalesmit Montenegro Armas

Autor
Ing. Angel Vinicio Sarabia Zapata

Año
2015

DECLARACIÓN DEL PROFESOR GUÍA

“Declaro haber dirigido este trabajo a través de reuniones periódicas con el estudiante, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”.

_____

Carlos Estalesmit Montenegro Armas
Magister en Sistemas
C. I.: 1704448818

DECLARACIÓN DE AUTORÍA DEL MAESTRANTE

“Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes”.

_____

Angel Vinicio Sarabia Zapata
Ingeniero en Electrónica y telecomunicaciones
C. I.: 0502520208

AGRADECIMIENTOS

Esta tesis es el resultado de un conjunto de esfuerzos y oportunidades guiadas por Dios y la Virgen María, con el apoyo de una gran familia.

A MI ESPOSA E HIJAS: Mayra Bastidas, Katherine y Meredith por ser mi fuente de motivación diaria.

A MIS PADRES: Galo Sarabia y Marina Zapata, por ser las columnas de mi formación académica y social.

A MI HERMANA: Olga Sarabia y su familia, por darme su apoyo incansable.

DEDICATORIA

A mí esposa Mayra Bastidas e hijas Katherine Valeska y Meredith Doménica, por ser el regalo más grande de Dios, quienes iluminan mi camino al andar, y; me inspiran levantarme día a día y luchar por ser mejor padre, esposo, hijo y mejor ser humano. Muy seguro estoy me impulsarán a conseguir nuevas metas. Por y para ustedes mis princesas mágicas.

RESUMEN

La Superintendencia de Bancos del Ecuador define normativas para el funcionamiento y operación de los sistemas e información, de manera que éstos se encuentren disponibles en todo momento, sin descuidar la seguridad informática de los activos intangibles de las Organizaciones Financieras, dado que eventos no planificados llamados disruptivos pueden provocar interrupciones en los servicios de TI y acceso a la información, afectando significativamente la calidad del servicio y rentabilidad de las compañías.

Este proyecto tiene como objetivo elaborar un modelo de gestión de continuidad de Infraestructura Tecnológica, que garantice la operación de los servicios de TI en Compañías Financieras, basados en Sistemas de Gestión de Continuidad del Negocio y Sistemas de Gestión de Seguridad de la Información (normas ISO 22301 e ISO 27001) respectivamente, el modelo permitirá disminuir el impacto, riesgo y tiempo de indisponibilidad de servicios de TI en producción, y que éstos no incidan directamente en los objetivos organizacionales de la compañía.

Para la validación del modelo diseñado se utiliza la metodología de pruebas, aplicando a un caso de estudio de una Organización Financiera (Banco KLM), obteniendo resultados positivos sobre la capacidad de resistir a un incidente disruptivo-interrupción, pudiendo restablecer las operaciones normales de los servicios en los tiempos exigidos; se constató que el Banco KLM se encuentra preparado para afrontar un desastre que afecta sus servicios tecnológicos, basado en sus políticas de seguridad y alta disponibilidad bien definidas. Para la aplicación del modelo diseñado en el presente trabajo se anexa formularios detallados, que facilitan su implementación por partes, pudiendo iniciar por los servicios más críticos.

ABSTRACT

The Superintendency of Banks defines standards for the functioning and operation of systems and information, so that they are available at all times, without neglecting the security of intangible assets of financial organizations, as called disruptive unplanned events IT services and access to information, significantly affecting the quality of service and profitability of the companies.

This project aims to develop a management model of continuity of technological infrastructure, to ensure the operation of IT services in financial companies, based on systems management and business continuity management systems information security (ISO 22301 and ISO 27001) respectively, the model allow lessen the impact, risk and downtime of IT services into production, and they do not directly affect the organizational objectives of the company.

To validate the model designed use the test methodology, using a study case of a financial organization (Bank KLM), with positive results on the ability to resist disruptive-interruption incident may restore normal operations the services in time required; was found that the KLM Bank is prepared to face a disaster affecting its technology services, based on their security policies and well-defined high availability. For the application of the model designed in this paper detailed attached forms, to facilitate its implementation by parties, and can start with the most critical services is attached.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

La Superintendencia de Bancos del Ecuador (Superintendencia de Bancos del Ecuador - SBS , 2005) establece: “Las instituciones controladas deben contar con la tecnología de la información que garantice la captura, procesamiento, almacenamiento y transmisión de la información de manera oportuna y confiable; evitar interrupciones del negocio y lograr que la información, inclusive aquella bajo la modalidad de servicios provistos por terceros, sea íntegra, confidencial y esté disponible para una apropiada toma de decisiones)”, para lo cual las Empresa Financieras deben implementar planes de contingencia normados, que garanticen la continuidad de los servicios ofrecidos.

Los planes tienen como finalidad el recuperar la operación de los servicios en producción, mitigando riesgos y afectación al negocio con consecuencias como pérdida de ingresos o mala imagen para la Compañía. Por otro lado la planificación para contingencias y recuperación de desastres permiten a las Organizaciones afrontar interrupciones en la operación y entrega de servicios de manera ordenada, ágil y oportuna, bajo normativas de buenas prácticas, convirtiéndose en un proceso orientado al negocio.

Para éstas respuestas de servicios, dirigidas a la tecnología de la información y en particular a las áreas de Infraestructura Tecnológica se desarrolla un modelo de gestión de continuidad de infraestructura tecnológica para las Empresas Financieras contextualizado en la operación de servicios de TI, mediante normas internacionales de estandarización como ISO 22301 e ISO 27001.

El presente trabajo facilita un modelo de gestión que permite enfrentar incidentes disruptivos de manera eficaz y oportuna, integrando normativas legales y técnicas, se cita un caso de estudio que permite identificar su funcionalidad y aplicabilidad (caso de estudio –Banco KLM).

1. ANÁLISIS DEL MARCO NORMATIVO Y TÉCNICO A CERCA DE LOS PROCESOS DE CONTINUIDAD EN SERVICIOS DE TI

1.1. Normativa legal de Continuidad de Negocio en el Ecuador

En la actualidad la dependencia de la sociedad con las tecnologías de la información y las comunicaciones (TIC) es indiscutible. En el Ecuador las transacciones comerciales, los procesos de producción, la prestación de servicios en general exigen infraestructuras, procesos y productos tecnológicos fiables, predecibles y eficientes.

1.1.1. Ámbito Público

La legislación nacional mediante los organismos encargados del control de la utilización de los recursos estatales, establecen la disponibilidad de los sistemas y la información de las personas y empresas. Según la norma de control interno 410-11de la Contraloría General del Estado "Corresponde a la unidad de tecnología de información la definición, aprobación e implementación de un plan de contingencias que describa las acciones a tomar en caso de una emergencia o suspensión en el procesamiento de la información por problemas en los equipos, programas o personal relacionado" (Contraloría General del Estado, 14 de Diciembre de 2009).

Para asegurar la continuidad del negocio, la Constitución de la República del Ecuador en sus Artículos 389 y 390 establece:

"**Art. 389.-** El Estado protegerá a las personas, las colectividades y la naturaleza frente a los efectos negativos de los desastres de origen natural o antrópico mediante la prevención ante el riesgo, la mitigación de desastres, la recuperación…".

“**Art. 390.-** Los riesgos se gestionarán bajo el principio de descentralización subsidiaria, que implicará la responsabilidad directa de las instituciones dentro de su ámbito geográfico…” (Asamblea Nacional Constituyente, 2008).

1.1.2. Ámbito Privado

El Organismo Regulador para las instituciones financieras en el Ecuador es la SB (Superintendencia de Bancos), éste define normativas para el funcionamiento y operación de los sistemas e información, de manera que se encuentren disponibles en todo momento. A continuación se cita el artículo concerniente a la Continuidad del Negocio.

"**Art 15.-** Las instituciones controladas deben administrar la continuidad del negocio, manteniendo procedimientos actualizados, a fin de garantizar su capacidad para operar en forma continua y minimizar las pérdidas en caso de una interrupción del negocio (artículo sustituido con resolución No. JB-2014-3066 de 2 de septiembre del 2014).

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 o el que lo sustituya, y considerar al menos lo siguiente....."

Durante esta última década, se ha desarrollado una serie de recomendaciones para las buenas prácticas, la anticipación a incidentes, respuestas y técnicas para su evaluación como se puede apreciar en la Figura 1. A continuación se detalla una breve reseña histórica sobre las normas: (Alexander, 2012).

- **NFPA 1600:** es el lineamiento más antiguo, fue publicado en 1995, este documento estableció una serie de conjuntos de criterios para la gestión de desastres, emergencias y programas de continuidad para las organizaciones.

- **Disaster Recovery Institute International (DRII):** publicada en 1997 establece las “Prácticas Profesionales para la Gestión del Negocio”.

- **Business Continuity Institute:** en el año 2002 publicó los lineamientos de “Buenas Prácticas para la Continuidad del Negocio”.

- **PAS 56:** fue publicada en el 2003, este documento estableció el proceso, principios y terminología de un sistema de gestión de continuidad del negocio.

- **BS 25999-1:** publicada en el 2006, ésta norma británica describió de manera concreta el ciclo de vida de la continuidad del negocio.

- **BS 25999-2:** publicada en el año 2007, fue el primer estándar internacional certificable y auditable, establece los requisitos para un Sistema de Gestión de la Continuidad (SGC).

- **ISO/PAS 22399**: publicada en el año 2007, generó lineamientos orientados al desempeño de preparación ante incidentes y continuidad de operaciones.

- **ISO/IEC 24762:** se publicó en el 2008, generó lineamientos para la provisión de información y comunicación frente a la recuperación de desastres.

- **BS 25777:** publicada en el 2008, definió un código de buenas prácticas sobre continuidad orientado a IT de las organizaciones.

- **ASIS/BSI (Business Continuity Management Standard)**: en el año 2010 se publicó el este lineamiento, especifica requerimientos para permitir a las organizaciones identificar, desarrollar e implementar políticas, objetivos, capacidades, procesos y programas.

- **PAS 200:** publicada en el 2011, llamada "Gestión de Crisis -Lineamiento y Buena Práctica", diseñado para ayudar a las empresas a tomar pasos prácticos para mejorar su habilidad de manejar crisis.

- **ISO/IEC 27031:** también publicada en el 2011, se describe los conceptos y principios de tecnología de información y comunicación para preparar a una organización para la continuidad del negocio.

- **ISO 22301:2012:** norma publicada en el año 2012, "Seguridad de la Sociedad: Sistemas de Continuidad del Negocio-Requisitos" aplica el ciclo **Plan-Do-Check-Act** (PDCA por sus siglas en inglés) para la planificación, establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y la mejora continua de su efectividad. El modelo fue creado en consistencia con otros estándares de gestión, tales como: ISO 9001:2008, ISO 27001:2005, ISO 20000-1:2011, ISO 14001:2004 y con el ISO 28000:2007.

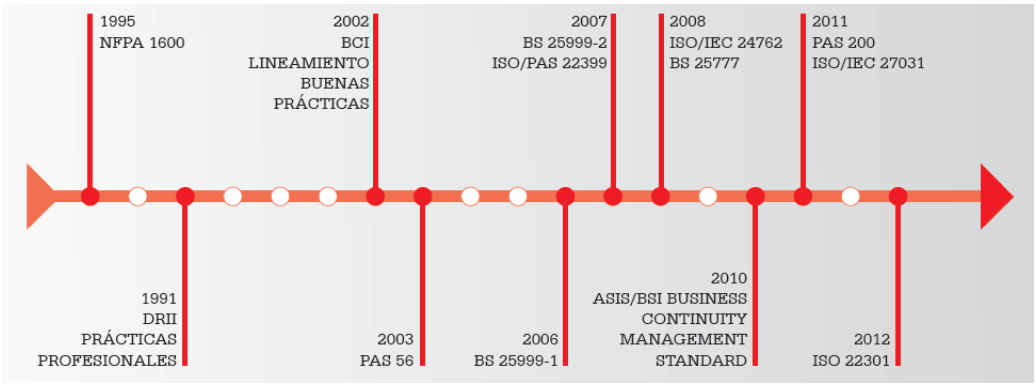

Figura 1. Evolución de los estándares en continuidad del negocio.

Tomado de: (Alexander, 2012).

1.2. Estándares y buenas prácticas de Continuidad de Negocio

En la actualidad los Planes para la Recuperación de Desastres y Continuidad del Negocio (PRD/CN), se manejan mediante el estándar de buenas prácticas

internacionales ISO 22301-2012, "El comité técnico 223 de la Organización Internacional para la Normalización (ISO, por sus siglas en inglés), publicó la versión final ISO 22301:2012. Esta norma reemplazará al estándar BS 25999-2:2007" (NORMA ISO 22301, 2012).

1.2.1. BS25999

Las normas BS son estándares Británicos, éstas fueron publicadas en los años 2006 y 2007 respectivamente en 2 versiones, en la actualidad continúan siendo utilizadas en algunos países (Advisera, 2015).

a) BS 25999-1

La norma fue publicada en el año 2006, se centró en las opciones de continuidad del negocio en las organizaciones, describiendo el ciclo de vida de la continuidad del negocio, y; desarrolló como plan de continuidad del negocio conocido como Business Continuity Management (BCM).

b) BS 25999-2

El estándar BS 25999-2:2007 publicado en el año 2007, es el primer estándar internacional que permite certificar y auditar, su objetivo es definir los requisitos para sistemas de gestión de la continuidad del negocio, basado en buenas prácticas; su uso está dado para organizaciones de volumen grande, mediano y pequeño que operan en todos los sectores comerciales.

1.2.2. ISO 22301

La norma ISO 22301 (NORMA ISO 22301, 2012) es una norma del Sistema de Gestión de Continuidad del Negocio (SGCN), ésta puede ser utilizada por las organizaciones de todos los tamaños y tipos. Las organizaciones luego de implementar los estándares son capaces de obtener la certificación, lo cual

permite a las empresas demostrar ante entidades reguladoras, clientes, posibles clientes y otras partes interesadas que mantienen sistemas de gestión basados en buenas prácticas.

En la actualidad la norma puede ser utilizada para la obtención de la certificación, por ende incluye requisitos cortos y concisos que describen los elementos centrales de la gestión de la continuidad del negocio.

Provee un marco referencial para las organizaciones interesadas en la administración y gestión de la continuidad del negocio, que permite cumplir los requisitos reglamentarios y del cliente así como los propios de las empresas.

El estándar contiene sólo aquellos requisitos que pueden ser auditados objetivamente, por lo tanto puede ser utilizado por una organización para asegurar que las partes interesadas usen un SGCN apropiadas en su lugar; y ha sido diseñada para lograr una mayor seguridad social (proporcionar protección de la sociedad, y responder a, incidentes, emergencias y desastres provocados por actos humanos intencionales, riesgos naturales y fallas técnicas) (NORMA ISO 22301, 2012).

La ISO 22301 reemplazó a la norma británica BS 25999-2, estas dos normas son bastante similares, sin embargo la ISO/IEC 22301 es considerada como una actualización de la BS 25999-2, y; a diferencia de la norma británica ha sido aceptada por institutos de normas nacionales a nivel mundial.

La norma centra sus objetivos en 4 actividades principales que se muestran a continuación:

1) "Entender las necesidades de la organización y los requisitos para establecer políticas y objetivos para la gestión de la continuidad de negocio;

2) Implantar y operar controles y medidas para el manejo de la capacidad de una organización para la gestión de incidentes que causan interrupciones;

3) Seguimiento y revisión del desempeño y la efectividad del SGCN;

4) Mejora continua basada en mediciones objetivas"

El modelo actual de la norma ISO 22301 exige cierta documentación obligatoria, que una empresa de acuerdo a su alcance y estructura debe desarrollar, esta documentación es la siguiente (Alexander, 2012):

1) Lista de requisitos legales, normativos y de otra índole.
2) Alcance del SGCN.
3) Política de la continuidad del negocio.
4) Objetivos de la continuidad del negocio.
5) Evidencia de competencias del personal.
6) Registros de comunicación con las partes interesadas.
7) Análisis del impacto en el negocio.
8) Evaluación de riesgos, incluido un perfil del riesgo.
9) Estructura de respuesta a incidentes.
10) Planes de continuidad del negocio.
11) Procedimientos de recuperación.
12) Resultados de acciones preventivas.
13) Resultados de supervisión y medición.
14) Resultados de la auditoría interna.
15) Resultados de la revisión por parte de la dirección.
16) Resultados de acciones correctivas.

Cláusulas claves de ISO 22301:2012

Siguiendo la nueva estructura de la Guía ISO 83, la norma ISO 22301 está organizada en las siguientes cláusulas principales:

- Cláusula 4: Contexto de la organización.
- Cláusula 5: Liderazgo.
- Cláusula 6: Planificación.
- Cláusula 7: Soporte.
- Cláusula 8: Operación.
- Cláusula 9: Evaluación del desempeño.
- Cláusula 10: Mejora.

Cada una de estas actividades principales se describe brevemente a continuación:

<u>Cláusula 4:</u> Contexto de la organización

Esta cláusula determina los requerimientos necesarios para establecer el propósito del SGCN, como debe aplicar temas internos y externos que son relevantes para el propósito de la organización y que afectan su habilidad de alcanzar los resultados esperados como:

- Actividades de la organización, sus funciones, servicios, productos, sociedades, cadenas de suministros, relaciones con las partes interesadas y el impacto potencial relacionado con un incidente que genere una interrupción.

- Vínculos entre la política de continuidad de negocio y los objetivos de la organización y otras políticas, incluyendo, la estrategia de gestión de riesgos globales.

- Leyes, regulaciones y otros requisitos aplicables, a los cuales la organización está suscrita.

- Identificar el alcance del SGCN, tomando en cuenta los objetivos estratégicos de la organización.

Cláusula 5: **Liderazgo**

Esta cláusula realiza un resumen de las exigencias a la alta gerencia de la organización, en relación a su rol en el SGCN, de manera que el sistema de gestión pueda funcionar eficazmente en sinergia con los objetivos de la empresa. Existen nuevos requerimientos para la alta gerencia, tales como:

- Asegurarse que el sistema de gestión de continuidad del negocio es compatible con la dirección estratégica de la organización.

- Integración de los requerimientos del Sistema de Continuidad del Negocio en los procesos del negocio.

- Comunicar la importancia de una eficaz gestión de la continuidad del negocio.

Cláusula 6: **Planeación**

Esta es una etapa crítica en la que se establecen objetivos estratégicos de continuidad del negocio, estos objetivos deben estar relacionados a la política de continuidad del negocio de la organización, y, deben ser medibles mediante las metas alcanzadas. Los objetivos de la continuidad de negocio deben:

- Estar alineados con la política de continuidad de negocio.

- Considerar el nivel mínimo de productos y servicios que es aceptable para que la organización alcance sus objetivos.

- Ser medibles, tomando en cuenta requisitos aplicables.

- Ser controlados y actualizados, según sea apropiado.

Cláusula 7: Soporte

Esta cláusula detalla el soporte requerido para establecer, implementar y mantener un Sistema de Gestión de Continuidad del Negocio eficaz, considerando todos los recursos necesarios, así como requerimientos para la gestión y registro de documentos.

El tema de comunicaciones es adicionado a la cláusula, constituyendo un punto importantísimo al gestionar cualquier alteración en la organización.

Cláusula 8: Operación

Después de la planificación del SGCN, la organización debe ponerlo en funcionamiento. Esta cláusula incluye:

Cláusula 8.1: La cláusula planificación operacional y control

Esta cláusula requiere que la organización asegure la existencia de procesos que hayan sido desarrollados para gestionar que los riesgos al SGCN estén correctamente implementados.

Cláusula 8.2.2: El Business Impact Analysis

Esta cláusula introduce un nuevo término: “esquemas de tiempo priorizados” (NORMA ISO 22301, 2012), define el orden y los tiempos para la recuperación de actividades críticas que soportan los productos y servicios claves.

Cláusula 9: Evaluación del desempeño

Permite realizar un seguimiento del sistema, y establecer revisiones periódicas para mejorar su operación, luego de implementado el sistema de gestión. Entre las principales actividades se tienen:

- Seguimiento de la medida en la cual la política, objetivos y metas de continuidad de negocio son cumplidos.

- Medición del desempeño de los procesos, procedimientos y funciones que protegen las actividades priorizadas.

- Seguimiento de la conformidad con esta norma y con los objetivos de la continuidad de negocio.

- Seguimiento histórico de evidencia de desempeño deficiente del SGCN.

- Realización de auditorías internas a intervalos planificados; y

- Evaluación de todo lo anterior en las revisiones por la dirección, a intervalos planificados.

Cláusula 10: Mejora

Constituyen todas las acciones realizadas a lo largo de la organización, para aumentar la eficacia (cumplir objetivos) y la eficiencia (costo/beneficio óptimo) de los procesos y controles de seguridad, para brindar más beneficios a la organización y a sus partes interesadas.

1.2.3. ISO 27031

La norma ISO/IEC 27031:2011 Tecnología de Información - Técnicas de Seguridad - Directrices para la preparación de la información y tecnología de comunicación para la continuidad del negocio, la norma describe los conceptos y principios de la preparación de las tecnologías de la información y las comunicaciones para la continuidad del negocio, y proporciona un marco de métodos y procesos para identificar y especificar todos los aspectos (tales

como los criterios de desempeño, diseño e implantación) para la mejora de la preparación de las TICs de una organización para garantizar la continuidad del negocio.

El estándar es aplicable a cualquier organización (privadas, gubernamentales y no gubernamentales, independientemente de su tamaño) desarrollando su programa de adecuación de las TIC para la continuidad del negocio.

1.2.4. ISO 27001

Es la norma internacionalmente reconocida para la Gestión de Seguridad de la Información (SGSI), la gestión de la seguridad de la información se realiza mediante un proceso sistemático, documentado y conocido por toda la organización.

Mediante ésta norma se establece la necesidad de crear un SGSI, constituyendo en un eje vital para preservar la Continuidad del Negocio.

La seguridad de la información consiste en la preservación de su confidencialidad, integridad y disponibilidad, incluyendo todos los sistemas manejados dentro de las empresas. La base de la norma lo conforman 3 términos sobre los cuales se edifica la seguridad de la información:

1) **"Confidencialidad:** la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

2) **Integridad:** mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

3) **Disponibilidad:** acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran" (NORMA ISO 27001, 2005).

1.3. Estrategia de integración

La integración de las normas ISO 22301 e ISO 27001 aplicadas a las Empresas Financieras, permitirán una serie de sinergias que representan beneficios directos para las Compañías.

1.3.1. Análisis de integración

¿Por qué se puede integrar ISO 22301 e ISO 27001?

Los factores principales por los cuales se puede realizar la integración de las normas son:

a) Las dos normas son ISO y poseen una estructura similar de procesos, basado en el ciclo PDCA (Plan-Do-Check-Act) de Deming.

b) La Continuidad del Negocio y Seguridad Informática definidas por las normas ISO 22301 e ISO 27001 respectivamente, están relacionadas por las siguientes actividades:

- Análisis de riesgos de seguridad de la información para el impacto en el negocio.

- Manejo de incidentes de seguridad de la información para la recuperación y aseguramiento de la Continuidad del Negocio.

1.3.2. Estrategia

1.3.2.1. ¿Cómo integrar ISO 22301 e ISO 27001?

La integración de las normas ISO 22301 y 27001 resulta una necesidad más que una opción, considerando el entorno actual y dinámico de los servicios

bancarios. Para el nuevo modelo de Gestión de Continuidad de Infraestructura Tecnológica se integran las normas de la siguiente manera:

a) Seleccionando las cláusulas obligatorias de las ISO 22301 para el proceso de certificación, las cláusulas se muestran en la Tabla 1.

b) Complementando la lista de la Tabla 1 con la ISO 27001.

c) Definiendo documentos a partir de la lista de cláusulas seleccionadas.

Tabla 1. Cláusulas obligatorias de las ISO 22301.

Item	Cláusulas ISO 22301
1	Lista de requisitos legales, normativos y de otra índole.
2	Alcance del Sistema de gestión de continuidad
3	Política de la Continuidad del Negocio.
4	Objetivos de la Continuidad del Negocio.
5	Evidencia de competencias del personal.
6	Registros de comunicación con las partes interesadas.
7	Análisis del impacto en el negocio.
8	Evaluación de riesgos, incluido un perfil del riesgo.
9	Estructura de respuesta a incidentes.
10	Planes de Continuidad del Negocio.
11	Procedimientos de recuperación.
12	Resultados de acciones preventivas.
13	Resultados de supervisión y medición.
14	Resultados de la auditoría interna.
15	Resultados de la revisión por parte de la dirección.
16	Resultados de acciones correctivas.

Tomado de: (NORMA ISO 22301, 2012).

Como resultado de la integración de las normas ISO para el modelo de Gestión de Continuidad de Infraestructura Tecnológica, se obtienen nuevos documentos y registros, algunos contienen formularios de apoyo llamados índices, como se muestra en la Tabla 2.

Tabla 2. Modelo de gestión de continuidad para servicios de TI, mediante ISO 22301 e ISO 27001.

Nº	Documentos y Registros	ISO 22301	ISO 27001	Anexos
1	**Procedimiento para identificación de requisitos**	4.2	A.15.1.1	Anexo 1
2	Apéndice 1: Lista de requisitos legales, normativos, contractuales y de otra índole.	4.2	A.15.1.1	Anexo 1.1
3	**Política de la Continuidad del Negocio.** **Alcance del Sistema de Gestión de Continuidad del Negocio.** **Objetivos de la Continuidad del Negocio.**	4.1, 4.3, 5.3, 6.2, 9.1.1	A.14.1.1, A.14.1.4	Anexo 2
4	**Plan de capacitación y concienciación.**	7.2	5.2.2, A.8.2.2	Anexo 3
5	**Metodología para el análisis del impacto en el negocio.**	8.2.1, 8.2.2	A.14.1.2	Anexo 4
6	Apéndice 1: Cuestionario sobre el análisis del impacto en el negocio.	8.2.1, 8.2.2	A.14.1.2	Anexos: 4.1 (a) 4.1 (b) 4.1 (c)

7	**Estrategia de Continuidad del Negocio.**	8.2.2	A.14.1.2	Anexo 5
8	Apéndice 1: Lista de actividades	8.2.2	A.14.1.2	Anexo 5.1
9	Apéndice 2: Prioridades de recuperación para las actividades	8.2.2	A.14.1.2	Anexo 5.2
10	Apéndice 3:Objetivos de tiempo de recuperación para actividades	8.2.2	A.14.1.2	Anexo 5.3
11	Apéndice 4: Ejemplos de escenarios de incidentes disruptivos	8.5	A.14.1.2	Anexo 5.4
12	Apéndice 5: Plan de preparación para Continuidad del Negocio	6.2		Anexo 5.5
13	Apéndice 6: Estrategia de recuperación de actividad	8.3	A.14.1.2	Anexos: 5.6 (a) 5.6 (b) 5.6 (c)
14	**Plan de Continuidad del Negocio.**	8.4	A.14.1.3	Anexo 6
15	Apéndice 1: Plan de respuesta a los incidentes	8.4.3, 8.4.4	A.14.1.3	Anexo 6.1
16	Apéndice 2: Registro de incidentes	8.4.3	A.13.2.2	Anexo 6.2
17	Apéndice 3: Lista de ubicaciones para Continuidad del Negocio	8.4.4	A.14.1.3	Anexo 6.3
18	Apéndice 4: Plan de transporte	8.3.2	A.14.1.3	Anexo 6.4

19	Apéndice 5: Contactos clave	8.4.3	A.14.1.3	Anexo 6.5
20	Apéndice 6: Plan de recuperación de actividad	8.4.5	A.14.1.3	Anexos: 6.6 (a) 6.6 (b) 6.6 (c)
21	**Plan de prueba y verificación.**	8.5	A.14.1.5	Anexo 7
22	Apéndice 1: Formulario - Informe de prueba y verificación.	8.5	A.14.1.5	Anexo 7.1
23	**Formulario de revisión post incidente.**	9.1.2		Anexo 8
24	**Plan de mantenimiento y revisión del SGCN, resultados de supervisión y medición.**	9.1.2	A.14.1.5	Anexo 9
25	**Procedimiento para auditoría interna.**	9.2	cláusula 6, A.6.1.8	Anexo 10
26	Apéndice 1: Programa anual de auditoría interna	9.2	cláusula 6	Anexo 10.1
27	Apéndice 2: Informe de auditoría interna	9.2	cláusula 6	Anexo 10.2
28	**Minutas de Revisión por parte de la dirección.**	9.3	cláusula 7	Anexo 11
29	**Procedimiento para acciones correctivas y preventivas.**	10.1	cláusula 8	Anexo 12
30	Apéndice 1: Formulario para acciones correctivas y preventivas	6.1, 9.1.1,	cláusula 8	Anexo 12.1

		10.1		

Adaptado de: (Kosutic, 2015).

1.3.2.2. ¿Cómo definir un documento para continuidad para servicios de TI?

En general para definir un documento para el nuevo modelo de gestión, su contenido se determina a partir de la norma ISO 22301 y de la lista de cláusulas detalladas en la Tabla 1.

La información obligatoria solicitada en la norma ISO 22301, es plasmada en documentos organizados mediante plantillas-formularios. Estos contienen:

- **Lineamientos.-** Definen en contexto los planes, objetivos, políticas, estrategias, metodologías, etc.

- **Registros.-** Creados para control y seguimiento.

- **Apéndices.-** Formularios de apoyo, facilitan manejo de información.

Los formularios deben manejar niveles de confidencialidad, de acuerdo a las políticas de las Empresas e información que se registre sobre éstos, se recomienda manejar 3 niveles:

- **Baja.-** La información es de carácter público, y puede ser visualizada por cualquier empresa o persona.

- **Media.-** Se refiere a la información y documentación manejada únicamente por empleados de la compañía, y que no pueden ser divulgadas de manera externa.

- **Alta.-** Este nivel de confidencialidad se aplica para la información que únicamente debe ser manejada por el área de TI y personal autorizado dentro de la Empresa.

EJEMPLO:

A continuación se detalla los pasos a seguir, para la elaboración de cada uno de los documentos (formularios) considerados en el modelo de Gestión de Infraestructura Tecnológica.

Documento: Procedimiento para identificación de requisitos.

1. Se identifica la norma ISO 22301, 4.2.2 “La organización debe establecer, implementar y mantener procedimiento(s) para identificar, tener acceso a, y evaluar los requisitos legales y reglamentarios aplicables para la organización, relacionados con la continuidad de sus operaciones, productos y servicios, así como los intereses de las partes interesadas pertinentes” (NORMA ISO 22301, 2012).

“…La organización debe documentar esta información y mantenerla actualizada, requisitos legales nuevos o actualizaciones, reglamentarios y otros se comunicarán a los empleados afectados y otras partes interesadas” (Kosutic, 2015).

2. Crear la plantilla, considerando el logo y nombre de la institución.

3. Generar campos para la identificación y registros del documento.

Tabla 3. Identificación y registros del documento.

Código:	
Versión:	

Fecha de la versión:	
Creado por:	
Aprobado por:	
Nivel de confidencialidad:	

Tomado de: (Kosutic, 2015).

Nota: El sistema de codificación del documento debe coincidir con el sistema actual de codificación de documentos de la organización.

4. Generar campos para el registro de las modificaciones al documento, ver Tabla 4.

Tabla 4. Registro de modificaciones.

Fecha	Versión	Creado por	Descripción de la modificación

5. Describir una tabla de contenidos del documento, especificando el contexto de la plantilla. Ver Tabla 5.

Tabla 5. Contenido del documento.

1.	Objetivo, alcance y usuarios
2.	Documentos de referencia
3.	Identificación de requisitos y partes interesadas
4.	Revisión y evaluación
5.	Validez y gestión de documentos
6.	Apéndices

Tomado de: (Kosutic, 2015).

6. Se debe especificar los ítems de la norma asociada a los objetivos del negocio.

El objetivo del presente documento es definir el proceso de identificación de las partes interesadas, de los requisitos legales, normativos, contractuales y de otra índole relacionados con la Continuidad del Negocio y con la seguridad de la información, como también las responsabilidades para su cumplimiento.

7. En esta parte se lista los documentos de referencia relacionados a las normas ISO 22301 y 27001, consideradas para el nuevo modelo de gestión.

- Norma ISO/IEC 27001, control A.15.1.1
- Norma ISO 22301, punto 4.2
- Política del sistema de gestión de seguridad de la información.
- Política de la Continuidad del Negocio.

8. A continuación se identifica los requisitos y partes interesadas del documento, para esto se describe una persona a cargo de la coordinación quien es responsable de:

- Todas las personas u organizaciones que pueden afectar o ser afectadas por la gestión de la seguridad de la información o de la Continuidad del Negocio (partes interesadas).

- Todos los requisitos legales, normativos, contractuales y de otra índole que correspondan.

El responsable definirá los recursos a cargo del cumplimiento de cada requisito individual y qué partes interesadas serán notificadas cuando se produzcan modificaciones; debe enumerar todos los requisitos, partes interesadas y personas responsables en la “Lista de requisitos legales,

normativos, contractuales y de otra índole" (NORMA ISO 22301, 2012) y debe publicarla a las vista de todas las partes involucradas.

9. Luego de listadas las actividades, se debe realizar la revisión y evaluación del documento, revisar la lista de requisitos legales, normativos, contractuales y de otra índole cada cierto tiempo (se recomienda al menos cada 6 meses), actualizar cuando sea necesario, y; evaluar su cumplimiento al menos una vez al año.

10. Establecer un período de validez y evaluación del cumplimiento de sus objetivos, así como de actualizaciones, debiendo efectuarse al menos una vez al año. Para evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- Cantidad de obligaciones de la organización que ya existían pero que no fueron identificadas.

- Cantidad o monto de multas pagadas por el no cumplimiento de obligaciones.

- Cantidad de días de atraso en el cumplimiento de la obligación.

11. En caso de contar con documentación relacionada que facilite el cumplimiento de la plantilla, se describen como apéndices.

- Apéndice: Formulario: Lista de requisitos legales, normativos, contractuales y de otra índole.

12. Finalmente todo documento debe contar con el nombre y firma del coordinador del SGCN, y/o responsable a cargo (se sugiere con tinta azul).

Tabla 6. Firma del documento.

[Cargo del responsable] [Nombre del responsable]   _____ [Firma]

Tomado de: (Kosutic, 2015).

2. MODELO DE GESTIÓN DE CONTINUIDAD DE INFRAESTRUCTURA TECNOLÓGICA PARA LA OPERACIÓN DE SERVICIOS DE TI EN EMPRESAS FINANCIERAS.

2.1. Desarrollo del nuevo modelo de gestión sobre la base de las normas ISO 22301 e ISO 27001

2.1.1. Descripción de Empresas Financieras en el Ecuador

El Sistema Financiero Nacional controlado por la Superintendencia de Bancos, está conformado por: bancos privados, mutualistas, sociedades financieras y banca pública en el Ecuador, estas empresas se dedican a brindar servicios transaccionales, constituyendo los bancos el sector más significativo puesto que cubren más del 90% de las operaciones de todo el sistema (Tobar, 2004).

Según la Asociación de Bancos Privados del Ecuador, la seguridad es un aspecto innato para la actividad bancaria, permitiendo que la protección de los sistemas físicos y lógicos adquiera gran relevancia y formen parte de la gestión estratégica de las organizaciones financieras, la importancia de la seguridad de la información no sólo se centra en la necesidad de reducir los riesgos a nivel económico, sino también permite mantener la imagen y la reputación de las Empresas Financieras hacia los clientes, según el Presidente del Comité Ecuatoriano de Seguridad Bancaria “La Banca ecuatoriana cuenta al momento con similares o mejores controles de seguridad que los implementados en otras instituciones del exterior (Asociación de Bancos Privados del Ecuador, 2015)”

De acuerdo al boletín publicado por la SB, el sistema financiero nacional se encuentra en buen estado, alcanzando cifras rentables superiores al año anterior, se atribuye la solvencia de las Empresas Financieras a (Superintendencia de Bancos del Ecuador - SB , 2005) "el incremento de la relación de activos productivos frente al total de activos, fue producto de una mayor tasa de variación de los activos productivos (9,46%), respecto del total

de activos (7,63%), incidiendo dentro del referido comportamiento el incremento de la cartera de créditos"

2.1.1.1. Departamentos de TI (Tecnología de la Información)

El área de Tecnologías de la Información de las Empresas Financieras son gestionadas por los departamentos y Gerentes de TI, éstos departamentos constituyen un eje fundamental en cada una de las empresas, la dimensión de cada área y número de colaboradores depende de la empresa financiera, llegando éstos a construirse por cientos de empleados.

Generalmente la matriz de cada Organización Financiera se encuentran instaladas en las ciudades de fundación y mayor demanda de sus clientes, para los Bancos nacionales en su mayoría se encuentran en las ciudades de Quito y Guayaquil, en el caso de las Cooperativas y Mutualistas pueden estar ubicadas en las diferentes ciudades del territorio Ecuatoriano.

Las áreas y departamentos de TI ubicados en la matriz se encargan de brindar soporte centralizado a cada una de las sucursales, generalmente mediante vía remota a los usuarios, en otros casos la asistencia técnica es manejada por medio de los Outsourcing y gestionada por Administradores especializados.

Las políticas de TI se manejan de forma global para cada Organización, sin embargo éstas se encuentran adaptadas según las necesidades de cada sucursal y oficina remota, las políticas internas en varios casos son auditadas por organismos y certificaciones internacionales tales como PCI DSS (Payment Card Industry Data Security Standard).

2.1.1.2. Esquema Organizacional del departamento de TI

Los Organigramas de las Empresas Financieras varían dependiendo de su estructura y alcance de servicios, sin embargo en la parte de TI existe similitud

en cuanto a sus departamentos de: Infraestructura, seguridades, soporte y desarrollo.

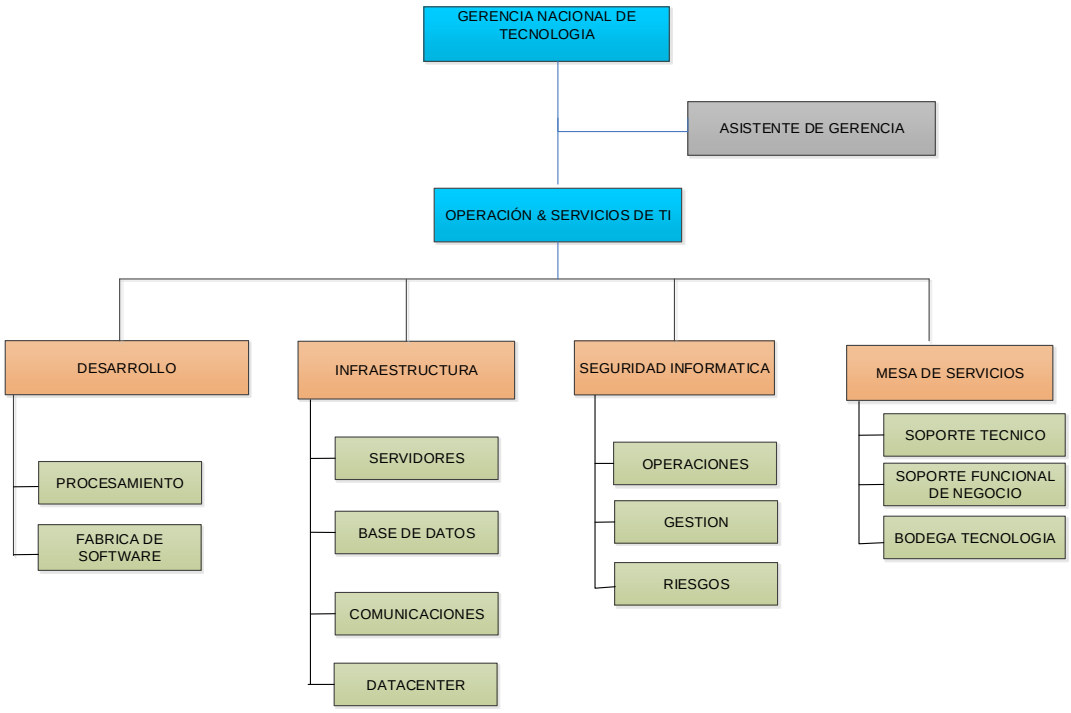

Figura 2. Organigrama Estructural de Tecnología para Empresas Financieras.

En la Figura 2, se describe un ejemplo común de esquema organizacional tecnológico y sus departamentos de TI dentro de instituciones financieras.

2.1.1.3. Descripción de los servicios que soportan los departamentos de TI.

De acuerdo al giro de negocio, las políticas y estándares informáticos globales regulatorios, las áreas de TI en el Ecuador se segmenta generalmente en 4 grandes bloques: Desarrollo, Seguridades Informáticas, Infraestructura y Help Desk, donde:

Desarrollo: Esta área busca ejecutar aplicativos, módulos que permitan cubrir las necesidades Tecnológicas de los usuarios internos y externos, asegurando el funcionamiento de los mismos, basados en condiciones normales y de excepción dentro de los tiempos y costos establecidos por la Organización.

Seguridad Informática: Los esquemas y procedimientos asociados al riesgo operativo se encuentran bajo ésta área, encargada de mitigar los riesgos ante amenazas que pueden vulnerar los sistemas de seguridad de las Organizaciones, establecen procedimientos y procesos tanto a nivel interno como externo.

Help Desk: Esta área se encarga de gestionar y direccionar los requerimientos y ayuda para los usuarios, brindando soporte remoto o presencial: La ejecución de procesos de soporte demandan un profundo conocimiento del negocio, del entorno y las políticas que gobiernan a cada Empresa Financiera:

Infraestructura: Encargada de administrar, gestionar el servicio de hardware de: aplicaciones, comunicaciones y seguridades que garanticen la operación del negocio, mediante "procedimientos definidos y personal responsable, innovador, dinámico con capacidad de optimizar el uso de la plataforma tecnológica (Arevalo, 2015)".

2.1.1.4. Infraestructura tecnológica que aporta al giro de negocio

Las instituciones financieras a nivel Nacional cuentan con sistemas y componentes tanto en hardware como software, que permiten mantener operativos sus servicios ofertados a los clientes, estos sistemas se encuentran apalancados en áreas o departamentos de TI. En la Figura 3 se muestra los departamentos e infraestructura necesaria que permite garantizar operatividad tecnológica.

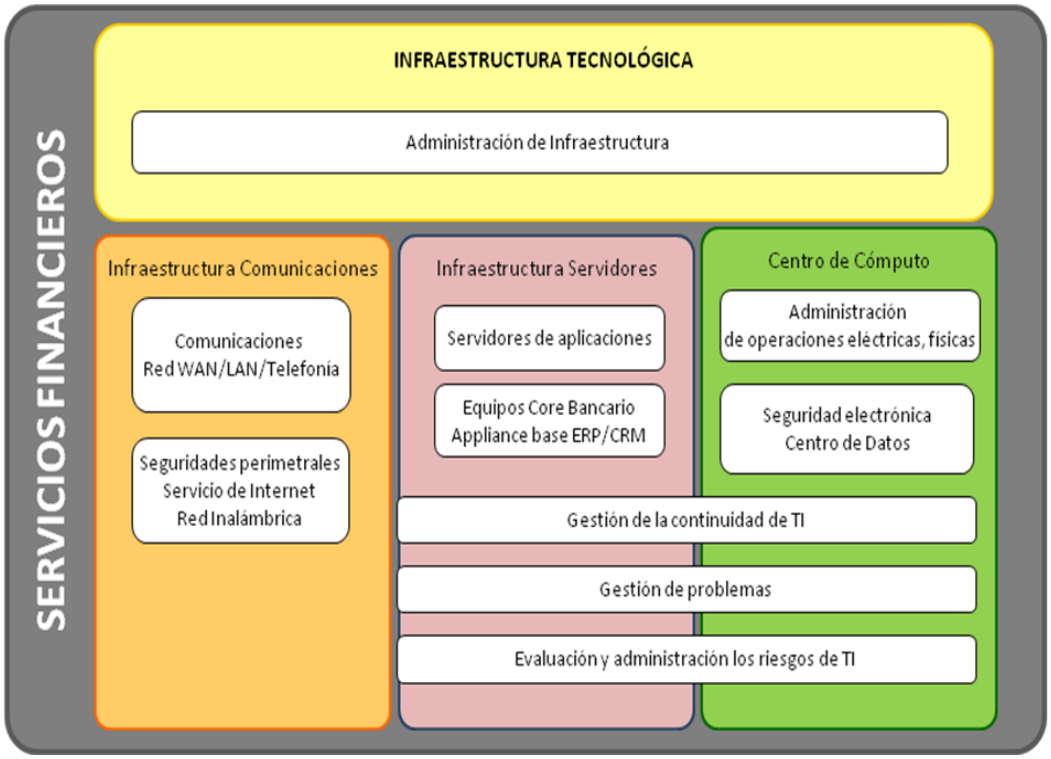

Figura 3. Infraestructura tecnológica crítica.

2.1.1.5. Servicios de TI que apalancan las áreas de negocio

A continuación se lista los servicios tecnológicos soportados por el departamento de TI para cada área (Ver Tabla 8), que aportan directamente a los objetivos del negocio de las Empresas Financieras, para mejor identificación se clasifican según su criticidad de acuerdo a la Tabla 7.

Tabla 7. Criticidad de servicios.

Criticidad	Representación
Baja	
Media	
Alta	

Tabla 8. Servicios de TI en organizaciones financieras.

DEPARTAMENTO	SERVICIO DE TI	CRITICIDAD
Financiero	Microsoft Office	Media
	Servidor de Archivos	Alta
	Bases de datos	Alta
	Aplicativos Core Bancario	Alta
	Aplicativos Financieros	Alta
	Aplicativos de gestión externa	Alta
	Mesa de Servicios	Media
	Conexión de red	Alta
	Carpetas compartidas	Baja
	Impresoras, copiadoras	Media
	Internet	Media
	Videoconferencia	Baja
	Telefonía fija	Media
Negocios	Microsoft Office	Media
	Servidor de Archivos	Alta
	Aplicativos Core Bancario	Alta
	Aplicativos de gestión externa	Alta
	Mesa de Servicios	Media
	Conexión de red	Alta
	Impresoras, copiadoras	Baja
	Internet	Media
	Videoconferencia	Media
	Telefonía fija, móvil	Alta
Tecnología	Microsoft Office	Media
	Aplicativos de monitoreo	Alta
	Aplicativos Tecnológicos	Alta
	Mesa de Servicios	Media
	Conexión de red	Alta
	Impresoras, copiadoras	Baja

	Telefonía fija y móvil	Media
Administrativo	Microsoft Office	Media
	Servidor de Archivos	Alta
	Aplicativos Administrativos	Alta
	Aplicativos de gestión externa	Alta
	Mesa de Servicios	Media
	Conexión de red	Alta
	Impresoras, copiadoras	Media
	Internet	Baja
	Telefonía fija y móvil	Media
Recursos Humanos	Microsoft Office	Media
	Telefonía fija, móvil	Media
	Aplicativos de gestión	Alta
	Mesa de Servicios	Media
	Conexión de red	Media
	Impresoras, copiadoras	Baja
	Internet	Media
	Videoconferencia	Baja
Call Center	Microsoft Office	Media
	Servidor de Archivos	Alta
	Bases de datos	Alta
	Aplicativos Core Bancario	Alta
	Aplicativos financieros	Alta
	Aplicativos de gestión	Alta
	Mesa de Servicios	Media
	Conexión de red	Alta
	Carpetas compartidas	Media
	Impresoras, copiadoras	Baja
	Internet	Baja
	Telefonía fija	Alta

Adaptado de: (Kosutic, 2015).

2.1.2. Modelo de gestión

Para desarrollar el modelo de Gestión de Continuidad de Infraestructura Tecnológica para la operación de servicios de TI en Empresas Financieras, se basa en las normas ISO 22301 e ISO 27001, obteniendo de ésta manera un modelo de continuidad integrado con seguridades de la información. El esquema utilizado para el nuevo modelo se basa en el ciclo de Deming Plan-Do-Check-Act (PDCA por sus siglas en inglés) (NORMA ISO 22301, 2012).

Figura 4. Ciclo de Deming.

Tomado de: (NORMA ISO 22301, 2012)

Debido a la necesidad de mantener los sistemas siempre disponibles y nunca parar las operaciones y servicios del negocio, se establece el presente modelo de gestión, el cual considera la operación de servicios de TI dentro de las Empresas Financieras, el modelo se encuentra soportado sobre Arquitecturas Tecnológicas con procesos Ad Hoc “Los procesos Ad Hoc consisten en una serie de actividades que no tienen un orden o un ejecutante definido” (Bizagi, 2011).

De acuerdo a las necesidades identificadas para las Empresas Financieras en el Ecuador, éste esquema se encuentra mapeado de manera que sea aplicable a la realidad de los departamentos de TI y el área de Infraestructura Tecnológica en sus operaciones de servicios.

El modelo de gestión se basa en el análisis de impacto en el negocio de las Empresas Financieras, desarrollado en base a la criticidad de la Infraestructura Tecnológica que soportan los principales aplicativos que brindan servicios de TI a la Organización y a la evaluación de riesgos de afectación para los servicios entregados por TI.

En la Figura 5 se muestra el Ciclo PDCA aplicado al proceso de Continuidad del Negocio, y como el SGCN "toma insumos de las partes interesadas, requerimientos para la gestión de la continuidad, y a través de las necesarias acciones y procesos produce resultados de continuidad para cumplir con los requerimientos" (NORMA ISO 22301, 2012).

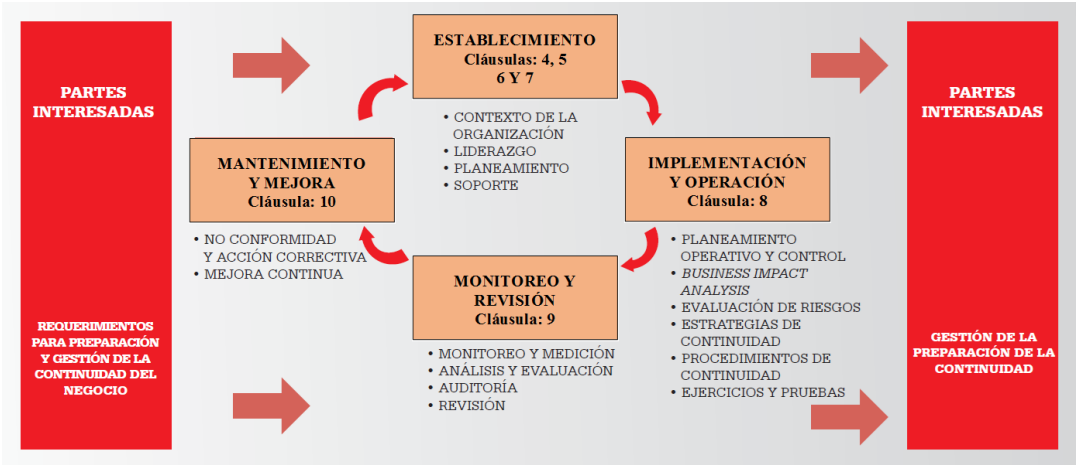

Figura 5. Ciclo PDCA aplicado al proceso de Continuidad del Negocio.

Tomado de: (Alexander, 2012).

2.1.2.1. Fase de Planificación

En la etapa de Planificación (Plan) se definen los objetivos estratégicos y tácticos del modelo, labores administrativas y operativas necesarias para el cumplimiento de dichos objetivos; así como la identificación de requerimientos y preparación de todos los elementos necesarios para la Continuidad del Negocio, el modelo considera los activos de Infraestructura Tecnológica como activos del negocio de tal forma que la continuidad de infraestructura tecnológica constituye la Continuidad del Negocio. En la Tabla 9 se describe los documentos relacionados a ésta fase.

Tabla 9. Documentos - Fase de Planificación.

Nº	Documentos y Registros
1	**Procedimiento para identificación de requisitos.**
2	Apéndice 1: Lista de requisitos legales, normativos, contractuales y de otra índole.
3	**Política de la Continuidad del Negocio.** **Alcance del Sistema de Gestión de Continuidad del Negocio.** **Objetivos de la Continuidad del Negocio.**
4	**Plan de capacitación y concienciación.**

Adaptado de: (Kosutic, 2015).

Procedimiento para identificación de requisitos:

Define el proceso de identificación de las partes interesadas, requisitos legales, normativos, contractuales y de otra índole, relacionados con la seguridad de la información y con la continuidad de la Infraestructura Tecnológica, como también las responsabilidades para su cumplimiento; se considera usuarios del

documento a todos los empleados de la empresa financiera puesto que todos consumen servicios de TI.

Lista de requisitos legales, normativos, contractuales y de otra índole:

Describe los requisitos legales, normativos, contractuales y de otra índole, especificando el recurso responsable a cargo y los tiempos considerados para su obtención, es aplicado a todo el Sistema de Gestión de Continuidad del Negocio (SGCN).

Política de la Continuidad del Negocio:

El documento tiene por propósito definir el objetivo, alcance y reglas básicas para la gestión de la Continuidad del Negocio de las Empresas Financieras, su estructura completa se muestra en el Anexo 2.

El objetivo de la gestión de la Continuidad del Negocio es identificar potenciales amenazas en las Empresas Financieras y los impactos que estas amenazas podrían tener sobre las operaciones de negocios; otro propósito es proporcionar un marco de referencia para establecer capacidad de respuesta efectiva ante afectaciones a la Continuidad del Negocio.

Para implementar la Gestión de Continuidad de Infraestructura Tecnológica para la operación de servicios de TI en Empresas Financieras sobre la base de las normas ISO 22301 e ISO 27001, se debe basar en los requisitos enumerados en la lista de requisitos legales, normativos, contractuales y de otra índole.

El encargado de garantizar que la gestión de la continuidad de Infraestructura Tecnológica sea establecida e implementada de acuerdo con esta Política y de proporcionar los recursos necesarios, es responsable de definir los objetivos

para todo el SGCN y el método para medir el cumplimiento de los mismo, los objetivos deben ser revisados al menos una vez por año.

Para cumplir estos objetivos se detallan acciones en el Plan de preparación para Continuidad del Negocio, en las acciones correctivas y preventivas según el Procedimiento para acciones correctivas y preventivas y en la Revisión por parte de la dirección.

El Sistema de gestión de la continuidad de Infraestructura Tecnológica se implementa para toda la organización, con especial atención sobre las actividades identificadas durante el Análisis de impactos en el negocio.

Todas las actividades relacionadas con los productos y servicios críticos de las Empresas Financieras, deben estar detalladas en la Estrategia de Continuidad de Infraestructura Tecnológica.

Responsabilidades específicas:

- El encargado de adoptar e implementar la continuidad de Infraestructura Tecnológica, también se encarga del Plan de capacitación y concienciación que corresponde a todas las personas que cumplen una función en la gestión de la continuidad.

- Al menos una vez por año deben ser probados y verificados los preparativos relacionados con la continuidad de la Infraestructura Tecnológica, utilizando diversos métodos para evaluar si pueden proteger a las actividades de la organización.

- Para ello, el encargado debe redactar un Plan de prueba y verificación que debe ser aprobado por la alta dirección. Luego de cada prueba y verificación, se debe elaborar un Informe de prueba y verificación.

- Se debe adoptar e implementar el Plan de mantenimiento y revisión del SGCN para que todos los elementos del SGCN estén operativos y actualizados.

- Cuando se activa un Plan de continuidad de Infraestructura Tecnológica, el encargado es el responsable de supervisar la eficacia de la gestión de la continuidad de los sistemas críticos y servicios asociados al negocio.

- Se debe supervisar las no conformidades, falsas alarmas, incidentes reales, etc. y de elevar las acciones preventivas necesarias.

2.1.2.2. Fase de Realización

Esta fase es el Do (hacer), se encuentra compuesta por los requerimientos de la sección 8 de la norma ISO 22301, se procede con la implementación del modelo basado en actividades establecidas en la Tabla 10, constituye la fase más larga del modelo en términos de tiempo y complejidad.

Tabla 10. Documentos - Fase de Realización.

Nº	Documentos y Registros
5	**Metodología para el análisis del impacto en el negocio.**
6	Apéndice 1: Cuestionario sobre el análisis del impacto en el negocio.
7	**Estrategia de Continuidad del Negocio.**
8	Apéndice 1: Lista de actividades.
9	Apéndice 2: Prioridades de recuperación para las actividades.
10	Apéndice 3: Objetivos de tiempo de recuperación para actividades.

11	Apéndice 4: Ejemplos de escenarios de incidentes disruptivos.
12	Apéndice 5: Plan de preparación para Continuidad del Negocio.
13	Apéndice 6: Estrategia de recuperación de actividad.
14	**Plan de Continuidad del Negocio.**
15	Apéndice 1: Plan de respuesta a los incidentes.
16	Apéndice 2: Registro de incidentes.
17	Apéndice 3: Lista de ubicaciones para Continuidad del Negocio.
18	Apéndice 4: Plan de transporte.
19	Apéndice 5: Contactos clave.
20	Apéndice 6: Plan de recuperación de actividad.

Adaptado de: (Kosutic, 2015).

Metodología para el análisis del impacto en el negocio:

El objetivo de este documento es definir la metodología y el proceso para evaluar los impactos de la interrupción de las actividades de las Empresas Financieras, y; determinar prioridades y objetivos de continuidad y de recuperación.

El análisis del impacto en el negocio se aplica a todo el alcance del Sistema de Gestión de Continuidad del Negocio. Cuando existe una afectación sobre la Infraestructura Tecnológica, el análisis del impacto en el negocio se implementa a través del “Cuestionario sobre el análisis del impacto en el negocio” (Anexo 4.1). El proceso es coordinado por el responsable y el análisis de las actividades individuales es realizado por la persona signada a cada actividad.

Impactos en el negocio:

El análisis del impacto en el negocio se realiza basado en la evaluación de riesgos, para que la información sobre los recursos necesarios pueda ser utilizada a partir de dicha evaluación. Los impactos del incidente disruptivo (ruptura brusca) sobre una actividad son evaluados a través de:

- **Impactos generales (evaluación cualitativa):** Permiten identificar la afectación de los procesos operativos de las Empresas Financieras.

- **Impacto financiero (evaluación cuantitativa):** Determina el impacto en términos de magnitud de daños económicos para las Empresas.

Ambos impactos deben ser evaluados para los siguientes períodos de tiempo:

- 1 hora
- 2 horas
- 4 horas
- 24 horas
- 48 horas
- 1 semana

Si alguna actividad es menos urgente, se pueden alargar los períodos para esa actividad particular; por ejemplo de 4 horas a 2 semanas, lo cual nos permite identificar el tiempo disponible para recuperar los sistemas y recursos una vez ocurrida la interrupción RTO (Recovery Time Objective).

Para la evaluación de la afectación de los servicios, los impactos se clasifican de la siguiente forma: (Tabla 11).

Tabla 11. Impactos del Negocio.

Consecuencia insignificante	1	La duración del incidente disruptivo no afecta significativamente las finanzas, las obligaciones legales o contractuales o el prestigio de la organización.
Consecuencia aceptable	2	La duración del incidente disruptivo provoca daños sobre las finanzas, las obligaciones legales o contractuales o el prestigio de la organización, pero ese daño todavía es aceptable teniendo en cuenta su magnitud y circunstancias específicas.
Consecuencia crítica	3	La duración del incidente disruptivo provoca daños sobre las finanzas, las obligaciones legales o contractuales o el prestigio de la organización y ese daño no es aceptable por su magnitud y circunstancias específicas.
Consecuencia catastrófica	4	La duración del incidente disruptivo provoca grandes daños sobre las finanzas, las obligaciones legales o contractuales o el prestigio de la organización que le harán perder la mayor parte de su capital y/o tendrá que cancelar sus operaciones en forma permanente.

Tomado de: (Kosutic, 2015).

Pérdida máxima de datos:

Para cada aplicación y servicio identificado en el análisis de servicios de TI, es necesario evaluar la cantidad máxima de datos que se pueden perder RPO

(Recovery Point Objective). La pérdida de datos se evalúa por la cantidad de datos creados o almacenados en las últimas horas:

- 1 hora
- 4 horas
- 24 horas
- 48 horas
- 1 semana

Análisis del impacto en el negocio:

El Análisis del impacto en el negocio establece cuantas actividades sostienen a servicios críticos de TI, de acuerdo a las consultas realizadas se establece que el período máximo tolerable de interrupción para negocios de tipo bancario (interrupción máxima aceptable) para cada actividad es determinado en el Cuestionario sobre el análisis del impacto en el negocio.

El impacto de la pérdida de datos se clasifica de la siguiente forma (Tabla 12):

Tabla 12. Clasificación de impacto.

Consecuencia insignificante	1	La cantidad de datos perdidos no afecta significativamente las finanzas, las obligaciones legales o contractuales o el prestigio de la organización.
Consecuencia aceptable	2	La cantidad de datos perdidos provoca daños sobre las finanzas, las obligaciones legales o contractuales o el prestigio de la organización, pero ese daño todavía es aceptable teniendo en cuenta su magnitud y circunstancias específicas.

Consecuencia crítica	3	La cantidad de datos perdidos provoca daños sobre las finanzas, las obligaciones legales o contractuales o el prestigio de la organización y ese daño no es aceptable teniendo en cuenta su magnitud y circunstancias específicas.
Consecuencia catastrófica	4	La cantidad de datos perdidos provoca grandes daños sobre las finanzas, las obligaciones legales o contractuales o el prestigio de la organización que le harán perder la mayor parte de su capital y/o tendrá que cancelar sus operaciones en forma permanente.

Tomado de: (Kosutic, 2015).

Cuestionario sobre el análisis del impacto en el negocio:

El cuestionario para el análisis del impacto en el negocio considera fundamentalmente la criticidad, basada en las consecuencias para los servicios ofrecidos por las Empresas Financieras.

Estrategia de Continuidad del Negocio:

Define cómo las Empresas Financieras garantizan, se cumplan todas las condiciones para reanudar las actividades relacionadas con Infraestructura Tecnológica ante un incidente disruptivo. Constituye la base para preparar el plan de Continuidad del Negocio y los planes de recuperación. Los usuarios de este documento son miembros de la alta dirección y personas que implementan el proyecto de gestión de la continuidad de Infraestructura Tecnológica (Ver Anexo 5).

Recuperación de actividades:

Para ésta actividad se debe designar un Gerente de recuperación; esta persona será responsable para la recuperación de los servicios ofrecidos por TI, se considera un tiempo de recuperación para esta actividad máximo en días, siendo el normal dado en horas.
A continuación se lista las actividades y su orden de recuperación:

1. **Recuperación de las actividades y servicios de TI en una ubicación alternativa:** reubicación de todos los recursos o actividades en una ubicación alternativa.

2. **Recuperación interna:** traslado de una actividad de gestión operativa a otra unidad organizativa.

3. **Externalización:** traslado de actividades de negocio a un socio.

4. **Reducción en la entrega de servicios:** reducción de la capacidad del servicio en volúmenes normales o entrega de servicios con lentitud.

Para la recuperación de las actividades de TI, se debe considerar la participación del personal capacitado e infraestructura necesaria, basado en el análisis de impacto en el negocio en la Tabla 13 se muestran los principales recursos requeridos.

Tabla 13. Recursos requeridos para la recuperación de actividades.

Nombre del recurso	Descripción	Cantidad	Cuándo es necesario el recurso
Personas:			
Aplicaciones de Core Bancario:			

Aplicaciones Financieras:			
Aplicaciones Administrativas:			
Bases de datos:			
Servidores Core:			
Servidores Web:			
Equipos de Red:			
Equipos de Seguridades:			
Telefonía:			
Equipos de seguridad electrónica:			
Sistema eléctrico:			
Canales de comunicación:			
Otros equipos:			
Instalaciones físicas:			
Servicios externos:			

Para la recuperación de recursos involucrados en la operación de Infraestructura Tecnológica se debe ejecutar como se muestra a continuación:

a) Adquisición previa e instalación del equipo en la ubicación alternativa: si el objetivo del tiempo de recuperación es corto, y si se trata de un equipo complejo (por ej., los servidores Core), será necesario instalarlo con anticipación, independientemente de que ocurra o no un potencial incidente (esquemas de alta disponibilidad).

b) Adquisición del equipo fuera de la organización: si este tipo de equipo existe en el mercado y es posible adquirirlo dentro del objetivo de tiempo de recuperación (por ejemplo; la adquisición de servidores en modalidad renta).

c) Uso de los servicios externalizados: si es demasiado costoso adquirir el equipo con antelación y/o es imposible adquirirlo dentro de un plazo tan corto, puede ser posible utilizar un servicio externo (por ejemplo alojamiento del sitio Web).

d) Documentar detalladamente los procedimientos para las actividades: esto permitirá que otras personas sean capaces de llevarlas a cabo.

e) Capacitar a los empleados o socios para una variedad de tareas.

f) Compartir los conocimientos o habilidades clave entre varias personas para dispersar el riesgo.

g) Utilizar proveedores externos para determinadas actividades ante el caso de indisponibilidad de los empleados de la organización.

h) Planificar reemplazos en caso de la no disponibilidad de ciertos empleados: los reemplazantes pueden ser personas de la misma área o personas que se encuentran más cerca de la ubicación alternativa.

i) Administrar el conocimiento de los ex-empleados y de los empleados actuales, de los proveedores y socios y documentarlo en diversas bases de conocimiento.

Procedimiento para copias de seguridad:

Para mantener los registros e información actualizada ante incidentes, es indispensable establecer repositorios de almacenamiento, donde se guarden

las copias de seguridad de los datos utilizados por esta actividad. En la parte baja se presenta un cuadro sugerido.

Tabla 14. Copias de la información.

Nombre de la aplicación, base de datos, carpeta, documento:	Frecuencia para creación de copias de seguridad	Procedimiento para copias de seguridad
Aplicaciones de Core Bancario Aplicaciones Financieras Aplicaciones Administrativas Bases de datos Financieras Bases de datos Administrativas Bases de datos de gestión Bases de datos de operaciones Bases de datos de clientes Aplicaciones Web Sistemas operativos	La frecuencia se determina de acuerdo a los resultados del cuestionario sobre el análisis del impacto en el negocio, ésta varía dependiendo de cada entidad financiera. La dinámica de las transacciones a obligado a las instituciones financieras a mantener los datos financieros de sus clientes actualizados en tiempo real, es decir se realizan copias cada 5min; para documentación e información no	a) Aplicaciones / bases de datos: procedimiento de respaldo automatizado basado en servidor; b) Documentos electrónicos: almacenamiento en carpetas de Intranet para las cuales se crean copias de seguridad en forma automática; c) Documentos en papel: recepción de todos los documentos de fax

Otras aplicaciones	considerada como crítica se pueden realizar copias 1 vez por semana o 1 al mes.	por medios electrónicos, o escaneo o copia de los documentos y almacenamiento en dos lugares separados.

Adaptado de: (Kosutic, 2015).

Lista de ubicaciones para continuidad de la Infraestructura Tecnológica:

Registra toda la información geográfica que permita ubicar a los recursos antes, durante y después del incidente.

Tabla 15. Ubicación de puntos de reunión.

Nombre de la actividad	Domicilio de la ubicación principal	Punto de encuentro 1	Punto de encuentro 2	Ubicación alternativa
Centro de crisis				
Nombre de la actividad 1				
Nombre de la actividad 2				

Tomado de: (Kosutic, 2015).

Plan de transporte:

En el Anexo 6.4 se detalla el plan de transporte para ingresa a operar, cuando se activen planes de recuperación, el transporte se organizará de la siguiente manera:

- **Ubicación de partida:**

  Se define las ubicaciones principales o puntos de encuentro, desde donde se movilizará.

- **Ubicación de destino:**

  Identifica el lugar de llegada (Centro de Crisis).

- **Quién o qué es transportado:**

  En caso de transportar gente, es necesario informar el nombre de su actividad o unidad organizativa y la cantidad de personas; si se transportan materiales o equipos, se debe especificar los elementos y cantidades de los mismos.

Persona responsable de la coordinación:

Es el responsable de coordinar el transporte en la organización, informa números de teléfono de contacto.

Medios de transporte:

Se debe detallar el tipo de transporte, por ejemplo, bus alquilado, taxi, transporte público, etc. Si las dos ubicaciones están cerca entre sí, la gente puede ir a pie.

Transportista:

Es la persona que realizará el transporte, pudiendo ser un empleado de la empresa financiera o una persona externa a la organización. Debe informar su número de teléfono de contacto.

Contactos clave:

Este documento se utiliza para registrar los contactos para recuperación. Los contactos clave son:

- Los miembros del Gabinete de crisis,
- Los miembros del Gabinete de apoyo de crisis,
- Gerentes de recuperación de actividades,
- Sus reemplazantes.

El formulario de contactos clave debe ser archivado en todas las ubicaciones en las que esté archivado el Plan de continuidad de Infraestructura Tecnológica, estos datos también deben ser guardados en los teléfonos móviles de los contactos.

Es importante que todas las personas clave tengan contacto con todas las demás personas clave con quienes tienen que implementar los planes. En caso de no ser posible almacenar los datos en teléfonos móviles, se recomienda imprimirlos en pequeñas hojas de papel y entregarlos a todas las personas clave para que lo lleven en sus billeteras.

2.1.2.3. Fase de verificación

Esta tercera fase denominada Check (Verificar) se encarga de comprobar que todas las tareas efectuadas en la fase anterior, fueron realizadas de forma correcta siguiendo la planificación y objetivos definidos e identificando cualquier desviación. Todas las actividades de verificación deben generar un tipo de evidencia, en la Tabla 16 se describen los documentos necesarios para ésta etapa.

Tabla 16. Fase de verificación.

Nº	Documentos y Registros
21	**Plan de prueba y verificación.**
22	Apéndice 1: Formulario - Informe de prueba y verificación.
23	**Formulario de revisión post incidente.**
24	**Plan de mantenimiento y revisión del SGCN, resultados de supervisión y medición.**
25	**Procedimiento para auditoría interna.**
26	Apéndice 1: Programa anual de auditoría interna
27	Apéndice 2: Informe de auditoría interna
28	**Minutas de Revisión por parte de la dirección.**

Adaptado de: (Kosutic, 2015).

Plan de prueba y verificación:

El objetivo de este Plan es determinar la frecuencia y los métodos de verificación para evaluar la factibilidad de las medidas y de los arreglos para la gestión de la Continuidad del Negocio, como también para establecer las acciones correctivas necesarias.

Este Plan debe contener un alcance de las pruebas, donde se aplica a todos los elementos que se encuentran dentro del alcance del SGCN, incluyendo los arreglos con los proveedores y socios de las Empresas Financieras.

La revisión de los resultados, deben incluir las acciones correctivas correspondientes, como también otras recomendaciones de mejora con su respectivo registro para el control de los resultados.

Plan de mantenimiento y revisión:

Este Plan permite mantener la exactitud y utilidad de todos los elementos del SGCN, siendo necesario para ello la revisión y actualización de acuerdo a un plan de frecuencias mostradas en el Anexo 9.

El Coordinador del SGCN será responsable del registro y archivo del plan, así como de la modificación y actualización del documento.

Procedimiento de auditoría interna:

Describe todas las actividades relacionadas con la auditoría: redacción del programa de auditoría, selección del auditor, realización de auditorías individuales e informes.

Por otro lado determina si los procedimientos, controles, procesos, acuerdos y demás actividades dentro del SGSN concuerdan con las normas ISO 22301 e ISO 27001, con las regulaciones y documentación interna manejadas por las Empresas Financieras.

El procedimiento se aplica a todas las actividades realizadas dentro del Sistema de Gestión de Continuidad del Negocio (SGCN). Se recomienda realizar al menos 1 auditoría por año y debe cumplir:

- Especificar fechas planificadas y de realización para la auditoría.
- Especificar el alcance de la auditoría áreas, procesos, etc.
- Criterios de auditoría (normas, disposiciones legales, documentación interna, obligaciones contractuales y/o normas corporativas).

- Métodos considerados para la auditoría, revisión de documentación, entrevistas con empleados, revisión de registros, de sistemas informáticos, etc.

- Especificar quién o quienes realizarán la auditoría.

Minutas de Revisión por parte de la dirección:

Establece mantener reuniones para revisar la conveniencia, adecuación y eficacia del Sistema de Gestión de Continuidad de Negocio.
Los materiales o información que se revisa en las reuniones son los siguientes:

- Informe de auditorías
- Revisiones sobre proveedores o socios
- Documento o descripción del feedback recibido de las partes involucradas
- Documentos o descripción de los métodos, productos o procedimientos, como también de las nuevas buenas prácticas y lineamientos, que se pueden utilizar para mejorar la eficacia del SGCN.
- Estado de las acciones preventivas y correctivas
- Documento o descripción de las amenazas y vulnerabilidades que no fueron tenidas en cuenta durante la evaluación de riesgos
- Documento del control y evaluación de medición de resultados
- Estado de las actividades de seguimiento que deberían haberse tomado luego de la revisión por parte de la dirección

2.1.2.4. Fase de ajuste

La fase de ajuste es la última del modelo, también llamada Act (Actuar) ejecuta una iteración completa, en caso de evidenciar problemas en esta fase se debe proceder con la corrección, y; realización de acciones que permitan procesos de mejora continua.

Para garantizar los niveles de servicios y efectividad del modelo implementado, la fase de ajuste es fundamental, puesto que si ésta fase no se realiza, no es posible mantener o mejorar la continuidad y seguridad en el futuro, además de constituir la entrada de la etapa de planificación. Los documentos necesarios se describen en la Tabla 17.

Tabla 17. Fase de ajuste.

Nº	Documentos y Registros
29	**Procedimiento para acciones correctivas y preventivas.**
30	Apéndice 1: Formulario para acciones correctivas y preventivas.

Adaptado de: (Kosutic, 2015).

Procedimiento para acciones correctivas y preventivas:

El procedimiento permite describir todas las actividades relacionadas con la iniciación, implementación y mantenimiento de registros de las acciones correctivas y preventivas.

No conformidades y correcciones:

Se debe considerar una no-conformidad como todo incumplimiento de los requerimientos de las normas, documentación interna, reglamentos, obligaciones contractuales y de otra clase dentro del SGCN.

Las no conformidades pueden ser identificadas durante una auditoría interna o externa, en base a resultados de la revisión por parte de la dirección, luego de incidentes, durante el transcurso normal de las operaciones de negocios o en cualquier otra situación.

Acciones correctivas:

Las acciones correctivas pueden ser iniciadas por cualquier empleado o, cuando sea pertinente, por cualquier cliente, proveedor o socio de la organización, pudiendo éstas demandar cambios sobre cualquier documento, proceso o acuerdo dentro del marco del SGSN.

Acciones preventivas:

La acción preventiva permite evitar los efectos no deseados, determinando las actividades orientadas a eliminar la causa de potenciales no-conformidades.

2.2. Proceso de aplicación del modelo

Luego de ocurrido un incidente en la Infraestructura Tecnológica, se establece un proceso que permita a la persona encargada liderar la recuperación operativa de los servicios afectados, pudiendo convocar a una reunión inicialmente solo a los responsables (administradores) de la plataforma afectada para realizar la evaluación del incidente y servicios impactados, una vez realizada la reunión se procederá a decidir si es necesario llamar al todo el equipo del plan de continuidad.

2.2.1. Procedimientos y políticas

Para la aplicación de lo modelo se define políticas que garanticen la ejecución del plan de continuidad de negocio, siendo éstas tipo departamentales (por áreas), que permiten decidir los detalles de implementación del SGCN, coordinar toda la operación de manejo y recuperación, asistir en la resolución de las incidencias presentadas.

Se debe definir acuerdos de nivel de servicio entre los miembros o responsables del área tecnológica y el equipo de diseño y elaboración del plan de continuidad, de tal manera que se desarrolle el proceso con total normalidad

en base a los compromisos realizados. Las implicaciones de las políticas para la continuidad se listan a continuación:

Antes del incidente:

- Las Empresas Financieras deberán contar con un coordinador de continuidad de negocio, quien es la persona encargada de liderar la recuperación operativa de los servicios.

- Para la ejecución del plan de Continuidad del Negocio, se requiere de recursos con alto expertice sobre las plataformas tecnológicas de servicios manejados en la empresa.

- Los miembros del departamento de TI y el equipo de diseño y elaboración del plan de continuidad deberán firmar acuerdos de nivel de servicio y de compromiso, para garantizar el cumplimiento de los procesos.

- La empresa debe aprobar el plan de Continuidad del Negocio.

- Garantizar la disponibilidad de la infraestructura de TI necesaria para la operación de servicios (Centro de Computo Alterno)

- Garantizar que el Plan de Continuidad permanezca actualizado, al menos 1 ves por año.

- Socializar el plan de Continuidad del Negocio con todo el departamento de TI.

- Realizar eventos de capacitación para el personal, que permitan enfrentar incidentes.

- Realizar reuniones para que el equipo de continuidad entienda su rol y responsabilidad dentro del SGCN.

- Efectuar simulacros controlados del modelo

- Asegurar que las pruebas y entrenamiento se ejecuten periódicamente

Durante el incidente:

Una vez ocurrido el evento, el coordinador del equipo de continuidad, debe convocar a los miembros e informar del sitio y hora de reunión.

- El incidente puede ser manejado mediante el plan de Continuidad del Negocio, dentro del centro de cómputo principal apalancado por los esquemas de alta disponibilidad de la Infraestructura Tecnológica, o mediante centros de cómputo alterno (contingencia).

- Debe existir el compromiso y colaboración de todos los miembros de TI a participar activamente en la recuperación de servicios asociados al plan de continuidad.

- Los jefes de cada área del departamento de TI de la empresa determinarán las personas claves, quienes serán los que proporcionen la mayor cantidad de la información que se requiere para recupera la operatividad de los servicios

- Debe existir el compromiso y colaboración de todos los miembros de TI a participar activamente en la recuperación de servicios asociados al plan de continuidad.

- En caso de no contar con el personal clave designado para el SGCN, el coordinador asignará a los empleados de rango alto rango de cada área y que están en posición de dirigir el Plan de Continuidad para que asuman el rol que corresponda.

- El coordinador en conjunto con los otros miembros del equipo de continuidad realizarán el análisis y valoración de afectación de los servicios.

- El Coordinador, declara formalmente la emergencia e informa que el plan de continuidad se ha activado.

- Basado en la información obtenida del análisis y valoración de la afectación, el coordinador con los miembros del equipo de continuidad planifican las actividades para gestionar la contingencia.

- El coordinador junto con los miembros del equipo del SGCN, determinan la manera como se conducirá el plan y que unidades administrativas deben trasladarse físicamente a otras oficinas así como la decisión de activar o no el Centro de Cómputo Alterno.

- El Coordinador monitorea y controla los procesos de recuperación de manera global.

- Los miembros del Equipo de Continuidad, monitorean y controlan los procesos de recuperación en lo que les compete.

- El Coordinador, facilita la adquisición de equipos, servicios y provisiones tomando en cuenta que se trata de una emergencia, que las formalidades pueden entorpecer las acciones de reparación y recuperación de las áreas afectadas.

- El Coordinador, informa permanentemente el Equipo de Manejo de Crisis, del avance de las actividades de recuperación.

- El Coordinador, disminuye las tensiones entre las/os empleados durante la contingencia.

- El Gerente de TI, en base al plan definido, coordina la activación del sitio alterno (Contingencia) para que asuma las instrucciones, supervisa el desarrollo de los procedimientos, coordina, monitorea y controla la recuperación y reconstrucción del Centro de Cómputo Principal.

Después del incidente:

Finalizado el incidente, el coordinador verificará el estado de cada una de las actividades realizadas para la recuperación de los servicios de TI.

- El personal que participa en el plan de Continuidad del Negocio debe mantener estricta confidencialidad sobre la información de la empresa que les sea proporcionada.

- En caso de levantar contingencia en el centro de cómputo alterno, el coordinador en conjunto con los otros miembros del equipo de continuidad, deben revisar y aprobar las actividades requeridas para volver a la normalidad, analizando las horas y fechas probables de retorno, estrategias y prioridades.

- El responsable de la infraestructura de TI afectada, realizará las siguientes actividades para la desactivación del procedimiento de incidente:

1) Verificar y comprobar que la infraestructura y servicios en el centro de cómputo principal ha sido reparado y los servicios están disponibles.

2) Verificar y comprobar la restauración de la información, aplicativos, sistemas operativos y servicios, en el centro de cómputo principal.

3) Asegurar la accesibilidad a las aplicaciones y datos por parte de los usuarios.

4) Autorizar la desactivación del centro alterno (en caso de haberse aplicado)

5) Monitorear el desempeño de los servicios de TI en el centro de cómputo principal

6) Verificar que los procesos de respaldo y recuperación se realizan con normalidad en el centro de cómputo luego de la normalización de servicios.

- El coordinador deberá disponer la realización de una auditoría sobre el resultado de las medidas de acción previstas en el plan de Continuidad del Negocio.

- El coordinador de continuidad dispondrá la recolección de información de daños y pérdidas ocasionadas por el incidente.

- El equipo de continuidad analiza los informes, evalúa los resultados y propone ajustes al plan en caso de ser necesario.

- El coordinador presentará el informe respectivo al equipo de manejo de crisis.

2.2.2. Roles y responsabilidades

El equipo que se encargará de la recuperación y del retorno a la operación de servicios de TI dentro de las Empresas Financieras está definido por el impacto del incidente en el negocio. El número de miembros del equipo de SGCN depende del alcance y la complejidad de cada organización, en base a las actividades y servicios de TI en las Empresas Financieras, se define contar con 12 roles que conformen el equipo de continuidad (ver Figura 6), en el caso de empresas pequeñas un miembro del equipo puede desempeñar hasta 3 roles.

Impacto / Roles	Insignificante	Aceptable	Crítico	Catastrófico
Gerente de Tecnología			X	X
Coordinador de la continuidad del negocio		X	X	X
Responsable de análisis y reporte	X	X	X	X
Responsable de redes y comunicaciones	X	X	X	X
Responsable de sistemas operativos/plataformas	X	X	X	X
Responsable de sistemas de bases de datos	X	X	X	X
Responsable de core bancario/aplicaciones	X	X	X	X
Responsable de control de seguridades	X	X	X	X
Responsable de comunicación y soporte a usuarios			X	X
Responsable de coordinación con outsourcing			X	X
Responsable de pruebas del negocio			X	X
Responsable de personal de apoyo				X

Figura 6. Equipo de Sistema de Gestión de Continuidad del Negocio vs. Impacto.

Tomado de: (Banco KLM, 2015).

La responsabilidad para el éxito de la Continuidad del Negocio es de todos los involucrados, llevando a cumplir y hacer cumplir las políticas de SGCN dentro de cada área. De acuerdo al análisis realizado para las Empresas Financieras su estructura de roles se define a continuación:

1) Gerente de Tecnología
2) Coordinador de la Continuidad del Negocio
3) Responsable de análisis y reporte
4) Responsable de redes y comunicaciones
5) Responsable de sistemas operativos/plataformas
6) Responsable de sistemas de bases de datos
7) Responsable de Core bancario/aplicaciones
8) Responsable de control de seguridades
9) Responsable de comunicación y soporte a usuarios
10) Responsable de coordinación con outsourcing
11) Responsable de pruebas del negocio
12) Responsable de personal de apoyo

2.2.3. Posibles problemas

La capacidad de brindar continuidad a la Infraestructura Tecnológica de TI, puede encontrase con algunos desafíos y complejidades traducidos en problemas; los servicios tecnológicos no pueden ser considerados fiables si no cumplen con los niveles de seguridad y continuidad demandados por las Empresas Financieras. Los principales problemas que se pueden presentar son:

- Falta de personal capacitado y disponible para asumir responsabilidades para implementar el plan de continuidad en caso de incidentes.

- Políticas organizacionales demasiado burocráticas, que dilatan la gestión del plan de continuidad dentro de la empresa.

- Falta de colaboración y compromiso de los miembros del departamento de TI o del equipo del plan de continuidad.

- Objetivos del plan de continuidad mal definidos, poco realistas o inalcanzables, como tiempos de recuperación muy cortos o demasiado largos.

- Falta de difusión del plan de Continuidad del Negocio a todo el departamento de TI.

- Cuando el departamento de TI no está alineado con los objetivos del negocio, el plan de continuidad puede perder su enfoque y objetividad.

- Presencia de factores externos como desastres naturales o huelgas que caoticen la ciudad y estado Ecuatoriano.

3. VALIDACIÓN DEL MODELO DE GESTIÓN

3.1. Descripción del caso de estudio

A continuación se aplicará el modelo de gestión diseñado en el Capítulo II, con esto se corroborará que el modelo de Gestión de Continuidad de Infraestructura Tecnológica para la operación de TI, es aplicable a cualquier Empresa Financiera.

3.1.1. Caso: Banco KLM

Por temas de confidencialidad de la Empresa Financiera elegida para el caso de estudio de esta tesis, en adelante se denominará como Banco KLM. Los datos mostrados reflejan el estado actual de la Organización; respecto de los aplicativos y plataformas manejados en el Banco, “la Organización mantendrá la confidencialidad sobre algunos y se omitirá citarlos” (Banco KLM, 2015).

El Banco KLM es una de las Empresas Financieras más sólidas en el Ecuador, constituye una marca internacional que opera a nivel mundial en más de 190 países, con una amplia red de establecimientos que supera los 13 millones (Banco KLM, 2015).

Una de sus características a nivel de la Empresa es el manejo de la información, la Organización mantiene políticas de uso en toda su cadena de procesos, estas políticas se encuentra alineadas con las normativas de la Superintendencia de Bancos del Ecuador y certificaciones Internacionales, mismas que se describen a continuación:

- **Política de Seguridad:**

  El Banco KLM ha desarrollado una cultura de seguridad de información orientada a proteger los datos de los socios; cumpliendo con los más altos estándares internacionales de seguridad, basados en normas aprobadas de uso de información; lo que garantiza su integridad, confidencialidad y

disponibilidad, complementando con capacitaciones permanentes para garantizar el conocimiento y aplicación de las normas en todos los niveles.

- **Política de Confidencialidad:**

  Existe un código de ética y confidencialidad que establece “nunca entregar datos e información del Socio a terceros, ya sea de carácter contable, administrativo, comercial o reservado” (Banco KLM, 2015).

- **Política de Sigilo Bancario:**

  El Código de Ética de la Compañía contempla un estricto cumplimiento de la obligación de confidencialidad sobre la información financiera de sus Socios, de acuerdo a la norma de Sigilo Bancario impuesta para las instituciones financieras.

- **Política de Transparencia:**

  La información de la Organización, tasas de interés son publicadas en medios de difusión masivos, organizamos de control, sucursales, página web, entre otros.

3.1.1.1. Estado actual de la Infraestructura Tecnológica

Las operaciones del Banco KLM a nivel local iniciaron hace más de 40 años, convirtiéndose desde sus inicios en la principal tarjeta de crédito en el Ecuador, con más de 30 mil establecimientos afiliados y cerca de 500 mil socios (Banco KLM, 2015).

El Banco KLM cuenta con el modelo Operacional de Tecnología mostrado en la Figura 7, el mismo que describe las verticales sobre las cuales operan sus 4

áreas principales, para la gestión del Gobierno de TI mediante estrategias tecnológicas de calidad en la entrega de servicios de TI.

Figura 7. Modelo Operacional de Tecnología Banco KLM.

El Banco KLM ofrece una amplia gama de servicios financieros: tarjetas de crédito, financiamiento, inversiones, seguros y asistencias, siendo su principal producto la tarjeta de crédito. Los servicios se encuentran apalancados en sistemas tecnológicos robustos, medios tecnológicos que facilitan las transacciones de los socios; generando servicios de TI continuos, eficientes, innovadores y de calidad. En la Figura 8 se observa la infraestructura de TI que soporta los servicios tecnológicos de la Organización.

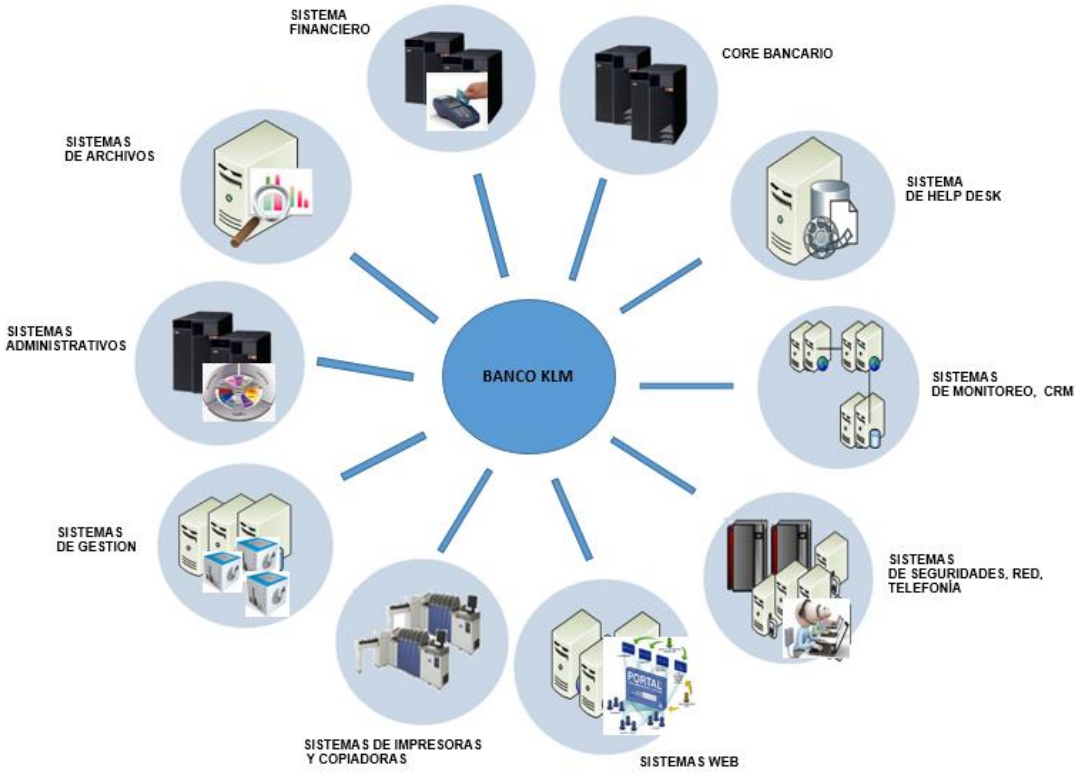

Figura 8. Infraestructura de TI Banco KLM.

Tomado de: (Banco KLM, 2015).

3.1.2. Esquema Organizacional del departamento de TI

El Banco KLM se encuentra compuesto por 4 áreas operacionales descritas en la parte baja, para la validación del modelo nos enfocaremos en el área de Infraestructura y servicios Tecnológicos.

- **Diseño y entrega de servicios**

  Se encarga del desarrollo y entrega de soluciones tecnológicas operativas demandadas por la Organización, enfocándose en la capacidad de entregar soluciones construidas con eficiencia y calidad, basadas en buenas prácticas.

- **Control Tecnológico**

  Esta área se ha convertido en una de las más importantes dentro de la organización, puesto que se encarga de velar por la seguridad informática y datos de los socios, según las normas establecidas por la Superintendencia de Bancos, así como las determinadas por la Empresa, minimizando el riesgo y evitando que usuarios no autorizados puedan acceder a los activos intangibles del Banco.

- **Estrategia y Planeación de servicios**

  Realiza la administración del ciclo de vida de los activos de TI, mediante un control de licencias de software y manejo de hardware, optimizando la utilización de la Infraestructura Tecnológica, alineados con los objetivos empresariales del Banco.

- **Infraestructura y servicios tecnológicos**

  Se encarga de administrar y gestionar el servicio de la Infraestructura Informática que soportan los aplicativos de la Organización, garantizando la continuidad de los servicios de TI para la operación del negocio, mediante procedimientos claros, dinámicos y eficientes que permiten optimizar el uso de la plataforma tecnológica. Para el caso de estudio nos enfocaremos en ésta área.

El Organigrama estructural del departamento de TI para el Banco KLM se representa en la Figura 9.

Figura 9. Organigrama estructural de TI Banco KLM.

Tomado de: (Banco KLM, 2015).

3.1.1.3. Gestión de Infraestructura y servicios

El área de Infraestructura forma parte del área de Producción y Servicios, dentro de sus responsabilidades se encuentra el garantizar un nivel de servicio tecnológico del 99.9% de disponibilidad (Banco KLM, 2015), apalancados en sus departamentos y recursos como se muestra en la Figura 10.

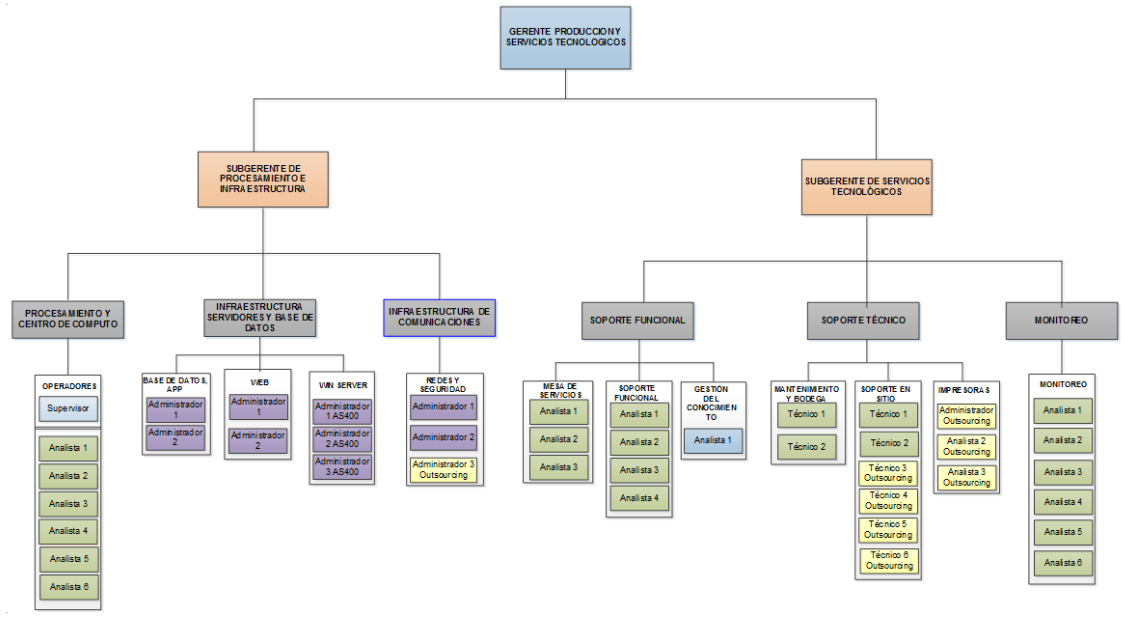

Figura 10. Organigrama de Producción e Infraestructura Tecnológica Banco KLM.

En la Tabla 18 se presenta una breve descripción de los servicios que soporta el Departamento de Infraestructura Tecnológica de TI, y la ubicación donde se encuentran alojados cada uno de ellos, considerando que el Banco KLM posee dos Centros de Computo geográficamente ubicados en diferentes ciudades, donde Quito es el Data Center principal y Guayaquil el secundario.

Tabla 18. Ubicación de Servicios soportados por TI.

SERVICIO DE TI (SERVIDORES)	UBICACIÓN (DATA CENTER)	
Microsoft Office	Principal	
Archivos, BackUps	Principal	Alterno
Bases de Datos	Principal	Alterno
Aplicativos Core Bancario	Principal	Alterno
Aplicativos Financieros	Principal	Alterno
Aplicativos de Gestión Externa	Principal	
Mesa de Servicios	Principal	Alterno

Comunicaciones, enlaces	Principal	Alterno
Seguridad Informática	Principal	Alterno
Carpetas compartidas	Principal	
Impresoras, copiadoras	Principal	
Internet	Principal	Alterno
VPNs	Principal	Alterno
Videoconferencia	Principal	
Central Telefónica	Principal	
Aplicativos de Monitoreo	Principal	Alterno
Aplicativos Tecnológicos	Principal	Alterno
Aplicativos Administrativos	Principal	Alterno
Aplicativos de Gestión	Principal	Alterno

Tomado de: (Banco KLM, 2015).

En la Tabla 19 se lista las áreas relacionadas con la entrega de servicios tecnológicos soportados por el departamento de TI, asociados a los sistemas e infraestructura para su operación diaria.

Tabla 19. Servicios de TI por Áreas.

ÁREA	SERVICIO DE TI
Financiera	Microsoft Office
	Servidor de Archivos, BackUps
	Bases de Datos (Oracle, MySQL, Teradata)
	Aplicativos Administrativos (People Soft, PCSistel)
	Aplicativos Core Bancario (Gestor, Autorizador, Atalla, Datafast)
	Aplicativos Financieros (WedID, CardSource)
	Aplicativos de Gestión Externa (Portero, Seriva)
	Mesa de Servicios (Tivoli)
	Carpetas compartidas

	Impresoras, copiadoras
	Internet
	Videoconferencia
	Comunicaciones, enlaces (Routers, Switches)
	Seguridad Informática (Firewalls, IPS)
	Telefonía fija (Central telefónica, grabador de llamadas)
Negocios	Microsoft Office
	Servidor de Archivos, BackUps
	Aplicativos Core Bancario (Gestor, Autorizador, Atalla, Datafast)
	Aplicativos de Gestión Externa (Portero, Seriva)
	Aplicativos de Gestión (Ticket Launch)
	Mesa de Servicios (Tivoli)
	Impresoras, copiadoras
	Internet
	Videoconferencia
	Seguridad Informática (Firewalls, IPS)
	Telefonía fija, móvil (Central telefónica, grabador de llamadas, bases celulares)
Tecnología	Microsoft Office
	Aplicativos de Monitoreo (Solarwinds, Cisco Prime)
	Aplicativos Tecnológicos (Sharepoint, tursis)
	Mesa de Servicios (Tivoli)
	Comunicaciones, enlaces (Routers, Switches)
	Internet
	VPNs (Cisco ASA, Juniper)
	Impresoras, copiadoras
	Aplicativos de Gestión (Ticket Launch)
	Seguridad Informática (Firewalls, IPS)
	Telefonía fija, móvil (Central telefónica, grabador de

	llamadas, bases celulares)
Administrativa	Microsoft Office
	Servidor de Archivos, BackUps
	Aplicativos Administrativos (People Soft, PCSistel)
	Comunicaciones, enlaces (Routers, Switches)
	Aplicativos de Gestión Externa (Portero, Seriva)
	Mesa de Servicios (Tivoli)
	Impresoras, copiadoras
	Internet
	Seguridad Informática (Firewalls, IPS)
	Telefonía fija, móvil (Central telefónica, grabador de llamadas, bases celulares)
Recursos Humanos	Microsoft Office
	Telefonía fija, móvil (Central telefónica, grabador de llamadas, bases celulares)
	Aplicativos de Gestión (Ticket Launch)
	Mesa de Servicios (Tivoli)
	Comunicaciones, enlaces (Routers, Switches)
	Impresoras, copiadoras
	Internet
	Seguridad Informática (Firewalls, IPS)
	Videoconferencia
Call Center	Microsoft Office
	Servidor de Archivos, BackUps
	Bases de datos (Oracle, MySQL, Teradata)
	Aplicativos Core Bancario (Gestor, Autorizador, Atalla, Datafast)
	Aplicativos Financieros (WedID, CardSource)
	Aplicativos de Gestión (Ticket Launch)
	Mesa de Servicios (Tivoli)
	Comunicaciones, enlaces (Routers, Switches)

	Carpetas compartidas
	Impresoras, copiadoras
	Internet
	Seguridad Informática (Firewalls, IPS)
	Telefonía fija, móvil (Central telefónica, grabador de llamadas, bases celulares)

Tomado de: (Banco KLM, 2015).

3.2. Aplicación del modelo

La aplicación del modelo de gestión se realiza en base a experiencias reales ocurridas en el Banco KLM y el esquema del nuevo modelo diseñado, como resultado de la integración de las normas ISO 22301 e ISO 27001, la información se registra en los formularios creados en el presente plan, dichos documentos se detallan en los Anexos del Proyecto.

Los formularios Anexos contienen toda la información del modelo aplicado al caso de estudio paso a paso, en éstos se puede evidenciar la ejecución de cada una de las Fases, incluyendo la descripción de su contenido, de manera que la implementación para quienes adopten el modelo sea ágil, adaptable y de fácil comprensión.

3.2.1. Fase de Planificación

Se definen los objetivos estratégicos y tácticos, labores administrativas y operativas necesarias para el cumplimiento de los objetivos del Banco KLM; así como la identificación de requerimientos y preparación de todos los elementos necesarios para la Continuidad del Negocio. En la Tabla 20 se describe los formularios Anexos relacionados a ésta fase para el Banco KLM.

Tabla 20. Caso Banco KLM - Fase de Planificación.

Nº	Documentos y Registros	Anexos
1	**Procedimiento para identificación de requisitos**	Anexo 1
2	Apéndice 1: Lista de requisitos legales, normativos, contractuales y de otra índole.	Anexo 1.1
3	**Política de la Continuidad del Negocio.** **Alcance del Sistema de Gestión de Continuidad del Negocio.** **Objetivos de la Continuidad del Negocio.**	Anexo 2
4	**Plan de capacitación y concienciación.**	Anexo 3

Adaptado de: (Kosutic, 2015).

3.2.2. Fase de Realización

Se procede con la implementación del modelo de gestión en el Banco KLM, basado en un análisis de impacto en el negocio y plan de continuidad para la respuesta ante incidentes, actividades detalladas en los formularios Anexos de la Tabla 21.

Tabla 21. Caso Banco KLM - Fase de Realización.

Nº	Documentos y Registros	Anexos
5	**Metodología para el análisis del impacto en el negocio.**	Anexo 4
6	Apéndice 1: Cuestionario sobre el análisis del impacto en el negocio.	Anexos: 4.1 (a) 4.1 (b) 4.1 (c)

7	**Estrategia de Continuidad del Negocio.**	Anexo 5
8	Apéndice 1: Lista de actividades	Anexo 5.1
9	Apéndice 2: Prioridades de recuperación para las actividades	Anexo 5.2
10	Apéndice 3:Objetivos de tiempo de recuperación para actividades	Anexo 5.3
11	Apéndice 4: Ejemplos de escenarios de incidentes disruptivos	Anexo 5.4
12	Apéndice 5: Plan de preparación para Continuidad del Negocio	Anexo 5.5
13	Apéndice 6: Estrategia de recuperación de actividad	Anexos: 5.6 (a) 5.6 (b) 5.6 (c)
14	**Plan de Continuidad del Negocio.**	Anexo 6
15	Apéndice 1: Plan de respuesta a los incidentes	Anexo 6.1
16	Apéndice 2: Registro de incidentes	Anexo 6.2
17	Apéndice 3: Lista de ubicaciones para Continuidad del Negocio	Anexo 6.3
18	Apéndice 4: Plan de transporte	Anexo 6.4
19	Apéndice 5: Contactos clave	Anexo 6.5
20	Apéndice 6: Plan de recuperación de actividad	Anexos: 6.6 (a) 6.6 (b)

		6.6 (c)

Adaptado de: (Kosutic, 2015).

El análisis de impacto en el negocio del Banco KLM, se realiza en base a la criticidad de la Infraestructura Tecnológica que soportan los principales aplicativos que brindan servicios de TI a la Organización, y; la evaluación de riesgos de afectación para los servicios entregados por TI mostrados en la Figura 11.

A continuación se presenta la Matriz de evaluación de impacto para incidentes disruptivos (ruptura brusca) sobre Servicios Tecnológicos en el Banco KLM.

Impacto	Nivel	Riesgo	Afectación
Aceptable	1	Perdida de servicios TI considerados poco críticos (Microsoft Office, Servidor de Archivos, BackUps Impresoras, copiadoras).	El incidente no provoca daños sobre las finanzas, las obligaciones legales, contractuales o el prestigio del Banco.
Crítico	2	Perdida de servicios TI considerados de criticidad media (Aplicativos Administrativos, Financieros y Tecnológicos).	El incidente provoca daños moderados sobre las finanzas, las obligaciones legales, contractuales o el prestigio del Banco.
Catastrófico	3	Perdida de servicios TI considerados de criticidad alta (Comunicaciones, enlaces, Aplicativos Core Bancario y Negocios).	El incidente provoca grandes daños sobre las finanzas, las obligaciones legales o contractuales o el prestigio del Banco. La mayor parte de su capital se pierde y/o tendrá que cancelar sus operaciones en forma permanente.

Figura 11. Matriz de Impacto Vs. Riesgo y Afectación de Servicios TI.

Tomado de: (Banco KLM, 2015).

Para el análisis del impacto, se determinó 3 grupos principales de servicios mapeados con las áreas correspondientes del Banco KLM, los cuales constituyen la columna vertebral de la Organización, y; permiten mantener la operatividad del giro de negocio.

Grupo 1: Comunicaciones, enlaces

- Videoconferencia
- Redes (Routers, Switches)
- Seguridad Informática (Firewalls, IPS)
- Telefonía fija (Central telefónica, grabador de llamadas)
- Telefonía fija, móvil (Central telefónica, grabador de llamadas, bases celulares)
- VPNs (Cisco ASA, Juniper)

Grupo 2: Aplicativos Core Bancario y Negocios

- Cobis
- Gestor
- Autorizador
- Atalla
- Datafast
- Peoplesoft
- WebID
- JD Edwards
- Teradata

Grupo 3: Aplicativos Administrativos, Financieros y Tecnológicos

- Altitud
- Sharepoint
- Adaptive planning
- Mastercard, Visa
- CardSource

- Portero
- Seriva
- Tivoli
- Ticket Launch

El cuestionario para el análisis del impacto en el negocio mostrado en el Anexo 4.1, considera fundamentalmente la disponibilidad de los servicios TI críticos entregados por Infraestructura Tecnológica.

3.2.3. Fase de Verificación

Se comprobó que todas las tareas efectuadas en la fase anterior, fueron realizadas de forma correcta siguiendo la planificación y objetivos definidos por el Banco KLM. En la Tabla 22 se describen los documentos registrados, los mismos que constan como Anexos de la aplicación del modelo diseñado.

Tabla 22. Caso Banco KLM - Fase de Verificación.

Nº	Documentos y Registros	Anexos
21	**Plan de prueba y verificación.**	Anexo 7
22	Apéndice 1: Formulario - Informe de prueba y verificación.	Anexo 7.1
23	**Formulario de revisión post incidente.**	Anexo 8
24	**Plan de mantenimiento y revisión del SGCN, resultados de supervisión y medición.**	Anexo 9
25	**Procedimiento para auditoría interna.**	Anexo 10
26	Apéndice 1: Programa anual de auditoría interna	Anexo 10.1
27	Apéndice 2: Informe de auditoría interna	Anexo 10.2

28	**Minutas de Revisión por parte de la dirección.**	Anexo 11

Adaptado de: (Kosutic, 2015).

3.2.4. Fase de Ajuste

Se ejecutó una iteración completa, considerando correcciones sobre la evidencia de algunos pequeños problemas encontrados, realizando acciones correctivas que permitieron culminar los procesos de mejora continua para el Banco KLM. Los formularios se describen en la Tabla 23 y se encuentran registrados a detalle en los Anexos respectivos.

Tabla 23. Caso Banco KLM - Fase de Ajuste.

Nº	Documentos y Registros	Anexos
29	**Procedimiento para acciones correctivas y preventivas.**	Anexo 12
30	Apéndice 1: Formulario para acciones correctivas y preventivas	Anexo 12.1

Adaptado de: (Kosutic, 2015).

3.2.5. Roles y responsabilidades

De acuerdo a los aplicativos y servicios TI descritos anteriormente para el Banco KLM, las pruebas controladas e incidentes reales presentados en el Banco KLM, se pudo identificar los siguientes cargos y roles en el proceso de recuperación ante un suceso que afecte servicios tecnológicos en producción, Ver Tabla 24.

Tabla 24. Roles y Cargos para el SGCN del Banco KLM.

ROLES	CARGOS (Principal)	CARGOS (BackUp)
Gerente de Tecnología	Gerente de Producción y Servicios	Subgerente de Servicios Tecnológicos
Coordinador de la Continuidad del Negocio	Gerente de Producción y Servicios	Subgerente de Servicios Tecnológicos
Responsable de análisis y reporte	Jefe de Monitoreo	Analista de Monitoreo
Responsable de redes y comunicaciones	Jefe de Comunicaciones	Administrador de Comunicaciones
Responsable de sistemas operativos/plataformas	Subgerente de Procesamiento e Infraestructura	Jefe de Servidores
Responsable de sistemas de bases de datos	Jefe de Servidores	Administrador de Base de Datos
Responsable de Core bancario/aplicaciones	Jefe de Centro de Computo	Supervisor de Centro de Computo
Responsable de control de seguridades	Subgerente de Control Tecnológico	Analista Auditor de Informática
Responsable de comunicación y soporte a usuarios	Jefe de Soporte Técnico	Técnico de Soporte
Responsable de coordinación con outsourcing	Subgerente de Procesamiento e Infraestructura	Jefe de Servidores
Responsable de pruebas del negocio	Subgerente de Servicios Tecnológicos	Jefe de Mesa de Servicios

Responsable de personal de apoyo	Jefe de Mesa de Servicios	Analista de Mesa de Servicios

Tomado de: (Banco KLM, 2015).

Gerente de Nacional de Tecnología:

- Se encarga de asegurar la recuperación de los servicios de TI en el menor tiempo posible, manteniendo eficacia y optimización de costos.

Coordinador de la Continuidad del Negocio:

- Conforma el equipo humano para la Continuidad del Negocio.
- Facilita los recursos de TI para la realización de las actividades, a cada miembro del equipo.
- Asegura la restauración del sitio original afectado en el menor tiempo posible.
- Registra acuerdos con proveedores, pagos, negociaciones con las aseguradoras, adquisición de recursos, etc.
- Realiza simulacros y pruebas periódicamente del plan para mantenerlo vigente y garantizar su funcionalidad.
- Difunde el plan de continuidad mientras sea posible, para que los miembros del Banco KLM estén al tanto de estas actividades.

Responsable de análisis y reporte:

- Registra los datos recuperados, validando que éstos sean consistentes.

Responsable de redes y comunicaciones:

- Asegura el correcto funcionamiento de las redes y comunicaciones tecnológicas antes, durante y después que se haya retornado a operaciones normales.

- Proporciona información, recursos y equipos de alta calidad que demande la empresa para la continuidad de los servicios.

- Garantiza la disponibilidad y administración de equipos de BackUp, en caso de falla física.

Responsable de sistemas operativos/plataformas:

- Asegura el correcto funcionamiento de los sistemas, paquetes operativos y aplicativos antes, durante y después que se haya retornado a operaciones normales.

- Proporciona información, recursos y equipos de alta calidad que demande la empresa para la continuidad de los servicios.

- Garantiza la disponibilidad de licencias, BackUp de instaladores, en caso de falla en los registros.

Responsable de sistemas de bases de datos:

- Asegura el correcto funcionamiento de las bases de datos y servidores del Banco KLM antes, durante y después que se haya retornado a operaciones normales.

- Proporciona información, recursos y equipos de alta calidad que demande la empresa para la continuidad de los servicios.

- Garantiza la disponibilidad y administración de equipos y BackUps de todas las base, en caso de requerir un restablecimiento.

Responsable de Core Bancario (Aplicaciones):

- Asegura el correcto funcionamiento de todos los aplicativos de los sistemas de Core Bancario antes, durante y después que se haya retornado a operaciones normales.

- Proporciona información, recursos y equipos de alta calidad que demande la empresa para la continuidad de los servicios.

- Garantiza la disponibilidad y administración de los equipos, sistemas, aplicativos, así como BackUps del Core Bancario.

Responsable de control de seguridades:

- Asegura el correcto funcionamiento de todas las seguridades informáticas, enfocadas en la mitigación de riegos e impacto, accesos a los sistemas del Banco antes, durante y después que se haya retornado a operaciones normales.

- Proporciona información, recursos y equipos de alta calidad que demande la empresa para la continuidad de los servicios.

- Garantiza la confidencialidad y seguridad de la información del Banco.

Responsable de comunicación y soporte a usuarios:

- Informa a los miembros del Banco acerca de la situación de recuperación y sus avances.

- Encargado de coordinar, registrar y brindar seguimiento a las capacitaciones de los miembros del grupo.

Responsable de coordinación con Outsourcing:

- Gestiona las actividades entre el equipo del plan de continuidad y las entidades externas (proveedores) que brindan servicios al Banco.

- Hace cumplir los acuerdos realizados previamente acerca de los servicios y tiempos de entrega.

Responsable de pruebas del negocio:

- Colabora en lo que sea posible en la recuperación del plan de continuidad.

- Se mantienen informado de la situación de recuperación y sus avances.

- Informa sus propias necesidades de TI al Coordinador de Continuidad del Negocio, y que sean transmitidos al equipo de recuperación.

Responsable de personal de apoyo:

- Garantiza el cumplimiento de los acuerdos realizados previamente entre las áreas para designación de personal y colaboración, acerca de los tiempos y niveles de servicio.

Durante un incidente disruptivo se debe tener en cuenta que el equipo del plan de continuidad se encargará de recuperar los recursos y servicios que soporta TI al negocio, más no de la recuperación del negocio como tal (Banco KLM, 2015).

3.2.6. Problemas para la aplicación del modelo de gestión

Durante la aplicación del modelo de continuidad de Infraestructura Tecnológica de TI dentro del Banco KLM, se encontró con algunas complejidades. A continuación se listan los problemas presentados:

- Falta de disponibilidad del personal por tareas asignadas del día a día.

- Falta de asistencia del personal a capacitaciones.

- Políticas organizacionales demasiado burocráticas, las aprobaciones de procesos toman demasiado tiempo.

- Tiempos dilatados en la gestión del plan de continuidad dentro del Banco KLM.

- Falta de colaboración y compromiso de algunos miembros del departamento de TI.

- Falta de facilidades para ventanas de trabajo y pruebas de contingencia en tiempo real (las pruebas realizadas fueron controladas).

- Tiempos de recuperación muy cortos por la criticidad de los servicios tecnológicos en producción.

- Falta de clasificación de servicios realmente críticos para el Banco KLM (todo se convierte en crítico para el usuario final).

- Falta de difusión del plan de Continuidad del Negocio, al menos a todo el departamento de TI y Organización.

- Presencia de factores externos no considerados como manifestaciones anti gobierno.

3.3. Discusión de resultados

3.3.1. Criterios de verificación del modelo

Para la verificación del modelo se considera el método de pruebas, aplicado a 2 incidentes disruptivos controlados (Ver Anexo 7.1: Apéndice 1 Informe de prueba y verificación), que permite evidenciar la efectividad del modelo que garantiza la Continuidad del Negocio.

A continuación se detalla las Pruebas Controladas para la Validación del modelo, ejecutadas sobre incidentes puntuales simulados:

Escenario 1

Tipo: Ataque de código malicioso

Siguiendo el plan de respuesta a los incidentes, el personal del Banco KLM realizó lo siguiente:

Paso 1: Un empleado de Tecnología recibe información sobre un incidente/lentitud con PCs.

- Problema encontrado: ninguno.

Paso 2: Como se trataba de un código malicioso desconocido, se notificó al Subgerente de Control Tecnológico.

- Problema encontrado: ninguno.

Paso 3: Se notificó al fabricante del software antivirus y proveedor del antivirus.

- Problema encontrado: no se obtiene respuesta del proveedor del software antivirus.

Paso 4: Se notificó a los empleados que intercambiaron mensajes con el sistema infectado.

- Problema encontrado: ninguno.

Paso 5: Se consultó a ciertos proveedores de servicios de TI y proveedores de software.

- Problema encontrado: ninguno.

Paso 6: Se dispuso a todos los empleados que poseen sus computadores infectados que desconecten físicamente la red, desactiven las redes inalámbricas, bluetooth, etc., mientras se confirma la gravedad del código malicioso.

- Problema encontrado: usuarios gerenciales resistentes a desconectarse

Paso 7: El personal de Control Tecnológico y Comunicaciones consideró necesario restringir todo el tráfico de datos/red para los usuarios con computadores infectados.

- Problema encontrado: los usuarios se vieron afectados, por la restricción y bloqueo a la red corporativa, sin embargo lo servicios de TI masivos continuaron siempre operativos.

Paso 8: Para los ordenadores que todavía no habían sido desconectados de la red, los administradores de las plataformas Tecnológicas involucradas se encargaron de evaluar si desconectaban los PCs para evitar mayor infección, además de desactivar las conexiones inalámbricas.

- Problema encontrado: ninguno.

Paso 9: Los administradores consideraron necesario notificar a los usuarios de los sistemas informáticos sobre la gravedad de la infección.

- Problema encontrado: ninguno.

Paso 10: Los administradores consiguieron información (internet, proveedores) sobre códigos maliciosos muy parecidos que dieron pauta mediante los pasos necesarios a su erradicación, lo cuáles fueron ejecutados en todos los computadores infectados, incluso en los servidores de manera centralizada.

- Problema encontrado: ninguno., no se evidenció afectación a la información, el problema fue controlado en aproximadamente 30min.

Escenario 2

Tipo: Falla en Telecomunicaciones

Siguiendo el plan de respuesta a los incidentes, el personal del banco KLM realizó lo siguiente:

Paso 1: Un empleado de la Mesa de Servicios recibe un reporte de incidente sobre un problema con el acceso a todos los sistemas, desde una sucursal.

- Problema encontrado: ninguno.

Paso 2: El tema es escalado al área de Comunicaciones, se verifica si todos los equipos de comunicación se encuentran encendidos.

- Problema encontrado: ninguno.

Paso 3: Verificar si los cables se encuentran conectados y en los sitios correctos.

- Problema encontrado: faltan etiquetas en algunos de los cables (temporales), lo que dificulta la tarea de revisión.

Paso 4: Verificar la configuración de los equipos de comunicación para identificar y corregir posibles problemas.

- Problema encontrado: el servidor de monitoreo se encuentra en estado intermitente, posiblemente tiene un daño en la tarjeta de video, lo cual ocasiona intermitencias de video continuas y un monitoreo ineficiente.

Paso 5: Reiniciar los equipos de comunicación por síntoma de inhibición.

- Problema encontrado: algunos equipos mantienen la alta disponibilidad de varias conexiones/sucursales sobre el mismo appliance.

Paso 6: Se confirma necesario coordinar el soporte con el proveedor de servicios de TI para reemplazo del equipo.

- Problema encontrado: ninguno, colocan un equipo backup.

Paso 7: Los usuarios de la sucursal no usan medios de comunicación alternativos.

- Problema encontrado: las comunicaciones son inevitablemente suspendidas mientras se reinicia el equipo.

Paso 8: Los administradores de Comunicaciones consideraron necesario notificar a los usuarios de los sistemas informáticos sobre la desconexión.

- Problema encontrado: ninguno.

Paso 9: El proveedor se dirige al sitio, instala un router backup para no afectar servicios, ubica el equipo con problemas y procede con el reinicio, las conexiones se normalizan en su totalidad.

- Problema encontrado: ninguno., no se evidenció afectación a la información, porque se manejó con equipos de respaldo, el problema fue controlado en aproximadamente 45min.

3.3.2. Evaluación del modelo de gestión

El modelo de gestión de Continuidad del Negocio de Infraestructura Tecnológica aplicado en el Banco KLM, permitió obtener resultados satisfactorios. La evaluación basada en pruebas descubrió escenarios de recuperación ágiles y oportunos, de manera que garantizan la Continuidad del

Negocio utilizando el plan propuesto, alineado con los objetivos estratégicos del Banco KLM.

La aplicación del modelo, permite generar recomendaciones importantes para mejorar la gestión de la Continuidad del Negocio, en caso de desastres posteriores en el Área de Infraestructura Tecnológica del Banco KLM.

A continuación se citan los principales hallazgos durante la aplicación del modelo de gestión realizado en el Banco KLM, mismos que se encuentran citados con mayor detalle en los Anexos respectivos.

- La información proporcionada por el Banco KLM refleja su realidad actual, en algunos casos se omite información susceptible y crítica que pudiera comprometer económica y legalmente a la Compañía.

- El Banco KLM tiene 3 Centros de Datos especializados fuera de las oficinas y en diferentes ciudades (dentro del Proyecto se citan 2 por temas de confidencialidad).

- El impacto financiero es muy variable, existen registros confidenciales de pérdidas que ascienden a cientos de miles de dólares en aproximadamente 10 min de indisponibilidad de servicios TI Core (Banco KLM, 2015).

- Resulta muy importante citar los esquemas de alta disponibilidad manejados por el Banco KLM, un 98% de toda su Infraestructura Tecnológica cuenta con BackUps en estado activo/activo, permitiendo minimizar riesgos y puntos únicos de falla.

- Para el análisis de impacto se evalúa los servicios agrupados por áreas, aplicativos e infraestructura que lo soporta, los no citados son parte de un servicio entregado o no son considerados críticos.

- Dentro del Plan de Continuidad del Banco, cada Rol tiene asignado un cargo con su respectivo BackUp.

- El centro de recuperación cuenta con equipos/servicios de comunicaciones necesarios para operar en tiempo real, lo cual denota la criticidad con la que se maneja los tiempos de respuesta ofrecidos por TI y la importancia para temas de continuidad manejadas por el Banco.

- Por disposición de la Gerencia (confidencialidad) no se citan todos los aplicativos, sistemas, recursos, proveedores y demás manejados en la Compañía.

- Los tiempos de recuperación, en el cual los usuarios retomaron las actividades normales fueron buenos, luego de superado el incidente disruptivo (uno a la vez).

- Durante los incidentes disruptivos, se mantuvo en todo momento la confiabilidad e Integridad de la información, confirmada telefónicamente por cada uno de los participantes en las pruebas realizadas.

- Se adquirió conocimientos mediante la investigación sobre como erradicar códigos maliciosos.

- Fue probada la disponibilidad de personal calificado por la empresa proveedora de servicios de Telecomunicaciones/enlaces para el cambio del equipo e implementación de un BackUp en caliente.

- El personal pudo diagnosticar y dar respuesta y solución en tiempos esperados para las fallas encontradas, y restablecimiento de los servicios de Comunicaciones.

- Sobre la base de los resultados anteriores se considera que el modelo es útil y adecuado para las Empresas Financieras, además de poder acoplarse a empresas con diferente giro de negocio, que requieren mantener la continuidad operativa de sus negocios.

- Para mayor comprobación del modelo, podría verificarse su aplicabilidad utilizando ejemplos más complejos.

- El modelo podría incorporar el manejo y administración de la documentación (archivos), mediante la utilización de una aplicación de software.

En base a los resultados de la prueba, se iniciaron las siguientes medidas correctivas:

- Se realiza el trámite para la renovación de las licencias del software antivirus.

- Etiquetar los cables de conexiones temporales, que no contienen su respectiva descripción.

- Implementar equipos/medios de comunicaciones alternativos e independientes.

- Considerar capacitaciones permanentes y en diferentes horarios, de manera que todos los recursos involucrados puedan asistir.

4. CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones

Respecto al nuevo modelo de gestión se identificó que es necesario discriminar entre el BCP total de la Compañía y la continuidad estratégica de la Infraestructura Tecnológica, así como esquemas de alta disponibilidad.

Para el análisis de riesgos las Empresas Financieras debe contar con la matriz actualizada de los mismos, permitiendo identificar riesgos e impactos que a futuro pueden ser perjudiciales para la continuidad de Infraestructura Tecnológica y la Organización.

Los tiempos de recuperación de la Infraestructura Tecnológica deben estar alineados con los objetivos del negocio, y; estar estrechamente ligados a cambios en los procesos o manejo de los mismos.

La estrategia de continuidad de Infraestructura Tecnológica está propuesta a nivel de áreas y aplicativos que soportan los servicios de TI operacionales, lo cual permiten cubrir todos los servicios tecnológicos brindados para la organización financiera.

El modelo presentado permite garantizar los servicios tecnológicos de TI en cualquier institución financiera nacional, y pretende concientizar y socializar la importancia fundamental de la Infraestructura Tecnológica en las empresas en el entono actual.

Para la aplicación del modelo se adjuntan los formularios respectivos, de manera que permita la aplicabilidad y comprensión del SGCN de una forma ágil.

La aplicación del modelo en el Banco KLM fue exitosa, gracias a la colaboración de todo el grupo de tecnología, políticas organizacionales de trabajo claras y amigables; y sobre todo a sus esquemas de Alta Disponibilidad en todos los frentes.

4.2. Recomendaciones

Se recomienda difundir adecuadamente todos los procesos y servicios críticos brindados por el área de Infraestructura Tecnológica, que permitan mantener la Continuidad del Negocio con la participación de todos sus colaboradores involucrados.

Es recomendable mantener actualizado el mapa de riesgos del negocio en todas sus áreas, con el objetivo de identificar la infraestructura que soporta a cada uno de los servicios de TI, fundamentalmente los críticos.

Armar el equipo de continuidad de Infraestructura Tecnológica idóneo, mediante personal interno y externo adecuado para la operación de servicios en caso de incidentes disruptivos, que dispongan de los recursos tangibles e intangibles necesarios para la activación de los servicios de TI.

Establecer anualmente períodos de revisión y actualización de información, archivos, documentos críticos del negocio, para que con esta información se planteen nuevas estrategias de recuperación por áreas o procesos, identificando tiempos y servicios críticos de operación para las Organizaciones.

Realizar pruebas de continuidad de Infraestructura Tecnológica en tiempo real, al menos una vez al año, incluyendo la adquisición de nuevos equipos y adecuaciones necesarias de los sitios alternos que garanticen la operación y continuidad.

Referencias

Advisera. (2014). *Advisera.* Recuperado el 15 de Enero de 2015, de http://advisera.com/27001academy/es/what-is-bs-25999/

Alexander, A. G. (2012). *Nuevo Estándar Internacional en Continuidad del Negocio ISO 22301:2012.* Recuperado el 20 de febrero de 2015, de http://www.gestion.com.do/pdf/018/018-nuevo-estandar-internacional.pdf

Arevalo, L. (11 de Mayo de 2015). Gerente de TI. *Operaciones de Infraestructura en Negocios Bancarios*. (V. Sarabia, Entrevistador) Quito, Ecuador.

Asamblea Nacional Constituyente. (2008). *Constitución de la República del Ecuador.* Quito, Ecuador: Registro Oficial 449 del 20 de octubre de 2008.

Asociación de Bancos Privados del Ecuador. (2015). *Evolución de la Banca Privada Ecuatoriana.* Quito, Ecuador: Boletín Informativo enero 2015.

Banco KLM. (2015). *Administración TI del Banco KLM.* Quito, Ecuador.

Bello, J. L. (2008). *BS 25999, la nueva norma para Sistemas de Gestión de la Continuidad del Negocio.* Recuperado el 16 de Marzo de 2015, de http://www.aec.es/c/document_library/get_file?uuid=99c086c1-9c20-4389-a9db-682ddbedc3c8&groupId=10128

Bizagi. (2011). *PROCESO AD HOC- CONSTRUCCIÓN.* Recuperado el 21 de enero de 2015, de https://www.bizagi.com/processcentral/Documents/1fa71816-4180-433e-9251-

11082dd0c394/docs/Proceso%20Ad%20Hoc%20Construcci%C3%B3n.pdf

Bryan C. Martin. (2002). *Disaster Recovery Plan Strategies and Processes.* Recuperado el 16 de marzo de 2015, de http://www.sans.org/reading-room/whitepapers/recovery/disaster-recovery-plan-strategies-processes-564

Contraloría General del Estado. (14 de Diciembre de 2009). *Normas Técnicas de Control Interno. Normas Técnicas de Control Interno.* Quito, Ecuador: Registro Oficial Suplemento 87.

Kosutic, D. (2015). *Paquete Premium ISO 27001 y ISO 22301.* Recuperado el 26 de febrero de 2015, de http://advisera.com/27001academy

NORMA ISO 22301. (2012). *INTERNATIONAL STANDARD ISO 22301:2012.* Ginebra, Suiza: Versión corregida 15 de junio de 2012.

NORMA ISO 27001. (2005). *INTERNATIONAL STANDARD ISO/IEC 27001.* Ginebra, Suiza: Primera edición 15 de octubre de 2005.

Sharp, J. (2012). *The Route Map to Business Continuity Management (2a. Ed.).* Londres, Reino Unido: British Standards Institution.

Superintendencia de Bancos del Ecuador - SB. (2005). *Codificación de Resoluciones de la Superintendencia de Bancos y Seguros y de la Junta Bancaria.* Quito, Ecuador: Título X, Capítulo V.

Tobar, L. (2004). ¿Qué pasa en el sistema financiero ecuatoriano? *Utopía*, 41-44.

Glosario de Términos

ACTIVO/ACTIVO: En informática se refiere a dos equipos que continente el mismo servicio, a los cuales los clientes pueden conectarse indistintamente.

ACTIVO/PASIVO: Dentro de TI hace referencia a dos equipos con el mismo servicio, sin embargo los clientes pueden conectarse al equipo pasivo únicamente cuando el equipo activo se encuentre fuera de servicio.

AD HOC: Consisten en una serie de actividades que no tienen un orden o un ejecutante definido.

BACKUP: En tecnologías de la información se refiere a una copia de los datos informáticos originales, se realiza con el fin de disponer de un medio de recuperación en caso de su pérdida.

BCM: Por sus siglas en inglés "Business Continuity Management", es un proceso de gestión integral, identifica potenciales impactos de una amenaza y provee estructuras de respuesta que resguarde los intereses de las empresas.

BCP: "Business Continuity Plan", es el plan para recuperar y restaurar las operaciones críticas parcial o totalmente, luego de interrumpidas por un incidente disruptivo.

CORE BANCARIO: En informática es el sistema principal del negocio de una institución bancaria.

DRII: Por sus siglas en inglés "Disaster Recovery Institute International", es una Organización Internacional de Continuidad del Negocio.

DRP: Es un plan de recuperación de desastres, consiste en un conjunto de procedimientos para recuperar y proteger la infraestructura tecnológica de una empresa en caso de un desastre.

FIREWALL: Es un sistema (físico o virtual) de Seguridad Informática, permite controlar y proteger el tráfico de datos de una red de computadores.

INCIDENTE DISRUPTIVO: Se refiere a una interrupción o ruptura brusca de una actividad o servicio.

IPS: "Intrusion Prevention System", sistemas dedicados a la prevención de intrusiones a partir de la identificación y bloqueo de ataques en el tránsito de la red.

LAN: Son las siglas en inglés para "Local Area Network", es un grupo de equipos que están conectados dentro de un área geográfica pequeña.

OUTSOURCING: Es un término inglés muy utilizado en el idioma español, consiste en desarrollar actividades por parte de la compañía subcontratada en nombre de la empresa contratante.

PCI DSS: Por sus siglas en inglés "Payment Card Industry Data Security Standard", son un conjunto de controles de seguridad que las compañías que procesan, guardan o trasmiten datos de tarjetas de pago deben cumplir.

PDCA: El nombre del Ciclo PDCA viene de las siglas Planificar, Hacer, Verificar y Actuar, en inglés "Plan, Do, Check, Act". También es conocido como Ciclo de mejora continua o Círculo de Deming.

ROUTER: Es un dispositivo de red informática, permite el enrutamiento de paquetes entre redes independientes.

RPO: “Recovery Point Objective”, determina la máxima cantidad de información que se puede perder, es el tiempo máximo establecido de la última copia de seguridad de los datos de la empresa, respecto a la anterior copia.

RTO: “Recovery Time Objective”, es el tiempo objetivo para la reanudación de los servicios tecnológicos después de un desastre.

SAN: “Storage Area Network”, es una red diseñada para interconectar servidores, librerías, permitiendo el tránsito de datos sin afectar a las redes por las que acceden los usuarios.

SBS: Superintendencia de Bancos y Seguros, entidad jurídica de derecho público, organismo técnico y autónomo, tiene a su cargo el control y la vigilancia de las instituciones del sistema financiero público y privado, así como de las compañías de seguros.

SGCN: Sistema de Gestión de Continuidad del Negocio, es un proceso integral de gestión que identifica los posibles impactos que amenazan a una organización, y ofrece un marco para disponer de los servicios en todo momento.

SGSI: Es la abreviatura utilizada para referirse a un Sistema de Gestión de Seguridad de la Información.

SWITCH: Dispositivo electrónico utilizado en redes de Computadoras LAN, permite interconectar varios equipos que conforman una red informática.

TI: “information technology” hace referencia a las tecnologías de la información, el término TI es un término más amplio y abarca a las TICs.

TICs: Se refiere a las Tecnologías de la Información y la Comunicación

VPN: Siglas en inglés de “Virtual Private Network”, es una tecnología de red, se establece entre 2 sitios lejanos mediante Internet, formando una red privada.

WAN: “Wide Area Network”, es una red de área amplia, abarca un área geográfica relativamente grande.

ANEXOS

ANEXO 1

Procedimiento para Identificación de Requisitos

Banco KLM

Banco KLM Compañía Anónima

Anexo 1: Procedimiento para Identificación de Requisitos

Código:	PRO-TI-2015-08
Versión:	1.0
Fecha de la versión:	3 de Agosto del 2015
Creado por:	Ing. Vinicio Sarabia
Aprobado por:	Ing. Santiago Pazmiño
Nivel de confidencialidad:	Medio

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
03/08/2015	1.0	Vinicio Sarabia	Creación de la primera versión del documento

Tabla de contenido

Objetivo, alcance y usuarios

El objetivo del presente documento es definir el proceso de identificación de las partes interesadas, de los requisitos legales, normativos, contractuales y de otra índole relacionados con la Continuidad del Negocio, como también las responsabilidades para su cumplimiento.

Este documento se aplica a todo el Sistema de Continuidad del Negocio (SGCN).

Los usuarios de este documento son todos los empleados del Banco KLM.

Documentos de referencia

- Norma ISO/IEC 27001, control A.15.1.1
- Norma ISO 22301, punto 4.2
- Política de la Continuidad del Negocio

Identificación de requisitos y partes interesadas

El Asesor Jurídico del Banco es responsable de identificar a (1) todas las personas u organizaciones que pueden afectar o ser afectadas por la gestión de la Continuidad del Negocio (partes interesadas) y a (2) todos los requisitos legales, normativos, contractuales y de otra índole que correspondan.

El Asesor Jurídico del Banco definirá quién será responsable del cumplimiento de cada requisito individual y qué partes interesadas serán notificadas cuando se produzcan modificaciones.

El Asesor Jurídico del Banco debe enumerar todos los requisitos, partes interesadas y personas responsables en la 'Lista de requisitos legales, normativos, contractuales y de otra índole" y debe publicarla en la carpeta “Documentos Públicos”, la misma que se encuentra en la ruta: \\SRVTECH\SGCN\DOCUMENTOS_VIGENTES.

Cada empleado del Banco KLM debe notificar al Asesor Jurídico si detecta o encuentra algún nuevo requisito legal, normativo, contractual o de otra índole que pueda ser importante para la gestión la Continuidad del Negocio.

Revisión y evaluación

El Asesor Jurídico del Banco es responsable de revisar la Lista de requisitos legales, normativos, contractuales y de otra índole al menos cada 6 meses y de actualizarla cuando sea necesario. El Asesor Jurídico notificará a todas las partes interesadas cuando realice cada actualización.

El Auditor Interno es responsable de evaluar el cumplimiento del SGCN respecto de los requisitos legales, normativos y contractuales correspondientes al menos 2 veces al año.

Validez y gestión de documentos

Este documento es válido desde la presente fecha hasta el 3 de Agosto del 2016, el propietario de este documento es el Asesor Jurídico del Banco, que debe verificar, y si es necesario actualizar, el documento por lo menos una vez al año.

Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

Cantidad de obligaciones de la organización que ya existían pero que no fueron identificadas.

Cantidad o monto de multas pagadas por el no cumplimiento de obligaciones.

Cantidad de días de atraso en el cumplimiento de la obligación.

Apéndices

- Apéndice: Formulario: Lista de requisitos legales, normativos, contractuales y de otra índole

Asesor Jurídico

Ab. Cesar Oswaldo Sabando Recalde

_____

Firma

ANEXO 1.1

Lista de requisitos legales, normativos, contractuales y de otra índole

Anexo 1: Procedimiento para Identificación de Requisitos

Apéndice 1: Lista de requisitos legales, normativos, contractuales y de otra índole

Tabla 25. Lista de requisitos legales, normativos, contractuales y de otra índole.

Requisito	Documento que impone el requisito	Persona responsable del cumplimiento	Plazos	Partes interesadas
Procedimientos para minimizar pérdidas o interrupción del negocio	Normas de la SBS para Control de Instituciones Financieras privadas, Art 15, sustituido con resolución No. JB-2014-3066 de 2 de septiembre del 2014	Todos los empleados del Banco KLM	Continuo	Alta Gerencia, Órganos de Control y Regulación, Socios, empleados
Acuerdos y Niveles de servicio internos y externos	Plan Estratégico Vigente en la Organización90	Todos los empleados del Banco KLM	Continuo	Alta Gerencia, Órganos de Control y Regulación, Socios
Procedimientos de Seguridad de la	Políticas y reglamentos de Seguridad de la Información y	Todos los empleados del Banco KLM	3 años	Alta Gerencia, Órganos de Control y

Información	Confidencialidad Vigente en la Organización			Regulación, Socios, empleados
DRP para el área de Tecnología y Servicios Informáticos	Plan Estratégico de TI Vigente en la Organización	Todos los empleados del Banco KLM	3 años	Alta Gerencia, Órganos de Control y Regulación, Socios
Continuidad de los Servicios de TI	Plan Estratégico Operativo Anual 2015	Todos los empleados del Banco KLM	1 año	Alta Gerencia, Órganos de Control y Regulación, Socios

ANEXO 2

Política de Continuidad del Negocio

Banco KLM

Banco KLM Compañía Anónima

Anexo 2: Política de Continuidad del Negocio

Código:	POL-TI-2015-08
Versión:	1.0
Fecha de la versión:	3 de Agosto del 2015
Creado por:	Ing. Vinicio Sarabia
Aprobado por:	Ing. Santiago Pazmiño
Nivel de confidencialidad:	Medio

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
03/08/2015	1.0	Vinicio Sarabia	Creación de la primera versión del documento

Tabla de contenido

Objetivo, alcance y usuarios

El propósito de esta Política es definir el objetivo, alcance y reglas básicas para la gestión de la Continuidad del Negocio.

Esta Política se aplica a todo el Sistema de Gestión de Continuidad del Negocio (SGCN).

Los usuarios de este documento son todos los empleados del Banco KLM, como también todos los proveedores y socios que cumplen alguna función en el SGCN.

Documentos de referencia

- Norma ISO 22301, puntos 4.1, 4.3, 5.3, 6.2 y 9.1.1
- Norma ISO/IEC 27001, puntos A.14.1.1, A.14.1.4
- Plan del proyecto para la implementación del Sistema de Gestión de Continuidad del Negocio.
- Lista de requisitos legales, normativos, contractuales y de otra índole; Plan de tratamiento del riesgo
- Plan de preparación para Continuidad del Negocio
- Procedimiento para acciones correctivas y preventivas

- Normas de la SBS para Control de Instituciones Financieras privadas, Art 15, sustituido con resolución No. JB-2014-3066 de 2 de septiembre del 2014
- Plan Estratégico Vigente en la Organización
- Políticas y reglamentos de Seguridad de la Información y Confidencialidad Vigente en la Organización
- Plan Estratégico Operativo Anual 2015

Gestión de la Continuidad del Negocio

Objetivo de la gestión de la Continuidad del Negocio

El objetivo de la gestión de la Continuidad del Negocio es identificar potenciales amenazas en una organización y los impactos que esas amenazas podrían tener sobre las operaciones de negocios; también sirven para proporcionar un marco de referencia para construir resiliencia organizacional con la capacidad de una respuesta efectiva.

Relación con los objetivos generales y otros documentos

Con la implementación de la Continuidad del Negocio, el Banco KLM desea cumplir sus objetivos estratégicos y comerciales como son: (1) Brindar servicios Bancarios de calidad a clientes finales; (2) Mantener la disponibilidad de los servicios Tecnológicos y de negocio en todo momento; y (3) Continuar siendo una Empresa financiera de alta rentabilidad.

La gestión de la Continuidad del Negocio se implementa conforme a los requisitos enumerados en la Lista de requisitos legales, normativos, contractuales y de otra índole, y dentro del marco referencial definido por los siguientes documentos:

- Plan Estratégico Vigente en la Organización
- Políticas y reglamentos de Seguridad de la Información Vigente en la Organización
- Plan Estratégico Operativo Anual 2015

Definición de objetivos de Continuidad del Negocio

El Gerente Nacional de Tecnología es el responsable de definir los objetivos para todo el SGCN y el método para medir el cumplimiento de los mismo (esos objetivos y métodos están documentados en “Objetivos del SGCN y métodos de medición de cumplimiento”). El Gerente Nacional de Tecnología tiene la responsabilidad de revisar esos objetivos al menos una vez cada 6 meses.

Los objetivos para elementos individuales del SGCN son propuestos y documentados por el Gerente de Producción y Servicios (Coordinador de la Continuidad del Negocio), el Responsable de pruebas del negocio y autorizados por el Gerente de Tecnología; estos objetivos deben ser revisados al menos cada 6 meses por las mismas personas que los propusieron.

Las acciones para cumplir estos objetivos serán determinadas en el Plan de tratamiento de riesgos, en el Plan de preparación para Continuidad del Negocio, en las acciones correctivas y preventivas según el Procedimiento para acciones correctivas y preventivas y en la Revisión por parte de la dirección.

Alcance

El Sistema de Gestión de Continuidad del Negocio se implementa única y exclusivamente para el área de Infraestructura Tecnológica del Banco KLM, con especial atención sobre las actividades identificadas durante el Análisis de impactos en el negocio.

Las ubicaciones de negocios de la organización incluidas en el alcance:

- Oficina Matriz – Quito

- Sucursales – Guayaquil, Cuenca, Ambato, Manta, Machala

Unidades organizativas incluidas en el alcance:

- Infraestructura Tecnológica

Productos y servicios clave

Los siguientes productos y servicios clave son suministrados por el área de Infraestructura y Servicios Tecnológicos del banco KLM dentro del alcance definido en la sección anterior:

- Archivos, BackUps
- Bases de datos
- Aplicativos Core Bancario
- Aplicativos Financieros
- Aplicativos de Gestión externa
- Mesa de Servicios
- Microsoft Office
- Comunicaciones, enlaces
- Seguridades perimetrales
- Carpetas compartidas
- Impresoras, copiadoras
- Internet
- VPNs
- Videoconferencia
- Central telefónica
- Aplicativos de monitoreo
- Aplicativos Tecnológicos
- Aplicativos Administrativos
- Aplicativos de gestión

La gestión de la Continuidad del Negocio debe garantizar que los productos mencionados precedentemente se recuperarán a un nivel predefinido.

Todas las actividades relacionadas con esos productos y servicios están detalladas en la Estrategia de Continuidad del Negocio.

Responsabilidades para la gestión de la Continuidad del Negocio

Responsabilidades generales:

- El Gerente Nacional de Tecnología es el responsable de garantizar que la gestión de la Continuidad del Negocio sea establecida e implementada de acuerdo con esta Política y de proporcionar los recursos necesarios.

- El Coordinador de la Continuidad del Negocio es responsable de la implementación operativa y del mantenimiento del Sistema de Gestión de Continuidad del Negocio.

- El Directorio debe revisar el SGCN al menos una vez por año o cada vez que se produzca una modificación significativa, y debe elaborar un informe de la revisión. El objetivo de la revisión por parte de la dirección es establecer la conveniencia, adecuación y eficacia del SGCN.

Responsabilidades específicas:

- El Coordinador de la Continuidad del Negocio es el responsable de adoptar e implementar el Plan de capacitación y concienciación que corresponde a todas las personas que cumplen una función en la gestión de la Continuidad del Negocio.

- Los preparativos relacionados con la Continuidad del Negocio deben ser probados y verificados al menos una vez por año utilizando diversos métodos para evaluar si pueden proteger a las actividades de la organización. Para ello, el Coordinador de la Continuidad del Negocio debe redactar un Plan de prueba y verificación que debe ser aprobado por la alta dirección. Luego de cada prueba y verificación, el Coordinador de la Continuidad del Negocio debe elaborar un Informe de prueba y verificación.

- El Coordinador de la Continuidad del Negocio es el responsable de adoptar e implementar el Plan de mantenimiento y revisión del SGCN para que todos los elementos del SGCN estén operativos y actualizados.

- Cada vez que se activa un Plan de Continuidad del Negocio, un Plan de recuperación o un Plan de respuesta a los incidentes, el Gerente de Tecnología es el responsable de supervisar la eficacia de la gestión de la Continuidad del Negocio.

- El Gerente de Tecnología es responsable de supervisar las no conformidades, falsas alarmas, incidentes reales, etc. y de elevar las acciones preventivas necesarias.

Medición

El Banco KLM medirá lo siguiente:

1. Si los objetivos definidos de acuerdo a esta Política son cumplidos: al menos una vez por año, generalmente antes de la revisión por parte de la Dirección.

2. Efectividad y adecuación de los planes de Continuidad del Negocio: según la frecuencia definida en el mismo Plan de Continuidad del Negocio.

El Coordinador de la Continuidad del Negocio elaborará un informe con los resultados de la medición, mientras que el análisis y evaluación de los resultados se realizará en la Revisión por parte de la dirección.

Comunicación de la Política

El Comunicador Social debe asegurarse de que todos los empleados del Banco KLM, como también los proveedores y socios que cumplen una función en el SGCN, estén familiarizados con esta Política.

Apoyo para la implementación del SGCN

A través del presente, el Gerente de Tecnología declara que en todos los elementos de la implementación del SGCN se contará con el apoyo de los recursos adecuados para lograr todas las metas y objetivos establecidos en esta Política, como también para cumplir con todos los requisitos identificados.

Validez y gestión de documentos

Este documento es válido desde el 3 de Agosto del 2015. El propietario de este documento es el Coordinador de la Continuidad del Negocio, que debe verificar, y si es necesario actualizar, el documento por lo menos una vez al año.

Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- Cantidad de empleados y proveedores/socios que no conocen este documento.
- No-conformidad de gestión de la Continuidad del Negocio con disposiciones legales, obligaciones contractuales y demás documentos internos de la organización.
- Ineficacia de la implementación y mantenimiento del SGCN.
- Responsabilidades ambiguas para la implementación del SGCN.

Gerente de Tecnología

Ing. Santiago Pazmiño

_____

Firma

ANEXO 3

Plan de capacitación y concienciación

Anexo 3: Plan de capacitación y concienciación

Con el objetivo de preparar al personal para que pueda ejecutar sus tareas cumpliendo una función en la gestión de la Continuidad del Negocio, se debe llevar a cabo la siguiente capacitación:

Tabla 26. Plan de capacitación y concienciación.

Cargo o nombre	Conocimientos y habilidades necesarias para implementar la Continuidad del Negocio	Qué capacitación es necesaria	Registro de implementación de capacitación necesaria	¿Se han logrado los objetivos de la capacitación?	Conocimientos, habilidades y experiencia logrados
Gerente de Producción y Servicios	• Procesos del negocio • Políticas Organizacionales • Normas de control y regulación • Manejo de la gestión de	• Plan de Continuidad del Negocio • Gobierno de TI • Regulaciones y normas de la SBS • Técnicas de			

	recuperación • Liderazgo • Decisión • Compromiso • Facilidad de expresión • Políticas de seguridades informáticas de la Organización	trabajo en equipo y liderazgo			
Subgerente de Procesamiento e Infraestructura	• Procesos del negocio • Normas de control y regulación • Manejo de la gestión de recuperación • Liderazgo • Compromiso • Facilidad de	• Plan de Continuidad del Negocio • Gobierno de TI • Regulaciones y normas de la SBS • Técnicas de trabajo en equipo y liderazgo			
Subgerente de Servicios Tecnológicos					
Subgerente de Control Tecnológico					

	expresión • Políticas de seguridades informáticas de la Organización				
Jefe de Monitoreo	• Procesos del negocio • Normas de control y regulación • Manejo de la gestión de recuperación • Liderazgo • Compromiso • Manejo avanzado de sistemas y equipos informáticos.	• Plan de Continuidad del Negocio • Regulaciones y normas de la SBS • Técnicas de trabajo en equipo y liderazgo • Herramientas de monitoreo			
Jefe de Comunicaciones	• Procesos del negocio	• Plan de Continuidad del			

	• Normas de control y regulación • Manejo de la gestión de recuperación • Liderazgo • Compromiso • Manejo avanzado de redes • Configuración de equipos de red	Negocio • Regulaciones y normas de la SBS • Técnicas de trabajo en equipo y liderazgo • Configuración avanzada de equipos de Networking • Troubleshooting de red			
Jefe de Servidores	• Procesos del negocio • Normas de control y regulación • Manejo de la gestión de recuperación	• Plan de Continuidad del Negocio • Regulaciones y normas de la SBS • Técnicas de			

	• Liderazgo • Compromiso • Manejo y configuración avanzada de servidores y bases de datos	trabajo en equipo y liderazgo • Configuración avanzada de bases de datos y servidores • Administración y mantenimiento de bases de datos			
Jefe de Centro de Computo	• Procesos del negocio • Normas de control y regulación • Manejo de la gestión de recuperación • Liderazgo • Compromiso	• Plan de Continuidad del Negocio • Regulaciones y normas de la SBS • Técnicas de trabajo en equipo y liderazgo			

	• Manejo y configuración avanzada de equipos Core, BackUps, procesamiento	• Configuración avanzada de equipos Core • Administración y mantenimiento de equipos Core			
Jefe de Soporte Técnico	• Procesos del negocio • Normas de control y regulación • Manejo de la gestión de recuperación • Liderazgo • Compromiso • Manejo avanzado de sistemas operativos y equipos	• Plan de Continuidad del Negocio • Regulaciones y normas de la SBS • Técnicas de trabajo en equipo y liderazgo • Instalación de software y mantenimiento de sistemas			

	informáticos	informáticos, hardware			
Jefe de Mesa de Servicios	• Procesos del negocio • Normas de control y regulación • Manejo de la gestión de recuperación • Liderazgo • Compromiso • Manejo avanzado de aplicativos • Facilidad de expresión	• Plan de Continuidad del Negocio • Regulaciones y normas de la SBS • Técnicas de trabajo en equipo y liderazgo • Técnicas de expresión oral y comunicación • Manejo de herramientas de gestión			

Para que el personal comprenda la importancia de la gestión de la Continuidad del Negocio y su aporte al SGCN y acepte los planes de Continuidad del Negocio, se deben aplicar los siguientes métodos de concienciación: día informativo, artículos en

Intranet, boletín informativo, reuniones conjuntas, e-learning, mensajes de correo electrónico interno y grabaciones en vídeo informativos.

La implementación de capacitación y concienciación está programada de la siguiente forma:

Tabla 27. Cronograma de capacitación y concienciación programada.

Método de concienciación	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
Día informativo	X		X		X		X		X		X	
Capacitación inicial										X		
Capacitación habitual de empleados	X					X					X	
Artículos en Intranet	X			X			X			X		
Artículos en boletín informativo		X					X					X

Reuniones conjuntas	X	X	X	X	X	X	X	X	X	X	X	X
E-learning			X				X				X	
Mensajes de correo electrónico interno	X	X	X	X	X	X	X	X	X	X	X	X
Grabaciones en vídeo informativo			X				X				X	

Responsabilidades:

- El Coordinador de la Continuidad del Negocio en conjunto con la Gerencia de Recursos Humanos es responsable de coordinar toda la capacitación y concienciación.

- El Coordinador de la Continuidad del Negocio en conjunto con la Gerencia de Recursos Humanos son los responsables de llevar los registros de toda la capacitación.

- El Subgerente de Control Tecnológico es el responsable de evaluar el logro de los objetivos de capacitación.

- El Coordinador de la Continuidad del Negocio es el responsable de este plan, archivado en \\SRVTECH\SGCN\PLAN_DE_CAPACITACION; y esta persona tiene un derecho exclusivo para editar y modificar el documento; este registro de debe guardar por 3 años.

ANEXO 4

Metodología para el análisis del Impacto en el Negocio

Banco KLM

Banco KLM Compañía Anónima

Anexo 4: Metodología para el análisis del Impacto en el Negocio

Código:	MET-TI-2015-08
Versión:	1.0
Fecha de la versión:	3 de Agosto del 2015
Creado por:	Ing. Vinicio Sarabia
Aprobado por:	Ing. Santiago Pazmiño
Nivel de confidencialidad:	Alto

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
03/08/2015	1.0	Vinicio Sarabia	Creación de la primera versión del documento

Tabla de contenido

Objetivo, alcance y usuarios

El objetivo de este documento es definir la metodología y el proceso para evaluar los impactos de la interrupción de las actividades del Banco KLM y determinar prioridades y objetivos de continuidad y de recuperación.

El análisis del impacto en el negocio se aplica a todo el alcance del Sistema de Gestión de Continuidad del Negocio (SGCN); es decir, a todas las actividades que sustentan los productos y servicios del Banco KLM.

Los usuarios de este documento son todos los empleados del Banco KLM que participan en el establecimiento e implementación del SGCN.

Documentos de referencia

- ISO 22301 puntos 8.2.1 y 8.2.2
- Norma ISO/IEC 27001, control A.14.1.2
- Política de la Continuidad del Negocio
- Estrategia de Continuidad del Negocio
- Lista de requisitos legales, normativos, contractuales y de otra índole

Metodología para el análisis del impacto en el negocio

Organización

El análisis del impacto en el negocio se implementa a través de los Cuestionarios sobre el análisis del impacto en el negocio. El proceso es coordinado por Coordinador de la Continuidad del Negocio y el análisis de las actividades individuales es realizado por la persona responsable de cada actividad.

El análisis del impacto en el negocio se realiza una vez finalizada la evaluación de riesgos para que la información sobre los recursos necesarios pueda ser utilizada a partir de dicha evaluación.

El manejo de documentos confidenciales producidos de acuerdo a esta Metodología se realizará en conformidad con las Políticas de Seguridad de la Información y Confidencialidad del Banco KLM.

Identificación de actividades

El Coordinador de la Continuidad del Negocio es responsable de identificar todas las actividades que sustentan la provisión de productos y servicios y de designar la persona responsable para cada actividad.

Impactos del incidente disruptivo

Los impactos del incidente disruptivo sobre una actividad son evaluados a través de los (1) impactos generales (evaluación cualitativa) e (2) impacto financiero (evaluación cuantitativa). Ambos impactos son evaluados para los siguientes períodos de tiempo:

- 1 hora
- 2 horas
- 4 horas
- 24 horas
- 48 horas

- 1 semana

Si alguna actividad es menos urgente, se pueden alargar los períodos para esa actividad particular; por ejemplo de 4 horas a 2 semanas, o similar.

Para la evaluación general (1), los impactos se clasifican de la siguiente forma:

Tabla 28. Clasificación de impactos Banco KLM.

Consecuencia insignificante	1	La duración del incidente disruptivo no afecta significativamente las finanzas, las obligaciones legales o contractuales o el prestigio de la organización.
Consecuencia aceptable	2	La duración del incidente disruptivo provoca daños sobre las finanzas, las obligaciones legales o contractuales o el prestigio de la organización, pero ese daño todavía es aceptable teniendo en cuenta su magnitud y circunstancias específicas.
Consecuencia crítica	3	La duración del incidente disruptivo provoca daños sobre las finanzas, las obligaciones legales o contractuales o el prestigio de la organización y ese daño no es aceptable por su magnitud y circunstancias específicas.
Consecuencia catastrófica	4	La duración del incidente disruptivo provoca grandes daños sobre las finanzas, las obligaciones legales o contractuales o el prestigio de la organización que le harán perder la mayor parte de su capital y/o tendrá que cancelar sus operaciones en forma permanente.

Tomado de: (Kosutic, 2015)

Para la evaluación financiera (2), el impacto tiene que ser establecido en moneda local.

Determinación de la Interrupción máxima aceptable (MAO, por sus siglas en inglés)

La interrupción máxima aceptable o Período máximo tolerable de interrupción se determina en horas o días, de la siguiente forma:

- El tiempo más corto cuando el impacto general es nivel 3, o

- El tiempo más corto cando el impacto financiero es inaceptable en comparación con las acciones/ganancias/presupuesto/ingresos.

Cantidad de trabajo

En esta parte del análisis se identifican los períodos con los picos de mayor carga de trabajo y se establecen los objetivos mínimos de Continuidad del Negocio.

Recursos necesarios para la recuperación

Es necesario identificar los siguientes tipos de recursos:

- Personas
- Aplicaciones / bases de datos
- Datos almacenados en formato electrónico (no incluidos en aplicaciones / bases de datos)
- Datos almacenados en papel
- Equipos de TI y comunicaciones
- Canales de comunicación
- Otros equipos
- Instalaciones e infraestructura
- Capital de trabajo
- Servicios externos

Para cada recurso es necesario determinar las siguientes necesidades:

- Cantidad de recursos que se requieren para la recuperación de una actividad
- Si el recurso en cuestión es un Punto único de falla
- Tiempo que puede transcurrir hasta que se necesite el recurso (tiempo posterior a la reanudación de la actividad)

Dependencia de terceros

En esta parte del análisis es necesario identificar la dependencia en relación a (1) otras actividades, (2) socios externos y (3) proveedores.

Para cada socio externo y proveedor es necesario analizar lo siguiente:

- Qué documento define los requisitos en caso de un incidente disruptivo
- El nivel existente de capacidad para la Continuidad del Negocio

Pérdida máxima de datos

Para cada base de datos, aplicación o pieza de información identificada en el análisis, es necesario evaluar la cantidad máxima de datos que se pueden perder. La pérdida de datos se evalúa por la cantidad de datos creada en las últimas:

- 1 hora
- 4 horas
- 24 horas
- 48 horas
- 1 semana

Si es necesario, es posible acortar o alargar las escalas en una actividad particular para que se ajuste al tipo de datos de dicha actividad.

El impacto de la pérdida de datos se clasifica de la siguiente forma:

Tabla 29. Clasificación de impactos de acuerdo a la pérdida de datos.

Consecuencia insignificante	1	La cantidad de datos perdidos no afecta significativamente las finanzas, las obligaciones legales o contractuales o el prestigio de la organización.
Consecuencia aceptable	2	La cantidad de datos perdidos provoca daños sobre las finanzas, las obligaciones legales o contractuales o el prestigio de la organización, pero ese daño todavía es aceptable teniendo en cuenta su magnitud y circunstancias específicas.
Consecuencia crítica	3	La cantidad de datos perdidos provoca daños sobre las finanzas, las obligaciones legales o contractuales o el prestigio de la organización y ese daño no es aceptable teniendo en cuenta su magnitud y circunstancias específicas.
Consecuencia catastrófica	4	La cantidad de datos perdidos provoca grandes daños sobre las finanzas, las obligaciones legales o contractuales o el prestigio de la organización que le harán perder la mayor parte de su capital y/o tendrá que cancelar sus operaciones en forma permanente.

Tomado de: (Kosutic, 2015)

Presentación de los resultados

La información recabada mediante los Cuestionarios sobre el análisis del impacto en el negocio se envía al Coordinador de la Continuidad del Negocio, que tiene la responsabilidad de reunirla y documentarla a través de la Estrategia de Continuidad del Negocio.

Revisión periódica del análisis del impacto en el negocio

El Coordinador de la Continuidad del Negocio debe realizar una revisión de los Cuestionarios sobre el análisis del impacto en el negocio y, en función de ello, debe actualizar la Estrategia de Continuidad del Negocio. La revisión se realiza al menos una vez por año, o con mayor frecuencia en caso de cambios organizacionales significativos, cambios importantes en tecnología, en los objetivos de negocios, en el entorno empresarial, etc.

Gestión de registros guardados en base a este documento

Tabla 30. Gestión de registros del SGCN del Banco KLM.

Nombre del registro	Ubicación de archivo	Persona responsable del archivo	Controles para la protección del registro	Tiempo de retención
Cuestionarios sobre el análisis del impacto en el negocio (formulario electrónico, documento de Excel)	Ordenador del Coordinador de la Continuidad del Negocio	Coordinador de la Continuidad del Negocio	Los cuestionarios tienen que ser guardados en formato de sólo lectura.	Los datos son almacenados por el plazo de 5 años.

Adaptado de: (Kosutic, 2015)

Solamente el Coordinador de la Continuidad del Negocio puede permitir a otros empleados el acceso a los documentos mencionados precedentemente.

Validez y gestión de documentos

Este documento es válido desde el 3 de Agosto del 2015. El propietario de este documento es el Coordinador de la Continuidad del Negocio, que debe verificar

y, si es necesario, actualizar el documento por lo menos una vez al año, antes de la revisión periódica sobre los Cuestionarios sobre el análisis del impacto en el negocio.

Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- La cantidad de recursos no incluidos en los Cuestionarios sobre el análisis de la Continuidad del Negocio.
- La imposibilidad de recuperar actividades debido a errores en el proceso de análisis del impacto en el negocio.
- La cantidad de errores en el proceso de análisis del impacto en el negocio debido a definiciones poco claras de funciones y responsabilidades.

Apéndices

- Apéndice: Cuestionario sobre el análisis del impacto en el negocio

Gerente de Producción y Servicios

Ing. Luis Antonio Arevalo

_____

Firma

ANEXO 4.1 (a)

Cuestionario sobre el análisis del impacto en el negocio - Disponibilidad de los servicios de Comunicaciones

Anexo 4.1 (a): Metodología para el análisis del Impacto en el Negocio

Apéndice 1: Cuestionario sobre el análisis del impacto en el negocio - Disponibilidad de los servicios de Comunicaciones

Tabla 31. Cuestionario sobre el análisis del impacto en el negocio - Disponibilidad del Servicio de Comunicaciones.

1. Información general sobre la actividad			
Nombre de la organización:	Banco KLM	Nombre de la persona responsable:	Subgerente de Procesamiento e Infraestructura, Subgerente de Control Tecnológico
Nombre de la actividad:	Realizar acciones preventivas y correctivas para garantizar la disponibilidad de los servicios de Comunicaciones	Correo electrónico:	bsocasi@bklm.com.ec
Domicilio:	Quito, Av. Amazonas y Villalengua	Fecha:	03/08/2015

2. Descripción de la actividad		
Breve descripción de la actividad:	Tareas clave y obligaciones legales y/o contractuales:	Plazos de ejecución:
Mantener la funcionalidad operativa de los equipos de Comunicaciones, enlaces y los servicios de TI dependientes, mismos que son necesarios para la operatividad de los sistemas informáticos y actividades del negocio, para mantener la comunicación de los principales canales de los servicios Tecnológicos entregados por el Banco KLM.	Verificación del funcionamiento de los equipos de comunicaciones, en sitio Quito y Guayaquil	30min
	Pruebas de conectividad entre equipos de red	10min
	Verificación de alarmas y conexiones físicas	10min
	Monitoreo constante de los equipos de comunicaciones	5min
	Limpieza externa de los equipos de comunicaciones	30min
	Depuración de las configuraciones en los equipos	30min

	Verificación del ambiente en el Data Center, temperatura y humedad adecuada	5min
	Verificación del funcionamiento de la alta disponibilidad/respaldo de energía en el Data Center	5min

3. Impacto general del incidente disruptivo (1 - consecuencia insignificante; 2 - consecuencia aceptable; 3 - consecuencia mayor; 4 - consecuencia catastrófica)

	Descripción (si fuera necesario)	2 horas	4 horas	24 horas	48 horas	1 semana
Pérdida de la reputación de la organización en el mercado:	Nivel de posicionamiento en el mercado	2	2	3	3	4
Reacciones de los clientes:	Opinión de los clientes durante la paralización de la actividad	2	3	3	4	4
Impacto sobre otras actividades de la organización:	Otras actividades que se ven afectadas con la suspensión de este servicio	2	2	3	3	4
Consecuencias sobre la salud y seguridad del personal; consecuencias sobre el medioambiente:	Como se afecta la salud del personal cuando ocurre la suspensión del servicio y las consecuencias que pueda sufrir el ambiente dentro o fuera del entorno de trabajo	1	1	1	2	3
Qué tan difícil será ponerse al día con el trabajo atrasado:	Consecuencias que se tendrá para ponerse al día con el trabajo atrasado por la suspensión del servicio	1	2	3	3	4

4. Impacto financiero del incidente disruptivo: ¿Cuál sería la pérdida financiera producida por el incidente disruptivo (en dólares)

	Descripción (si fuera necesario)	2 horas	4 horas	24 horas	48 horas	1 semana
Consecuencias legales:	Gastos generados por incumplimiento con clientes	0	0	0	0	10.000

Consecuencias contractuales:	Pagos por multas en servicios entregados a asociados	0	0	5.000	10.000	30.000
Pérdida de ingresos de potenciales clientes:	Ventas a clientes nuevos	2.000	4.000	25.000	50.000	200.000
Pérdida de ingresos de clientes actuales:	Consumos de clientes actuales, fin de semana mayor volumen de ventas	20.000	40.000	240.000	480.000	1.680.000
Gastos adicionales (reparaciones, mantenimiento, etc.)	Costos adicionales a los contratos de mantenimiento vigentes, movilización de recursos	0	0	500	1.000	2.000

5. Comentarios / otra información importante:

Si ocurriese un incidente disruptivo con respecto a la actividad de DISPONIBILIDAD DEL SERVICIO DE COMUNICACIONES, esto paraliza todas la demás actividades de la organización, lo cual incurre pérdidas de gran magnitud para el Banco KLM.

6. Conclusiones (a completar por el Coordinador de gestión de Continuidad del Negocio)

Período máximo tolerable de interrupción (interrupción máxima aceptable):	4 horas

7. Cantidad de trabajo

Período(s) con mayor cantidad de trabajo:	Los meses de: mayo, julio, noviembre y diciembre
Cantidad de trabajo realizada durante períodos con mayor cantidad de trabajo:	8 incidentes resueltos en el servicio de Comunicaciones
Cantidad mínima aceptable de trabajo para la actividad inmediatamente después del desastre:	2 incidentes resueltos en el servicio de Comunicaciones por mes

Período a partir del cual se debe retomar la cantidad de trabajo o nivel de funcionamiento normal:	48 horas

8. Recursos necesarios para la recuperación

Nombre del recurso	Información específica	Cantidad	Punto único de falla	Tiempo a partir del cual es necesario el recurso						
				inmediatamente	1 hora	4 horas	24 horas	2 días	1 semana	otro (especificar)
Personas:										
Jefe de Comunicaciones	Liderazgo y Configuración de equipos de Comunicaciones	1			X					
Administrador de Comunicaciones	Administración los equipos de Comunicaciones, redes LAN, WAN, SAN; configuración, monitoreo, troubleshooting	1		X						
Administrador de Telefonía	Administración los equipos de Telefonía, configuración, monitoreo, troubleshooting	1		X						

Técnico de Comunicaciones	Soporte operativo y funcional de los equipos de Comunicaciones, redes	2				X				
Aplicaciones / bases de datos:										
Sistema operativo de Switches	Software para la actualización del SO de los switches	6		X						
Sistema operativo de Firewalls	Software para la actualización del SO de los Firewalls	3		X						
Sistema operativo de Routers	Software para la actualización del SO de los Routers	5		X						
Sistema operativo de Ips	Software para la actualización del SO de los IPS	2		X						
Software de monitoreo de redes	WhatsUp Gold, Solarwinds, Quest Network Tools, Cisco Prime	4		X						
Sistema operativo de Centrales Telefónicas	Software para la actualización del SO de las Centrales Telefónicas	2		X						
Software de reportería	Cat Tools Enterprise	1		X						
Datos almacenados en formato electrónico (no incluidos en aplicaciones / bases de datos):										

Copia de respaldo de configuración de equipos de comunicación (switches, firewalls, routers, centrales telefónicas, IPs)	Almacenados en un Servidor de Comunicaciones con seguridades y PC de Administrador de Comunicaciones	2		X						
Arquitectura de red institucional	Almacenado en un repositorio/server con seguridades	1		X						
Manuales digitales de los equipos de Comunicaciones	Almacenado en un repositorio/server con seguridades	1		X						
Respaldos de Bases de Datos de los equipos destinados para monitoreo de la Red	Almacenados en un Servidor de Comunicaciones con seguridades	1			X					
Instaladores y licencias del Software de Monitoreo	Almacenados en un Servidor de Comunicaciones con seguridades	1		X						
Datos almacenados en papel:										
Arquitectura de red institucional impresa	Archivador de Jefatura y Administrador de Comunicaciones	2		X						
Manuales impresos para la configuración de los equipos de Comunicaciones	Archivador de Jefatura y Administrador de Comunicaciones	2		X						

Contactos internos y externos para la gestión de TI	Archivador de Jefatura y Administrador de Comunicaciones	2		X						
Equipos de TI y comunicaciones:										
PCs de escritorio	AllOne Core i7 2.4 GHz, 8 GB de memoria ram, disco duro sata de 1TB, 2 monitores LCD, teclado completo y mouse.	2		X						
Laptop	AllOne Core i5 3.0 GHz, 8 GB de memoria ram, disco duro de 500 GB	2		X						
Servidor	Servidor físico Lenovo i7, 2.4 GHz, 8 GB de memoria ram, disco duro sata de 500 GB.	1				X				
Servidor	Servidor virtual ubicado en el Data Center, Intel Xeon 2.9 GHz, 8 GB de memoria ram, disco duro SCSI de 500 GB, Windows server 2008 R2	1			X					
Switch	Cisco Nexus 7k	2		X						
Switch	Cisco Nexus 2k	8		X						

Switch	Cisco Catalyst 6500	2		X						
Switch	Cisco Catalyst 4500	2		X						
Switch	Cisco Catalyst 3850	4		X						
Switch	Cisco Catalyst 2960	30			X					
Firewall	Cisco ASA 5585	2		X						
Firewall	Cisco ASA 5540	2		X						
Firewall	Cisco ASA 5520	2		X						
Router	Cisco ASR 1000	4		X						
Router	Cisco 3900	4		X						
Router	Cisco 2900	4		X						
Router	Cisco 1900	4			X					
Router	Cisco 881	10				X				
IPS	Proventia GX6116	2		X						
Impresora	Xerox workcentre	2					X			
Teléfono	Teléfono IP Alcatel 4038	4			X					
Teléfono Celular	BlackBerry Curve, con paquete de datos	4		X						
Canales de comunicación:										
Líneas fijas de teléfono	Líneas habilitadas de telefonía fija con salida a celulares	4			X					

Líneas celulares	Teléfonos celulares habilitados con paquetes de voz, datos y salida internacional	3		X						
Acceso a internet	Enlace dedicado fibra óptica de 35Mbps	2			X					
Correo electrónico	Servidor de correo con cuentas habilitadas, con capacidad de 5 MB	2			X					
Otros equipos:										
Televisor	Televisor Panasonic de 42"	1				X				
Instalaciones e infraestructura:										
Puntos de Red de computadoras	Red LAN de cableado vertical y horizontal categoría 6a	8			X					
BackBone de servidores	Red LAN, SAN de cableado de Fibra Óptica	50		X						
Muebles de oficina	Sillas y escritorios individuales para uso del personal técnico	6			X					
Capital de trabajo necesario:										

Capital inicial necesario	Para habilitación de los principales recursos no existentes	10000		X						
Servicios externos:										
Electricidad	Alimentación eléctrica de la red pública	2		X						
Agua potable	Servicio de agua potable	1		X						
Oficinas	Renta de Oficinas para uso del personal de Comunicaciones	1		X						

9. Dependencia de terceros (quién es necesario para la recuperación de esta actividad)			
Dependencia de otras actividades de la organización:		Qué documentos o procedimientos definen cómo se asegura la Continuidad del Negocio para productos o servicios suministrados por socios o proveedores ante el caso de un incidente disruptivo:	Evaluación de sus capacidades existentes para Continuidad del Negocio (1 - inadecuada; 2 - alguna capacidad tiene pero debe ser mejorada; 3 - adecuada):
Dependencia de socios:			
Dependencia de proveedores:	Telconet	Contrato de servicio de enlaces	2
	Cnt	Contrato de servicio de enlaces, telefonía	1
	Level3	Contrato de servicio de enlaces	2
	AT&T	Contrato de servicio de enlaces	2
	Claro	Contrato de servicio de telefonía	2

	Empresa eléctrica	Contrato de servicio básico	2
	Todouno	Contrato de servicio de internet	2

10. Pérdida máxima de datos: cantidad de datos que se pueden perder (1 - consecuencia insignificante; 2 - cons. aceptable; 3 - cons. mayor; 4 - cons. catastrófica)

	1 hora	4 horas	24 horas	48 horas	1 semana	¿Se crean copias de seguridad? (SÍ/NO) ¿Con qué frecuencia?
Aplicaciones / bases de datos:						
Sistema operativo de Switches	2	3	3	4	4	Semanal
Sistema operativo de Firewalls	2	3	3	4	4	Semanal
Sistema operativo de Routers	2	3	3	4	4	Semanal
Sistema operativo de Ips	2	3	3	4	4	Semanal
Software de monitoreo de redes	1	2	3	3	4	Semanal
Sistema operativo de Centrales Telefónicas	2	3	3	4	4	Semanal
Software de reportería	1	2	3	3	4	Semanal
Datos almacenados en formato electrónico:						
Copia de respaldo de configuración de equipos de comunicación (switches, firewalls, routers, centrales telefónicas, IPs)	2	3	3	4	4	Diaria
Arquitectura de red institucional	1	1	1	2	3	Mensual
Manuales digitales de los equipos de Comunicaciones	1	2	3	3	4	Mensual
Respaldos de Bases de Datos de los equipos destinados para monitoreo de la Red	1	1	2	3	4	Mensual
Instaladores y licencias del Software de Monitoreo	1	1	2	3	4	Mensual
Datos almacenados en papel:						
Arquitectura de red institucional impresa	1	1	1	2	3	Mensual

Manuales impresos para la configuración de los equipos de Comunicaciones	1	2	3	3	4	Mensual
Contactos internos y externos para la gestión de TI	1	2	3	3	4	Mensual
11. Alternativas en el caso de un desastre						
¿Pueden otras actividades continuar con el funcionamiento de esta actividad? En caso afirmativo, ¿cuáles?	NINGUNA					
¿Es posible realizar algunas actividades en forma manual, sin equipos de TI ni de otro tipo?	NO, NINGUNA					
12. Experiencias anteriores						
¿Con qué frecuencia se han producido incidentes disruptivos en el negocio hasta ahora? ¿Cuánto tiempo duraron?	1 vez al año, duro 2 días					
¿Cómo se manejaron esas situaciones?	Se manejó de forma improvisada, primero descartando todas las posibles causas y luego levantando los servicios de manera rápida mientras se encontraba la causa exacta del problema y su posterior corrección					
13. Comentarios / otra información importante:						
Las comunicaciones dentro del banco constituyen un eje fundamental para el negocio						

Adaptado de: (Kosutic, 2015).

ANEXO 4.1 (b)

Cuestionario sobre el análisis del impacto en el negocio - Disponibilidad de los aplicativos de Core Bancario y Negocios.

Anexo 4.1 (b): Metodología para el análisis del Impacto en el Negocio.

Apéndice 1: Cuestionario sobre el análisis del impacto en el negocio - Disponibilidad de los aplicativos de Core Bancario y Negocios.

Tabla 32. Cuestionario sobre el análisis del impacto en el negocio - Disponibilidad de los aplicativos de Core Bancario y Negocios.

1. Información general sobre la actividad			
Nombre de la organización:	Banco KLM	Nombre de la persona responsable:	Gerente de Producción y Servicios , Jefe de Centro de Computo
Nombre de la actividad:	Realizar acciones preventivas y correctivas para garantizar la disponibilidad de los aplicativos de Core Bancario y Negocios	Correo electrónico:	laarevalo@bklm.com.ec
Domicilio:	Quito, Av. Amazonas y Villalengua	Fecha:	03/08/2015

2. Descripción de la actividad		
Breve descripción de la actividad:	Tareas clave y obligaciones legales y/o contractuales:	Plazos de ejecución:
Consiste en realizar pruebas de verificación para mantener operativos y funcionado los equipos donde se encuentran almacenados los sistemas o aplicaciones de Core Bancario y Negocio.	Verificación del correcto funcionamiento de los servidores de aplicaciones de Core Bancario y Negocios	10min
	Pruebas de conectividad de los servidores y bases de datos	10min
	Verificación de alarmas y conexiones físicas	10min
	Monitoreo constante del aplicativo de Core Bancario	10min

	Verificar la disponibilidad de los equipos de Comunicaciones	15min
	Limpieza externa de los servidores de Core Bancario y Negocios	30min
	Depuración de las configuraciones en los equipos	30min
	Verificación del ambiente en el Data Center, temperatura y humedad adecuada	5min
	Verificación del funcionamiento de la alta disponibilidad/respaldo de energía en el Data Center	5min
	Escalar el incidente al proveedor de la aplicación, equipo en caso de ser necesario	10min
	Respuesta del proveedor una vez escalado el incidente	15min
	Solución al problema por parte del proveedor (caso extremo)	24 horas

3. Impacto general del incidente disruptivo (1 - consecuencia insignificante; 2 - consecuencia aceptable; 3 - consecuencia mayor; 4 - consecuencia catastrófica)

	Descripción (si fuera necesario)	2 horas	4 horas	24 horas	48 horas	1 semana
Pérdida de la reputación de la organización en el mercado:	Nivel de posicionamiento en el mercado	1	2	3	4	4
Reacciones de los clientes:	Opinión de los clientes durante la paralización de la actividad	1	2	3	3	4
Impacto sobre otras actividades de la organización:	Otras actividades que se ven afectadas con la suspensión de este servicio	1	2	3	3	4

Consecuencias sobre la salud y seguridad del personal; consecuencias sobre el medioambiente:	Como se afecta la salud del personal cuando ocurre la suspensión del servicio y las consecuencias que pueda sufrir el ambiente dentro o fuera del entorno de trabajo	1	2	2	3	3
Qué tan difícil será ponerse al día con el trabajo atrasado:	Consecuencias que se tendrá para ponerse al día con el trabajo atrasado por la suspensión del servicio	1	2	2	3	4

4. Impacto financiero del incidente disruptivo: ¿Cuál sería la pérdida financiera producida por el incidente disruptivo (en [moneda local])

	Descripción (si fuera necesario)	2 horas	4 horas	24 horas	48 horas	1 semana
Consecuencias legales:	Gastos generados por incumplimiento con clientes	0	0	0	0	10.000
Consecuencias contractuales:	Pagos por multas en servicios entregados a asociados	0	0	5.000	10.000	30.000
Pérdida de ingresos de potenciales clientes:	Ventas a clientes nuevos	2.000	4.000	25.000	50.000	200.000
Pérdida de ingresos de clientes actuales:	Consumos de clientes actuales, fin de semana mayor volumen de ventas	20.000	40.000	240.000	480.000	1.680.000
Gastos adicionales (reparaciones, mantenimiento, etc.)	Costos adicionales a los contratos de mantenimiento vigentes, movilización de recursos	500	1.000	2.000	5.000	10.000

5. Comentarios / otra información importante:

Si ocurriese un incidente disruptivo con respecto a la actividad de DISPONIBILIDAD DEL SERVICIO DE APLICATIVOS DE CORE BANCARIO Y NEGOCIOS, esto paraliza el todas las actividades Bancarias de la Organización, derivando en pérdidas financieras para el Banco KLM.

6. Conclusiones (a completar por el Coordinador de gestión de Continuidad del Negocio)

Período máximo tolerable de interrupción (interrupción máxima aceptable):	2 horas

7. Cantidad de trabajo	
Período(s) con mayor cantidad de trabajo:	Los meses de: mayo, julio, noviembre y diciembre
Cantidad de trabajo realizada durante períodos con mayor cantidad de trabajo:	4 incidentes resueltos en el servicio de Aplicativos de Core Bancario y Negocios
Cantidad mínima aceptable de trabajo para la actividad inmediatamente después del desastre:	1 incidente resuelto en el servicio de Aplicativos de Core Bancario y Negocios por mes
Período a partir del cual se debe retomar la cantidad de trabajo o nivel de funcionamiento normal:	24 horas

8. Recursos necesarios para la recuperación

Nombre del recurso	Información específica	Cantidad	Punto único de falla	Tiempo a partir del cual es necesario el recurso						
				inmediatamente	1 hora	4 horas	24 horas	2 días	1 semana	otro (especificar)
Personas:										
Gerente de Producción y Servicios	Liderazgo, comunicación, decisión, coordinación	1		X						

Jefe de Servidores	Liderazgo y Configuración de servidores, bases de datos, aplicativos	1		X						
Jefe de Centro de Computo	Liderazgo, configuración de sistemas y aplicaciones de Core Bancario (AS400)	1		X						
Jefe de Comunicaciones	Liderazgo y Configuración de equipos de Comunicaciones	1		X						
Administrador de Servidores	Administrar los servidores de Aplicativos, bases de datos; configuración, monitoreo, troubleshooting	2		X						
Administrador de Comunicaciones	Administración los equipos de Comunicaciones, redes LAN, WAN, SAN; configuración, monitoreo, troubleshooting	1		X						

Analista de Monitoreo	Soporte operativo y funcional de los aplicativos de Monitoreo	2		X						
Aplicaciones / bases de datos:										
Sistema AS400	Sistemas de Core Bancario	4		X						
Microsoft SQL Server 2005	Gestor de Base de datos SQL Server 2005	2			X					
Sistemas Operativos de Comunicaciones	Software para Comunicaciones de datos	2		X						
PeopleSoft, CRM, ERP	Sistemas de Negocio	2		X						
Big Data	Almacenamiento y gestión de la información del Banco	4		X						
Datos almacenados en formato electrónico (no incluidos en aplicaciones / bases de datos):										
Copia de respaldo de configuración de los servidores y bases de datos	Almacenados en un Servidor del Centro de Computo bajo seguridades informáticas	2		X						

Detalle diario de transacciones financieras (consumos)	Almacenado en un repositorio/server con seguridades	2		X						
Copias diarias de respaldo de las bases de datos del Core Bancario	Almacenado en un repositorio/server con seguridades	1			X					
Paquete instalador de los gestores de bases de datos, Core Bancario y aplicativos de Negocios	Almacenados en un Servidor del Centro de Computo con seguridades informáticas	2		X						
Estados de cuenta de los Clientes	Almacenados en un Servidor del Centro de Computo bajo seguridades informáticas	2				X				
Datos almacenados en papel:										
Reporte consolidado del movimiento financiero diario	Archivador de Gerencia de Negocios y Financiera	2				X				
Manuales impresos para la configuración y manejo aplicativos de Core Bancario	Archivador de Jefaturas de Servidores y Soporte Técnico	2		X						

Contactos internos y externos para la gestión de TI	Archivador de las Jefaturas y Administradores de Comunicaciones, Servidores, Centro de Computo	2		X						
Equipos de TI y comunicaciones:										
PCs de escritorio	AllOne Core i7 2.4 GHz, 8 GB de memoria ram, disco duro sata de 1TB, 2 monitores LCD, teclado completo y mouse.	9		X						
Laptop	AllOne Core i5 3.0 GHz, 8 GB de memoria ram, disco duro de 500 GB	3		X						
Servidor de Monitoreo AS400	Servidor físico Lenovo i7, 2.4 GHz, 8 GB de memoria ram, disco duro sata de 500 GB.	4		X						
Servidor de Aplicaciones	IBM Power 8000	2		X						
Impresora	Xerox workcentre	4				X				

Teléfono	Teléfono IP Alcatel 4038	9			X					
Teléfono Celular	BlackBerry Curve, con paquete de datos	9		X						
Canales de comunicación:										
Líneas fijas de teléfono	Líneas habilitadas de telefonía fija con salida a celulares	9			X					
Líneas celulares	Teléfonos celulares habilitados con paquetes de voz, datos y salida internacional	9		X						
Acceso a internet	Enlace dedicado fibra óptica de 35Mbps	2		X						
Correo electrónico	Cuentas para reporte de alarmas e incidencias	9			X					
Otros equipos:										
Televisor	Televisor Panasonic de 42"	3				X				
Instalaciones e infraestructura:										

Puntos de Red de computadoras	Red LAN de cableado vertical y horizontal categoría 6a	15			X					
BackBone de equipos de Core Bancario	Red LAN, SAN de cableado de Fibra Óptica	30		X						
Muebles de oficina	Sillas y escritorios individuales para uso del personal técnico	15			X					
Capital de trabajo necesario:										
Capital inicial necesario	Para habilitación de los principales recursos no existentes	25000		X						
Servicios externos:										
Electricidad	Alimentación eléctrica de la red pública	2		X						
Agua potable	Servicio de agua potable	1		X						
Oficinas	Renta de Oficinas para uso del personal de Comunicaciones	1		X						

Servicios de soporte del proveedor correspondiente	Servicio de soporte de las empresas proveedoras de los aplicativos	1		X						

9. Dependencia de terceros (quién es necesario para la recuperación de esta actividad)			
Dependencia de otras actividades de la organización:		Qué documentos o procedimientos definen cómo se asegura la Continuidad del Negocio para productos o servicios suministrados por socios o proveedores ante el caso de un incidente disruptivo:	Evaluación de sus capacidades existentes para Continuidad del Negocio (1 - inadecuada; 2 - alguna capacidad tiene pero debe ser mejorada; 3 - adecuada):
Dependencia de socios:			
Dependencia de proveedores:	IBM	Contrato de servicio de Core Bancario	2
	Kruger	Contrato de servicio de Core Bancario	1
	TATA	Contrato de servicio de Core Bancario	2
	Qmatic	Contrato de servicio de Negocio	2
	CNT	Contrato de servicio de telefonía	2
	Empresa eléctrica	Contrato de servicio básico	2
	Todouno	Contrato de servicio de internet	2

10. Pérdida máxima de datos: cantidad de datos que se pueden perder (1 - consecuencia insignificante; 2 - cons. aceptable; 3 - cons. mayor; 4 - cons. catastrófica)						
	1 hora	4 horas	24 horas	48 horas	1 semana	¿Se crean copias de seguridad? (SÍ/NO) ¿Con qué frecuencia?
Aplicaciones / bases de datos:						
Sistema AS400	2	3	3	4	4	Diario

Microsoft SQL Server 2005	1	2	3	4	4	Diario
Sistemas Operativos de Comunicaciones	1	2	3	3	4	Semanal
PeopleSoft, CRM, ERP	1	2	3	3	4	Semanal
Big Data	1	2	3	4	4	Diario
Datos almacenados en formato electrónico:						
Copia de respaldo de configuración de los servidores y bases de datos	1	2	3	3	4	Semanal
Detalle diario de transacciones financieras (consumos)	2	2	3	3	4	Diario
Copias diarias de respaldo de las bases de datos del Core Bancario	2	2	3	4	3	Diario
Paquete instalador de los gestores de bases de datos, Core Bancario y aplicativos de Negocios	1	2	3	4	4	Semanal
Estados de cuenta de los Clientes	1	2	2	3	4	Diario
Datos almacenados en papel:						
Reporte consolidado del movimiento financiero diario	1	2	2	3	4	Diario
Manuales impresos para la configuración y manejo aplicativos de Core Bancario	1	1	2	3	3	Mensual
Contactos internos y externos para la gestión de TI	1	2	3	3	4	Semanal
11. Alternativas en el caso de un desastre						

¿Pueden otras actividades continuar con el funcionamiento de esta actividad? En caso afirmativo, ¿cuáles?	NINGUNA
¿Es posible realizar algunas actividades en forma manual, sin equipos de TI ni de otro tipo?	NO, NINGUNA
12. Experiencias anteriores	
¿Con qué frecuencia se han producido incidentes disruptivos en el negocio hasta ahora? ¿Cuánto tiempo duraron?	1 vez al año, duro 4 horas
¿Cómo se manejaron esas situaciones?	Se manejó de forma improvisada, primero levantando los servicios de manera URGENTE mediante BackUps, para posteriormente encontrar la causa exacta del problema y corrección
13. Comentarios / otra información importante:	
Los servidores y bases de datos de aplicativos de Core Bancario poseen arquitecturas/arreglos en alta disponibilidad	

Adaptado de: (Kosutic, 2015).

ANEXO 4.1 (c)

Cuestionario sobre el análisis del impacto en el negocio - Disponibilidad de los sistemas y aplicativos Administrativos, Financieros y Tecnológicos.

Anexo 4.1 (c): Metodología para el análisis del Impacto en el Negocio.

Apéndice 1: Cuestionario sobre el análisis del impacto en el negocio - Disponibilidad de los sistemas y aplicativos Administrativos, Financieros y Tecnológicos.

Tabla 33. Cuestionario sobre el análisis del impacto en el negocio - Disponibilidad de los sistemas y aplicativos Administrativos, Financieros y Tecnológicos.

1. Información general sobre la actividad			
Nombre de la organización:	Banco KLM	Nombre de la persona responsable:	Subgerente de Procesamiento e Infraestructura, Subgerente de Servicios Tecnológicos
Nombre de la actividad:	Realizar acciones preventivas y correctivas para garantizar las disponibilidad de los sistemas y aplicativos Administrativos, Financieros y Tecnológicos	Correo electrónico:	bsocasi@bklm.com.ec
Domicilio:	Quito, Av. Amazonas y Villalengua	Fecha:	03/08/2015

2. Descripción de la actividad		
Breve descripción de la actividad:	Tareas clave y obligaciones legales y/o contractuales:	Plazos de ejecución:
Consiste en realizar pruebas de verificación en primer nivel del funcionamiento de los equipos donde se encuentran almacenados los sistemas o aplicaciones informáticas	Verificación del correcto funcionamiento de los servidores de aplicaciones y base de datos	30min
	Pruebas de conectividad de los servidores y bases de datos	15min
	Verificación de alarmas y conexiones físicas	15min

Para situaciones de cambios, correcciones en la configuración o actualizaciones de versión se escalará el incidente al respectivo proveedor.	Monitoreo constante de los aplicativos, servidores y bases de datos	10min
	Verificar la disponibilidad de los equipos de Comunicaciones	15min
	Limpieza externa de los servidores	60min
	Depuración de las configuraciones en los equipos	30min
	Verificación del ambiente en el Data Center, temperatura y humedad adecuada	5min
	Verificación del funcionamiento de la alta disponibilidad/respaldo de energía en el Data Center	5min
	Escalar el incidente al proveedor de la aplicación, equipo en caso de ser necesario	30min
	Respuesta del proveedor una vez escalado el incidente	15min
	Solución al problema por parte del proveedor (caso extremo)	24 horas

3. Impacto general del incidente disruptivo (1 - consecuencia insignificante; 2 - consecuencia aceptable; 3 - consecuencia mayor; 4 - consecuencia catastrófica)

	Descripción (si fuera necesario)	2 horas	4 horas	24 horas	48 horas	1 semana
Pérdida de la reputación de la organización en el mercado:	Nivel de posicionamiento en el mercado	1	2	2	3	4
Reacciones de los clientes:	Opinión de los clientes durante la paralización de la actividad	1	1	2	3	4

Impacto sobre otras actividades de la organización:	Otras actividades que se ven afectadas con la suspensión de este servicio	1	1	2	3	4
Consecuencias sobre la salud y seguridad del personal; consecuencias sobre el medioambiente:	Como se afecta la salud del personal cuando ocurre la suspensión del servicio y las consecuencias que pueda sufrir el ambiente dentro o fuera del entorno de trabajo	1	1	1	2	3
Qué tan difícil será ponerse al día con el trabajo atrasado:	Consecuencias que se tendrá para ponerse al día con el trabajo atrasado por la suspensión del servicio	1	2	2	2	3

4. Impacto financiero del incidente disruptivo: ¿Cuál sería la pérdida financiera producida por el incidente disruptivo (en [moneda local])

	Descripción (si fuera necesario)	2 horas	4 horas	24 horas	48 horas	1 semana
Consecuencias legales:	Gastos generados por incumplimiento con clientes	0	0	0	0	500
Consecuencias contractuales:	Pagos por multas en servicios entregados a asociados	0	0	5.000	10.000	30.000
Pérdida de ingresos de potenciales clientes:	Ventas a clientes nuevos	1.000	2.000	10.000	20.000	100.000
Pérdida de ingresos de clientes actuales:	Consumos de clientes actuales, fin de semana mayor volumen de ventas	5.000	10.000	100.000	250.000	800.000
Gastos adicionales (reparaciones, mantenimiento, etc.)	Costos adicionales a los contratos de mantenimiento vigentes, movilización de recursos	500	1.000	2.000	5.000	10.000

5. Comentarios / otra información importante:

Si ocurriese un incidente disruptivo con respecto a la actividad de DISPONIBILIDAD DEL SERVICIO DE APLICATIVOS FINANCIEROS, ADMINISTRATIVOS Y TECNOLÓGICOS, esto paraliza gran parte de las demás actividades de la organización, lo cual incurre pérdidas considerables para el Banco KLM.

6. Conclusiones (a completar por el Coordinador de gestión de Continuidad del Negocio)	
Período máximo tolerable de interrupción (interrupción máxima aceptable):	48 horas

7. Cantidad de trabajo	
Período(s) con mayor cantidad de trabajo:	Los meses de: mayo, julio, noviembre y diciembre
Cantidad de trabajo realizada durante períodos con mayor cantidad de trabajo:	20 incidentes resueltos en el servicio de Aplicativos Financieros, Administrativos y Tecnológicos
Cantidad mínima aceptable de trabajo para la actividad inmediatamente después del desastre:	4 incidentes resueltos en el servicio de Aplicativos Financieros, Administrativos y Tecnológicos por mes
Período a partir del cual se debe retomar la cantidad de trabajo o nivel de funcionamiento normal:	48 horas

8. Recursos necesarios para la recuperación										
Nombre del recurso	Información específica	Cantidad	Punto único de falla	Tiempo a partir del cual es necesario el recurso						
				inmediatamente	1 hora	4 horas	24 horas	2 días	1 semana	otro (especificar)
Personas:										

Jefe de Monitoreo	Liderazgo y Configuración de aplicativos de Monitoreo	1			X					
Jefe de Servidores	Liderazgo y Configuración de servidores, bases de datos, aplicativos	1			X					
Jefe de Soporte Técnico	Liderazgo, configuración de sistemas operativos, soporte operativo y funcional de aplicaciones	1			X					
Jefe de Mesa de Servicios	Liderazgo, comunicación y soporte funcional de los aplicativos del Banco	1			X					
Administrador de Servidores	Administrar los servidores de Aplicativos, bases de datos; configuración, monitoreo, troubleshooting	6		X						

Analista de Monitoreo	Soporte operativo y funcional de los aplicativos de Monitoreo	2		X						
Técnico de Soporte	Soporte operativo y funcional de las aplicaciones institucionales, asistente de redes y soporte de equipos informáticos	4				X				
Aplicaciones / bases de datos:										
Oracle 11g	Gestor de Base de datos Oracle 11g	2		X						
Microsoft SQL Server 2005	Gestor de Base de datos SQL Server 2005	2		X						
Office 2010	Paquetes de Licencias corporativas adquirida por el Banco	4				X				
Correo electrónico exchange	Correo electrónico corporativo enterprise	2			X					

PeopleSoft	Gestor de casos y reportes	4			X					
Business intelligence	Software para gestión de la información del Banco	2			X					
SharePoint	Software para colaboración del Banco	2					X			
Datos almacenados en formato electrónico (no incluidos en aplicaciones / bases de datos):										
Copia de respaldo de configuración de los servidores y bases de datos	Almacenados en un Servidor del Centro de Computo bajo seguridades informáticas	2		X						
Arquitectura de conexiones IT	Almacenado en un repositorio/server con seguridades	1		X						
Manuales digitales de los servidores, aplicativos y bases de datos	Almacenado en un repositorio/server con seguridades	1		X						

Paquete instalador de los gestores de bases de datos utilizados en la institución	Almacenados en un Servidor del Centro de Computo bajo seguridades informáticas	2			X					
Instaladores de los sistemas operativos manejados en la institución y de las herramientas administrativas, financieras y tecnológicas de gestión de aplicaciones	Almacenados en un Servidor del Centro de Computo bajo seguridades informáticas	2			X					
Datos almacenados en papel:										
Arquitectura de conexiones IT	Archivador de Jefatura y Administrador de Servidores	2		X						
Manuales impresos para la configuración de servidores, aplicaciones y bases de datos	Archivador de Jefaturas de Servidores y Soporte Técnico	2		X						

Contactos internos y externos para la gestión de TI	Archivador de Jefaturas de Mesa de Servicios y Analista de Soluciones	2		X						
Equipos de TI y comunicaciones:										
PCs de escritorio	AllOne Core i7 2.4 GHz, 8 GB de memoria ram, disco duro sata de 1TB, 2 monitores LCD, teclado completo y mouse.	16		X						
Laptop	AllOne Core i5 3.0 GHz, 8 GB de memoria ram, disco duro de 500 GB	2		X						
Servidor de Monitoreo	Servidor físico Lenovo i7, 2.4 GHz, 8 GB de memoria ram, disco duro sata de 500 GB.	4				X				

Servidor de Aplicaciones	Servidor virtual ubicado en el Data Center, Intel Xeon 2.9 GHz, 8 GB de memoria ram, disco duro SCSI de 500 GB, Windows server 2008 R2	30		X						
Impresora	Xerox workcentre	3					X			
Teléfono	Teléfono IP Alcatel 4038	16			X					
Teléfono Celular	BlackBerry Curve, con paquete de datos	10		X						
Canales de comunicación:										
Líneas fijas de teléfono	Líneas habilitadas de telefonía fija con salida a celulares	6			X					
Líneas celulares	Teléfonos celulares habilitados con paquetes de voz, datos y salida internacional	10		X						

Acceso a internet	Enlace dedicado fibra óptica de 35Mbps	2			X					
Correo electrónico	Cuentas masivas para reporte de alarmas e incidencias	4			X					
Otros equipos:										
Televisor	Televisor Panasonic de 42"	3				X				
Instalaciones e infraestructura:										
Puntos de Red de computadoras	Red LAN de cableado vertical y horizontal categoría 6a	16			X					
BackBone de servidores	Red LAN, SAN de cableado de Fibra Óptica	50		X						
Muebles de oficina	Sillas y escritorios individuales para uso del personal técnico	20			X					
Capital de trabajo necesario:										

Capital inicial necesario	Para habilitación de los principales recursos no existentes	15000		X						
Servicios externos:										
Electricidad	Alimentación eléctrica de la red pública	2		X						
Agua potable	Servicio de agua potable	1		X						
Oficinas	Renta de Oficinas para uso del personal de Comunicaciones	1		X						
Servicios de soporte del proveedor correspondiente	Servicio de soporte de las empresas proveedoras de los aplicativos	1		X						

9. Dependencia de terceros (quién es necesario para la recuperación de esta actividad)			
Dependencia de otras actividades de la organización:		Qué documentos o procedimientos definen cómo se asegura la Continuidad del Negocio para productos o servicios suministrados por socios o proveedores ante el caso de un incidente disruptivo:	Evaluación de sus capacidades existentes para Continuidad del Negocio (1 - inadecuada; 2 - alguna capacidad tiene pero debe ser mejorada; 3 - adecuada):
Dependencia de socios:			

Dependencia de proveedores:	IBM	Contrato de servicio de servidores y aplicaciones	2
	Desca	Contrato de servicio de aplicaciones	1
	Kruger	Contrato de servicio de aplicaciones	2
	Teradata	Contrato de servicio de almacenamiento	2
	CNT	Contrato de servicio de telefonía	2
	Empresa eléctrica	Contrato de servicio básico	2
	Todouno	Contrato de servicio de internet	2

10. Pérdida máxima de datos: cantidad de datos que se pueden perder (1 - consecuencia insignificante; 2 - cons. aceptable; 3 - cons. mayor; 4 - cons. catastrófica)

	1 hora	4 horas	24 horas	48 horas	1 semana	¿Se crean copias de seguridad? (SÍ/NO) ¿Con qué frecuencia?
Aplicaciones / bases de datos:						
Oracle 11g	1	2	2	3	4	Semanal
Microsoft SQL Server 2005	1	2	2	3	4	Semanal
Office 2010	1	1	1	2	3	Semanal
Correo electrónico exchange	1	1	2	3	4	Semanal
PeopleSoft	1	2	3	3	4	Semanal
Business intelligence	1	2	3	3	4	Semanal
SharePoint	1	1	2	2	3	Semanal
Datos almacenados en formato electrónico:						
Copia de respaldo de configuración de los servidores y bases de datos	1	2	3	4	4	Mensual

Arquitectura de conexiones IT	1	1	1	2	3	Mensual
Manuales digitales de los servidores, aplicativos y bases de datos	1	1	2	3	3	Mensual
Paquete instalador de los gestores de bases de datos utilizados en la institución	1	2	3	4	4	Mensual
Instaladores de los sistemas operativos manejados en la institución y de las herramientas administrativas, financieras y tecnológicas de gestión de aplicaciones	1	2	2	3	4	Mensual
Datos almacenados en papel:						
Arquitectura de conexiones IT	1	1	1	2	3	Mensual
Manuales impresos para la configuración de servidores, aplicaciones y bases de datos	1	1	2	3	3	Mensual
Contactos internos y externos para la gestión de TI	1	2	2	3	4	Mensual
11. Alternativas en el caso de un desastre						
¿Pueden otras actividades continuar con el funcionamiento de esta actividad? En caso afirmativo, ¿cuáles?	Sí. Esta actividad encierra errores de Aplicativos Financieros, Administrativos y Tecnológicos en general que actúan comúnmente de forma independiente de cada aplicación, por lo cual el área que reportó el incidente debe realizar una evaluación del impacto a sus procesos, a fin de suspender dicho proceso hasta que el proveedor y el personal de TI solucionen el error.					
¿Es posible realizar algunas actividades en forma manual, sin equipos de TI ni de otro tipo?	Si, depende del área, se puede realizar registros manuales para luego digitalizarlos					
12. Experiencias anteriores						

¿Con qué frecuencia se han producido incidentes disruptivos en el negocio hasta ahora? ¿Cuánto tiempo duraron?	4 veces al año, con un promedio de duración de 48h cada uno
¿Cómo se manejaron esas situaciones?	Se manejó de forma improvisada, primero descartando todas las posibles causas y luego levantando los servicios de manera rápida mediante BackUps de equipos y bases de datos, para posteriormente encontrar la causa exacta del problema y su posterior corrección
13. Comentarios / otra información importante:	
Los servidores y bases de datos poseen en su gran mayoría respaldos y arquitecturas/arreglos en alta disponibilidad	

Adaptado de: (Kosutic, 2015).

ANEXO 5

Estrategia de Continuidad del Negocio

Banco KLM

Banco KLM Compañía Anónima

Anexo 5: Estrategia de Continuidad del Negocio

Código:	EST-TI-2015-08
Versión:	1.0
Fecha de la versión:	3 de Agosto del 2015
Creado por:	Ing. Vinicio Sarabia
Aprobado por:	Ing. Santiago Pazmiño
Nivel de confidencialidad:	Alto

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
03/08/2015	1.0	Vinicio Sarabia	Creación de la primera versión del documento

Tabla de contenido

Objetivo, alcance y usuarios

El objetivo de este documento es definir cómo el Banco KLM garantizará que se cumplan todas las condiciones para reanudar las actividades comerciales ante el caso de un desastre u otro incidente disruptivo. Constituye la base para preparar el Plan de Continuidad del Negocio y los planes de recuperación.

Este documento se aplica a todo el alcance del SGCN, según se define en la Política de la gestión de Continuidad del Negocio.

Los usuarios de este documento son miembros de la alta dirección y personas que implementan el proyecto de gestión de la Continuidad del Negocio.

Documentos de referencia

- Norma ISO 22301, punto 8.2.2
- Norma ISO/IEC 27001, punto A.14.1.2
- Política de la gestión de Continuidad del Negocio
- Cuestionarios sobre el análisis del impacto en el negocio
- Matriz de evaluación de riesgos
- Tratamiento de riesgos
- Plan de Continuidad del Negocio que contiene el Plan de respuesta a los incidentes y los planes de recuperación.

Datos de la estrategia

Esta estrategia está redactada en base a los resultados del Análisis del impacto en el negocio y de la evaluación y tratamiento del riesgo.

Análisis del impacto en el negocio

El Análisis del impacto en la Infraestructura Tecnológica establece que 3 actividades sostienen a los productos y servicios clave que (consultar el Anexo 5 - Apéndice 1 para obtener una lista de esas actividades).

El período máximo tolerable de interrupción (interrupción máxima aceptable) para cada actividad ha sido determinado en el Cuestionario sobre el análisis del impacto en el negocio (consultar el Anexo 4 - Apéndice 1).

El Anexo 5 - Apéndice 3 determina los objetivos de tiempo de recuperación para cada actividad tomando en cuenta las dependencias con otras actividades.

Gestión de riesgos

La evaluación de riesgos que pueden afectar la Continuidad del Negocio se detalla en “Matriz de evaluación de riesgos”. Los mayores riesgos que podrían producir un incidente disruptivo, es decir, una interrupción del negocio identificada durante la evaluación de riesgos, son los siguientes:

- El personal de las áreas de TI posee varias actividades que consumen todo su tiempo
- Ausencia de personal en las capacitaciones
- El personal con acceso a los sistemas del Banco no han sido debidamente capacitados en el uso y manejo responsable de estas aplicaciones.
- Políticas organizacionales demasiado burocráticas, las aprobaciones de procesos toman demasiado tiempo
- El personal con las capacidades técnicas necesarias para el SGCN, no brinda la información requerida
- No existe la disponibilidad de los sistemas y equipos para realizar pruebas, mantenimientos
- Los usuarios consideran a todos los servicios como críticos

Para todos los riesgos / incidentes mencionados es necesario:

- Aplicar medidas preventivas para reducir la probabilidad de tales incidentes (las acciones se detallan en el documento “Tratamiento de riesgos.
- Aplicar medidas preventivas para minimizar las posibles consecuencias de tales incidentes (estas acciones también se detallan en el documento “Tratamiento de riesgos.
- Preparar escenarios de eventos que describan cómo esos incidentes afectarían el funcionamiento de la organización (los escenarios están

detallados en el Apéndice 4 de esta Estrategia y deben ser utilizados más adelante para los planes de prueba.

- Definir en el Plan de respuesta a los incidentes la forma adecuada para responder a cada uno de los incidentes.

El Gerente Nacional de Negocios es el responsable de la redacción de las medidas preventivas y el Gerente de Producción y Servicios es el responsable de confeccionar el Plan de respuesta a los incidentes.

Estructura de respuesta a incidentes

Gabinete de crisis y Gabinete de apoyo de crisis

Gabinete de crisis

Si se activan los planes de Continuidad del Negocio, se conforma un organismo operativo denominado Gabinete de crisis, que está autorizado a tomar las decisiones necesarias para resolver la situación. Los miembros del Gabinete de crisis son:

- Gerente Nacional del Centro de Servicios
- Gerente Nacional de Tecnología
- Gerente Nacional de Recursos Humanos
- Gerente Financiero
- Gerente de Producción y Servicios
- Subgerente de Procesamiento e Infraestructura
- Jefe de Comunicación Social
- Subgerente de Control Tecnológico
- Jefe de Comunicaciones

- Jefe de Servidores
- Jefe de Centro de Computo

El Gabinete de crisis está dirigido por el Gerente de crisis. El Gerente Nacional del Centro de Servicios cumplirá la función de Gerente de crisis; en caso de estar ausente, la función será realizada por el Gerente Nacional de Tecnología.

El Gabinete de crisis gestiona el incidente disruptivo desde una instalación denominada Centro de crisis, cuya ubicación se especifica en el punto 0 de esta Estrategia.

Gabinete de apoyo de crisis

El Gabinete de apoyo de crisis tiene la función de relevar al Gabinete de crisis de tareas administrativas y de otras actividades operativas para que pueda concentrarse en solucionar el incidente disruptivo.

Los miembros del Gabinete de apoyo de crisis son:

- 2 Asistentes administrativos (Gerencia Comercial).
- 2 Mensajeros (Gerencia Comercial y Gerencia Técnica).
- 1 Auxiliar de Servicios (Gerencia Técnica).
- 1 Técnico en operación y mantenimiento (Gerencia Comercial, personal para reparación de equipos que no sean de TIC).
- 2 Asistentes del área Administrativa
- 2 Asistentes del área Financiera

El Gabinete de apoyo de crisis trabajará en ubicaciones especificadas por el Gabinete de crisis.

Equipamiento del Centro de crisis

Para que puedan funcionar el Gabinete de crisis y el Gabinete de apoyo de crisis, el Centro de crisis debe estar equipado de la siguiente manera:

Tabla 34. Equipamiento de los Gabinetes de crisis y Gabinete de apoyo de crisis.

Nombre del recurso	Descripción	Cantidad	Cuándo es necesario el recurso
Aplicaciones / bases de datos:			
People Soft / Oracle 11g		1	Dentro de las 2 horas
Big Data / Teradata		1	Dentro de las 2 horas
SharePoint / Server 2005		1	Dentro de las 2 horas
Business intelligence / Oracle 11g		1	Dentro de las 2 horas
Datos almacenados en formato electrónico:			
Estrategia de Continuidad del Negocio y planes para todas las actividades		16	Dentro de las 2 horas
Directorio telefónico de la ciudad de Quito		16	Dentro de las 2 horas
Directorio telefónico específico de las dependencias públicas de seguridad de la ciudad de Quito		16	Dentro de las 2 horas
Datos almacenados en			

papel:			
Estrategia de Continuidad del Negocio y planes para todas las actividades		16	inmediatamente
Directorio telefónico de la ciudad de Quito		16	Dentro de las 2 horas
Directorio telefónico específico de las dependencias públicas de seguridad de la ciudad de Quito		16	inmediatamente
Equipos de TI y comunicaciones:			
Estaciones de trabajo		8	Dentro de las 2 horas
Teléfonos		8	inmediatamente
Teléfonos móviles		16	inmediatamente
Impresora		2	Dentro de las 2 horas
Equipo de fax		1	inmediatamente
Canales de comunicación:			
Líneas fijas de teléfono		16	inmediatamente
Acceso a Internet		1	Dentro de las 2 horas
Otros equipos:			
Televisor		2	inmediatamente
Radio		2	inmediatamente
Instalaciones e infraestructura:			
Red de computadoras		3	Dentro de las 2

			horas
Muebles		5	inmediatamente
Servicios externos:			
Electricidad		2	Inmediatamente
Agua potable		1	Inmediatamente

Adaptado de: (Kosutic, 2015).

El Gerente de Producción y Servicios es el responsable de la preparación del Gabinete de crisis y del Gabinete de apoyo de crisis para que conozcan su función durante un incidente disruptivo. El Gerente de Producción y Servicios es el responsable de equipar el Centro de crisis.

Comunicación y toma de decisiones

Los incidentes son comunicados de la siguiente forma:

- Todos los incidentes relacionados con tecnología de la información y comunicación son informados al Gerente de Producción y Servicios.
- Todos los demás incidentes son informados al Jefe de Seguridad y Salud Ocupacional.

Si las personas mencionadas no pueden resolver el incidente, deben informar al Gerente de crisis, que decidirá si es necesario activar los planes de recuperación.

Las autorizaciones para la toma de decisiones son las siguientes:

Tabla 35. Responsables para toma de decisiones frente a incidentes.

Tipo de decisión	Quién está autorizado
Cómo se solucionan incidentes menores relacionados con tecnología de información y comunicación.	Empleados en el área de Tecnología.
Cómo se solucionan otros incidentes menores.	Empleados en el área de Negocios.
Toma una decisión sobre la activación de planes de recuperación	Gerente de crisis
Implementación de todas las tareas necesarias para la recuperación de actividades individuales.	Gerente de recuperación para actividades individuales.
Selección de información para suministrar a los medios públicos durante un incidente disruptivo.	Gerente de Recursos Humanos
Adquisiciones durante el incidente disruptivo: mayores a USD 5000.	Gerente Financiero
Adquisiciones durante el incidente disruptivo: hasta USD 5000.	Jefe Administrativo

El Gerente de Producción y Servicios es el responsable de preparar a los empleados del área de Tecnología e Infraestructura para que reconozcan y reaccionen ante incidentes relacionados con tecnología de la información y comunicación. El Jefe de Seguridad y Salud Ocupacional es el responsable de preparar a los empleados del Banco KLM para que puedan manejar otros incidentes.

Colaboración con las autoridades

Las siguientes personas están a cargo de la colaboración con las autoridades públicas y con los servicios de emergencia:

Tabla 36. Listado del personal encargado de colaborar con cada una de las instituciones y servicios de emergencia.

Autoridad	Quién está a cargo
Policía	Jefe de Seguridad y Salud Ocupacional
Ambulancia	Jefe de Seguridad y Salud Ocupacional
Bomberos	Jefe de Seguridad y Salud Ocupacional
Secretaría Nacional de Gestión de Riesgo	Jefe de Seguridad y Salud Ocupacional

Las personas mencionadas deben implementar todas las actividades preliminares para garantizar que la interoperabilidad con las autoridades durante el incidente disruptivo sea de un nivel satisfactorio. Las actividades preliminares pueden incluir consultar a las autoridades las instrucciones acerca del tipo de información necesaria en el caso de un incidente disruptivo y cómo se espera que reaccione la organización.

Evacuación del edificio y puntos de encuentro

Cada edificio se evacua de acuerdo a lo especificado en el plan de evacuación de edificios en caso de incendios.

Luego de evacuar el edificio Matriz del Banco KLM, los empleados deben reunirse en los siguientes puntos de encuentro:

Tabla 37. Puntos de encuentro del personal del Baco KLM en caso de siniestros.

	Punto de encuentro 1	Punto de encuentro 2
Edificio Matriz	Parque la Carolina (Calles Japón y Av. Amazonas, esquina)	Centro Comercial CCI (Puerta de Acceso 1)

Nota: Si no está disponible el Punto de encuentro 1, los empleados deben reunirse en el Punto de encuentro 2.

El Jefe de Seguridad y Salud Ocupacional es el responsable de preparar y mantener los planes de evacuación en casos de incendio.

Vías de comunicación

En caso de un incidente disruptivo, se utilizarán las siguientes vías de comunicación (las que se encuentran al principio de la lista se utilizarán primero, las que están cerca del final, se usarán sólo si las primeras no están disponibles):

a) teléfonos móviles (corporativos y privados)

b) teléfonos (corporativos y privados)

c) correo electrónico (enviado desde ordenadores corporativos o privados)

d) servicios de mensajería Skype

e) mensajeros (empleados de la organización o servicios especializados)

El Jefe de Comunicaciones es el responsable de adquirir, preparar y, cuando sea necesario, mantener, las vías de comunicación mencionadas para garantizar su disponibilidad durante un incidente disruptivo.

Transporte hacia las ubicaciones alternativas

Los empleados de la organización serán trasladados desde la ubicación primaria hacia la alternativa de las siguientes formas:

Tabla 38. Medios de transporte de los miembros del SGCN en caso de siniestro.

Miembros del SGCN	Medio de transporte
Gabinete de crisis y Gabinete de apoyo de crisis	Vehículo empresarial
Empleados del Área de Infraestructura Tecnológica	Vehículo personal
Empleados del Área Comercial que intervienen en el SGCN	Vehículo personal
Empleados del Área Administrativa que intervienen en el SGCN	Vehículo personal
Empleados del Área Financiera que intervienen en el SGCN	Vehículo personal

Adaptado de: (Kosutic, 2015).

El Jefe Administrativo es el responsable de proporcionar todos los medios de transporte.

Comunicación con las partes interesadas

El Banco KLM manejará las relaciones con las diversas partes interesadas a través de la designación de personas que, ante un incidente disruptivo, se comunicarán con ellos a través de las siguientes vías de comunicación:

Tabla 39. Medios de comunicación, partes interesadas y responsables.

Entes	Teléfono	Reuniones	Correo electrónico	Conferencias de prensa	Medios públicos
Empleados		Coordinador de la Continuidad del Negocio	Gerente de Producción y Servicios		
Propietarios / accionistas	Gerente de Tecnología				
Familiares de empleados		Gerente de Recursos Humanos			
Clientes			Gerente de Negocios		
Medios públicos				Periodista	
Asociaciones					Periodista
Servicios de emergencia	Jefe de Seguridad y Salud Ocupacional				
Diversas autoridades públicas				Gerente de Tecnología	

Adaptado de: (Kosutic, 2015).

El Gerente de Producción y Servicios es el responsable de preparar a todas las personas mencionadas anteriormente para realizar las comunicaciones en casos de incidentes disruptivos.

El Jefe de Comunicación Social es responsable de preparar plantillas para las declaraciones a los medios, que cubrirán todos los incidentes disruptivos relacionados con los riesgos más altos mencionados anteriormente.

Estrategia para los recursos

Ubicaciones e infraestructura

Las ubicaciones de recuperación del Banco KLM son las siguientes:

Tabla 40. Matriz de la ubicación e infraestructura de recuperación utilizada en caso de siniestros.

Nombre	Ubicación principal	Estrategia de ubicación alternativa	Cantidad mínima de estaciones de trabajo	Equipos*	Ubicación alternativa (cerca)	Ubicación alternativa (remota)
Centro de crisis	Quito, Av. Amazonas y Villalengua	Ubicaciones alternativas dentro de la organización	6	Caliente	Centro Comercial CCI Agencia del Banco	Guayaquil, Urdesa Agencia del Banco
Disponibilidad de los Servicios de Comunicaciones	Quito, Av. Amazonas y Villalengua	Ubicaciones alternativas dentro de la organización	4	Espejo	Centro Comercial CCI Agencia del Banco	Guayaquil, Urdesa Agencia del Banco
Disponibilidad del Servicio de Aplicativos Financieros, Administrativo	Quito, Av. Amazonas y Villalengua	Ubicaciones alternativas dentro de la organización	8	Espejo	Centro Comercial CCI Agencia del Banco	Guayaquil, Urdesa Agencia del Banco

s y Tecnológicos						
Disponibilidad del Servicio de Core Bancario y Negocios	Quito, Av. Amazonas y Villalengua	Ubicaciones alternativas dentro de la organización	8	Espejo	Centro Comercial CCI Agencia del Banco	Guayaquil, Urdesa Agencia del Banco

Adaptado de: (Kosutic, 2015).

*Los términos utilizados en esta columna tienen el siguiente significado:

a) Frío: ubicación sin infraestructura ni equipos.

b) Templado: ubicación que cuenta con infraestructura básica (red, etc.), vínculos y equipos, cuya adquisición demanda mucho tiempo.

c) Caliente: ubicación que cuenta infraestructura preinstalada, con todos los equipos, vínculos y software.

d) Espejo: ubicación con la infraestructura, todo los equipos, vínculos y software instalados previamente y con datos en tiempo real.

El Jefe de Comunicaciones es el responsable de realizar todos los preparativos necesarios relacionados con las ubicaciones alternativas. El Jefe de Comunicaciones es el responsable de equipar a las ubicaciones alternativas.

Proveedores y socios

Las relaciones con los proveedores y socios deben ser manejadas de la siguiente forma:

Tabla 41. Proceso a seguir con los proveedores y socios en caso de siniestros.

Nombre del proveedor / socio	Estrategia
Telconet Cnt Level3	Estimular u obligar a los proveedores o socios a aumentar el nivel de su capacidad para la Continuidad del Negocio (de esta manera se reduce el riesgo de ocurrencia de un incidente y de sus consecuencias
AT&T Claro Todouno IBM	Se contratan servicios a diversos proveedores o socios en forma simultánea; si alguno de ellos no está disponible, se pueden utilizar los servicios de otro
Kruger TATA Qmatic Desca Teradata	Obligar por contrato a los proveedores o socios a la entrega de mercancías o servicios independientemente del incidente disruptivo y definir sanciones (de esta manera, los proveedores o socios están obligados implementar la Continuidad del Negocio y, a la vez, se traslada a ellos una parte del riesgo financiero
	Determinar proveedores o socios alternativos (de esta forma, se puede preparar el traslado de actividades del negocio, aunque la relación comercial no se iniciará hasta que se produzca un

	incidente disruptivo
	Regreso de las actividades a la organización (se prepara a la organización para retomar las actividades que hayan sido externalizadas
	Se contratan servicios a diversos proveedores o socios en forma simultánea; si alguno de ellos no está disponible, se pueden utilizar los servicios de otro

Adaptado de: (Kosutic, 2015).

El Gerente de Producción y Servicios es responsable de gestionar las relaciones con los proveedores y con los socios externos para garantizar que la interoperabilidad durante un incidente disruptivo sea de un nivel satisfactorio.

Aplicaciones / bases de datos

Todas las aplicaciones y bases de datos necesarias estarán instaladas en la ubicación alternativa dentro de las 24 horas de producido el incidente disruptivo; para aquellas aplicaciones y bases de datos que no son necesarias dentro de las 24 horas, los medios de instalación se almacenarán en la ubicación alternativa.

El Jefe de Servidores es el responsable de la instalación de aplicaciones y bases de datos y de la preparación de los medios de instalación.

Datos

Se deben realizar copias de seguridad de los datos compartidos por varias actividades con los siguientes intervalos:

Tabla 42. Procedimiento y frecuencia para crear copias de seguridad de datos compartidos.

Nombre de la aplicación, base de datos, carpeta, documento:	Frecuencia para creación de copias de seguridad	Procedimiento para copias de seguridad
Core Bancario	Continuo (en tiempo real)	Aplicaciones / bases de datos: procedimiento de respaldo automatizado basado en servidor
PeopleSoft, CRM, ERP, Sistema de Negocios	Cada 4 horas	Aplicaciones / bases de datos: procedimiento de respaldo automatizado basado en servidor
Detalle diario de transacciones financieras (consumos)	Cada 4 horas	Aplicaciones / bases de datos: procedimiento de respaldo automatizado basado en servidor
Reporte consolidado del movimiento financiero diario	Cada 8 horas	Documentos en papel: recepción de todos los documentos de fax por medios electrónicos, o escaneo o copia de los documentos y almacenamiento en dos lugares separados

Adaptado de: (Kosutic, 2015).

Nota: la frecuencia para crear copias de seguridad de los datos utilizados por una única actividad se define en la estrategia para dicha actividad.

El Subgerente de Control Tecnológico es el responsable de la creación de copias de seguridad para los datos mencionados anteriormente.

Evitar un punto único de falla

Se utilizan las siguientes estrategias para evitar un punto único de falla, que puede ocasionar la interrupción de una actividad:

Tabla 43. Estrategias para evitar un punto único de falla e interrupción de las actividades.

Punto único de falla	Actividad en la que se produce	Estrategia para evitarlo
Caída del Core Bancario	Caída del servidor AS400	• Servidor alternativo • Copias continuas de seguridad y base de datos
Caída del Sistema de Negocios	Caída del servidor Teradata	• Servidor alternativo • Copias continuas de seguridad y base de datos
Caída del Sistema Financiero	Caída del servidor Teradata	• Servidor alternativo • Copias continuas de seguridad y base de datos
Caída del Sistema Administrativo	Caída del servidor Teradata	• Servidor alternativo • Copias

		continuas de seguridad y base de datos
Caída de la infraestructura de red	Problemas en los equipos de Comunicaciones	Además de tener 2 proveedores, es decir un proveedor principal y un proveedor alternativo de los enlaces de Comunicaciones, es importante realizar pruebas controladas de alta disponibilidad

Adaptado de: (Kosutic, 2015).

NOTA: Los Servidores y Sistemas cuentan con alta disponibilidad, sin embargo se consideran como puntos únicos de falla dada la criticidad de los servicios TI.

El Subgerente de Procesamiento e Infraestructura es el responsable de implementar la estrategia para evitar la ocurrencia de un punto único de falla.

Suministro de recursos financieros

El Banco KLM necesita $ 351.500,00 (valor estimado durante la interrupción máxima permitida) para capital de trabajo para todas las actividades, más $ 140.600,00 (valor estimado) para compras de emergencia en caso que se produzca un incidente disruptivo.

En caso de producirse un incidente disruptivo, los recursos financieros serán suministrados de la siguiente forma: El Gerente Financiero en coordinación con el Gerente de Producción y Servicios mantendrá en forma constante el nivel necesario de liquidez en dinero y en recurso humano durante el tiempo que

dure la recuperación del incidente disruptivo, este recurso económico suministrado será negociado mediante un contrato de financiación contingente disponible a corto plazo.

El Gerente Financiero es el responsable de realizar todos los preparativos necesarios relacionados con la provisión de recursos financieros.

Estrategia de recuperación para actividades individuales

La estrategia de recuperación para actividades individuales está definida en los Apéndices 6a, 6b y 6c (Ver Anexo 13) de la presente Estrategia.

La persona designada como Gerente de recuperación para una actividad individual es la responsable de la redacción de los Planes de recuperación para dicha actividad. El Subgerente de Procesamiento e Infraestructura es el responsable de preparar todos los recursos necesarios para actividades individuales.

Implementación de todos los preparativos necesarios

El Apéndice 5 (Ver Anexo 12) enumera todos los preparativos necesarios para la implementación de esta Estrategia. El Gerente Financiero debe definir los recursos financieros y de otra naturaleza necesarios y debe definir plazos para la implementación de cada preparativo; y el Gerente de Producción y Servicios está a cargo de supervisar la coordinación y ejecución de todas las acciones preparativas, como también de informar sobre su implementación.

Gestión de registros guardados en base a este documento

Tabla 44. Registro guardado de las principales características de los documentos.

Nombre del registro	Ubicación de archivo	Persona responsable del archivo	Controles para la protección del registro	Tiempo de retención
Plan de	Ordenador	Gerente de	Solamente el	El Plan es

preparación para Continuidad del Negocio (en formato electrónico).	del Gerente de Producción y Servicios.	Producción y Servicios.	Gerente de Producción y Servicios puede ingresar y modificar los datos del Plan.	almacenado por el plazo de 3 años.

Adaptado de: (Kosutic, 2015).

Validez y gestión de documentos

Este documento es válido hasta el 03 de Agosto del 2018.

El propietario de este documento es el Gerente de Producción y Servicios, que debe verificar, y si es necesario actualizar, el documento por lo menos una vez al año.

Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- Si la organización tuvo éxito en la recuperación de las actividades críticas dentro del objetivo de tiempo de recuperación.
- Si se han implementado todos los preparativos necesarios para la Continuidad del Negocio.

Apéndices

- Apéndice 1: Lista de actividades (Ver Anexo 5.1)
- Apéndice 2: Prioridades de recuperación para las actividades (Ver Anexo 5.2)
- Apéndice 3: Objetivos de tiempo de recuperación para actividades (Ver Anexo 5.3)

- Apéndice 4: Ejemplos de escenarios de incidentes disruptivos (Ver Anexo 5.4)
- Apéndice 5: Plan de preparación para Continuidad del Negocio (Ver Anexo 5.5)
- Apéndice 6a: Estrategia de recuperación para la actividad realizar acciones preventivas y correctivas para garantizar la disponibilidad de los servicios de Comunicaciones (Ver Anexo 5.6)
- Apéndice 6b: Estrategia de recuperación para la actividad realizar acciones preventivas y correctivas para los aplicativos de Core Bancario y Negocios (Ver Anexo 5.6)
- Apéndice 6c: Estrategia de recuperación para la actividad realizar acciones preventivas y correctivas para los sistemas y aplicativos Administrativos, Financieros y Tecnológicos (Ver Anexo 5.6)

Gerente de Producción y Servicios

Ing. Luis Antonio Arevalo

_____

Firma

ANEXO 5.1

Lista de actividades

Anexo 5.1: Estrategia de Continuidad del Negocio

Apéndice 1: Lista de actividades

Esta lista incluye todas las actividades que respaldan la provisión de productos y servicios clave en el Banco KLM.

Las actividades se encuentran listadas (no necesariamente en orden de ejecución), de manera que se minimice el tiempo para el retorno a la normalidad de las actividades de negocio de Banco KLM.

Tabla 45. Actividades que respaldan la provisión de servicios para el SGCN.

Nombre de la actividad
Verificar el correcto funcionamiento de los equipos de Comunicaciones
Realizar monitoreo constante de los equipos de Comunicaciones
Verificar alarmas y conexiones físicas de los equipos de Comunicaciones
Ejecutar acciones preventivas y correctivas de los equipos de Comunicaciones
Verificar el correcto funcionamiento de los servidores, base de datos de aplicaciones de Core Bancario, Negocios, Administrativos y Tecnológicos
Realizar el monitoreo constante del aplicativo de Core Bancario
Ejecutar acciones preventivas y correctivas de los servidores de aplicativos de Core Bancario y Negocios
Limpieza externa de los equipos de Comunicaciones
Realizar acciones preventivas y correctivas para garantizar la disponibilidad de los servicios de Comunicaciones
Realizar acciones preventivas y correctivas para los aplicativos de Core Bancario y Negocios
Realizar acciones preventivas y correctivas para los sistemas y aplicativos Administrativos, Financieros y Tecnológicos

Adaptado de: (Kosutic, 2015).

Se incluyen las actividades generales que no necesariamente respaldan productos y servicios claves en el Banco KLM, pero si ayudan a mantener el buen desempeño del resto de actividades:

Tabla 46. Actividades que no necesariamente respaldan la provisión de servicios para el SGCN.

Nombre de la actividad
Ejecutar acciones que garanticen la seguridad de los sistemas de información.
Instalar hardware y software que garanticen la seguridad en el acceso a los sistemas y aplicaciones institucionales.
Realizar acciones preventivas y correctivas para garantizar la seguridad de los sistemas de la información.
Realizar tareas de escaneo y desinfección permanente de los equipos informáticos antivirus, malware o algún otro tipo de código malicioso.
Verificación del ambiente en el Data Center, temperatura y humedad adecuada para los equipos informáticos

Adaptado de: (Kosutic, 2015).

ANEXO 5.2

Prioridades de recuperación para las actividades

Anexo 5.2: Estrategia de Continuidad del Negocio

Apéndice 2: Prioridades de recuperación para las actividades

Esta lista define los períodos máximos tolerables de interrupción (interrupciones máximas aceptables) para cada actividad y establece prioridades en consecuencia.

Tabla 47. Prioridades de recuperación para las actividades.

Nombre de la actividad	Período máximo tolerable de interrupción
Verificar el correcto funcionamiento de los equipos de Comunicaciones	30 min
Realizar monitoreo constante de los equipos de Comunicaciones	10 min
Verificar alarmas y conexiones físicas de los equipos de Comunicaciones	10 min
Ejecutar acciones preventivas y correctivas de los equipos de Comunicaciones	4 horas
Verificar el correcto funcionamiento de los servidores, base de datos de aplicaciones de Core Bancario, Negocios, Administrativos y Tecnológicos	2 horas
Realizar el monitoreo constante del aplicativo de Core Bancario	10 min
Ejecutar acciones preventivas y correctivas de los servidores de aplicativos de Core Bancario y Negocios	2 horas
Limpieza externa de los equipos de Comunicaciones	30 min

Realizar acciones preventivas y correctivas para garantizar la disponibilidad de los servicios de Comunicaciones	4 horas
Realizar acciones preventivas y correctivas para los aplicativos de Core Bancario y Negocios	2 horas
Realizar acciones preventivas y correctivas para los sistemas y aplicativos Administrativos, Financieros y Tecnológicos	2 días
Ejecutar acciones que garanticen la seguridad de los sistemas de información.	30 min
Instalar hardware y software que garanticen la seguridad en el acceso a los sistemas y aplicaciones institucionales.	2 horas
Realizar acciones preventivas y correctivas para garantizar la seguridad de los sistemas de la información.	2 horas
Realizar tareas de escaneo y desinfección permanente de los equipos informáticos antivirus, malware o algún otro tipo de código malicioso.	1 día
Verificación del ambiente en el Data Center, temperatura y humedad adecuada para los equipos informáticos (Automatizado)	1 día

Adaptado de: (Kosutic, 2015).

Nota: esta lista no determina los objetivos de tiempo de recuperación ya que estos se definen una vez que se hayan identificado las dependencias entre las actividades individuales.

ANEXO 5.3

Objetivos de tiempo de recuperación para actividades

Anexo 5.3: Estrategia de Continuidad del Negocio

Apéndice 3: Objetivos de tiempo de recuperación para actividades

Esta lista define los objetivos de tiempo de recuperación para cada actividad en el Banco KLM:

Tabla 48. Objetivos a cumplir en los tiempos de recuperación del Banco KLM, por cada actividad.

Nombre de la actividad	Período máximo tolerable de interrupción (interrupción máxima aceptable)	Dependencia de otras actividades	Objetivo de tiempo de recuperación
Verificar el correcto funcionamiento de los equipos de Comunicaciones	30 min	No	15min
Realizar monitoreo constante de los equipos de Comunicaciones	10 min	No	5min
Verificar alarmas y conexiones físicas de los equipos de Comunicaciones	10 min	No	10 min
Ejecutar acciones preventivas y correctivas de los	4 horas	Verificar el correcto funcionamiento	1 hora

equipos de Comunicaciones		de los equipos de Comunicaciones	
Verificar el correcto funcionamiento de los servidores, base de datos de aplicaciones de Core Bancario, Negocios, Administrativos y Tecnológicos	2 horas	Verificar el correcto funcionamiento de los equipos de Comunicaciones	1.5 horas
Realizar el monitoreo constante del aplicativo de Core Bancario	10 min	Realizar monitoreo constante de los equipos de Comunicaciones	5 min
Ejecutar acciones preventivas y correctivas de los servidores de aplicativos de Core Bancario y Negocios	2 horas	Verificar el correcto funcionamiento de los servidores, base de datos de aplicaciones de Core Bancario, Negocios, Administrativos y Tecnológicos	1.5 horas
Limpieza externa de los equipos de Comunicaciones	30 min	No	30 min
Realizar acciones	4 horas	Ejecutar acciones	2 horas

preventivas y correctivas para garantizar la disponibilidad de los servicios de Comunicaciones		preventivas y correctivas de los equipos de Comunicaciones	
Realizar acciones preventivas y correctivas para los aplicativos de Core Bancario y Negocios	2 horas	Ejecutar acciones preventivas y correctivas de los servidores de aplicativos de Core Bancario y Negocios	1.5 horas
Realizar acciones preventivas y correctivas para los sistemas y aplicativos Administrativos, Financieros y Tecnológicos	2 días	Ejecutar acciones preventivas y correctivas de los equipos de Comunicaciones	4 horas
Ejecutar acciones que garanticen la seguridad de los sistemas de información.	30 min	Realizar monitoreo constante de los equipos de Comunicaciones	15 min
Instalar hardware y software que garanticen la seguridad en el	2 horas	No	1 hora

acceso a los sistemas y aplicaciones institucionales.			
Realizar acciones preventivas y correctivas para garantizar la seguridad de los sistemas de la información.	2 horas	Ejecutar acciones que garanticen la seguridad de los sistemas de información.	1.5 horas
Realizar tareas de escaneo y desinfección permanente de los equipos informáticos antivirus, malware o algún otro tipo de código malicioso.	1 día	No	4 horas
Verificación del ambiente en el Data Center, temperatura y humedad adecuada para los equipos informáticos (Automatizado)	1 día	No	4 horas

Adaptado de: (Kosutic, 2015).

ANEXO 5.4

Ejemplos de escenarios de incidentes disruptivos

Anexo 5.4: Estrategia de Continuidad del Negocio

Apéndice 4: Ejemplos de escenarios de incidentes disruptivos

Incendio

Una gran cantidad de empleados se reunió en la organización para celebrar el aniversario de la misma. Contra todas las expectativas, los empleados se estaban divirtiendo mucho y el festejo se extendió mucho más de lo planeado. Como no quería arruinar la fiesta, el director general permitió que se fumara, violando todas las normas. En la cocina, uno de los empleados tiró un cigarrillo encendido en un cesto lleno de papeles y el cesto se prendió fuego cuando no había nadie en ese lugar. El fuego se hizo evidente cuando ya se había extendido a todos los elementos de la cocina; los empleados intentaron apagarlo pero se tardó varios minutos en encontrar y hacer funcionar el extintor. Mientras tanto, el fuego creció y se extendió a las oficinas. Cuando llegaron los bomberos, el incendio ya había destrozado todo el archivo que contenía contratos y documentación importante de clientes.

Terremoto

En el transcurso de la noche, un terremoto catastrófico azotó a la ciudad y a zonas aledañas, provocando graves consecuencias. Las oficinas centrales de la organización resultaron parcialmente dañadas, lo que provocó una interrupción de algunos equipos de TI y de comunicación. Aproximadamente el veinte por ciento de los empleados resultó herido y no podrá asistir al trabajo; algunos están desaparecidos y se informó que algunos murieron. Las comunicaciones, tráfico y demás infraestructura (suministro de agua y de electricidad) de la ciudad están dañados y su uso está interrumpido.

Amenaza de bomba

Una secretaria recibió un llamado telefónico en el que informaban que había sido colocada una bomba en el edificio de la organización. Inmediatamente, le informó al director general y a la Policía. El director decidió no alarmar a los

empleados y optó por retener esta información hasta que la Policía tuviera la posibilidad de evaluar la situación. La patrulla de Policía llegó relativamente rápido, en 10 minutos, e inmediatamente ordenó la evacuación de todo el edificio. No se les permitió a los empleados que llevaran nada con ellos y podían no terminar las tareas en las que estaban trabajando. El escuadrón anti-bombas llegó en una hora, pero debido al poco equipamiento y a la complejidad del edificio, la búsqueda de la bomba demandó más de 5 horas. Finalmente, la Policía informó que no había ninguna bomba en el edificio y que todos los empleados podían regresar; sin embargo, ya era bastante más tarde del horario operativo y no era posible contactar a los clientes con los que se habían realizado gestiones más temprano.

Falla en los vínculos de comunicación

En la mayor parte de la ciudad, los sistemas de comunicación presentaron fallas debido a problemas técnicos del suministro de energía. La energía en la organización es suministrada sin inconvenientes por un generador. Sin embargo, la red telefónica de los tres proveedores de telecomunicaciones e Internet está caída, y la red móvil está prácticamente inutilizada por sobrecarga. Es necesario cerrar un contrato importante en tres días; en caso de demoras, la organización deberá pagar multas significativas.

Interrupción del suministro eléctrico

Se están realizando trabajos de construcción en las oficinas centrales de la organización. Por error, una excavadora corta el cable principal de electricidad, y también el cable que conecta el edificio con el generador de electricidad. Hay una UPS pero solamente puede suministrar electricidad por un tiempo limitado. Como se acerca el final del trimestre, el departamento de contabilidad debe preparar los informes financieros finales y la junta directiva de la organización ya ha programado una conferencia de prensa dentro de dos días para anunciar sus resultados comerciales.

Pandemia de gripe aviar

Ha estallado una pandemia de gripe aviar que se extendió por todo el país. En la mayoría de los casos, la gripe no es fatal pero la enfermedad y la recuperación duran un promedio de cuatro semanas. La dirección ha tomado todas las medidas para evitar que se expanda la infección dentro de la organización (utilizando máscaras, etc.). Sin embargo, la naturaleza del negocio hace que no se pueda restringir el contacto con los clientes. A pesar de las precauciones, la gripe se ha extendido entre empleados de la organización, por lo que el porcentaje de empleados enfermos ahora excede el 50%; en algunas de las unidades organizativas más pequeñas, todos los empleados están enfermos. Por otro lado, es evidente que hay menos clientes que, frente a la crisis en que se encuentra el país, no quieren gastar dinero en servicios que ofrece la organización.

ANEXO 5.5

Plan de preparación para Continuidad del Negocio

Anexo 5: Estrategia de Continuidad del Negocio

Apéndice 5: Plan de preparación para Continuidad del Negocio

Para implementar la Estrategia de Continuidad del Negocio es necesario realizar los siguientes preparativos para cumplir con las condiciones para retomar en forma satisfactoria las actividades comerciales luego de un incidente disruptivo:

Tabla 49. Preparativos y condiciones para retomar las actividades comerciales luego de un incidente disruptivo.

Descripción del preparativo	Punto en la Estrategia	Recursos generales y financieros necesarios ($)	Persona responsable	Plazos de inicio y finalización	Método para evaluación de resultados
Determinar medidas preventivas en base a la evaluación de riesgos.	3.2.	0,00	Gerente Nacional de Negocios	Inicia: 10/08/2015 Finaliza: 12/08/2015	Cuestionario de control interno, aplicando pruebas de cumplimiento
Redactar un Plan de respuesta	3.2.	0,00	Gerente de	Inicia:	Cuestionario de

a los incidentes.			Producción y Servicios	10/08/2015 Finaliza: 12/08/2015	control interno, aplicando pruebas de cumplimiento y pruebas sustantivas
Preparar escenarios de incidentes disruptivos	3.2.	0,00	Gerente de Producción y Servicios	Inicia: 13/08/2015 Finaliza: 14/08/2015	Revisión de los escenarios preparados, comprobando su aplicabilidad
Preparar a los miembros del Gabinete de crisis y del Gabinete de apoyo de crisis para su función en el manejo de un incidente disruptivo.	4.1.	1.000,00	Gerente de Producción y Servicios	Inicia: 17/08/2015 Finaliza: 18/08/2015	Simulacro sorpresa dirigido a los miembros del gabinete de crisis y gabinete de apoyo de crisis
Preparar a los empleados del Banco KLM para que manejen incidentes relacionados con tecnología de la información y comunicación.	4.2.	1.000,00	Gerente de Producción y Servicios	Inicia: 19/08/2015 Finaliza: 20/08/2015	Simulacro sorpresa dirigido a los empleados del área de Infraestructura del Banco KLM

Preparar a los empleados del Banco KLM para manejar otros incidentes.	4.2.	500,00	Gerente de Recursos Humanos	Inicia: 21/08/2015 Finaliza: 21/08/2015	Simulacro sorpresa dirigido a todos los empleados del Banco KLM
Crear todas las condiciones necesarias para colaborar con la Policía.	4.3.	0,00	Jefe de Seguridad y Salud Ocupacional	Inicia: 24/08/2015 Finaliza: 24/08/2015	Verificación de los métodos utilizados para la comunicación con la Policía
Crear todas las condiciones necesarias para colaborar con la Ambulancia.	4.3.	0,00	Jefe de Seguridad y Salud Ocupacional	Inicia: 24/08/2015 Finaliza: 24/08/2015	Verificación de los métodos utilizados para la comunicación con los bomberos
Crear todas las condiciones necesarias para colaborar con los Bomberos.	4.3.	0,00	Jefe de Seguridad y Salud Ocupacional	Inicia: 24/08/2015 Finaliza: 24/08/2015	Verificación de los métodos utilizados para la comunicación con los bomberos
Redactar y mantener planes de	4.4.	0,00	Jefe de	Inicia:	Simulacro de

evacuación en caso de incendio.			Seguridad y Salud Ocupacional	25/08/2015 Finaliza: 25/08/2015	evacuación
Comprar/preparar y, si es necesario, mantener vías de comunicación.	4.5.	3.000,00	Jefe de Comunicaciones	Inicia: 26/08/2015 Finaliza: 26/08/2015	Revisión de las vías alternas de comunicación
Preparar todos los medios de transporte.	4.6.	500,00	Jefe Administrativo	Inicia: 26/08/2015 Finaliza: 26/08/2015	Revisión de la disponibilidad de los vehículos necesarios para el transporte previsto
Preparar a personas responsables de la comunicación durante un incidente disruptivo.	4.7.	500,00	Gerente de Producción y Servicios	Inicia: 27/08/2015 Finaliza: 27/08/2015	Simulacro aplicando diferentes escenarios de incidentes disruptivos
Preparar plantillas para declaraciones a los medios	4.7.	300,00	Jefe de Comunicación Social	Inicia: 28/08/2015 Finaliza:	Revisión de las plantillas preparadas para los

				28/08/2015	incidentes disruptivos
Realizar todos los arreglos necesarios en relación a las ubicaciones alternativas.	5.1.	5.000,00	Jefe de Comunicaciones	Inicia: 31/08/2015 Finaliza: 01/09/2015	Simulacro de prueba
Manejar las relaciones con proveedores y socios.	5.2.	0,00	Gerente de Producción y Servicios	Inicia: 02/09/2015 Finaliza: 02/09/2015	Comprobar mediante simulacros la disponibilidad de los proveedores y socios
Instalación de aplicaciones/bases de datos, preparación de los medios de instalación.	5.3	500,00	Jefe de Servidores	Inicia: 02/09/2015 Finaliza: 02/09/2015	Comprobación de la disponibilidad de los medios de instalación de la paquetería de software necesaria
Creación de copias de	5.4.	0,00	Subgerente de	Inicia:	Revisión periódica y

seguridad.			Control Tecnológico	02/09/2015 Finaliza: 02/09/2015	sorpresiva de las copias de seguridad de las aplicaciones y datos
Implementar estrategias para evitar el punto único de falla.	5.5.	3.000,00	Subgerente de Procesamiento e Infraestructura	Inicia: 02/09/2015 Finaliza: 02/09/2015	Simulacro aplicado a los puntos únicos de falla
Realizar todos los preparativos necesarios para la provisión de recursos financieros	5.6.	0,00	Gerente Financiero	Inicia: 03/09/2015 Finaliza: 03/09/2015	Revisar convenios de pago y propuestas de financiamiento elaborados en consideración de los incidentes disruptivos
Redactar planes de recuperación para actividades individuales.	6.	0,00	Gerente de recuperación de actividades	Inicia: 04/09/2015 Finaliza: 07/09/2015	Revisión y aplicación de los planes de recuperación

					mediante simulacros específicos para cada actividad
Preparar recursos para actividades individuales	6.	5.000,00	Subgerente de Procesamiento e Infraestructura	Inicia: 04/09/2015 Finaliza: 07/09/2015	Simulacros específicos para cada actividad individual

Gerente General

Ing. Pablo Tobar

_____

Firma

ANEXO 5.6 (a)

Estrategia de recuperación para la actividad realizar acciones preventivas y correctivas para garantizar la disponibilidad de los servicios de Comunicaciones

Anexo 5.6: Estrategia de Continuidad del Negocio

Apéndice 6a: Estrategia de recuperación para la actividad realizar acciones preventivas y correctivas para garantizar la disponibilidad de los servicios de Comunicaciones

Introducción

El objetivo de tiempo de recuperación para esta actividad es 2 horas.

El Gerente de recuperación; es decir, la persona responsable para la recuperación de esta actividad es el Jefe de Comunicaciones.

La actividad se recuperará de la siguiente forma: recuperación de la actividad en una ubicación alternativa: reubicación de todos los recursos o actividades en una ubicación alternativa

Cumplimiento de tareas y obligaciones clave

La actividad debe cumplir con las siguientes tareas y obligaciones:

Tabla 50. Actividades y obligaciones claves - Disponibilidad de los servicios de Comunicaciones.

Tarea / Obligación	Plazos
Verificación del funcionamiento de los equipos de comunicaciones, en sitio Quito y Guayaquil	30min
Pruebas de conectividad entre equipos de red	10min
Verificación de alarmas y conexiones físicas	10min
Monitoreo constante de los equipos de comunicaciones	5min
Limpieza externa de los equipos de comunicaciones	30min
Depuración de las configuraciones en los equipos	30min
Verificación del ambiente en el Data Center, temperatura	5min

y humedad adecuada	
Verificación del funcionamiento de la alta disponibilidad/respaldo de energía en el Data Center	5min

Recuperación de recursos

Los siguientes recursos son necesarios para la recuperación de la actividad:

Tabla 51. Recursos utilizados para la recuperación de cada una de las actividades - Disponibilidad de los servicios de Comunicaciones

Nombre del recurso	Descripción	Cantidad	Cuándo es necesario el recurso
Personas:			
Jefe de Comunicaciones	Liderazgo y Configuración de equipos de Comunicaciones	1	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo
Administrador de Comunicaciones	Administración los equipos de Comunicaciones, redes LAN, WAN, SAN; configuración, monitoreo, troubleshooting	1	Inmediatamente después de ocurrido el incidente disruptivo
Administrador de Telefonía	Administración los equipos de Telefonía, configuración, monitoreo, troubleshooting	1	Inmediatamente después de ocurrido el incidente disruptivo

Técnico de Comunicaciones	Soporte operativo y funcional de los equipos de Comunicaciones, redes	2	Inmediatamente después de 4 s de ocurrido el incidente disruptivo
Aplicaciones / bases de datos:			
Sistema operativo de Switches	Software para la actualización del SO de los switches	6	Inmediatamente después de ocurrido el incidente disruptivo
Sistema operativo de Firewalls	Software para la actualización del SO de los Firewalls	3	Inmediatamente después de ocurrido el incidente disruptivo
Sistema operativo de Routers	Software para la actualización del SO de los Routers	5	Inmediatamente después de ocurrido el incidente disruptivo
Sistema operativo de Ips	Software para la actualización del SO de los IPS	2	Inmediatamente después de ocurrido el incidente disruptivo
Software de monitoreo de	WhatsUp Gold, Solarwinds, Quest	4	Inmediatamente después de

redes	Network Tools, Cisco Prime		ocurrido el incidente disruptivo
Sistema operativo de Centrales Telefónicas	Software para la actualización del SO de las Centrales Telefónicas	2	Inmediatamente después de ocurrido el incidente disruptivo
Software de reportería	Cat Tools Enterprise	1	Inmediatamente después de ocurrido el incidente disruptivo
Datos almacenados en formato electrónico:			
Arquitectura de red institucional	Almacenado en un repositorio/server con seguridades	1	Inmediatamente después de ocurrido el incidente disruptivo
Manuales digitales de los equipos de Comunicaciones	Almacenado en un repositorio/server con seguridades	1	Inmediatamente después de ocurrido el incidente disruptivo
Respaldos de Bases de Datos	Almacenados en un Servidor de	1	Inmediatamente después de 1

de los equipos destinados para monitoreo de la Red	Comunicaciones con seguridades		hora de ocurrido el incidente disruptivo
Instaladores y licencias del Software de Monitoreo	Almacenados en un Servidor de Comunicaciones con seguridades	1	Inmediatamente después de ocurrido el incidente disruptivo
Datos almacenados en papel:			
Arquitectura de red institucional impresa	Archivador de Jefatura y Administrador de Comunicaciones	2	Inmediatamente después de ocurrido el incidente disruptivo
Manuales impresos para la configuración de los equipos de Comunicaciones	Archivador de Jefatura y Administrador de Comunicaciones	2	Inmediatamente después de ocurrido el incidente disruptivo
Contactos internos y externos para la gestión de TI	Archivador de Jefatura y Administrador de Comunicaciones	2	Inmediatamente después de ocurrido el incidente disruptivo
Equipos de TI y comunicaciones:			

PCs de escritorio	AllOne Core i7 2.4 GHz, 8 GB de memoria ram, disco duro sata de 1TB, 2 monitores LCD, teclado completo y mouse.	2	Inmediatamente después de ocurrido el incidente disruptivo
Laptop	AllOne Core i5 3.0 GHz, 8 GB de memoria ram, disco duro de 500 GB	2	Inmediatamente después de ocurrido el incidente disruptivo
Servidor	Servidor físico Lenovo i7, 2.4 GHz, 8 GB de memoria ram, disco duro sata de 500 GB.	1	Inmediatamente después de 4 horas de ocurrido el incidente disruptivo
Servidor	Servidor virtual ubicado en el Data Center, Intel Xeon 2.9 GHz, 8 GB de memoria ram, disco duro SCSI de 500 GB, Windows server 2008 R2	1	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo
Switch	Cisco Nexus 7k	2	Inmediatamente después de ocurrido el incidente disruptivo

Switch	Cisco Nexus 2k	8	Inmediatamente después de ocurrido el incidente disruptivo
Switch	Cisco Catalyst 6500	2	Inmediatamente después de ocurrido el incidente disruptivo
Switch	Cisco Catalyst 4500	2	Inmediatamente después de ocurrido el incidente disruptivo
Switch	Cisco Catalyst 3850	4	Inmediatamente después de ocurrido el incidente disruptivo
Switch	Cisco Catalyst 2960	30	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo
Firewall	Cisco ASA 5585	2	Inmediatamente después de ocurrido el incidente

			disruptivo
Firewall	Cisco ASA 5540	2	Inmediatamente después de ocurrido el incidente disruptivo
Firewall	Cisco ASA 5520	2	Inmediatamente después de ocurrido el incidente disruptivo
Router	Cisco ASR 1000	4	Inmediatamente después de ocurrido el incidente disruptivo
Router	Cisco 3900	4	Inmediatamente después de ocurrido el incidente disruptivo
Router	Cisco 2900	4	Inmediatamente después de ocurrido el incidente disruptivo
Router	Cisco 1900	4	Inmediatamente después de 1 hora de ocurrido

			el incidente disruptivo
Router	Cisco 881	10	Inmediatamente después de 4 horas de ocurrido el incidente disruptivo
IPS	Proventia GX6116	2	Inmediatamente después de ocurrido el incidente disruptivo
Impresora	Xerox workcentre	2	Inmediatamente después de 4 horas de ocurrido el incidente disruptivo
Teléfono	Teléfono IP Alcatel 4038	4	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo
Teléfono Celular	BlackBerry Curve, con paquete de datos	4	Inmediatamente después de ocurrido el incidente disruptivo
Canales de comunicación:			

Líneas fijas de teléfono	Líneas habilitadas de telefonía fija con salida a celulares	4	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo
Líneas celulares	Teléfonos celulares habilitados con paquetes de voz, datos y salida internacional	3	Inmediatamente después de ocurrido el incidente disruptivo
Acceso a internet	Enlace dedicado fibra óptica de 35Mbps	2	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo
Correo electrónico	Servidor de correo con cuentas habilitadas, con capacidad de 5 MB	2	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo
Otros equipos:			
Televisor	Televisor Panasonic de 42"	1	Inmediatamente después de 4 horas de ocurrido el incidente disruptivo
Instalaciones e infraestructura:			
Puntos de Red	Red LAN de cableado vertical y horizontal	8	Inmediatamente después de 1

de computadoras	categoría 6a		hora de ocurrido el incidente disruptivo
BackBone de servidores	Red LAN, SAN de cableado de Fibra Óptica	50	Inmediatamente después de ocurrido el incidente disruptivo
Muebles de oficina	Sillas y escritorios individuales para uso del personal técnico	6	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo
Servicios externos:			
Electricidad	Alimentación eléctrica de la red pública	2	Inmediatamente después de ocurrido el incidente disruptivo
Agua potable	Servicio de agua potable	1	Inmediatamente después de ocurrido el incidente disruptivo
Oficinas	Renta de Oficinas para uso del personal de Comunicaciones	1	Inmediatamente después de ocurrido el incidente disruptivo

La recuperación de recursos para esta actividad se ejecutará de la siguiente forma:

- Hardware y otros equipos de TIC se recuperarán de la siguiente manera: a) adquisición previa e instalación del equipo en la ubicación alternativa: si el objetivo del tiempo de recuperación es corto, y si se trata de un equipo complejo (por ej., los servidores), será necesario instalarlo con anticipación, independientemente de que ocurra o no un potencial incidente; b) adquisición del equipo fuera de la organización: si este tipo de equipo existe en el mercado y es posible adquirirlo dentro del objetivo de tiempo de recuperación (por ejemplo; la adquisición de ordenadores); c) uso de los servicios externalizados: si es demasiado costoso adquirir el equipo con antelación y/o es imposible adquirirlo dentro de un plazo tan corto, puede ser posible utilizar un servicio externo (alojamiento del sitio Web, por ejemplo).

- Los recursos humanos se recuperarán de la siguiente manera: a) documentar detalladamente los procedimientos para las actividades permitirá que otras personas sean capaces de llevarlas a cabo; b) capacitar a los empleados o socios para una amplia gama de tareas; c) divulgar los conocimientos o habilidades clave entre varias personas para dispersar el riesgo; d) utilizar proveedores externos para determinadas actividades ante el caso de indisponibilidad de los empleados de la organización; e) planificar reemplazos en caso de la no disponibilidad de ciertos empleados: los reemplazantes pueden ser personas de la misma unidad organizativa o personas que se encuentran más cerca de la ubicación alternativa; y f) administrar el conocimiento de los ex-empleados y de los empleados actuales, de los proveedores y socios y documentarlo en diversas bases de conocimiento.

- Otros equipos, reservas y materiales se recuperarán de la siguiente manera:

Tabla 52. Actividades para la recuperación de otros equipos, materiales y reservas - Disponibilidad de los servicios de Comunicaciones.

Nombre del equipo, reserva o material	Estrategia de recuperación
Sistema operativo de Switches	Almacenamiento previo en la ubicación alternativa, independientemente de que ocurra o no el potencial incidente
Sistema operativo de Firewalls	Almacenamiento previo en la ubicación alternativa, independientemente de que ocurra o no el potencial incidente
Sistema operativo de Routers	Almacenamiento previo en la ubicación alternativa, independientemente de que ocurra o no el potencial incidente
Sistema operativo de Ips	Almacenamiento previo en la ubicación alternativa, independientemente de que ocurra o no el potencial incidente
Software de monitoreo de redes	Almacenamiento previo en la ubicación alternativa, independientemente de que ocurra o no el potencial incidente
Sistema operativo de Centrales Telefónicas	Almacenamiento previo en la ubicación alternativa, independientemente de que ocurra o no el potencial incidente
Software de reportería	Almacenamiento previo en la ubicación alternativa, independientemente de que ocurra o no el potencial incidente
Arquitectura de red institucional	Almacenamiento previo en la ubicación alternativa, independientemente de que

	ocurra o no el potencial incidente
Manuales digitales de los equipos de Comunicaciones	Almacenamiento previo en la ubicación alternativa, independientemente de que ocurra o no el potencial incidente
Respaldos de Bases de Datos de los equipos destinados para monitoreo de la Red	Almacenamiento previo en la ubicación alternativa, independientemente de que ocurra o no el potencial incidente
Instaladores y licencias del Software de Monitoreo	Almacenamiento previo en la ubicación alternativa, independientemente de que ocurra o no el potencial incidente
Arquitectura de red institucional impresa	Almacenamiento previo en la ubicación alternativa, independientemente de que ocurra o no el potencial incidente
Manuales impresos para la configuración de los equipos de Comunicaciones	Almacenamiento previo en la ubicación alternativa, independientemente de que ocurra o no el potencial incidente
Contactos internos y externos para la gestión de TI	Almacenamiento previo en la ubicación alternativa, independientemente de que ocurra o no el potencial incidente
PCs de escritorio	Adquisición de nuevos equipos que contribuyan a la recuperación de la actividad
Laptop	Adquisición de nuevos equipos que contribuyan a la recuperación de la actividad
Servidores	• Almacenamiento previo en la ubicación alternativa, independientemente de que ocurra o no el potencial incidente • Desvío de suministros actuales al sitio

	alternativo • Re direccionamiento del montaje de una parte de los productos al sitio alternativo • Mantenimiento del equipo viejo que puede ser usado como sustituto
Switches	• Almacenamiento previo en la ubicación alternativa, independientemente de que ocurra o no el potencial incidente • Desvío de suministros actuales al sitio alternativo • Re direccionamiento del montaje de una parte de los productos al sitio alternativo • Mantenimiento del equipo viejo que puede ser usado como sustituto
Firewalls	• Almacenamiento previo en la ubicación alternativa, independientemente de que ocurra o no el potencial incidente • Desvío de suministros actuales al sitio alternativo • Re direccionamiento del montaje de una parte de los productos al sitio alternativo • Mantenimiento del equipo viejo que puede ser usado como sustituto
Routers	• Almacenamiento previo en la ubicación alternativa, independientemente de que ocurra o no el potencial incidente • Desvío de suministros actuales al sitio alternativo • Re direccionamiento del montaje de una parte de los productos al sitio alternativo • Mantenimiento del equipo viejo que

	puede ser usado como sustituto
IPS	• Almacenamiento previo en la ubicación alternativa, independientemente de que ocurra o no el potencial incidente • Desvío de suministros actuales al sitio alternativo • Re direccionamiento del montaje de una parte de los productos al sitio alternativo • Mantenimiento del equipo viejo que puede ser usado como sustituto
Impresora	Desvío de suministros actuales al sitio alternativo
Teléfono	Desvío de suministros actuales al sitio alternativo
Teléfono Celular	Adquisición de nuevos equipos que contribuyan a la recuperación de la actividad
Líneas fijas de teléfono	Desvío de suministros actuales al sitio alternativo
Líneas celulares	Adquisición de nuevos equipos que contribuyan a la recuperación de la actividad
Acceso a internet	• Almacenamiento previo en la ubicación alternativa, independientemente de que ocurra o no el potencial incidente • Desvío de suministros actuales al sitio alternativo • Re direccionamiento del montaje de una parte de los productos al sitio alternativo • Mantenimiento del equipo viejo que puede ser usado como sustituto
Correo electrónico	• Almacenamiento previo en la ubicación alternativa, independientemente de que

	ocurra o no el potencial incidente • Desvío de suministros actuales al sitio alternativo • Re direccionamiento del montaje de una parte de los productos al sitio alternativo • Mantenimiento del equipo viejo que puede ser usado como sustituto
Televisor	Adquisición de nuevos equipos que contribuyan a la recuperación de la actividad
Puntos de Red de computadoras	Adquisición de nuevos equipos que contribuyan a la recuperación de la actividad
BackBone de servidores	• Almacenamiento previo en la ubicación alternativa, independientemente de que ocurra o no el potencial incidente • Desvío de suministros actuales al sitio alternativo • Re direccionamiento del montaje de una parte de los productos al sitio alternativo • Mantenimiento del equipo viejo que puede ser usado como sustituto
Muebles de oficina	Desvío de suministros actuales al sitio alternativo

Adaptado de: (Kosutic, 2015).

Nota: la estrategia de recuperación para aplicaciones/bases de datos y servicios externos se especificará en la parte general de la Estrategia.

Procedimiento para copias de seguridad

Se deben realizar copias de seguridad de los datos utilizados por esta actividad con los siguientes intervalos:

Tabla 53. Copias de seguridad de los datos utilizados por cada actividad - Disponibilidad de los servicios de Comunicaciones.

Nombre de la aplicación, base de datos, carpeta, documento:	Frecuencia para creación de copias de seguridad	Procedimiento para copias de seguridad
Sistema operativo de Switches	3 Meses	Descarga de nuevas versiones desde la página oficial del fabricante
Sistema operativo de Firewalls	3 Meses	Descarga de nuevas versiones desde la página oficial del fabricante
Sistema operativo de Routers	3 Meses	Descarga de nuevas versiones desde la página oficial del fabricante
Sistema operativo de Ips	3 Meses	Descarga de nuevas versiones desde la página oficial del fabricante
Software de monitoreo de redes	12 Meses	Descarga de nuevas versiones desde la página oficial del fabricante
Sistema operativo de Centrales Telefónicas	3 Meses	Descarga de nuevas versiones desde la página oficial del fabricante

Software de reportería	12 Meses	Descarga de nuevas versiones desde la página oficial del fabricante
Copia de respaldo de configuración de equipos de comunicación (switches, firewalls, routers, centrales telefónicas, IPs)	Diaria	Procedimiento de respaldo automatizado basado en servidor
Arquitectura de red institucional	3 Meses	Bajo demanda, cuando existan cambios en la red de cableado
Manuales digitales de los equipos de Comunicaciones	3 Meses	Descarga de nuevas versiones desde la página oficial del fabricante Bajo demanda, cuando existan cambios en la red de cableado
Respaldos de Bases de Datos de los equipos destinados para monitoreo de la Red	1 Mes	Procedimiento de respaldo automatizado basado en servidor
Instaladores y licencias del Software de Monitoreo	12 Meses	Descarga de nuevas versiones desde la página oficial del fabricante
Manuales impresos para	3 Meses	Descarga de nuevas

la configuración de los equipos de Comunicaciones		versiones desde la página oficial del fabricante
Contactos internos y externos para la gestión de TI	1 Mes	Bajo demanda, mediante conexión a un servidor TFTP

Adaptado de: (Kosutic, 2015).

Nota: la frecuencia para la creación de copias de seguridad de datos compartidos por otras actividades está definida en la parte general de la Estrategia.

ANEXO 5.6 (b)

Estrategia de recuperación para la actividad realizar acciones preventivas y correctivas para garantizar la disponibilidad de los aplicativos de Core Bancario y Negocios

Anexo 5.6: Estrategia de Continuidad del Negocio

Apéndice 6b: Estrategia de recuperación para la actividad realizar acciones preventivas y correctivas para garantizar la disponibilidad de los aplicativos de Core Bancario y Negocios

Introducción

El objetivo de tiempo de recuperación para esta actividad es 1.5 horas.

El Gerente de recuperación; es decir, la persona responsable para la recuperación de esta actividad es el Subgerente de Procesamiento e Infraestructura.

La actividad se recuperará de la siguiente forma: recuperación de la actividad en una ubicación alternativa: reubicación de todos los recursos o actividades en una ubicación alternativa

Cumplimiento de tareas y obligaciones clave

La actividad debe cumplir con las siguientes tareas y obligaciones:

Tabla 54. Actividades y obligaciones claves - Disponibilidad de los aplicativos de Core Bancario y Negocios.

Tarea / Obligación	Plazos
Verificación del correcto funcionamiento de los servidores de aplicaciones de Core Bancario y Negocios	10min
Pruebas de conectividad de los servidores y bases de datos	10min
Verificación de alarmas y conexiones físicas	10min
Monitoreo constante del aplicativo de Core Bancario	10min
Verificar la disponibilidad de los equipos de Comunicaciones	15min
Limpieza externa de los servidores de Core Bancario y Negocios	30min
Depuración de las configuraciones en los equipos	30min
Verificación del ambiente en el Data Center, temperatura y	5min

humedad adecuada	
Escalar el incidente al proveedor de la aplicación, equipo en caso de ser necesario	10min
Respuesta del proveedor una vez escalado el incidente	15min
Solución al problema por parte del proveedor (caso extremo)	24 horas

Recuperación de recursos

Los siguientes recursos son necesarios para la recuperación de la actividad:

Tabla 55. Recursos utilizados para la recuperación de cada una de las actividades - Disponibilidad de los aplicativos de Core Bancario y Negocios.

Nombre del recurso	Descripción	Cantidad	Cuándo es necesario el recurso
Personas:			
Gerente de Producción y Servicios	Liderazgo, comunicación, decisión, coordinación	1	Inmediatamente después de ocurrido el incidente disruptivo
Jefe de Servidores	Liderazgo y Configuración de servidores, bases de datos, aplicativos	1	Inmediatamente después de ocurrido el incidente disruptivo
Jefe de Centro de Computo	Liderazgo, configuración de sistemas y aplicaciones de Core Bancario (AS400)	1	Inmediatamente después de ocurrido el incidente disruptivo

Jefe de Comunicaciones	Liderazgo y Configuración de equipos de Comunicaciones	1	Inmediatamente después de ocurrido el incidente disruptivo
Administrador de Servidores	Administrar los servidores de Aplicativos, bases de datos; configuración, monitoreo, troubleshooting	2	Inmediatamente después de ocurrido el incidente disruptivo
Administrador de Servidores	Administrar los servidores de Aplicativos, bases de datos; configuración, monitoreo, troubleshooting	2	Inmediatamente después de ocurrido el incidente disruptivo
Administrador de Comunicaciones	Administración los equipos de Comunicaciones, redes LAN, WAN, SAN; configuración, monitoreo, troubleshooting	1	Inmediatamente después de ocurrido el incidente disruptivo
Analista de Monitoreo	Soporte operativo y funcional de los aplicativos de Monitoreo	2	Inmediatamente después de ocurrido el incidente disruptivo
Aplicaciones /			

bases de datos:			
Sistema AS400	Sistemas de Core Bancario	4	Inmediatamente después de ocurrido el incidente disruptivo
Microsoft SQL Server 2005	Gestor de Base de datos SQL Server 2005	2	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo
Sistemas Operativos de Comunicaciones	Software para Comunicaciones de datos	2	Inmediatamente después de ocurrido el incidente disruptivo
PeopleSoft, CRM, ERP	Sistemas de Negocio	2	Inmediatamente después de ocurrido el incidente disruptivo
Big Data	Almacenamiento y gestión de la información del Banco	4	Inmediatamente después de ocurrido el incidente disruptivo
Datos almacenados en formato electrónico:			
Copia de respaldo de configuración de los servidores y bases de	Almacenados en un Servidor del Centro de Computo bajo	2	Inmediatamente después de ocurrido el

datos	seguridades informáticas		incidente disruptivo
Detalle diario de transacciones financieras (consumos)	Almacenado en un repositorio/server con seguridades	2	Inmediatamente después de ocurrido el incidente disruptivo
Copias diarias de respaldo de las bases de datos del Core Bancario	Almacenado en un repositorio/server con seguridades	1	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo
Paquete instalador de los gestores de bases de datos, Core Bancario y aplicativos de Negocios	Almacenados en un Servidor del Centro de Computo con seguridades informáticas	2	Inmediatamente después de ocurrido el incidente disruptivo
Estados de cuenta de los Clientes	Almacenados en un Servidor del Centro de Computo bajo seguridades informáticas	2	Inmediatamente después de 4 horas de ocurrido el incidente disruptivo
Datos almacenados en papel:			
Reporte consolidado del movimiento financiero diario	Archivador de Gerencia de Negocios y Financiera	2	Inmediatamente después de 4 horas de ocurrido el incidente disruptivo
Manuales impresos	Archivador de	2	Inmediatamente

para la configuración y manejo aplicativos de Core Bancario	Jefaturas de Servidores y Soporte Técnico		después de ocurrido el incidente disruptivo
Contactos internos y externos para la gestión de TI	Archivador de las Jefaturas y Administradores de Comunicaciones, Servidores, Centro de Computo	2	Inmediatamente después de ocurrido el incidente disruptivo
Equipos de TI y comunicaciones:			
PCs de escritorio	AllOne Core i7 2.4 GHz, 8 GB de memoria ram, disco duro sata de 1TB, 2 monitores LCD, teclado completo y mouse.	9	Inmediatamente después de ocurrido el incidente disruptivo
Laptop	AllOne Core i5 3.0 GHz, 8 GB de memoria ram, disco duro de 500 GB	3	Inmediatamente después de ocurrido el incidente disruptivo
Servidor de Monitoreo AS400	Servidor físico Lenovo i7, 2.4 GHz, 8 GB de memoria ram, disco duro sata de 500 GB.	4	Inmediatamente después de ocurrido el incidente disruptivo
Servidor de Aplicaciones	IBM Power 8000	2	Inmediatamente después de ocurrido el

			incidente disruptivo
Impresora	Xerox workcentre	4	Inmediatamente después de 4 horas de ocurrido el incidente disruptivo
Teléfono	Teléfono IP Alcatel 4038	9	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo
Teléfono Celular	BlackBerry Curve, con paquete de datos	9	Inmediatamente después de ocurrido el incidente disruptivo
Canales de comunicación:			
Líneas fijas de teléfono	Líneas habilitadas de telefonía fija con salida a celulares	9	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo
Líneas celulares	Teléfonos celulares habilitados con paquetes de voz, datos y salida internacional	9	Inmediatamente después de ocurrido el incidente disruptivo
Acceso a internet	Enlace dedicado fibra óptica de	2	Inmediatamente después de

	35Mbps		ocurrido el incidente disruptivo
Correo electrónico	Servidor de correo con cuentas habilitadas, con capacidad de 5 MB	9	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo
Otros equipos:			
Televisor	Televisor Panasonic de 42"	1	Inmediatamente después de 4 horas de ocurrido el incidente disruptivo
Instalaciones e infraestructura:			
Puntos de Red de computadoras	Red LAN de cableado vertical y horizontal categoría 6a	15	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo
BackBone de equipos de Core Bancario	Red LAN, SAN de cableado de Fibra Óptica	30	Inmediatamente después de ocurrido el incidente disruptivo
Muebles de oficina	Sillas y escritorios individuales para uso del personal técnico	15	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo

Servicios externos:			
Electricidad	Alimentación eléctrica de la red pública	2	Inmediatamente después de ocurrido el incidente disruptivo
Agua potable	Servicio de agua potable	1	Inmediatamente después de ocurrido el incidente disruptivo
Oficinas	Renta de Oficinas para uso del personal de Comunicaciones	1	Inmediatamente después de ocurrido el incidente disruptivo
Servicios de soporte del proveedor correspondiente	Servicio de soporte de las empresas proveedoras de los aplicativos	1	Inmediatamente después de ocurrido el incidente disruptivo

Adaptado de: (Kosutic, 2015).

La recuperación de recursos para esta actividad se ejecutará de la siguiente forma:

- Hardware y otros equipos de TIC se recuperarán de la siguiente manera: a) adquisición previa e instalación del equipo en la ubicación alternativa: si el objetivo del tiempo de recuperación es corto, y si se trata de un equipo complejo (por ej., los servidores), será necesario instalarlo con anticipación, independientemente de que ocurra o no un potencial incidente; b) adquisición del equipo fuera de la organización: si este tipo de equipo existe

en el mercado y es posible adquirirlo dentro del objetivo de tiempo de recuperación (por ejemplo; la adquisición de ordenadores); c) uso de los servicios externalizados: si es demasiado costoso adquirir el equipo con antelación y/o es imposible adquirirlo dentro de un plazo tan corto, puede ser posible utilizar un servicio externo (alojamiento del sitio Web, por ejemplo).

- Los recursos humanos se recuperarán de la siguiente manera: a) documentar detalladamente los procedimientos para las actividades permitirá que otras personas sean capaces de llevarlas a cabo; b) capacitar a los empleados o socios para una amplia gama de tareas; c) divulgar los conocimientos o habilidades clave entre varias personas para dispersar el riesgo; d) utilizar proveedores externos para determinadas actividades ante el caso de indisponibilidad de los empleados de la organización; e) planificar reemplazos en caso de la no disponibilidad de ciertos empleados: los reemplazantes pueden ser personas de la misma unidad organizativa o personas que se encuentran más cerca de la ubicación alternativa; y f) administrar el conocimiento de los ex-empleados y de los empleados actuales, de los proveedores y socios y documentarlo en diversas bases de conocimiento.

- Otros equipos, reservas y materiales se recuperarán de la siguiente manera:

Tabla 56. Actividades para la recuperación de otros equipos, materiales y reservas - Disponibilidad de los aplicativos de Core Bancario y Negocios.

Nombre del equipo, reserva o material	Estrategia de recuperación
Sistema AS400	• Almacenamiento previo en la ubicación alternativa, independientemente de que ocurra o no el potencial incidente • Desvío de suministros actuales al sitio

	alternativo • Re direccionamiento del montaje de una parte de los productos al sitio alternativo • Mantenimiento del equipo viejo que puede ser usado como sustituto
Microsoft SQL Server 2005	• Almacenamiento previo en la ubicación alternativa, independientemente de que ocurra o no el potencial incidente • Desvío de suministros actuales al sitio alternativo • Re direccionamiento del montaje de una parte de los productos al sitio alternativo • Mantenimiento del equipo viejo que puede ser usado como sustituto
Sistemas Operativos de Comunicaciones	Almacenamiento previo en la ubicación alternativa, independientemente de que ocurra o no el potencial incidente
PeopleSoft, CRM, ERP	• Almacenamiento previo en la ubicación alternativa, independientemente de que ocurra o no el potencial incidente • Desvío de suministros actuales al sitio alternativo • Re direccionamiento del montaje de una parte de los productos al sitio alternativo • Mantenimiento del equipo viejo que puede ser usado como sustituto
Big Data	• Almacenamiento previo en la ubicación alternativa, independientemente de que ocurra o no el potencial incidente • Desvío de suministros actuales al sitio alternativo

	• Re direccionamiento del montaje de una parte de los productos al sitio alternativo • Mantenimiento del equipo viejo que puede ser usado como sustituto
Copia de respaldo de configuración de los servidores y bases de datos	Almacenamiento previo en la ubicación alternativa, independientemente de que ocurra o no el potencial incidente
Detalle diario de transacciones financieras (consumos)	Almacenamiento previo en la ubicación alternativa, independientemente de que ocurra o no el potencial incidente
Copias diarias de respaldo de las bases de datos del Core Bancario	Almacenamiento previo en la ubicación alternativa, independientemente de que ocurra o no el potencial incidente
Paquete instalador de los gestores de bases de datos, Core Bancario y aplicativos de Negocios	Almacenamiento previo en la ubicación alternativa, independientemente de que ocurra o no el potencial incidente
Estados de cuenta de los Clientes	Almacenamiento previo en la ubicación alternativa, independientemente de que ocurra o no el potencial incidente
Reporte consolidado del movimiento financiero diario	Almacenamiento previo en la ubicación alternativa, independientemente de que ocurra o no el potencial incidente
Manuales impresos para la configuración y manejo aplicativos de Core Bancario	Almacenamiento previo en la ubicación alternativa, independientemente de que ocurra o no el potencial incidente
Contactos internos y	Almacenamiento previo en la ubicación

externos para la gestión de TI	alternativa, independientemente de que ocurra o no el potencial incidente
PCs de escritorio	Adquisición de nuevos equipos que contribuyan a la recuperación de la actividad
Laptop	Adquisición de nuevos equipos que contribuyan a la recuperación de la actividad
Servidor de Monitoreo AS400	• Almacenamiento previo en la ubicación alternativa, independientemente de que ocurra o no el potencial incidente • Desvío de suministros actuales al sitio alternativo • Re direccionamiento del montaje de una parte de los productos al sitio alternativo • Mantenimiento del equipo viejo que puede ser usado como sustituto
Servidor de Aplicaciones	• Almacenamiento previo en la ubicación alternativa, independientemente de que ocurra o no el potencial incidente • Desvío de suministros actuales al sitio alternativo • Re direccionamiento del montaje de una parte de los productos al sitio alternativo • Mantenimiento del equipo viejo que puede ser usado como sustituto
Impresora	Desvío de suministros actuales al sitio alternativo
Teléfono	Desvío de suministros actuales al sitio alternativo
Teléfono Celular	Adquisición de nuevos equipos que contribuyan a la recuperación de la actividad
Líneas fijas de teléfono	Desvío de suministros actuales al sitio alternativo
Líneas celulares	Adquisición de nuevos equipos que contribuyan

	a la recuperación de la actividad
Acceso a internet	• Almacenamiento previo en la ubicación alternativa, independientemente de que ocurra o no el potencial incidente • Desvío de suministros actuales al sitio alternativo • Re direccionamiento del montaje de una parte de los productos al sitio alternativo • Mantenimiento del equipo viejo que puede ser usado como sustituto
Correo electrónico	• Almacenamiento previo en la ubicación alternativa, independientemente de que ocurra o no el potencial incidente • Desvío de suministros actuales al sitio alternativo • Re direccionamiento del montaje de una parte de los productos al sitio alternativo • Mantenimiento del equipo viejo que puede ser usado como sustituto
Televisor	Adquisición de nuevos equipos que contribuyan a la recuperación de la actividad
Puntos de Red de computadoras	Adquisición de nuevos equipos que contribuyan a la recuperación de la actividad
BackBone de servidores	• Almacenamiento previo en la ubicación alternativa, independientemente de que ocurra o no el potencial incidente • Desvío de suministros actuales al sitio alternativo • Re direccionamiento del montaje de una parte de los productos al sitio alternativo • Mantenimiento del equipo viejo que puede

	ser usado como sustituto
Muebles de oficina	Desvío de suministros actuales al sitio alternativo
Servicios de soporte del proveedor correspondiente	Adquisición de nuevos equipos que contribuyan a la recuperación de la actividad

Adaptado de: (Kosutic, 2015).

Nota: la estrategia de recuperación para aplicaciones/bases de datos y servicios externos se especificará en la parte general de la Estrategia.

Procedimiento para copias de seguridad

Se deben realizar copias de seguridad de los datos utilizados por esta actividad con los siguientes intervalos:

Tabla 57. Copias de seguridad de los datos utilizados por cada actividad - Disponibilidad de los aplicativos de Core Bancario y Negocios.

Nombre de la aplicación, base de datos, carpeta, documento:	Frecuencia para creación de copias de seguridad	Procedimiento para copias de seguridad
Sistema AS400	3 Meses	Descarga de nuevas versiones desde la página oficial del fabricante
Microsoft SQL Server 2005	3 Meses	Descarga de nuevas versiones desde la página oficial del fabricante
Sistemas Operativos de Comunicaciones	3 Meses	Descarga de nuevas versiones desde la página oficial del

		fabricante
PeopleSoft, CRM, ERP	3 Meses	Descarga de nuevas versiones desde la página oficial del fabricante
Big Data	3 Meses	Descarga de nuevas versiones desde la página oficial del fabricante
Copia de respaldo de configuración de los servidores y bases de datos	Diaria	Procedimiento de respaldo automatizado basado en servidor
Detalle diario de transacciones financieras (consumos)	Diaria	Procedimiento de respaldo automatizado basado en servidor
Copias diarias de respaldo de las bases de datos del Core Bancario	Diaria	Procedimiento de respaldo automatizado basado en servidor
Paquete instalador de los gestores de bases de datos, Core Bancario y aplicativos de Negocios	3 Meses	Bajo demanda, mediante conexión a un servidor TFTP
Estados de cuenta de los Clientes	Diaria	Procedimiento de respaldo automatizado basado en servidor
Reporte consolidado del movimiento financiero diario	Diaria	Procedimiento de respaldo automatizado basado en servidor

Manuales impresos para la configuración y manejo aplicativos de Core Bancario	3 Meses	Descarga de nuevas versiones desde la página oficial del fabricante
Contactos internos y externos para la gestión de TI	1 Mes	Bajo demanda, mediante conexión a un servidor TFTP

Adaptado de: (Kosutic, 2015).

Nota: la frecuencia para la creación de copias de seguridad de datos compartidos por otras actividades está definida en la parte general de la Estrategia.

ANEXO 5.6 (c)

Estrategia de recuperación para la actividad realizar acciones preventivas y correctivas para garantizar la disponibilidad de los sistemas y aplicativos Administrativos, Financieros y Tecnológicos

Anexo 5.6: Estrategia de Continuidad del Negocio

Apéndice 6c: Estrategia de recuperación para la actividad realizar acciones preventivas y correctivas para garantizar la disponibilidad de los sistemas y aplicativos Administrativos, Financieros y Tecnológicos

Introducción

El objetivo de tiempo de recuperación para esta actividad es 4 horas.

El Gerente de recuperación; es decir, la persona responsable para la recuperación de esta actividad es el Jefe de Servidores.

La actividad se recuperará de la siguiente forma: recuperación de la actividad en una ubicación alternativa: reubicación de todos los recursos o actividades en una ubicación alternativa

Cumplimiento de tareas y obligaciones clave

La actividad debe cumplir con las siguientes tareas y obligaciones:

Tabla 58. Actividades y obligaciones claves - Disponibilidad de los sistemas y aplicativos Administrativos, Financieros y Tecnológicos.

Tarea / Obligación	Plazos
Verificación del correcto funcionamiento de los servidores de aplicaciones y base de datos	30min
Pruebas de conectividad de los servidores y bases de datos	15min
Verificación de alarmas y conexiones físicas	15min
Monitoreo constante de los aplicativos, servidores y bases de satos	10min
Verificar la disponibilidad de los equipos de Comunicaciones	15min
Limpieza externa de los servidores	60min
Depuración de las configuraciones en los equipos	30min
Verificación del ambiente en el Data Center, temperatura y humedad adecuada	5min

Verificación del funcionamiento de la alta disponibilidad/respaldo de energía en el Data Center	5min
Escalar el incidente al proveedor de la aplicación, equipo en caso de ser necesario	30min
Respuesta del proveedor una vez escalado el incidente	15min
Solución al problema por parte del proveedor (caso extremo)	24 horas

Recuperación de recursos

Los siguientes recursos son necesarios para la recuperación de la actividad:

Tabla 59. Recursos utilizados para la recuperación de cada una de las actividades - Disponibilidad de los sistemas y aplicativos Administrativos, Financieros y Tecnológicos.

Nombre del recurso	Descripción	Cantidad	Cuándo es necesario el recurso
Personas:			
Jefe de Monitoreo	Liderazgo y Configuración de aplicativos de Monitoreo	1	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo
Jefe de Servidores	Liderazgo y Configuración de servidores, bases de datos, aplicativos	1	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo
Jefe de Soporte Técnico	Liderazgo, configuración de sistemas operativos, soporte operativo y	1	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo

	funcional de aplicaciones		
Jefe de Mesa de Servicios	Liderazgo, comunicación y soporte funcional de los aplicativos del Banco	1	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo
Administrador de Servidores	Administrar los servidores de Aplicativos, bases de datos; configuración, monitoreo, troubleshooting	6	Inmediatamente después de ocurrido el incidente disruptivo
Analista de Monitoreo	Soporte operativo y funcional de los aplicativos de Monitoreo	2	Inmediatamente después de ocurrido el incidente disruptivo
Técnico de Soporte	Soporte operativo y funcional de las aplicaciones institucionales, asistente de redes y soporte de equipos informáticos	4	Inmediatamente después de 4 horas de ocurrido el incidente disruptivo
Aplicaciones / bases de datos:			
Oracle 11g	Gestor de Base de datos Oracle 11g	2	Inmediatamente después de ocurrido el

			incidente disruptivo
Microsoft SQL Server 2005	Gestor de Base de datos SQL Server 2005	2	Inmediatamente después de ocurrido el incidente disruptivo
Office 2010	Paquetes de Licencias corporativas adquirida por el Banco	4	Inmediatamente después de 4 horas de ocurrido el incidente disruptivo
Correo electrónico exchange	Correo electrónico corporativo enterprise	2	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo
PeopleSoft	Gestor de casos y reportes	4	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo
Business intelligence	Software para gestión de la información del Banco	2	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo
SharePoint	Software para colaboración del Banco	2	Inmediatamente después de 4 horas de ocurrido el

			incidente disruptivo
Datos almacenados en formato electrónico:			
Copia de respaldo de configuración de los servidores y bases de datos	Almacenados en un Servidor del Centro de Computo bajo seguridades informáticas	2	Inmediatamente después de ocurrido el incidente disruptivo
Arquitectura de conexiones IT	Almacenado en un repositorio/server con seguridades	1	Inmediatamente después de ocurrido el incidente disruptivo
Manuales digitales de los servidores, aplicativos y bases de datos	Almacenado en un repositorio/server con seguridades	1	Inmediatamente después de ocurrido el incidente disruptivo
Paquete instalador de los gestores de bases de datos utilizados en la institución	Almacenados en un Servidor del Centro de Computo bajo seguridades informáticas	2	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo
Instaladores de los sistemas operativos manejados en la institución y de las herramientas	Almacenados en un Servidor del Centro de Computo bajo seguridades	2	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo

administrativas, financieras y tecnológicas de gestión de aplicaciones	informáticas		
Datos almacenados en papel:			
Arquitectura de conexiones IT	Archivador de Jefatura y Administrador de Servidores	2	Inmediatamente después de ocurrido el incidente disruptivo
Manuales impresos para la configuración de servidores, aplicaciones y bases de datos	Archivador de Jefaturas de Servidores y Soporte Técnico	2	Inmediatamente después de ocurrido el incidente disruptivo
Contactos internos y externos para la gestión de TI	Archivador de Jefaturas de Mesa de Servicios y Analista de Soluciones	2	Inmediatamente después de ocurrido el incidente disruptivo
Equipos de TI y comunicaciones:			
PCs de escritorio	AllOne Core i7 2.4 GHz, 8 GB de memoria ram, disco duro sata de 1TB, 2 monitores LCD, teclado completo y mouse.	16	Inmediatamente después de ocurrido el incidente disruptivo
Laptop	AllOne Core i5 3.0	2	Inmediatamente

	GHz, 8 GB de memoria ram, disco duro de 500 GB		después de ocurrido el incidente disruptivo
Servidor de Monitoreo	Servidor físico Lenovo i7, 2.4 GHz, 8 GB de memoria ram, disco duro sata de 500 GB.	4	Inmediatamente después de 4 horas de ocurrido el incidente disruptivo
Servidor de Aplicaciones	Servidor virtual ubicado en el Data Center, Intel Xeon 2.9 GHz, 8 GB de memoria ram, disco duro SCSI de 500 GB, Windows server 2008 R2	30	Inmediatamente después de ocurrido el incidente disruptivo
Impresora	Xerox workcentre	3	Después de 24 horas de ocurrido el incidente disruptivo
Teléfono	Teléfono IP Alcatel 4038	16	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo
Teléfono Celular	BlackBerry Curve, con paquete de datos	10	Inmediatamente después de ocurrido el

			incidente disruptivo
Canales de comunicación:			
Líneas fijas de teléfono	Líneas habilitadas de telefonía fija con salida a celulares	6	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo
Líneas celulares	Teléfonos celulares habilitados con paquetes de voz, datos y salida internacional	10	Inmediatamente después de ocurrido el incidente disruptivo
Acceso a internet	Enlace dedicado fibra óptica de 35Mbps	2	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo
Correo electrónico	Servidor de correo con cuentas habilitadas, con capacidad de 5 MB	4	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo
Otros equipos:			
Televisor	Televisor Panasonic de 42"	1	Inmediatamente después de 4 horas de ocurrido el incidente disruptivo

Instalaciones e infraestructura:			
Puntos de Red de computadoras	Red LAN de cableado vertical y horizontal categoría 6a	16	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo
BackBone de equipos de Core Bancario	Red LAN, SAN de cableado de Fibra Óptica	50	Inmediatamente después de ocurrido el incidente disruptivo
Muebles de oficina	Sillas y escritorios individuales para uso del personal técnico	20	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo
Servicios externos:			
Electricidad	Alimentación eléctrica de la red pública	2	Inmediatamente después de ocurrido el incidente disruptivo
Agua potable	Servicio de agua potable	1	Inmediatamente después de ocurrido el incidente disruptivo
Oficinas	Renta de Oficinas para uso del personal de Comunicaciones	1	Inmediatamente después de ocurrido el incidente

			disruptivo
Servicios de soporte del proveedor correspondiente	Servicio de soporte de las empresas proveedoras de los aplicativos	1	Inmediatamente después de ocurrido el incidente disruptivo

Adaptado de: (Kosutic, 2015).

La recuperación de recursos para esta actividad se ejecutará de la siguiente forma:

- Hardware y otros equipos de TIC se recuperarán de la siguiente manera: a) adquisición previa e instalación del equipo en la ubicación alternativa: si el objetivo del tiempo de recuperación es corto, y si se trata de un equipo complejo (por ej., los servidores), será necesario instalarlo con anticipación, independientemente de que ocurra o no un potencial incidente; b) adquisición del equipo fuera de la organización: si este tipo de equipo existe en el mercado y es posible adquirirlo dentro del objetivo de tiempo de recuperación (por ejemplo; la adquisición de ordenadores); c) uso de los servicios externalizados: si es demasiado costoso adquirir el equipo con antelación y/o es imposible adquirirlo dentro de un plazo tan corto, puede ser posible utilizar un servicio externo (alojamiento del sitio Web, por ejemplo).

- Los recursos humanos se recuperarán de la siguiente manera: a) documentar detalladamente los procedimientos para las actividades permitirá que otras personas sean capaces de llevarlas a cabo; b) capacitar a los empleados o socios para una amplia gama de tareas; c) divulgar los conocimientos o habilidades clave entre varias personas para dispersar el riesgo; d) utilizar proveedores externos para determinadas actividades ante el caso de indisponibilidad de los empleados de la organización; e) planificar reemplazos en caso de la no disponibilidad de ciertos empleados: los reemplazantes pueden ser personas de la misma unidad organizativa o

personas que se encuentran más cerca de la ubicación alternativa; y f) administrar el conocimiento de los ex-empleados y de los empleados actuales, de los proveedores y socios y documentarlo en diversas bases de conocimiento.

- Otros equipos, reservas y materiales se recuperarán de la siguiente manera:

Tabla 60. Actividades para la recuperación de otros equipos, materiales y reservas - Disponibilidad de los sistemas y aplicativos Administrativos, Financieros y Tecnológicos

Nombre del equipo, reserva o material	Estrategia de recuperación
Oracle 11g	• Almacenamiento previo en la ubicación alternativa, independientemente de que ocurra o no el potencial incidente • Desvío de suministros actuales al sitio alternativo • Re direccionamiento del montaje de una parte de los productos al sitio alternativo • Mantenimiento del equipo viejo que puede ser usado como sustituto
Microsoft SQL Server 2005	• Almacenamiento previo en la ubicación alternativa, independientemente de que ocurra o no el potencial incidente • Desvío de suministros actuales al sitio alternativo • Re direccionamiento del montaje de una parte de los productos al sitio alternativo • Mantenimiento del equipo viejo que puede ser usado como sustituto
Office 2010	Almacenamiento previo en la ubicación

	alternativa, independientemente de que ocurra o no el potencial incidente
Correo electrónico exchange	• Almacenamiento previo en la ubicación alternativa, independientemente de que ocurra o no el potencial incidente • Desvío de suministros actuales al sitio alternativo • Re direccionamiento del montaje de una parte de los productos al sitio alternativo • Mantenimiento del equipo viejo que puede ser usado como sustituto
PeopleSoft	• Almacenamiento previo en la ubicación alternativa, independientemente de que ocurra o no el potencial incidente • Desvío de suministros actuales al sitio alternativo • Re direccionamiento del montaje de una parte de los productos al sitio alternativo • Mantenimiento del equipo viejo que puede ser usado como sustituto
Business intelligence	Almacenamiento previo en la ubicación alternativa, independientemente de que ocurra o no el potencial incidente
SharePoint	Almacenamiento previo en la ubicación alternativa, independientemente de que ocurra o no el potencial incidente
Copia de respaldo de configuración de los servidores y bases de datos	Almacenamiento previo en la ubicación alternativa, independientemente de que ocurra o no el potencial incidente
Arquitectura de	Almacenamiento previo en la ubicación

conexiones IT	alternativa, independientemente de que ocurra o no el potencial incidente
Manuales digitales de los servidores, aplicativos y bases de datos	Almacenamiento previo en la ubicación alternativa, independientemente de que ocurra o no el potencial incidente
Paquete instalador de los gestores de bases de datos utilizados en la institución	Almacenamiento previo en la ubicación alternativa, independientemente de que ocurra o no el potencial incidente
Instaladores de los sistemas operativos manejados en la institución y de las herramientas administrativas, financieras y tecnológicas de gestión de aplicaciones	Almacenamiento previo en la ubicación alternativa, independientemente de que ocurra o no el potencial incidente
Arquitectura de conexiones IT	Almacenamiento previo en la ubicación alternativa, independientemente de que ocurra o no el potencial incidente
Manuales impresos para la configuración de servidores, aplicaciones y bases de datos	Almacenamiento previo en la ubicación alternativa, independientemente de que ocurra o no el potencial incidente
Contactos internos y externos para la gestión de TI	Almacenamiento previo en la ubicación alternativa, independientemente de que ocurra o no el potencial incidente
PCs de escritorio	Adquisición de nuevos equipos que contribuyan a la recuperación de la actividad
Laptop	Adquisición de nuevos equipos que contribuyan a la recuperación de la actividad

Servidor de Monitoreo	Adquisición de nuevos equipos que contribuyan a la recuperación de la actividad
Servidor de Aplicaciones	Adquisición de nuevos equipos que contribuyan a la recuperación de la actividad
Impresora	Desvío de suministros actuales al sitio alternativo
Teléfono	Desvío de suministros actuales al sitio alternativo
Teléfono Celular	Adquisición de nuevos equipos que contribuyan a la recuperación de la actividad
Líneas fijas de teléfono	Desvío de suministros actuales al sitio alternativo
Líneas celulares	Adquisición de nuevos equipos que contribuyan a la recuperación de la actividad
Acceso a internet	• Almacenamiento previo en la ubicación alternativa, independientemente de que ocurra o no el potencial incidente • Desvío de suministros actuales al sitio alternativo • Re direccionamiento del montaje de una parte de los productos al sitio alternativo • Mantenimiento del equipo viejo que puede ser usado como sustituto
Correo electrónico	• Almacenamiento previo en la ubicación alternativa, independientemente de que ocurra o no el potencial incidente • Desvío de suministros actuales al sitio alternativo • Re direccionamiento del montaje de una parte de los productos al sitio alternativo • Mantenimiento del equipo viejo que puede

	ser usado como sustituto
Televisor	Adquisición de nuevos equipos que contribuyan a la recuperación de la actividad
Puntos de Red de computadoras	Adquisición de nuevos equipos que contribuyan a la recuperación de la actividad
BackBone de equipos de Core Bancario	• Almacenamiento previo en la ubicación alternativa, independientemente de que ocurra o no el potencial incidente • Desvío de suministros actuales al sitio alternativo • Re direccionamiento del montaje de una parte de los productos al sitio alternativo Mantenimiento del equipo viejo que puede ser usado como sustituto
Muebles de oficina	Desvío de suministros actuales al sitio alternativo
Servicios de soporte del proveedor correspondiente	Adquisición de nuevos equipos que contribuyan a la recuperación de la actividad

Adaptado de: (Kosutic, 2015).

Nota: la estrategia de recuperación para aplicaciones/bases de datos y servicios externos se especificará en la parte general de la Estrategia.

Procedimiento para copias de seguridad

Se deben realizar copias de seguridad de los datos utilizados por esta actividad con los siguientes intervalos:

Tabla 61. Copias de seguridad de los datos utilizados por cada actividad - Disponibilidad de los sistemas y aplicativos Administrativos, Financieros y Tecnológicos

Nombre de la aplicación, base de datos, carpeta, documento:	Frecuencia para creación de copias de seguridad	Procedimiento para copias de seguridad
Oracle 11g	3 Meses	Descarga de nuevas versiones desde la página oficial del fabricante
Microsoft SQL Server 2005	3 Meses	Descarga de nuevas versiones desde la página oficial del fabricante
Office 2010	12 Meses	Descarga de nuevas versiones desde la página oficial del fabricante
Correo electrónico exchange	3 Meses	Descarga de nuevas versiones desde la página oficial del fabricante
PeopleSoft	3 Meses	Descarga de nuevas versiones desde la página oficial del fabricante
Business intelligence	6 Meses	Descarga de nuevas versiones desde la página oficial del fabricante
SharePoint	12 Meses	Descarga de nuevas

		versiones desde la página oficial del fabricante
Copia de respaldo de configuración de los servidores y bases de datos	Diaria	Procedimiento de respaldo automatizado basado en servidor
Arquitectura de conexiones IT	3 Meses	Bajo demanda, mediante conexión a un servidor TFTP
Manuales digitales de los servidores, aplicativos y bases de datos	3 Meses	Bajo demanda, mediante conexión a un servidor TFTP
Paquete instalador de los gestores de bases de datos utilizados en la institución	3 Meses	Descarga de nuevas versiones desde la página oficial del fabricante
Instaladores de los sistemas operativos manejados en la institución y de las herramientas administrativas, financieras y tecnológicas de gestión de aplicaciones	3 Meses	Descarga de nuevas versiones desde la página oficial del fabricante
Arquitectura de conexiones IT	3 Meses	Bajo demanda, cuando existan cambios en la red de cableado
Manuales impresos para	3 Meses	Descarga de nuevas

la configuración de servidores, aplicaciones y bases de datos		versiones desde la página oficial del fabricante
Contactos internos y externos para la gestión de TI	1 Mes	Bajo demanda, mediante conexión a un servidor TFTP

Adaptado de: (Kosutic, 2015).

Nota: la frecuencia para la creación de copias de seguridad de datos compartidos por otras actividades está definida en la parte general de la Estrategia.

ANEXO 6

Plan de Continuidad del Negocio

Banco KLM

Banco KLM Compañía Anónima

Anexo 6: Plan de Continuidad del Negocio

Código:	PLA-TI-2015-08
Versión:	1.0
Fecha de la versión:	3 de Agosto del 2015
Creado por:	Ing. Vinicio Sarabia
Aprobado por:	Ing. Santiago Pazmiño
Nivel de confidencialidad:	Alto

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
03/08/2015	1.0	Vinicio Sarabia	Creación de la primera versión del documento

Tabla de contenido

Objetivo, alcance y usuarios

El objetivo del Plan de Continuidad del Negocio es definir de forma precisa cómo el Banco KLM gestionará los incidentes en caso de un desastre o de otro incidente disruptivo y cómo recuperará sus actividades dentro de plazos establecidos. El objetivo de este plan es mantener en un nivel aceptable el daño producido por un incidente disruptivo.

Este plan se aplica a todas las actividades críticas dentro del alcance del Sistema de Gestión de Continuidad del Negocio (SGCN).

Los usuarios de este documento son todos los miembros del personal, tanto internos como externos, que cumplan una función en la Continuidad del Negocio.

Documentos de referencia

- Norma ISO 22301, punto 8,4
- Norma ISO/IEC 27001, punto A.14.1.3
- Lista de requisitos legales, normativos, contractuales y de otra índole

- Política de la Continuidad del Negocio
- Cuestionarios sobre el análisis del impacto en el negocio
- Estrategia de Continuidad del Negocio

Plan de Continuidad del Negocio

Contenido del plan

Este Plan de Continuidad del Negocio está formado por dos grandes secciones:

- Plan de respuesta a los incidentes (Apéndice 1 - Anexo 6.1): un plan que define la respuesta directa ante la ocurrencia de diversos tipos de incidentes.
- Planes de recuperación para actividades individuales (Apéndices 6a, 6b, 6c - Ver Anexo 6.6): planes acerca de la recuperación de los recursos necesarios para cada actividad (se preparan por separado para cada actividad).

Cada uno de estos planes define su procedimiento de activación.

Supuestos

Para que este plan resulte efectivo, todos los recursos y preparativos especificados en la Estrategia de Continuidad del Negocio deben estar preparados.

Nombramientos y autoridades

Se conformarán las siguientes entidades cuando se produzca un incidente disruptivo:

Tabla 62. Entidades y funciones del Gabinetes de crisis para un incidente disruptivo.

Gabinete de crisis		
Miembros:	**Reemplazantes:**	**Función:**
Presidente del Directorio o su Delegado	Delegado del Presidente del Directorio	Promotor del Proyecto del SGCN, Miembro del gabinete de crisis
Gerente Nacional de Tecnología	Gerente de Producción y Servicios	Gerente de SGCN, Gerente de recuperación, Gerente de crisis, Gerente del proyecto del SGCN, Miembro del gabinete de crisis
Gerente de Producción y Servicios	Subgerente de Servicios Tecnológicos	Gerente de crisis suplente, Miembro del gabinete de crisis, Coordinador de recuperación
Jefe de Comunicación Social	Periodista	Miembro del gabinete de crisis
Jefe de Seguridad y Salud Ocupacional	Supervisor de Salud Ocupacional	Miembro del gabinete de crisis
Gerente Financiero	Jefe Administrativo	Miembro del gabinete de crisis
Jefe de Comunicaciones	Administrador de Comunicaciones	Miembro del gabinete de crisis
Jefe de Servidores	Administrador de Base de Datos	Miembro del gabinete de crisis
Jefe de Centro de Computo	Supervisor de Centro de Computo	Miembro del gabinete de crisis
Subgerente de Control	Analista Auditor de Informática	Miembro del gabinete de crisis

Tecnológico		
Gabinete de apoyo de crisis		
Miembros:	**Reemplazantes:**	**Función:**
Gerente Nacional de Negocios	Asistente de Negocios	Miembro del gabinete de apoyo de crisis
Jefe de Monitoreo	Analista de Monitoreo	Miembro del gabinete de apoyo de crisis
Jefe de Soporte Técnico	Técnico de Soporte	Miembro del gabinete de apoyo de crisis
Jefe de Mesa de Servicios	Analista de Mesa de Servicios	Miembro del gabinete de apoyo de crisis
Mensajero – Dirección Técnica	Auxiliar de Servicios – Dirección Técnica	Miembro del gabinete de apoyo de crisis
Mensajero – Dirección Comercial	Asistente de Servicios – Dirección Comercial	Miembro del gabinete de apoyo de crisis
Técnico en Operación y Mantenimiento	Asistente de Servicios – Administrativo	Miembro del gabinete de apoyo de crisis

Adaptado de: (Kosutic, 2015).

El objetivo del Gabinete de crisis es tomar todas las decisiones clave y coordinar las acciones durante el incidente disruptivo; el objetivo del Gabinete de apoyo de crisis es aliviar al Gabinete de crisis en tareas administrativas y otras actividades operativas para que pueda concentrarse en solucionar el incidente disruptivo. Los miembros del Gabinete de apoyo de crisis dependen directamente del Gabinete de crisis.

Los Gerentes de recuperación para las actividades individuales son nombrados en los planes de recuperación para dichas actividades.

Las autorizaciones para actuar durante un incidente disruptivo son las siguientes:

Tabla 63. Autoridades autorizadas para toma de decisiones durante un incidente disruptivo.

Tipo de decisión	Quién está autorizado
Cómo se solucionan incidentes menores relacionados con tecnología de información y comunicación.	Empleados del área de Infraestructura Tecnológica
Cómo se solucionan otros incidentes menores.	Empleados del área de Infraestructura Tecnológica
Toma de decisión sobre la invocación de los planes de recuperación.	Gerente de crisis
Tomar una decisión sobre la elección de la ubicación alternativa (utilización de la ubicación cercana o la remota).	Gerente de crisis
Informar a los empleados sobre la activación de los planes de recuperación.	Gerente de crisis, si no puede hacerlo, es reemplazado por el Gerente de recuperación de cada actividad individual.
Implementación de todas las tareas necesarias para la recuperación de actividades individuales.	Gerente de recuperación para actividades individuales.
Contenido de la comunicación para las diferentes partes interesadas.	Gerente de crisis
Selección de información para suministrar a los medios públicos durante un incidente disruptivo.	Jefe de Comunicación Social
Adquisiciones durante el incidente disruptivo: mayores a USD 5000,00.	Gerente Financiero
Adquisiciones durante el incidente disruptivo: hasta USD 5000,00	Jefe Administrativo

Adaptado de: (Kosutic, 2015).

Activación y desactivación del plan

El Plan de respuesta a los incidentes se activa automáticamente en caso que se produzca un incidente o que un potencial incidente amenace sus actividades. El Plan de respuesta a los incidentes es desactivado una vez que el incidente ha sido controlado o erradicado.

Los planes de recuperación para actividades particulares son activados exclusivamente por decisión del Gerente de crisis, cuando éste evalúa si una actividad determinada permanecerá interrumpida por un período mayor que el objetivo de tiempo de recuperación para esa actividad. La decisión del Gerente de crisis puede ser escrita u oral.

Los planes de recuperación pueden ser desactivados por los gerentes de recuperación de las actividades individuales una vez que determinan que se han cumplido todas las condiciones necesarias para retomar las actividades del negocio. Los planes de recuperación son desactivados al retomar las actividades habituales del negocio.

Comunicación

Se utilizarán las siguientes vías de comunicación entre el Gabinete de crisis y las actividades y entre las diversas actividades. Están ordenadas por prioridad (la primera de la lista se utilizará primero; en caso que no esté disponible, se utilizará la siguiente):

1. Teléfonos móviles (corporativos o privados)
2. Teléfonos fijos (corporativos o privados)
3. Correo electrónico (enviado desde ordenadores y equipos móviles corporativos o privados)
4. Internet (corporativo o privados)

El Jefe de Comunicación Social del Gabinete de crisis es el responsable de coordinar la comunicación con todas las actividades.

Las responsabilidades de comunicación con la cada parte interesada están especificadas en el Plan de respuesta a los incidentes.

Ubicaciones y transporte

El Jefe de Seguridad y Salud Ocupacional es el responsable de garantizar el acceso a cada ubicación alternativa a utilizar. El Apéndice 3 especifica todas las ubicaciones alternativas a utilizar, ver Anexo 6.3.

Las responsabilidades relacionadas con el transporte a las ubicaciones alternativas están detalladas en el Apéndice 4: Plan de transporte, ver Anexo 6.4.

Orden de recuperación para las actividades

Las actividades se deben recuperar en el siguiente orden:

Tabla 64. Orden y tiempo de recuperación de cada una de las actividades.

N°	Nombre de la actividad	Objetivo de tiempo de recuperación
1	Ejecutar acciones preventivas y correctivas para garantizar la disponibilidad del servicio de Comunicaciones	1 hora
2	Ejecutar acciones preventivas y correctivas para garantizar la disponibilidad de los servicios de Aplicativos de Core Bancario y Negocios	1.5 horas

3	Ejecutar acciones preventivas y correctivas para garantizar la disponibilidad de los servicios de Aplicativos Administrativos, Financieros y Tecnológicos	4 horas

Interdependencias e interacciones

La dependencia e interacción entre actividades, como también con los proveedores y entidades externas, están detalladas en el Plan de respuesta a los incidentes ver Anexo 6.1 y en los planes individuales de recuperación para las actividades, ver Anexo 6.6.

Recursos necesarios

Recursos necesarios para la recuperación de las actividades detalladas en sus planes de recuperación.

El Centro de crisis, que presta servicio al Gabinete de crisis y al Gabinete de apoyo de crisis, está equipado de la siguiente manera:

Tabla 65. Recursos y equipos necesarios para el funcionamiento del centro de crisis.

Nombre del recurso	Descripción	Cantidad	Cuándo es necesario el recurso	Persona responsable de conseguir el recurso
Aplicaciones / bases de datos:				
People Soft / Oracle 11g	Sistema Comercial, gestor de base de datos	1	Dentro de las 2 horas	Administrador de base de datos

Big Data / Teradata	Sistema Financiero, gestor de base de datos	1	Dentro de las 2 horas	Administrador de base de datos
SharePoint / Server 2005	Sistema Administrativo, gestor de base de datos	1	Dentro de las 2 horas	Administrador de base de datos
Business intelligence / Oracle 11g	Sistema Comercial, gestor de base de datos	1	Dentro de las 2 horas	Administrador de base de datos
Datos en formato electrónico:				
Estrategia de Continuidad del Negocio y planes para todas las actividades	Documentos propios del SGCN	16	Dentro de las 2 horas	Gerente de Producción y Servicios
Directorio telefónico de la ciudad de Quito	Directorio telefónico actualizado	16	Dentro de las 2 horas	Jefe de Comunicaciones
Directorio telefónico específico de las dependencias públicas de seguridad de la	Directorio telefónico actualizado con contactos públicos	16	Dentro de las 2 horas	Jefe de Comunicaciones

ciudad de Quito				
Datos en papel:				
Estrategia de Continuidad del Negocio y planes para todas las actividades	Documentos propios del SGCN	16	inmediatamente	Gerente de Producción y Servicios
Directorio telefónico de la ciudad de Quito	Directorio telefónico actualizado	16	Dentro de las 2 horas	Jefe de Comunicaciones
Directorio telefónico específico de las dependencias públicas de seguridad de la ciudad de Quito	Directorio telefónico actualizado con contactos públicos	16	inmediatamente	Jefe de Comunicaciones
Equipos de TI y comunicaciones:				
Estaciones de trabajo	Cubículos de trabajo con similares características	8	Dentro de las 2 horas	Jefe Administrativo
Teléfonos	Teléfonos IP y digitales	8	inmediatamente	Jefe Administrativo
Teléfonos móviles	Teléfonos celulares inteligentes	16	inmediatamente	Jefe Administrativo

Impresora	Impresoras multifunción	2	Dentro de las 2 horas	Jefe Administrativo
Equipo de fax	Teléfonos de fax dedicados	1	inmediata mente	Jefe Administrativo
Canales de comunicación:				
Líneas fijas de teléfono	Líneas telefónicas del proveedor local	16	inmediata mente	Jefe Administrativo
Acceso a Internet	Proveedor principal y secundario de internet	1	Dentro de las 2 horas	Jefe Administrativo
Otros equipos:				
Televisor	Televisor LCD de 50”	2	inmediata mente	Jefe Administrativo
Radio	Radio para sincronización de frecuencias AM y FM	2	inmediata mente	Jefe Administrativo
Instalaciones e infraestructura:				
Red de computadoras	Para interconexión de PCs	3	Dentro de las 2 horas	Jefe de Comunicaciones
Muebles	Muebles de oficina	5	inmediata mente	Jefe Administrativo

Servicios externos:				
Electricidad	Proveedor local de electricidad	2	Inmediata mente	Jefe Administrativo
Agua potable	Proveedor local de agua potable	1	Inmediata mente	Jefe Administrativo

Adaptado de: (Kosutic, 2015).

Restauración y reactivación de actividades comerciales a partir de las medidas temporales

El objetivo de la restauración y reactivación de las actividades comerciales a partir de las medidas temporales es lograr nuevamente el desarrollo de estas actividades en su forma habitual; es decir, recuperar su estado natural, tal como se realizaban antes del incidente disruptivo.

En los pasos que se describen en esta sección el tiempo no es un factor crítico; se realizarán en proporción al impacto del incidente disruptivo y de acuerdo con los recursos disponibles. La decisión de activar cada uno de los siguientes pasos la toma el Gerente de crisis.

Es necesario realizar los siguientes pasos en este orden:

1. Preservación de los activos dañados y evaluación del daño.
2. Evaluación de la situación y determinación de opciones y responsabilidades.
3. Desarrollo de un plan de acción: determinar los pasos necesarios para retornar las actividades a su estado normal.

Preservación de los activos dañados y evaluación del daño

El Gerente de Producción y Servicios nombrará al equipo para preservar los activos dañados; este equipo se concentrará en evitar que se extienda el daño.

El Gerente de Producción y Servicios nombrará al equipo para la evaluación del daño. La evaluación debe incluir lo siguiente: nombre del activo, ubicación del activo, tipo y costo del daño.

Evaluación de la situación y determinación de opciones y responsabilidades

Según la magnitud del daño, el Gerente de crisis necesita decidir lo siguiente: (1) si retornar a la ubicación primaria o buscar una nueva ubicación, (2) si comprar nuevo equipamiento o reparar el existente, (3) cuándo y dónde se recuperarán o retomarán el funcionamiento de actividades que no soportan productos y servicios clave (actividades con menor prioridad) y (4) si hay suficientes recursos humanos para soportar las operaciones normales, etc.

En función a estas decisiones, el Gerente de crisis debe nombrar personas responsables para lo siguiente:

a) Gestionar reclamaciones contra pólizas de seguro
b) Restauración de instalaciones
c) Adquisición de nuevas instalaciones
d) Logística para mudanza a otras ubicaciones
e) Reparación de equipamiento
f) Compra de nuevo equipamiento
g) Contratación de nuevo personal
h) Recuperación de actividades con menor prioridad

Desarrollo de planes de acción

Cada persona responsable debe desarrollar un plan de acción para su área de responsabilidad que, entre otro tipo de información, incluirá lo siguiente: (1)

pasos a tomar, (2) recursos humanos necesarios, (3) recursos financieros necesarios y (4) plazos.

El Gerente de crisis debe definir (1) cómo proporcionar los fondos necesarios, (2) obtención de procesos y autorizaciones, (3) qué informes se enviarán al Gabinete de crisis y (4) quién realizará la revisión de los pasos una vez que se hayan completado.

Validez y gestión de documentos

Este documento es válido desde el 03 de Agosto del 2015.

Este documento se archiva de la siguiente forma:

- El documento en papel se archiva en las siguientes ubicaciones: Centro de crisis, el cual su ubicación alternativa cerca es: Quito, Centro Comercial Iñaquito, local # P-55, Sector la Carolina

- El documento en formato electrónico se archiva de la siguiente forma: con el nombre de “PLAN_DE_CONTINUIDAD_DEL_NEGOCIO” en la carpeta de la intranet.

\\SRVTECH\SGCN\PLAN_DE_CONTINUIDAD_DEL_NEGOCIO.

El propietario de este documento es el Gerente Nacional del Centro de Servicios, que debe verificar, y si es necesario actualizar, el documento por lo menos una vez al año.

Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- ¿Se recuperaron las actividades dentro del plazo requerido?
- ¿Están sincronizados los planes de recuperación con el Plan de respuesta a los incidentes?
- ¿La ejercitación y prueba cumplieron los objetivos?

Apéndices

- Apéndice 1: Plan de respuesta a los incidentes (Ver Anexo 6.1)
- Apéndice 2: Registro de incidentes (Ver Anexo 6.2)
- Apéndice 3: Lista de ubicaciones para Continuidad del Negocio (Ver Anexo 6.3)
- Apéndice 4: Plan de transporte (Ver Anexo 6.4)
- Apéndice 5: Contactos clave (Ver Anexo 6.5).
- Apéndice 6a: Plan de recuperación de la actividad ejecutar acciones preventivas y correctivas para garantizar la disponibilidad del servicio de Comunicaciones (Ver Anexo 6.6).
- Apéndice 6b: Plan de recuperación de la actividad ejecutar acciones preventivas y correctivas para garantizar la disponibilidad los servicios de Aplicativos de Core Bancario y Negocios (Ver Anexo 6.6).
- Apéndice 6c: Plan de recuperación de la actividad ejecutar acciones preventivas y correctivas para garantizar la disponibilidad de los servicios de Aplicativos Administrativos, Financieros y Tecnológicos (Ver Anexo 6.6).

Gerente Nacional del Centro de Servicios

Msc. Fernanda Ayala

_____

Firma

ANEXO 6.1

Plan de respuesta a los incidentes

Anexo 6: Plan de Continuidad del Negocio

Apéndice 1: Plan de respuesta a los incidentes

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
03/08/2015	1.0	Vinicio Sarabia	Creación de la primera versión del documento

TABLA DE CONTENIDO

Objetivo, alcance y usuarios

El objetivo de este Plan es asegurar la protección de la salud y de la seguridad de las personas ante el caso de un desastre o de otro incidente, como también contener el incidente. El objetivo es reducir al mínimo posible el daño sobre el negocio.

Este plan se aplica a todos los incidentes graves que amenazan con interrumpir cualquier actividad crítica dentro del alcance del SGCN por un período mayor al objetivo de tiempo de recuperación de cada actividad individual (en adelante, incidentes disruptivos).

Los usuarios de este documento son todos los empleados del Banco KLM.

Autorizaciones y responsabilidades en la respuesta a los incidentes

Tabla 66. Autorizaciones y responsabilidades de los colaboradores del Banco KLM en caso de incidentes disruptivos.

Función en la recuperación / cargo	Autorizaciones y responsabilidades
Cualquier empleado	Notificación del incidente a la unidad organizativa responsable
Empleados del Área de Infraestructura Tecnológica	Todos los pasos necesarios para resolver incidentes relacionados con tecnología de la información y de la comunicación
Jefe de Seguridad y Salud Ocupacional	Todos los pasos necesarios para resolver otros incidentes, (que no sean de tecnología de la información y comunicaciones)

Gerente de Crisis	Activación de planes de recuperación para las actividades
Jefe de Comunicación Social	Comunicación con los medios públicos: esta persona tiene una autorización exclusiva para comunicarse con los medios públicos
Jefe de Recursos Humanos	Ayuda psicológica para los empleados

Adaptado de: (Kosutic, 2015).

Comunicación

El siguiente cuadro detalla las responsabilidades para la comunicación (tanto envío como recepción de información y respuesta a solicitudes de información) con diversos tipos de partes involucradas:

Tabla 67. Medios de comunicación y partes interesadas.

	Teléfono	**Reuniones**	**Correo electrónico**	**Conferencias de prensa**	**Medios**
Empleados		Coordinador de la Continuidad del Negocio	Gerente de Producción y Servicios		
Propietarios / accionistas	Gerente de Tecnología				
Familiares de empleados		Gerente de Recursos Humanos			
Clientes			Gerente de		

			Negocios		
Medios públicos				Periodista	
Asociaciones					Periodista
Servicios de emergencia	Jefe de Seguridad y Salud Ocupacional				
Diversas autoridades públicas				Gerente de Tecnología	

Adaptado de: (Kosutic, 2015).

El procedimiento de comunicación es el siguiente:

1. Cualquier empleado que reciba una solicitud de comunicación o que desee iniciar la comunicación con las partes involucradas debe enviar esa solicitud a la persona responsable indicada en el cuadro anterior.

2. Una persona responsable debe estar de acuerdo con el Gerente de Tecnología sobre el contenido de la comunicación.

3. Si la comunicación con las entidades externas incluye riesgos e impactos considerables, la decisión sobre esa comunicación debe ser documentada y formalmente autorizada por el Gerente de Tecnología antes de ser transmitida.

4. Luego de obtener la autorización correspondiente, la persona responsable le proporciona la información a la parte interesada.

La persona responsable indicada en el cuadro anterior tiene la responsabilidad de documentar cada pieza de comunicación con una parte involucrada.

Procedimientos para incidentes disruptivos

Gestión de un incidente disruptivo

Todos los empleados tienen la obligación de reportar incidentes

Todos los empleados están obligados a informar cualquier incidente disruptivo de la siguiente manera:

- Todos los incidentes relacionados con tecnología de la información y de la comunicación son informados telefónicamente al Jefe de Mesa de Servicios o Área de Infraestructura Tecnológica.

- Todos los demás incidentes son informados telefónicamente al Jefe de Seguridad y Salud Ocupacional.

Cualquier otro evento o vulnerabilidad del sistema que todavía no se hubiera convertido en un incidente disruptivo debe ser informado de la misma forma.

Si un incidente demanda la intervención de la policía, de ambulancias o de los bomberos, la primera persona disponible debe llamar al 911 y, desde allí, informar a la persona responsable de su unidad organizativa o al Gerente de crisis.

En caso que ocurra un incidente, los empleados pueden comunicarse libremente sólo con sus familiares y con la policía, o los bomberos; mientras que cualquier otro tipo de comunicación se delega en el Gabinete de crisis.

Gestión de incidentes disruptivos

La persona que recibe la información sobre el incidente debe evaluar si el incidente, o potencial incidente, es real o falso, y si es real, activa inmediatamente este plan respetando los siguientes pasos:

- Comenzar a controlar y erradicar el incidente de acuerdo a lo detallado en las siguientes secciones del presente documento.
- Informar a todas las personas responsables sobre la ocurrencia del incidente dentro de su área de responsabilidad.
- Notificar a Jefe de Seguridad y Salud Ocupacional, que debe evaluar si es necesario alertar a alguna de las partes interesadas.
- Controla el estado del incidente y, si es necesario, informa a quien lo reportó y a los demás empleados involucrados, acerca del progreso en la gestión del incidente.

En caso que una persona no pueda controlar y/o erradicar el incidente, debe informarlo al Gerente de crisis. La información que se envía al Gerente de crisis debe incluir la naturaleza y alcance del incidente disruptivo, como también su potencial impacto.

La persona responsable de erradicar el incidente debe registrar en el Registro de incidentes todas las acciones tomadas.

Gerente de crisis

El Gerente de crisis debe supervisar el progreso en la gestión del incidente y el período de interrupción de las actividades individuales y debe evaluar el tiempo necesario para solucionar el incidente.

Si el tiempo necesario para solucionar el incidente es mayor que el objetivo de tiempo de recuperación de una actividad particular, se debe activar el plan de recuperación para la actividad interrumpida ver Anexo 6.6. En ese caso, el Gerente de crisis debe notificárselo a todos los gerentes de recuperación, quienes activarán sus planes de recuperación.

Control y erradicación de un incidente

Evacuación del edificio (independientemente del tipo de incidente)

Se evacua el edificio y se dirige al personal hacia los puntos de encuentro especificados en la Lista de ubicaciones para Continuidad del Negocio, incluida como apéndice al Plan de Continuidad del Negocio.

Tabla 68. Acciones a seguir para la evacuación del edificio Matriz en caso de incidentes.

Gerente de crisis	• En caso que esté en riesgo la vida o la salud de las personas, emite una orden de evacuación. • Si el Punto de encuentro 1 no está disponible, envía a alguien a señalizar la ubicación del Punto de encuentro 2 (señales de papel, flechas de dirección, banderas, señalización de vehículos, etc.). • En caso de una amenaza maliciosa (por ej., amenaza de bomba), decide la nueva ubicación del punto de encuentro (Punto de encuentro 3) y lo notifica a la persona responsable de ejecutar la evacuación.
Personas responsables de ejecutar la evacuación	• Dirige la evacuación hacia el punto de encuentro. • Verifica que todas las habitaciones estén vacías luego de la evacuación, sale de las habitaciones y cierra las puertas con llave. • En caso que alguien no haya podido salir del edificio, lo informa al 911.
Todos los empleados	• Evacuan según los planes de evacuación para su edificio. • Siguen las instrucciones suministradas por las personas responsables de dirigir la evacuación. • No utilizan teléfonos móviles durante la evacuación. • Al evacuar, solamente llevan su bolso de mano y billetera, no llevan ningún otro elemento.

	• Ayudan a evacuar a otras personas, si necesitan ayuda.
Gabinete de apoyo de crisis	• Cuando la gente se ha reunido en el punto de encuentro, lleva un registro de todas las personas presentes y las que faltan.

Incendio

Se evacua el edificio de acuerdo con el plan de evacuación del edificio del Banco KLM.

Tabla 69. Acciones a seguir para la evacuación del edificio en caso de incendios.

Responsable	Acción
Gerente de crisis	• En caso que esté en riesgo la vida o la salud de las personas, el Gerente de crisis emite una orden de evacuación. • Escoge las medidas para disminuir el daño o salvar bienes, a menos que esto represente un riesgo para las personas.

Interrupción del suministro eléctrico

Tabla 70. Acciones a seguir en el caso de interrupción del suministro eléctrico.

Responsable	Acción
Gabinete de apoyo de crisis	• Establece la causa de la interrupción; es originada por el cableado o por el distribuidor de electricidad.
Jefe de	• Soluciona el problema junto con el distribuidor de

Seguridad y Salud Ocupacional	electricidad.
Todos los empleados	• Cumpliendo con los planes de recuperación, proceden con las formas alternativas para ejecutar actividades, sin el uso de electricidad.
Empleados del Área de Infraestructura Tecnológica	• Supervisan los dispositivos UPS y desconectan el sistema informático si es necesario.

Terremoto

Se evacua el edificio de acuerdo con el plan de evacuación del edificio del Banco KLM.

Tabla 71. Acciones a seguir para la evacuación del edificio en caso de terremoto.

Responsable	Acción
Todos los empleados	• Buscan refugio bajo el marco de una puerta, cerca de una pared interior de apoyo, o debajo de un escritorio. • No utilizan los ascensores. • No corren hacia el exterior del edificio hasta que termine el terremoto. • Una vez que el terremoto ha finalizado, intentan salvar a otras personas salvo que se haga más daño a la persona herida. • En caso que se ordene la evacuación, proceden de acuerdo al plan de evacuación.
Gerente de crisis	• En caso que esté en riesgo la vida o la salud de las personas, ordena la evacuación del edificio una vez que haya terminado el terremoto.

Gabinete de apoyo de crisis	• Apaga todos los servicios: gas, electricidad, calefacción, ventilación, suministro de agua. • Asegura el edificio y demás bienes.

Carta de amenaza

Tabla 72. Acciones a seguir en caso de recibir una carta de amenaza.

Responsable	Acción
Todos los empleados	• Si reciben una carta sospechosa, no la abren, la sostienen sólo por sus bordes externos. • La colocan en un sobre vacío. • Informa al Jefe de Seguridad y Salud Ocupacional. • Proceden según las instrucciones del Jefe de Seguridad y Salud Ocupacional.
Jefe de Seguridad y Salud Ocupacional	• Notifica a la policía a través del [número de teléfono]. • Notifica al superior del empleado que informó sobre la carta. • Ejecuta las medidas impartidas por la policía.

Llamado de amenaza / amenaza de bomba

Tabla 73. Acciones a seguir en caso de recibir un llamado de amenaza de bomba.

Responsable	Acción
Todos los empleados	• Si reciben una llamada de amenaza, anotan la hora exacta y el número de teléfono que llamó. • Anota las palabras exactas de la persona que llamó. • Dejan que quien llama hable lo más posible, sin interrupciones: - intentan hacerlo o hacerla hablar;

	- repiten sus preguntas, dicen que no comprenden lo que dijo; - si sus teléfono tienen altavoz, ponen la llamada en altavoz y piden a otra persona que tome notas; - repiten cada solicitud realizada por la persona que llama. • En caso de una amenaza de bomba, le hacen las siguientes preguntas a la persona que llama: - ¿Estallará la bomba? ¿Cuándo? - ¿Es posible desactivarla? ¿Cómo? - ¿Dónde está ubicada? - ¿Cómo es? - ¿Por qué fue colocada? ¿Cuáles son las demandas? - ¿Quién habla? ¿Puede decir quién es? • Abren las puertas de la oficina sólo si están seguros de que no está conectada a la bomba. • ¡No buscan la bomba en el edificio! Este es trabajo de la policía. • No tocan ningún objeto desconocido. • Si se ordena la evacuación, proceden de acuerdo al plan de evacuación.
Gerente de crisis	• Notifica a la persona responsable de la unidad organizativa hacia la cual se dirige la amenaza. • No utiliza los puntos de encuentro habituales; escoge uno nuevo. • Si evalúa que la bomba realmente puede detonarse, ordena la evacuación; el punto de encuentro debe estar alejado 300 metros como mínimo. • Informa a las personas responsables de la

	evacuación y al Gabinete de apoyo de crisis la ubicación del nuevo punto de encuentro. • En caso de una explosión, toma una decisión para alejar de la zona afectada, lo antes posible, a los heridos.

Falla en las telecomunicaciones

Tabla 74. Acciones a seguir en caso de fallas en las telecomunicaciones.

Responsable	Acción
Empleado del Área de Infraestructura Tecnológica	• Cualquier empleado recibe información sobre la falla. • Si es necesario, coordina el proceso con proveedores de servicios de TI.
Empleados - usuarios de servicios de comunicación	• Utilizan vías de comunicación alternativas.

Falla en el sistema de información

Tabla 75. Acciones a seguir en caso de fallas en el sistema de información.

Responsable	Acción
Empleado del Área de Infraestructura Tecnológica	• Cualquier empleado recibe información sobre el incidente. • Si es necesario, coordina el proceso con proveedores de servicios de TI. • Toma las medidas necesarias para evitar o controlar

	el incidente del sistema de información.
Gerente de crisis	• Se asesora sobre todos los servicios importantes, evalúa la gravedad del incidente.
Todos los empleados	• Si es posible, realizan procedimientos alternativos para llevar adelante las actividades.

Ataque de código malicioso

Tabla 76. Acciones a seguir en caso de ataque de código malicioso

Responsable	Acción
Empleado del Área de Infraestructura Tecnológica	• Cualquier empleado recibe información sobre el incidente. • Si se trata de un código malicioso desconocido, notifica al Subgerente de Control Tecnológico. • Notifica al fabricante del software antivirus. • Si se ha identificado el origen externo del código malicioso, contacta a la persona responsable de TI de esa organización. • Coordina la notificación a otros empleados; particularmente aquellos que intercambiaron mensajes con el sistema infectado. • Si es necesario, coordina el proceso con proveedores de servicios de TI.
Todos los empleados	• Desconectan físicamente de la red cualquier ordenador infectado, desactivan las redes inalámbricas, de Bluetooth, etc. • No apagan los dispositivos de red y servidores; este es un trabajo de los empleados del Área de Infraestructura Tecnológica.

Empleados del Área de Infraestructura Tecnológica	• Si el ordenador todavía no ha sido desconectado de la red, evalúa si lo desconecta para evitar mayor infección. • Desactiva todas las conexiones inalámbricas del ordenador. • Cierra su software (incluido el sistema operativo); para los servidores, evalúa si es necesario notificar primero a los usuarios del sistema. • Consigue información sobre el tipo de código malicioso y sobre los pasos necesarios para su erradicación (desde Internet, de los proveedores). • Procede de acuerdo a las instrucciones recibidas.

Violación de reglas internas o externas

Tabla 77. Acciones a seguir en caso de violación de reglas internas o externas.

Responsable	Acción
Gerente Nacional de Recursos Humanos	• El procedimiento se realiza de acuerdo a lo establecido en los procedimientos disciplinarios regulados por las leyes laborales y por la propia organización.

Gestión de registros guardados en base a este documento

Tabla 78. Registros guardados de las principales características del documento.

Nombre del registro	Ubicación de archivo	Persona responsable del archivo	Controles para la protección del registro	Tiempo de retención

Registro de incidentes	Carpeta compartida en Intranet: \\SRVTECH\SGCN\PLAN_DE_RESPUESTA_A_INCIDENTES	Jefe de Seguridad y Salud Ocupacional: Gerente de Producción y Servicios	Solamente el Gerente de Producción y Servicios puede editar la lista	3 años

Adaptado de: (Kosutic, 2015).

Solamente el Gerente de Producción y Servicios puede permitir el acceso a los registros a otros empleados.

Validez y gestión de documentos

Este documento es válido desde el 03 de Agosto del 2015. Este documento, junto con todos los materiales adicionales, es archivado de la siguiente forma:

- El documento en papel se archiva en las siguientes ubicaciones: Centro de crisis y todas las ubicaciones alternativas para actividades
- El documento en formato electrónico se archiva en la siguiente ruta: \\SRVTECH\SGCN\PLAN_DE_RESPUESTA_A_INCIDENTES

El propietario de este documento es el Gerente de Producción y Servicios, que debe verificar, y si es necesario actualizar, el documento por lo menos una vez al año.

Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- Cantidad de incidentes no contemplados en el presente documento.

- Si los pasos detallados en el presente documento son factibles en situaciones reales.
- Tiempo de respuesta a los incidentes.

Gerente de Producción y Servicios

Ing. Luis Antonio Arevalo

_____

Firma

ANEXO 6.2

Registro de incidentes

Anexo 6.2: Plan de Continuidad del Negocio

Apéndice 2: Registro de incidentes

Los incidentes se clasifican dentro de los siguientes tipos:

- Relacionados con la información (directamente relacionados con tecnología de la información y comunicación)
    - Ataque malicioso
    - Acceso sin autorización a los sistemas o sus datos
    - Denegación de servicios
    - Uso desautorizado al Core Bancario
    - Uso desautorizado de las bases de datos
    - Cambio no autorizado en el hardware, firmware o software de los sistemas
    - Errores o fallas de los sistemas
    - Infección de virus, malware o cualquier tipo de código malicioso que se esté ejecutando o con riesgos de ejecutarse
    - Falla en las telecomunicaciones
    - Errores o fallas de las aplicaciones o sistemas informáticos institucionales
- No relacionados con la información (todos los demás incidentes)
    - Desastres naturales y fuerza mayor
    - Error humano involuntario
    - Atentado terrorista

- Inundaciones
- Incendios
- Interrupción del suministro eléctrico
- Terremotos
- Carta de amenaza

Información sobre los incidentes:

Tabla 79. Formato para el registro de incidentes.

N°	Fecha del incidente	Tipo	Breve descripción (nombre) del incidente	Persona responsable del manejo del incidente	Descripción detallada: impactos, duración, sistemas y/o datos afectados por el incidente, acciones realizadas, etc.	Costos $: directos e indirectos	Referencia al Formulario para acciones correctivas y preventivas
1.							
2.							
3.							
4.							
5.							

Tomado de: (Kosutic, 2015).

ANEXO 6.3

Lista de ubicaciones para Continuidad del Negocio

Anexo 6.3: Plan de Continuidad del Negocio

Apéndice 3: Lista de ubicaciones para Continuidad del Negocio

Se proporcionan las siguientes ubicaciones para asegurar la Continuidad del Negocio:

Tabla 80. Ubicaciones que aseguran la Continuidad del Negocio del Banco KLM.

Nombre de la actividad	Domicilio de la ubicación principal	Punto de encuentro 1	Punto de encuentro 2	Ubicación alternativa (cerca)	Ubicación alternativa (remota)
Centro de crisis	Quito, Av. Amazonas y Villalengua	Parque la Carolina (Calles Japón y Av. Amazonas, esquina)	Centro Comercial CCI (Puerta de Acceso 1)	Centro Comercial CCI Agencia del Banco	Guayaquil, Urdesa Agencia del Banco
Disponibilidad del servicio de Comunicaciones	Quito, Av. Amazonas y Villalengua	Parque la Carolina (Calles Japón y Av. Amazonas, esquina)	Centro Comercial CCI (Puerta de Acceso 1)	Centro Comercial CCI Agencia del Banco	Guayaquil, Urdesa Agencia del Banco
Disponibilidad de los servicios de Aplicativos de Core	Quito, Av. Amazonas y Villalengua	Parque la Carolina (Calles Japón y Av.	Centro Comercial CCI (Puerta de Acceso 1)	Centro Comercial CCI Agencia del Banco	Guayaquil, Urdesa Agencia del Banco

Bancario y Negocios		Amazonas, esquina)			
Disponibilidad de los servicios de Aplicativos Administrativos, Financieros y Tecnológicos	Quito, Av. Amazonas y Villalengua	Parque la Carolina (Calles Japón y Av. Amazonas, esquina)	Centro Comercial CCI (Puerta de Acceso 1)	Centro Comercial CCI Agencia del Banco	Guayaquil, Urdesa Agencia del Banco

ANEXO 6.4

Plan de transporte

Anexo 6.4: Plan de Continuidad del Negocio

Apéndice 4: Plan de transporte

En caso que se activen planes de recuperación, el transporte se organizará de la siguiente manera:

Tabla 81. Plan de transporte en caso de recuperación.

Ubicación de partida	Ubicación de destino	Quién o qué es transportado	Persona responsable de la coordinación	Medios de transporte	Transportista
Quito, Av. Amazonas y Villalengua	Centro Comercial CCI Agencia del Banco	4 Computadores portátiles de Área de Infraestructura Tecnológica	Jefe Administrativo Teléfonos: 2981500 Ext. 111 0984319133	Vehículo Empresarial	Sr. Sebastián Palomeque Teléfono: 0984319144
Quito, Av. Amazonas y Villalengua	Centro Comercial CCI Agencia del Banco	Miembros del Gabinete de apoyo de crisis que se encuentren en las oficinas Matriz del Banco KLM (Av. Amazonas y Villalengua)	Jefe Administrativo Teléfonos: 2981500 Ext. 111 0984319133	Vehículo Empresarial	Sr. Alfonso Tapia Teléfono: 0984319155

Todos los demás miembros que intervienen en el DRP que no se mencionan en la tabla anterior se trasladarán por sus propios medios hacia la ubicación de destino en un tiempo máximo de 30 minutos contados a partir de la comunicación de aviso dada a cada empleado. En la tabla N° 81 Se han detallado los casos más generales de incidentes disruptivos; para los casos no contemplados se dispone que todos los empleados que intervienen en la recuperación de las actividades se trasladen por sus propios medios hasta la ubicación de destino.

ANEXO 6.5

Contactos

Anexo 6.5: Plan de Continuidad del Negocio

Apéndice 5: Contactos

Tabla 82. Contactos claves para la Continuidad del Negocio.

N°	Función durante un incidente disruptivo	Nombre	Cargo / unidad organizativa	Teléfono móvil	Teléfono fijo	Correo electrónico	Domicilio particular	N° de reemplazo (Referencia)
1.	Gabinete de Crisis	Msc. Fernanda Ayala	Gerente Nacional del Centro de Servicios	0984308213	ND	fayala@bklm.com.ec	Cumbaya, conjunto praderas	2.
2.	Gabinete de Crisis	Ing. Santiago Pazmiño	Gerente Nacional de Tecnología	0984358942	ND	spazmino@bklm.com.ec	Ciudadela Gonzales Suarez	5.
3.	Gabinete de Crisis	Msc. Santiago Acosta	Gerente Nacional de Recursos Humanos	0984332157	ND	sacosta@bklm.com.ec	Av. América y Mañosca	7.
4.	Gabinete de Crisis	Ing. Nicolás	Gerente Financiero	0984345687	ND	nperez@bklm.com.ec	Chillogallo	1.

		Pérez						
5.	Gabinete de Crisis	Ing. Luis Arévalo	Gerente de Producción y Servicios	0984368912	ND	larevalo@bklm.com.ec	Sangolqui, conjunto puertas del sol	6.
6.	Gabinete de Crisis	Ing. Bolívar Socasi	Subgerente de Procesamiento e Infraestructura	0984335621	ND	bsocasi@bklm.com.ec	Av. Mariscal Sucre y Michelena	10.
7.	Gabinete de Crisis	Ing. Paola Jaramillo	Jefe de Comunicación Social	0984300235	ND	pjaramillo@bklm.com.ec	Las 5 esquinas	3.
8.	Gabinete de Crisis	Msc. Jorge Montenegro	Subgerente de Control Tecnológico	0984385992	ND	jmontenegro@bklm.com.ec	Barrio el Condado	5.
9.	Gabinete de Crisis	Ing. Paúl Ramírez	Jefe de Comunicaciones	0984332066	ND	pramirez@bklm.com.ec	Calle de los trigales y belladonas	10.

10.	Gabinete de Crisis	Ing. Eduardo Ortiz	Jefe de Servidores	0984399820	ND	eortiz@bklm.com.ec	Ciudadela el ejército	9.
11.	Gabinete de Crisis	Ing. Edgar Carrillo	Jefe de Centro de Computo	0984325480	ND	ecarrillo@bklm.com.ec	Av. La Coruña y Whimper	6.
12.	Gabinete de Apoyo de Crisis	Ing. Rocío Mendoza	Asistente Administrativa Gerencia Comercial	0984300268	ND	rmendoza@bklm.com.ec	Ciudadela el Recreo	13.
13.	Gabinete de Apoyo de Crisis	Srta. Tania Guevara	Asistente Administrativa Gerencia Comercial	0984312455	ND	tguevara@bklm.com.ec	San Rafael, conjuntos paraíso	12.
14.	Gabinete de Apoyo de Crisis	Sr. Andrés Gualpa	Mensajero Gerencia Comercial	0984335689	ND	aguelpa@bklm.com.ec	Carcelén bajo	15.
15.	Gabinete de Apoyo de	Sr. Julio Corredores	Mensajero Gerencia Técnica	0984377870	ND	jcorredores@bklm.com.ec	Barrio monjas	14.

	Crisis							
16.	Gabinete de Apoyo de Crisis	Sr. Jaime Esquivel	Auxiliar de Servicios	0984302581	ND	jesquivel@bklm.com.ec	Calle Chile y Cuenca	17.
17.	Gabinete de Apoyo de Crisis	Tec. Alexis Proaño	Técnico en operación y mantenimiento	0984366018	ND	aproano@bklm.com.ec	Calle Salinas y Buenos Aires	16.
18.		Ing. Diego Procel	Asistente Administrativo	0984389957		dprocel@bklm.com.ec	Calle José Larrea y Antonio Flor	19.
19.		Ing. Carlos Aguilar	Asistente Administrativo	0984311578		caguilar@bklm.com.ec	Conjuntos Chiriyacu	18.
20.		Ing. Paulina Vallejos	Asistente Financiero	0984396822		pvallejos@bklm.com.ec	Barrio San Juan	21.
21.		Srta. Lorena	Asistente Financiero	0984394426		lmoreno@bklm.com.ec	Calle Ramírez	20.

		Moreno					Dávalos y Av. América	

Nota: este formulario debe ser archivado en todas las ubicaciones en las que esté archivado el Plan de Continuidad del Negocio, pero estos datos también deben ser guardados en los teléfonos móviles de los contactos.

ANEXO 6.6 (a)

Plan de recuperación de la actividad ejecutar acciones preventivas y correctivas para garantizar la disponibilidad del servicio de Comunicaciones

Anexo 6.6: Plan de Continuidad del Negocio

Apéndice 6a: Plan de recuperación de la actividad ejecutar acciones preventivas y correctivas para garantizar la disponibilidad del servicio de Comunicaciones

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
03/08/2015	1.0	Vinicio Sarabia	Creación de la primera versión del documento

Tabla de contenido

Objetivo, alcance y usuarios

El objetivo del Plan de recuperación es definir de forma precisa cómo el Banco KLM recuperará sus actividades dentro de plazos establecidos ante el caso de

un desastre o de un incidente disruptivo. El objetivo de este Plan es terminar la recuperación de esta actividad dentro del objetivo de tiempo de recuperación establecido.

Este Plan incluye todos los recursos y procesos necesarios para la recuperación de esta actividad.

Los usuarios de este documento son los miembros del Gabinete de crisis y los empleados necesarios para la recuperación de esta actividad.

General

Tabla 83. Responsabilidades en la recuperación de actividades – Disponibilidad de servicios de Comunicaciones

Objetivo de tiempo de recuperación:	2 horas
Persona responsable de la activación del plan y de los medios de activación:	Gerente de Recuperación o Gerente de crisis (Gerente Nacional de Tecnología) / escrito
Personas a las que se debe notificar la activación del plan / quién es responsable:	Gerente Nacional del Centro de Servicios ; Gerente de Producción y Servicios; Gerente de Negocios; Gerente Financiero; Gerente Nacional de Recursos Humanos ; Subgerente de Procesamiento e Infraestructura ; Subgerente de Control Tecnológico , Jefe Administrativo; Jefe de Comunicación Social; Jefe de Comunicaciones; Jefe de Servidores; Jefe de Centro de Computo / responsable: Secretaria de Gerencia Técnica

Persona responsable de la desactivación del plan de recuperación / medios de desactivación / criterios:	Gerente de Recuperación o Gerente de crisis (Gerente Nacional de Tecnología) / escrito / Se deben cumplir todas las condiciones para retomar las actividades de Negocio de la actividad crítica.
Tareas / obligaciones clave y sus respectivos plazos:	Verificación del funcionamiento de los equipos de comunicaciones, en sitio Quito y Guayaquil: 30 min; Pruebas de conectividad entre equipos y dispositivos de red: 10 min; Verificación de alarmas y conexiones físicas : 10min; Monitoreo constante de los equipos de comunicación: 5 min; Limpieza externa de los equipos de comunicaciones: 30 min; Depuración de las configuraciones en los equipos : 30min; Verificación del ambiente en el Data Center, temperatura y humedad adecuada: 5 min; Verificación del funcionamiento de la alta disponibilidad/respaldo de energía en el Data Center: 5 min.
Cantidad mínima aceptable de trabajo inmediatamente después del desastre (MBCO, objetivo mínimo para la Continuidad del Negocio):	2 incidentes resueltos en el servicio de Comunicaciones / por mes

Período a partir del cual se debe retomar el nivel de funcionamiento normal:	48 horas
Instrucciones para trabajo manual si los recursos de TIC no están disponibles:	No es posible realizar tareas manuales en el servicio de Comunicaciones

Funciones e información de contacto para la actividad:

Tabla 84. Funciones e información de los contactos necesarios para la Continuidad del Negocio – Disponibilidad de servicios de Comunicaciones

N°	Función en la recuperación	Nombre	Cargo / unidad organizativa	Teléfono móvil	Teléfono fijo	Correo electrónico	Domicilio particular	N° de reemplazo
1.	Gerente de recuperación	Ing. Santiago Pazmiño	Gerente Nacional de Tecnología	0984358942	ND	spazmino@bklm.com.ec	Ciudadela Gonzales Suarez	5.
2.	Coordinador de recuperación	Ing. Luis Arevalo	Gerente de Producción y Servicios	0984368912	ND	larevalo@bklm.com.ec	Sangolqui, conjunto puertas del sol	6.
3.	Supervisor de recuperación	Ing. Bolívar Socasi	Subgerente de Procesamiento e Infraestructura	0984335621	ND	bsocasi@bklm.com.ec	Av. Mariscal Sucre y Michelena	10.
4.	Operador de recuperación	Ing. Paúl Ramírez	Jefe de Comunicaciones	0984332066	ND	pramirez@bklm.com.ec	Calle de los trigales y belladonas	10.

5.	Auxiliar de recuperación	Gabinete de Apoyo de Crisis	Tec. Alexis Proaño	Técnico en operación y mantenimiento	0984366018	ND	aproano@bklm.com.ec	Calle Salinas y Buenos Aires

Otras actividades:

Tabla 85. Funciones e información de los contactos necesarios para otras actividades en la Continuidad del Negocio – Disponibilidad de servicios de Comunicaciones

N°	Nombre	Cargo / unidad organizativa	Teléfono móvil	Teléfono fijo	Correo electrónico	N° de reemplazo
6.	Ing. Vinicio Sarabia	Administrador de Comunicaciones	0981944260	ND	vsarabia@bklm.com.ec	9.
7.	Ing. Jorge Vinueza	Administrador de Telefonía	0984345729	ND	jvinueza@bklm.com.ec	9.
8.	Ing. Víctor Pichucho	Técnico de Comunicaciones	0984309812	ND	vpichucho@bklm.com.ec	17.

Contactos externos:

Tabla 86. Contactos externos para el Sistema de Continuidad del Negocio - Servicios de Comunicaciones.

N°	Nombre de la organización	Nombre	Cargo / unidad organizativa	Teléfono móvil	Teléfono fijo	Correo electrónico	N° de reemplazo
9.	Telconet	Operador asignado	Call Center / Soporte Técnico	ND	1700835266	soportedatos@telconet.ec	11.
10.	Cnt	Operador asignado	Call Center / Soporte Técnico	ND	1800268268	soporte@cnt.gob.ec	11.
11.	Level3	Operador asignado	Call Center / Soporte Técnico	ND	1700268268	nocecu@level3.com.ec	9.
12.	AT&T	Operador asignado	Call Center / Soporte Técnico	ND	18776771330	noc@att.com	-
13.	Claro	Operador asignado	Call Center / Soporte Técnico	ND	1800252763	soporte@claro.com.ec	10.
14.	Empresa eléctrica	Operador asignado	Call Center / Soporte Técnico	ND	1700396470	portalweb@eeq.com.ec	-
15.	Todouno	Operador asignado	Call Center / Soporte Técnico	ND	1700202020	incidentes@todouno.com	-

Autorizaciones en una crisis

Tabla 87. Autorizaciones que deben ser ejecutadas en casos de crisis - Disponibilidad de servicios de Comunicaciones.

Función en la recuperación / cargo	Autorizaciones
Gerente de recuperación	Autorizado para tomar todos los pasos mencionados en el Plan de Continuidad del Negocio y en este Plan de recuperación para recuperar la actividad.
Coordinador de recuperación	Autorizado para adquisiciones urgentes de equipos/servicios hasta $ 5000,00
Supervisor de recuperación	Autorizado para comunicarse con los clientes
Operador de recuperación	Autorizado para comunicarse con el 911 (Ecu)
Auxiliar de recuperación	Autorizado para colaborar en la comunicación con el proveedor de energía eléctrica

Nota: Sólo el Jefe de Comunicación Social está autorizado para comunicarse con el público a través de los medios de comunicación.

Recursos necesarios

Los siguientes recursos serán utilizados para la recuperación de la actividad:

Tabla 88. Recursos a utilizar para las acciones preventivas y correctivas - Disponibilidad de servicios de Comunicaciones.

Nombre del recurso	Descripción	Cantidad	Cuándo es necesario el recurso	Persona responsable de conseguir el recurso
Personas:				
Jefe de Comunicaciones	Liderazgo y Configuración de equipos de Comunicaciones	1	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo	Gerente de Producción y Servicios
Administrador de Comunicaciones	Administración los equipos de Comunicaciones, redes LAN, WAN, SAN; configuración, monitoreo, troubleshooting	1	Inmediatamente después de ocurrido el incidente disruptivo	Gerente de Producción y Servicios
Administrador de Telefonía	Administración los equipos de Telefonía,	1	Inmediatamente después de ocurrido el incidente	Gerente de Producción y Servicios

	configuración, monitoreo, troubleshooting		disruptivo	
Técnico de Comunicaciones	Soporte operativo y funcional de los equipos de Comunicaciones, redes	2	Inmediatamente después de 4 s de ocurrido el incidente disruptivo	Gerente de Producción y Servicios
Aplicaciones / bases de datos:				
Sistema operativo de Switches	Software para la actualización del SO de los switches	6	Inmediatamente después de ocurrido el incidente disruptivo	Representante legal de la Empresa Todouno
Sistema operativo de Firewalls	Software para la actualización del SO de los Firewalls	3	Inmediatamente después de ocurrido el incidente disruptivo	Representante legal de la Empresa Todouno
Sistema operativo de Routers	Software para la actualización del SO de los Routers	5	Inmediatamente después de ocurrido el incidente disruptivo	Representante legal de la Empresa Todouno
Sistema operativo de Ips	Software para la actualización del SO de los IPS	2	Inmediatamente después de ocurrido el incidente disruptivo	Representante legal de la Empresa Todouno

Software de monitoreo de redes	WhatsUp Gold, Solarwinds, Quest Network Tools, Cisco Prime	4	Inmediatamente después de ocurrido el incidente disruptivo	Representante legal de la Empresa Todouno
Sistema operativo de Centrales Telefónicas	Software para la actualización del SO de las Centrales Telefónicas	2	Inmediatamente después de ocurrido el incidente disruptivo	Representante legal de la Empresa Todouno
Software de reportería	Cat Tools Enterprise	1	Inmediatamente después de ocurrido el incidente disruptivo	Jefe de Comunicaciones
Datos almacenados en formato electrónico:				
Arquitectura de red institucional	Almacenado en un repositorio/server con seguridades	1	Inmediatamente después de ocurrido el incidente disruptivo	Jefe de Comunicaciones
Manuales digitales de los equipos de Comunicaciones	Almacenado en un repositorio/server con seguridades	1	Inmediatamente después de ocurrido el incidente disruptivo	Representante legal de la Empresa Todouno

Respaldos de Bases de Datos de los equipos destinados para monitoreo de la Red	Almacenados en un Servidor de Comunicaciones con seguridades	1	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo	Jefe de Comunicaciones
Instaladores y licencias del Software de Monitoreo	Almacenados en un Servidor de Comunicaciones con seguridades	1	Inmediatamente después de ocurrido el incidente disruptivo	Jefe de Comunicaciones
Datos almacenados en papel:				
Arquitectura de red institucional impresa	Archivador de Jefatura y Administrador de Comunicaciones	2	Inmediatamente después de ocurrido el incidente disruptivo	Jefe de Comunicaciones
Manuales impresos para la configuración de los equipos de	Archivador de Jefatura y Administrador de Comunicaciones	2	Inmediatamente después de ocurrido el incidente disruptivo	Representante legal de la Empresa Todouno

Comunicaciones				
Contactos internos y externos para la gestión de TI	Archivador de Jefatura y Administrador de Comunicaciones	2	Inmediatamente después de ocurrido el incidente disruptivo	Jefe de Comunicaciones
Equipos de TI y comunicaciones:				
PCs de escritorio	AllOne Core i7 2.4 GHz, 8 GB de memoria ram, disco duro sata de 1TB, 2 monitores LCD, teclado completo y mouse.	2	Inmediatamente después de ocurrido el incidente disruptivo	Jefe Administrativo
Laptop	AllOne Core i5 3.0 GHz, 8 GB de memoria ram, disco duro de 500 GB	2	Inmediatamente después de ocurrido el incidente disruptivo	Jefe Administrativo
Servidor	Servidor físico Lenovo i7, 2.4 GHz, 8 GB de memoria ram, disco duro sata de 500 GB.	1	Inmediatamente después de 4 horas de ocurrido el incidente disruptivo	Jefe Administrativo
Servidor	Servidor virtual ubicado en el Data Center, Intel	1	Inmediatamente después de 1 hora de ocurrido el	Jefe Administrativo

	Xeon 2.9 GHz, 8 GB de memoria ram, disco duro SCSI de 500 GB, Windows server 2008 R2		incidente disruptivo	
Switch	Cisco Nexus 7k	2	Inmediatamente después de ocurrido el incidente disruptivo	Representante legal de la Empresa Todouno
Switch	Cisco Nexus 2k	8	Inmediatamente después de ocurrido el incidente disruptivo	Representante legal de la Empresa Todouno
Switch	Cisco Catalyst 6500	2	Inmediatamente después de ocurrido el incidente disruptivo	Representante legal de la Empresa Todouno
Switch	Cisco Catalyst 4500	2	Inmediatamente después de ocurrido el incidente disruptivo	Representante legal de la Empresa Todouno
Switch	Cisco Catalyst 3850	4	Inmediatamente después de ocurrido el incidente disruptivo	Representante legal de la Empresa Todouno
Switch	Cisco Catalyst 2960	30	Inmediatamente después	Representante legal de la

			de 1 hora de ocurrido el incidente disruptivo	Empresa Todouno
Firewall	Cisco ASA 5585	2	Inmediatamente después de ocurrido el incidente disruptivo	Representante legal de la Empresa Todouno
Firewall	Cisco ASA 5540	2	Inmediatamente después de ocurrido el incidente disruptivo	Representante legal de la Empresa Todouno
Firewall	Cisco ASA 5520	2	Inmediatamente después de ocurrido el incidente disruptivo	Representante legal de la Empresa Todouno
Router	Cisco ASR 1000	4	Inmediatamente después de ocurrido el incidente disruptivo	Representante legal de la Empresa Todouno
Router	Cisco 3900	4	Inmediatamente después de ocurrido el incidente disruptivo	Representante legal de la Empresa Todouno
Router	Cisco 2900	4	Inmediatamente después de ocurrido el incidente disruptivo	Representante legal de la Empresa Todouno

Router	Cisco 1900	4	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo	Representante legal de la Empresa Todouno
Router	Cisco 881	10	Inmediatamente después de 4 horas de ocurrido el incidente disruptivo	Representante legal de la Empresa Todouno
IPS	Proventia GX6116	2	Inmediatamente después de ocurrido el incidente disruptivo	Representante legal de la Empresa Todouno
Impresora	Xerox workcentre	2	Inmediatamente después de 4 horas de ocurrido el incidente disruptivo	Jefe Administrativo
Teléfono	Teléfono IP Alcatel 4038	4	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo	Jefe Administrativo
Teléfono Celular	BlackBerry Curve, con paquete de datos	4	Inmediatamente después de ocurrido el incidente disruptivo	Jefe Administrativo
Canales de comunicación:				

Líneas fijas de teléfono	Líneas habilitadas de telefonía fija con salida a celulares	4	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo	Jefe Administrativo
Líneas celulares	Teléfonos celulares habilitados con paquetes de voz, datos y salida internacional	3	Inmediatamente después de ocurrido el incidente disruptivo	Jefe Administrativo
Acceso a internet	Enlace dedicado fibra óptica de 35Mbps	2	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo	Jefe de Comunicaciones
Correo electrónico	Servidor de correo con cuentas habilitadas, con capacidad de 5 MB	2	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo	Jefe de Comunicaciones
Otros equipos:				
Televisor	Televisor Panasonic de 42"	1	Inmediatamente después de 4 horas de ocurrido el incidente disruptivo	Jefe Administrativo
Instalaciones e infraestructura:				
Puntos de Red de	Red LAN de cableado	8	Inmediatamente después	Jefe de Comunicaciones

computadoras	vertical y horizontal categoría 6a		de 1 hora de ocurrido el incidente disruptivo	
BackBone de servidores	Red LAN, SAN de cableado de Fibra Óptica	50	Inmediatamente después de ocurrido el incidente disruptivo	Jefe de Comunicaciones
Muebles de oficina	Sillas y escritorios individuales para uso del personal técnico	6	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo	Jefe Administrativo
Servicios externos:				
Electricidad	Alimentación eléctrica de la red pública	2	Inmediatamente después de ocurrido el incidente disruptivo	Jefe Administrativo
Agua potable	Servicio de agua potable	1	Inmediatamente después de ocurrido el incidente disruptivo	Jefe Administrativo
Oficinas	Renta de Oficinas para uso del personal de Comunicaciones	1	Inmediatamente después de ocurrido el incidente disruptivo	Jefe Administrativo

Adaptado de: (Kosutic, 2015).

Pasos de recuperación para la actividad

Esta actividad se debe recuperar de la siguiente forma:

Tabla 89. Pasos de recuperación que garanticen la disponibilidad de los servicios de Comunicaciones.

Procedimientos de recuperación (pasos principales / tareas individuales)	Personas responsables de la implementación	Comunicación (contenido, destinatario)	Registro de implementación (fecha / hora)
1. Reunión del equipo en la ubicación alternativa			
1.1 Verificar si todos los miembros del equipo se encuentran presentes	Auxiliar de recuperación	Verificación realizada con éxito por medio de la toma de asistencia, Gerente de recuperación	ND
1.2 Informar a los miembros del equipo del incidente disruptivo ocurrido	Gerente de recuperación	Comunicación publicada con éxito, Gabinete de crisis	ND
1.3 Dar directrices puntuales necesarias a los miembros del equipo	Coordinador de recuperación	Comunicación de directrices, Gabinete de crisis	ND

2. Verificación y recuperación de la infraestructura y muebles básicos			
2.1 Verificar si se cuenta con la infraestructura necesaria para iniciar la recuperación de la actividad	Supervisor de recuperación	Verificación de infraestructura realizada con éxito, Coordinador de recuperación	ND
2.2 Levantar un informe de la infraestructura disponible y de la infraestructura faltante necesaria	Supervisor de recuperación	Informe de infraestructura realizado con éxito, Coordinador de recuperación	ND
2.3 Instalación de muebles básicos necesarios para iniciar la recuperación	Auxiliar de recuperación	Instalación de muebles realizada con éxito, Supervisor de recuperación	ND
3. Verificación y recuperación de los equipos y vínculos de TIC			
3.1 Verificar si se cuenta con los equipos y vínculos necesarios para iniciar la recuperación de la actividad	Operador de recuperación	Verificación de equipos y vínculos realizada con éxito, Supervisor de recuperación	ND

3.2 Levantar un informe sobre los equipos faltantes (si los hubiera) y de cuál es la capacidad operativa con los equipos actuales	Operador de recuperación	Informe de equipos realizado con éxito, Supervisor de recuperación	ND
3.3 Poner operativos los equipos necesarios para iniciar la recuperación de la actividad	Supervisor de recuperación	Equipos puestos en operación, Coordinador de recuperación	ND
4. Verificación y recuperación de aplicaciones			
4.1 Verificar si se cuenta con las aplicaciones y los instaladores de estas para iniciar la recuperación de la actividad	Operador de recuperación	Verificación de las aplicaciones e instaladores realizada con éxito, Supervisor de recuperación	ND
4.2 Poner en marcha las aplicaciones necesarias para la recuperación de la actividad	Supervisor de recuperación	Puesta en marcha de aplicaciones necesarias, Coordinador de recuperación	ND

4.3 Levantar un informe sobre el funcionamiento de las aplicaciones puestas en marcha y la carga de trabajo que pueden soportar	Supervisor de recuperación	Informe sobre funcionamiento de aplicaciones realizado con éxito, Coordinador de recuperación	ND
5. Verificación y recuperación de datos y documentos (en formato electrónico o papel)			
5.1 Verificar si se cuenta con los datos y documentos necesarios para iniciar la recuperación de la actividad	Operador de recuperación	Verificación de datos y documentos realizado con éxito, Supervisor de recuperación	ND
5.2 Poner a disposición de las personas correspondientes los datos y los documentos necesarios para iniciar la recuperación de la actividad	Operador de recuperación	Datos y documentos entregados al personal correspondiente, Supervisor de recuperación	ND

Adaptado de: (Kosutic, 2015).

Gestión de registros guardados en base a este documento

Tabla 90. Registros guardados de las principales características del documento.

Nombre del registro	Ubicación de archivo	Persona responsable del archivo	Controles para la protección del registro	Tiempo de retención
Registro de implementación de pasos de recuperación (registro en papel)	Archivo del Gerente de recuperación	Gerente Nacional de Tecnología	Los registros se guardan en un gabinete con llave	3 años

Solamente el Gerente Nacional de Tecnología puede permitir el acceso a los registros a otros empleados.

Validez y gestión de documentos

Este documento es válido desde el 03 de Agosto del 2015.

Este documento, junto con todos los documentos adicionales, es archivado de la siguiente forma:

- El documento en papel se archiva en las siguientes ubicaciones: Centro de crisis y todas las ubicaciones alternativas para actividades
- El documento en formato electrónico se archiva en la siguiente ruta: \\SRVTECH\SGCN\PLAN_DE_RESPUESTA_A_INCIDENTES\Anexo 6.6 Apendice_6a_Plan de recuperación para la disponibilidad de Comunicaciones

El propietario de este documento es el Gerente Nacional de Tecnología, que debe verificar, y si es necesario actualizar, el documento por lo menos una vez al año.

Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- Cantidad de medidas correctivas de acuerdo a los ejercicios realizados.
- Cantidad de medidas correctivas en base a la implementación del plan en una crisis.
- En caso de crisis, si la recuperación se consiguió dentro de los objetivos de tiempo de recuperación.

Documentos adicionales

- Documentación técnica de los equipos de Comunicaciones (Switches, routers, firewalls, IPs).
- Planes de recuperación detallados para los sistemas individuales de TIC.
- Instrucciones de funcionamiento de los equipos de Comunicaciones y hardware en general.

Gerente Nacional de Tecnología

Ing. Santiago Pazmiño

_____

Firma

ANEXO 6.6 (b)

Plan de recuperación de la actividad ejecutar acciones preventivas y correctivas para garantizar la disponibilidad los servicios de Aplicativos de Core Bancario y Negocios

Anexo 6.6: Plan de Continuidad del Negocio

Apéndice 6b: Plan de recuperación de la actividad ejecutar acciones preventivas y correctivas para garantizar la disponibilidad los servicios de Aplicativos de Core Bancario y Negocios

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
03/08/2015	1.0	Vinicio Sarabia	Creación de la primera versión del documento

Tabla de contenido

Objetivo, alcance y usuarios

El objetivo del Plan de recuperación es definir de forma precisa cómo el Banco KLM recuperará sus actividades dentro de plazos establecidos ante el caso de un desastre o de un incidente disruptivo. El objetivo de este Plan es terminar la

recuperación de esta actividad dentro del objetivo de tiempo de recuperación establecido.

Este Plan incluye todos los recursos y procesos necesarios para la recuperación de esta actividad.

Los usuarios de este documento son los miembros del Gabinete de crisis y los empleados necesarios para la recuperación de esta actividad.

General

Tabla 91. Responsabilidades en la recuperación de actividades – Disponibilidad los servicios de Aplicativos de Core Bancario y Negocios.

Objetivo de tiempo de recuperación:	1.5 horas
Persona responsable de la activación del plan y de los medios de activación:	Gerente de Recuperación o Gerente de crisis (Gerente Nacional de Tecnología) / escrito
Personas a las que se debe notificar la activación del plan / quién es responsable:	Gerente Nacional del Centro de Servicios ; Gerente de Producción y Servicios; Gerente de Negocios; Gerente Financiero; Gerente Nacional de Recursos Humanos ; Subgerente de Procesamiento e Infraestructura ; Subgerente de Control Tecnológico , Jefe Administrativo; Jefe de Comunicación Social; Jefe de Comunicaciones; Jefe de Servidores; Jefe de Centro de Computo / responsable: Secretaria de Gerencia Técnica
Persona responsable de la desactivación del	Gerente de Recuperación o Gerente de crisis (Gerente Nacional de Tecnología) / escrito / Se deben cumplir todas las condiciones para retomar las actividades de

plan de recuperación / medios de desactivación / criterios:	Negocio de la actividad crítica.
Tareas / obligaciones clave y sus respectivos plazos:	Verificación del correcto funcionamiento de los servidores de aplicaciones de Core Bancario y Negocios: 10 min; Pruebas de conectividad de los servidores y bases de datos: 10 min; Verificación de alarmas y conexiones físicas : 10min; Monitoreo constante del aplicativo de Core Bancario: 10 min; Verificar la disponibilidad de los equipos de Comunicaciones : 15 min; Limpieza externa de los servidores de Core Bancario y Negocios: 30 min; Depuración de las configuraciones en los equipos : 30min; Verificación del ambiente en el Data Center, temperatura y humedad adecuada: 5 min; Verificación del funcionamiento de la alta disponibilidad/respaldo de energía en el Data Center: 5 min; Escalar el incidente al proveedor de la aplicación, equipo en caso de ser necesario: 10 min; Respuesta del proveedor una vez escalado el incidente: 15 min
Cantidad mínima aceptable de trabajo inmediatamente después del desastre (MBCO, objetivo mínimo para la Continuidad del Negocio):	1 incidente resuelto en el servicio de Aplicativos de Core Bancario y Negocios por mes

Período a partir del cual se debe retomar el nivel de funcionamiento normal:	24 horas
Instrucciones para trabajo manual si los recursos de TIC no están disponibles:	No es posible realizar tareas manuales en el servicio de Aplicativos de Core Bancario y Negocios

Adaptado de: (Kosutic, 2015).

Funciones e información de contacto para la actividad:

Tabla 92. Funciones e información de los contactos necesarios para la Continuidad del Negocio – Disponibilidad los servicios de Aplicativos de Core Bancario y Negocios.

N°	Función en la recuperación	Nombre	Cargo / unidad organizativa	Teléfono móvil	Teléfono fijo	Correo electrónico	Domicilio particular	N° de reemplazo
1.	Gerente de recuperación	Ing. Santiago Pazmiño	Gerente Nacional de Tecnología	0984358942	ND	spazmino@bklm.com.ec	Ciudadela Gonzales Suarez	5.
2.	Coordinador de recuperación	Ing. Luis Arevalo	Gerente de Producción y Servicios	0984368912	ND	larevalo@bklm.com.ec	Sangolqui, conjunto puertas del sol	6.
3.	Supervisor de recuperación	Ing. Bolívar Socasi	Subgerente de Procesamiento e Infraestructura	0984335621	ND	bsocasi@bklm.com.ec	Av. Mariscal Sucre y Michelena	10.
4.	Operador de recuperación	Ing. Paúl Ramírez	Jefe de Servidores	0984399820	ND	eortiz@bklm.com.ec	Ciudadela el ejército	9.
5.	Auxiliar de	Gabinete	Tec. Alexis	Técnico en	0984366	ND	aproano@	Calle

	recuperación	de Apoyo de Crisis	Proaño	operación y mantenimiento	018		bklm.com.ec	Salinas y Buenos Aires
6.	Usuario de recuperación	Gabinete de Apoyo de Crisis	Ing. Paulina Vallejos	Asistente Financiero	0984396822	ND	pvallejos@bklm.com.ec	Barrio San Juan

Otras actividades:

Tabla 93. Funciones e información de los contactos necesarios para otras actividades en la Continuidad del Negocio – Disponibilidad los servicios de Aplicativos de Core Bancario y Negocios.

N°	Nombre	Cargo / unidad organizativa	Teléfono móvil	Teléfono fijo	Correo electrónico	N° de reemplazo (Referencia)
7.	Ing. Pablo Mera	Subgerente de Servicios Tecnológicos	0984317188	ND	pmera@bklm.com.ec	8.
8.	Ing. René	Jefe de Soporte	0984394426	ND	rfigueroa@bklm.com.e	7.

	Figueroa	Técnico			c	

Contactos externos:

Tabla 94. Contactos externos para el Sistema de Continuidad del Negocio - Servicios y Aplicativos de Core Bancario y Negocios.

N°	Nombre de la organización	Nombre	Cargo / unidad organizativa	Teléfono móvil	Teléfono fijo	Correo electrónico	N° de reemplazo
9.	IBM	Operador asignado	Call Center / Soporte Técnico	ND	1700-NOCIBM	soporte@ibm.ec	10.
10.	Kruger	Operador asignado	Call Center / Soporte Técnico	ND	1800-KRUGER	incidnetes@kruger.com	9.
11.	TATA	Operador asignado	Call Center / Soporte Técnico	ND	1700-NOCTCS	soporte@tcs.com	12.
12.	Qmatic	Operador asignado	Call Center / Soporte Técnico	ND	1800-QMATIC	incidentes@qmatic.com	11.
13.	CNT	Operador asignado	Call Center / Soporte Técnico	ND	1800-NOCCNT	soporte@cnt.gob.ec	-
14.	Empresa eléctrica	Operador asignado	Call Center / Soporte Técnico	ND	1700396470	portalweb@eeq.com.ec	-

15.	Todouno	Operador asignado	Call Center / Soporte Técnico	ND	1700202020	incidentes@todouno.com	-

Autorizaciones en una crisis

Tabla 95. Autorizaciones que deben ser ejecutadas en casos de crisis - Disponibilidad los servicios de Aplicativos de Core Bancario y Negocios.

Función en la recuperación / cargo	Autorizaciones
Gerente de recuperación	Autorizado para tomar todos los pasos mencionados en el Plan de Continuidad del Negocio y en este Plan de recuperación para recuperar la actividad.
Coordinador de recuperación	Autorizado para adquisiciones urgentes de equipos/servicios hasta $ 5000,00
Supervisor de recuperación	Autorizado para comunicarse con los clientes
Operador de recuperación	Autorizado para comunicarse con el 911 (Ecu)
Auxiliar de recuperación	Autorizado para colaborar en la comunicación con los proveedores de energía eléctrica y Cnt
Usuario de recuperación	Autorizado para realizar pruebas de los sistemas de Core Bancario y Negocios en producción, una vez que se encuentre recuperada su operación

Nota: Sólo el Jefe de Comunicación Social está autorizado para comunicarse con el público a través de los medios de comunicación.

Recursos necesarios

Los siguientes recursos serán utilizados para la recuperación de la actividad:

Tabla 96. Recursos a utilizar para las acciones preventivas y correctivas - Disponibilidad los servicios de Aplicativos de Core Bancario y Negocios.

Nombre del recurso	Descripción	Cantidad	Cuándo es necesario el recurso	Persona responsable de conseguir el recurso
Personas:				
Gerente de Producción y Servicios	Liderazgo, comunicación, decisión, coordinación	1	Inmediatamente después de ocurrido el incidente disruptivo	Gerente de Producción y Servicios
Jefe de Servidores	Liderazgo y Configuración de servidores, bases de datos, aplicativos	1	Inmediatamente después de ocurrido el incidente disruptivo	Gerente de Producción y Servicios
Jefe de Centro de Computo	Liderazgo, configuración de sistemas y aplicaciones de Core Bancario (AS400)	1	Inmediatamente después de ocurrido el incidente disruptivo	Gerente de Producción y Servicios
Jefe de Comunicaciones	Liderazgo y Configuración de equipos de	1	Inmediatamente después de ocurrido el incidente	Gerente de Producción y Servicios

	Comunicaciones		disruptivo	
Administrador de Servidores	Administrar los servidores de Aplicativos, bases de datos; configuración, monitoreo, troubleshooting	2	Inmediatamente después de ocurrido el incidente disruptivo	Gerente de Producción y Servicios
Administrador de Servidores	Administrar los servidores de Aplicativos, bases de datos; configuración, monitoreo, troubleshooting	2	Inmediatamente después de ocurrido el incidente disruptivo	Gerente de Producción y Servicios
Administrador de Comunicaciones	Administración los equipos de Comunicaciones, redes LAN, WAN, SAN; configuración, monitoreo, troubleshooting	1	Inmediatamente después de ocurrido el incidente disruptivo	Gerente de Producción y Servicios
Analista de Monitoreo	Soporte operativo y funcional de los aplicativos de Monitoreo	2	Inmediatamente después de ocurrido el incidente disruptivo	Gerente de Producción y Servicios
Aplicaciones / bases de datos:				
Sistema AS400	Sistemas de Core	4	Inmediatamente después de	Representante legal de la

	Bancario		ocurrido el incidente disruptivo	Empresa IBM
Microsoft SQL Server 2005	Gestor de Base de datos SQL Server 2005	2	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo	Representante legal de la Empresa IBM
Sistemas Operativos de Comunicaciones	Software para Comunicaciones de datos	2	Inmediatamente después de ocurrido el incidente disruptivo	Representante legal de la Empresa Todouno
PeopleSoft, CRM, ERP	Sistemas de Negocio	2	Inmediatamente después de ocurrido el incidente disruptivo	Representante legal de la Empresa IBM
Big Data	Almacenamiento y gestión de la información del Banco	4	Inmediatamente después de ocurrido el incidente disruptivo	Representante legal de la Empresa Kruger
Datos almacenados en formato electrónico:				
Copia de respaldo de configuración	Almacenados en un Servidor del Centro de	2	Inmediatamente después de ocurrido el incidente	Jefe de Servidores

de los servidores y bases de datos	Computo bajo seguridades informáticas		disruptivo	
Detalle diario de transacciones financieras (consumos)	Almacenado en un repositorio/server con seguridades	2	Inmediatamente después de ocurrido el incidente disruptivo	Jefe de Servidores
Copias diarias de respaldo de las bases de datos del Core Bancario	Almacenado en un repositorio/server con seguridades	1	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo	Jefe de Centro de Computo
Paquete instalador de los gestores de bases de datos, Core Bancario y aplicativos de Negocios	Almacenados en un Servidor del Centro de Computo con seguridades informáticas	2	Inmediatamente después de ocurrido el incidente disruptivo	Jefe de Servidores
Estados de cuenta de los Clientes	Almacenados en un Servidor del Centro de Computo bajo seguridades informáticas	2	Inmediatamente después de 4 horas de ocurrido el incidente disruptivo	Jefe de Centro de Computo

Datos almacenados en papel:				
Reporte consolidado del movimiento financiero diario	Archivador de Gerencia de Negocios y Financiera	2	Inmediatamente después de 4 horas de ocurrido el incidente disruptivo	Gerencia Comercial
Manuales impresos para la configuración y manejo aplicativos de Core Bancario	Archivador de Jefaturas de Servidores y Soporte Técnico	2	Inmediatamente después de ocurrido el incidente disruptivo	Jefe de Servidores
Contactos internos y externos para la gestión de TI	Archivador de las Jefaturas y Administradores de Comunicaciones, Servidores, Centro de Computo	2	Inmediatamente después de ocurrido el incidente disruptivo	Jefe de Servidores
Equipos de TI y comunicaciones:				

PCs de escritorio	AllOne Core i7 2.4 GHz, 8 GB de memoria ram, disco duro sata de 1TB, 2 monitores LCD, teclado completo y mouse.	9	Inmediatamente después de ocurrido el incidente disruptivo	Jefe Administrativo
Laptop	AllOne Core i5 3.0 GHz, 8 GB de memoria ram, disco duro de 500 GB	3	Inmediatamente después de ocurrido el incidente disruptivo	Jefe Administrativo
Servidor de Monitoreo AS400	Servidor físico Lenovo i7, 2.4 GHz, 8 GB de memoria ram, disco duro sata de 500 GB.	4	Inmediatamente después de ocurrido el incidente disruptivo	Jefe Administrativo
Servidor de Aplicaciones	IBM Power 8000	2	Inmediatamente después de ocurrido el incidente disruptivo	Representante legal de la Empresa IBM
Impresora	Xerox workcentre	4	Inmediatamente después de 4 horas de ocurrido el incidente disruptivo	Jefe Administrativo
Teléfono	Teléfono IP Alcatel 4038	9	Inmediatamente después de 1 hora de ocurrido el	Jefe Administrativo

			incidente disruptivo	
Teléfono Celular	BlackBerry Curve, con paquete de datos	9	Inmediatamente después de ocurrido el incidente disruptivo	Jefe Administrativo
Canales de comunicación:				
Líneas fijas de teléfono	Líneas habilitadas de telefonía fija con salida a celulares	9	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo	Jefe Administrativo
Líneas celulares	Teléfonos celulares habilitados con paquetes de voz, datos y salida internacional	9	Inmediatamente después de ocurrido el incidente disruptivo	Jefe Administrativo
Acceso a internet	Enlace dedicado fibra óptica de 35Mbps	2	Inmediatamente después de ocurrido el incidente disruptivo	Jefe de Comunicaciones
Correo electrónico	Servidor de correo con cuentas habilitadas, con capacidad de 5 MB	9	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo	Jefe de Comunicaciones
Otros equipos:				

Televisor	Televisor Panasonic de 42"	1	Inmediatamente después de 4 horas de ocurrido el incidente disruptivo	Jefe Administrativo
Instalaciones e infraestructura:				
Puntos de Red de computadoras	Red LAN de cableado vertical y horizontal categoría 6a	15	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo	Jefe de Comunicaciones
BackBone de equipos de Core Bancario	Red LAN, SAN de cableado de Fibra Óptica	30	Inmediatamente después de ocurrido el incidente disruptivo	Jefe de Comunicaciones
Muebles de oficina	Sillas y escritorios individuales para uso del personal técnico	15	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo	Jefe Administrativo
Servicios externos:				
Electricidad	Alimentación eléctrica de la red pública	2	Inmediatamente después de ocurrido el incidente disruptivo	Jefe Administrativo
Agua potable	Servicio de agua potable	1	Inmediatamente después de	Jefe Administrativo

			ocurrido el incidente disruptivo	
Oficinas	Renta de Oficinas para uso del personal de Comunicaciones	1	Inmediatamente después de ocurrido el incidente disruptivo	Jefe Administrativo
Servicios de soporte del proveedor correspondiente	Servicio de soporte de las empresas proveedoras de los aplicativos	1	Inmediatamente después de ocurrido el incidente disruptivo	Jefe de Servidores

Adaptado de: (Kosutic, 2015).

Pasos de recuperación para la actividad

Esta actividad se debe recuperar de la siguiente forma:

Tabla 97. Pasos de recuperación - Disponibilidad los servicios de Aplicativos de Core Bancario y Negocios.

Procedimientos de recuperación (pasos principales / tareas individuales)	Personas responsables de la implementación	Comunicación (contenido, destinatario)	Registro de implementación (fecha / hora)
1. Reunión del equipo en la ubicación alternativa			
1.1 Verificar si todos los miembros del equipo se encuentran presentes	Auxiliar de recuperación	Verificación realizada con éxito por medio de la toma de asistencia, Gerente de recuperación	ND
1.2 Informar a los miembros del equipo del incidente disruptivo ocurrido	Gerente de recuperación	Comunicación publicada con éxito, Gabinete de crisis	
1.3 Dar directrices puntuales necesarias a los miembros del equipo	Coordinador de recuperación	Comunicación de directrices, Gabinete de crisis	
2. Verificación y recuperación de la infraestructura y muebles básicos			
2.1 Verificar si se cuenta con la infraestructura necesaria para iniciar la recuperación de la actividad	Supervisor de recuperación	Verificación de infraestructura realizada con éxito, Coordinador de recuperación	

2.2 Levantar un informe de la infraestructura disponible y de la infraestructura faltante necesaria	Supervisor de recuperación	Informe de infraestructura realizado con éxito, Coordinador de recuperación	
2.3 Instalación de muebles básicos necesarios para iniciar la recuperación	Auxiliar de recuperación	Instalación de muebles realizada con éxito, Supervisor de recuperación	
3. Verificación y recuperación de los equipos y vínculos de TIC			
3.1 Verificar si se cuenta con los equipos y vínculos necesarios para iniciar la recuperación de la actividad	Operador de recuperación	Verificación de equipos y vínculos realizada con éxito, Supervisor de recuperación	
3.2 Levantar un informe sobre los equipos faltantes (si los hubiera) y de cuál es la capacidad operativa con los equipos actuales	Operador de recuperación	Informe de equipos realizado con éxito, Supervisor de recuperación	
3.3 Poner operativos los equipos necesarios para iniciar la recuperación de la actividad	Supervisor de recuperación	Equipos puestos en operación, Coordinador de recuperación	
4. Verificación y recuperación de aplicaciones			
4.1 Verificar si se cuenta con las	Operador de recuperación	Verificación de las aplicaciones e	

aplicaciones y los instaladores de estas para iniciar la recuperación de la actividad		instaladores realizada con éxito, Supervisor de recuperación	
4.2 Poner en marcha las aplicaciones necesarias para la recuperación de la actividad	Supervisor de recuperación	Puesta en marcha de aplicaciones necesarias, Coordinador de recuperación	
4.3 Levantar un informe sobre el funcionamiento de las aplicaciones puestas en marcha y la carga de trabajo que pueden soportar	Supervisor de recuperación	Informe sobre funcionamiento de aplicaciones realizado con éxito, Coordinador de recuperación	
5. Verificación y recuperación de datos y documentos (en formato electrónico o papel)			
5.1 Verificar si se cuenta con los datos y documentos necesarios para iniciar la recuperación de la actividad	Operador de recuperación	Verificación de datos y documentos realizado con éxito, Supervisor de recuperación	
5.2 Poner a disposición de las personas correspondientes los datos y los	Operador de recuperación	Datos y documentos entregados al personal correspondiente, Supervisor de	

documentos necesarios para iniciar la recuperación de la actividad		recuperación	

Adaptado de: (Kosutic, 2015).

Gestión de registros guardados en base a este documento

Tabla 98. Registros guardados de las principales características del documento - Disponibilidad los servicios de Aplicativos de Core Bancario y Negocios.

Nombre del registro	Ubicación de archivo	Persona responsable del archivo	Controles para la protección del registro	Tiempo de retención
Registro de implementación de pasos de recuperación (registro en papel)	Archivo del Gerente de recuperación	Gerente Nacional de Tecnología	Los registros se guardan en un gabinete con llave	3 años

Solamente el Gerente Nacional de Tecnología puede permitir el acceso a los registros a otros empleados.

Validez y gestión de documentos

Este documento es válido desde el 03 de Agosto del 2015.
Este documento, junto con todos los documentos adicionales, es archivado de la siguiente forma:

- El documento en papel se archiva en las siguientes ubicaciones: Centro de crisis y todas las ubicaciones alternativas para actividades

- El documento en formato electrónico se archiva en la siguiente ruta: \\SRVTECH\SGCN\PLAN_DE_RESPUESTA_A_INCIDENTES\Anexo 6.6 Apendice_6b_Plan de recuperación para la disponibilidad de Aplicaciones de Core Bancario y Negocios.

El propietario de este documento es el Gerente Nacional de Tecnología, que debe verificar, y si es necesario actualizar, el documento por lo menos una vez al año.

Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- Cantidad de medidas correctivas de acuerdo a los ejercicios realizados.
- Cantidad de medidas correctivas en base a la implementación del plan en una crisis.
- En caso de crisis, si la recuperación se consiguió dentro de los objetivos de tiempo de recuperación.

Documentos adicionales

- Documentación técnica de los equipos para los Aplicativos de Core Bancario y Negocios (Servidores, bases de datos, Switches, routers, firewalls, IPs).
- Planes de recuperación detallados para los sistemas individuales de TIC.
- Instrucciones de funcionamiento de los equipos utilizados para Aplicativos de Core Bancario y Negocios, hardware en general.

Gerente Nacional de Tecnología

Ing. Santiago Pazmiño

_____

Firma

ANEXO 6.6 (c)

Plan de recuperación de la actividad ejecutar acciones preventivas y correctivas para garantizar la disponibilidad de los servicios de Aplicativos Administrativos, Financieros y Tecnológicos

Anexo 6.6: Plan de Continuidad del Negocio

Apéndice 6c: Plan de recuperación de la actividad ejecutar acciones preventivas y correctivas para garantizar la disponibilidad de los servicios de Aplicativos Administrativos, Financieros y Tecnológicos

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
03/08/2015	1.0	Vinicio Sarabia	Creación de la primera versión del documento

Tabla de contenido

Objetivo, alcance y usuarios

El objetivo del Plan de recuperación es definir de forma precisa cómo el Banco KLM recuperará sus actividades dentro de plazos establecidos ante el caso de un desastre o de un incidente disruptivo. El objetivo de este Plan es terminar la recuperación de esta actividad dentro del objetivo de tiempo de recuperación establecido.

Este Plan incluye todos los recursos y procesos necesarios para la recuperación de esta actividad.

Los usuarios de este documento son los miembros del Gabinete de crisis y los empleados necesarios para la recuperación de esta actividad.

General

Tabla 99. Responsabilidades en la recuperación de actividades – Disponibilidad de los Aplicativos Administrativos, Financieros y Tecnológicos.

Objetivo de tiempo de recuperación:	4 horas
Persona responsable de la activación del plan y de los medios de activación:	Gerente de Recuperación o Gerente de crisis (Gerente Nacional de Tecnología) / escrito
Personas a las que se debe notificar la activación del plan / quién es responsable:	Gerente Nacional del Centro de Servicios ; Gerente de Producción y Servicios; Gerente de Negocios; Gerente Financiero; Gerente Nacional de Recursos Humanos ; Subgerente de Procesamiento e Infraestructura ; Subgerente de Control Tecnológico , Jefe Administrativo; Jefe de Comunicación Social; Jefe de Comunicaciones; Jefe de Servidores; Jefe de Centro de Computo / responsable: Secretaria de Gerencia Técnica
Persona responsable de la desactivación del plan de recuperación / medios de desactivación / criterios:	Gerente de Recuperación o Gerente de crisis (Gerente Nacional de Tecnología) / escrito / Se deben cumplir todas las condiciones para retomar las actividades de Negocio de la actividad crítica.
Tareas / obligaciones	Verificación del correcto funcionamiento de los

clave y sus respectivos plazos:	servidores de aplicaciones y base de datos: 30 min; Pruebas de conectividad de los servidores y bases de datos: 15 min; Verificación de alarmas y conexiones físicas: 15 min; Monitoreo constante de los aplicativos, servidores y bases de datos: 10 min; Verificar la disponibilidad de los equipos de Comunicaciones: 15 min; Limpieza externa de los servidores: 60 min; Depuración de las configuraciones en los equipos: 30 min; Verificación del ambiente en el Data Center, temperatura y humedad adecuada: 5 min; Verificación del funcionamiento de la alta disponibilidad/respaldo de energía en el Data Center: 5 min; Escalar el incidente al proveedor de la aplicación, equipo en caso de ser necesario: 30 min; Respuesta del proveedor una vez escalado el incidente: 15 min; Solución al problema por parte del proveedor (caso extremo): 24 horas
Cantidad mínima aceptable de trabajo inmediatamente después del desastre (MBCO, objetivo mínimo para la Continuidad del Negocio):	4 incidentes resueltos en el servicio de Aplicativos Financieros, Administrativos y Tecnológicos por mes
Período a partir del cual se debe retomar el nivel de funcionamiento normal:	48 horas
Instrucciones para trabajo manual si los	Redactar de forma manual los registros/solicitudes Financieras,

recursos de TIC no están disponibles:	Administrativas y Tecnológicas para luego digitalizarlos.

Adaptado de: (Kosutic, 2015).

Funciones e información de contacto para la actividad:

Tabla 100. Funciones e información de los contactos necesarios para la Continuidad del Negocio – Disponibilidad de los Aplicativos Administrativos, Financieros y Tecnológicos.

N°	Función en la recuperación	Nombre	Cargo / unidad organizativa	Teléfono móvil	Teléfono fijo	Correo electrónico	Domicilio particular	N° de reemplazo
1.	Gerente de recuperación	Ing. Santiago Pazmiño	Gerente Nacional de Tecnología	0984358942	ND	spazmino@bklm.com.ec	Ciudadela Gonzales Suarez	5.
2.	Coordinador de recuperación	Ing. Luis Arevalo	Gerente de Producción y Servicios	0984368912	ND	larevalo@bklm.com.ec	Sangolqui, conjunto puertas del sol	6.
3.	Supervisor de recuperación	Ing. Bolívar Socasi	Subgerente de Procesamiento e Infraestructura	0984335621	ND	bsocasi@bklm.com.ec	Av. Mariscal Sucre y Michelena	10.
4.	Operador de recuperación	Ing. Paúl Ramírez	Jefe de Servidores	0984399820	ND	eortiz@bklm.com.ec	Ciudadela el ejército	9.
5.	Auxiliar de	Gabinete de	Tec. Alexis	Técnico	0984366	ND	aproano@	Calle

	recuperación	Apoyo de Crisis	Proaño	en operación y mantenimiento	018		bklm.com.ec	Salinas y Buenos Aires
6.	Usuario de recuperación	Gabinete de Apoyo de Crisis	Ing. Paulina Vallejos	Asistente Financiero	0984396822	ND	pvallejos@bklm.com.ec	Barrio San Juan

Otras actividades:

Tabla 101. Funciones e información de los contactos necesarios para otras actividades en la Continuidad del Negocio – Disponibilidad de los Aplicativos Administrativos, Financieros y Tecnológicos.

N°	Nombre	Cargo / unidad organizativa	Teléfono móvil	Teléfono fijo	Correo electrónico	N° de reemplazo (Referencia)
7.	Ing. Pablo Mera	Subgerente de Servicios Tecnológicos	0984317188	ND	pmera@bklm.com.ec	8.

8.	Ing. René Figueroa	Jefe de Soporte Técnico	0984394426	ND	rfigueroa@bklm.com.ec	7.

Contactos externos:

Tabla 102. Contactos externos para el Sistema de Continuidad del Negocio - Disponibilidad de los Aplicativos Administrativos, Financieros y Tecnológicos.

N°	Nombre de la organización	Nombre	Cargo / unidad organizativa	Teléfono móvil	Teléfono fijo	Correo electrónico	N° de reemplazo
9.	IBM	Operador asignado	Call Center / Soporte Técnico	ND	1700-NOCIBM	soporte@ibm.ec	10.
10.	Teradata	Operador asignado	Call Center / Soporte Técnico	ND	18776775660	nocdatos@teradata.com	9.
11.	Kruger	Operador asignado	Call Center / Soporte Técnico	ND	1800-KRUGER	incidnetes@kruger.com	10.
12.	Desca	Operador asignado	Call Center / Soporte Técnico	ND	1800-NOCDES	centrodatos@desca.com.ec	-

13.	CNT	Operador asignado	Call Center / Soporte Técnico	ND	1800-NOCCNT	soporte@cnt.gob.ec	-
14.	Empresa eléctrica	Operador asignado	Call Center / Soporte Técnico	ND	1700396470	portalweb@eeq.com.ec	-
15.	Todouno	Operador asignado	Call Center / Soporte Técnico	ND	1700202020	incidentes@todouno.com	-

Autorizaciones en una crisis

Tabla 103. Autorizaciones que deben ser ejecutadas en casos de crisis - Disponibilidad de los Aplicativos Administrativos, Financieros y Tecnológicos.

Función en la recuperación / cargo	Autorizaciones
Gerente de recuperación	Autorizado para tomar todos los pasos mencionados en el Plan de Continuidad del Negocio y en este Plan de recuperación para recuperar la actividad.
Coordinador de recuperación	Autorizado para adquisiciones urgentes de equipos/servicios hasta $ 5000,00
Supervisor de recuperación	Autorizado para comunicarse con los clientes
Operador de recuperación	Autorizado para comunicarse con el 911 (Ecu)
Auxiliar de recuperación	Autorizado para colaborar en la comunicación con los proveedores de energía eléctrica y Cnt
Usuario de recuperación	Autorizado para realizar pruebas de los sistemas Financieros, Administrativos y Tecnológicos en producción, una vez que se encuentre recuperada su operación

Nota: Sólo el Jefe de Comunicación Social está autorizado para comunicarse con el público a través de los medios de comunicación.

Recursos necesarios

Los siguientes recursos serán utilizados para la recuperación de la actividad:

Tabla 104. Recursos a utilizar para las acciones preventivas y correctivas - Disponibilidad de los Aplicativos Administrativos, Financieros y Tecnológicos.

Nombre del recurso	Descripción	Cantidad	Cuándo es necesario el recurso	Persona responsable de conseguir el recurso
Personas:				
Jefe de Monitoreo	Liderazgo y Configuración de aplicativos de Monitoreo	1	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo	Gerente de Producción y Servicios
Jefe de Servidores	Liderazgo y Configuración de servidores, bases de datos, aplicativos	1	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo	Gerente de Producción y Servicios
Jefe de Soporte Técnico	Liderazgo, configuración de sistemas operativos, soporte operativo y funcional de aplicaciones	1	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo	Gerente de Producción y Servicios

Jefe de Mesa de Servicios	Liderazgo, comunicación y soporte funcional de los aplicativos del Banco	1	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo	Gerente de Producción y Servicios
Administrador de Servidores	Administrar los servidores de Aplicativos, bases de datos; configuración, monitoreo, troubleshooting	6	Inmediatamente después de ocurrido el incidente disruptivo	Gerente de Producción y Servicios
Analista de Monitoreo	Soporte operativo y funcional de los aplicativos de Monitoreo	2	Inmediatamente después de ocurrido el incidente disruptivo	Gerente de Producción y Servicios
Técnico de Soporte	Soporte operativo y funcional de las aplicaciones institucionales, asistente de redes y soporte de equipos informáticos	4	Inmediatamente después de 4 horas de ocurrido el incidente disruptivo	Gerente de Producción y Servicios
Aplicaciones / bases de datos:				
Oracle 11g	Gestor de Base de datos	2	Inmediatamente después de	Representante legal de la

	Oracle 11g		ocurrido el incidente disruptivo	Empresa Teradata
Microsoft SQL Server 2005	Gestor de Base de datos SQL Server 2005	2	Inmediatamente después de ocurrido el incidente disruptivo	Representante legal de la Empresa IBM
Office 2010	Paquetes de Licencias corporativas adquirida por el Banco	4	Inmediatamente después de 4 horas de ocurrido el incidente disruptivo	Representante legal de la Empresa Kruger
Correo electrónico exchange	Correo electrónico corporativo enterprise	2	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo	Jefe de Servidores
PeopleSoft	Gestor de casos y reportes	4	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo	Representante legal de la Empresa IBM
Business intelligence	Software para gestión de la información del Banco	2	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo	Representante legal de la Empresa IBM
SharePoint	Software para colaboración del Banco	2	Inmediatamente después de 4 horas de ocurrido el incidente disruptivo	Representante legal de la Empresa Desca
Datos almacenados en				

formato electrónico:				
Copia de respaldo de configuración de los servidores y bases de datos	Almacenados en un Servidor del Centro de Computo bajo seguridades informáticas	2	Inmediatamente después de ocurrido el incidente disruptivo	Jefe de Centro de Computo
Arquitectura de conexiones IT	Almacenado en un repositorio/server con seguridades	1	Inmediatamente después de ocurrido el incidente disruptivo	Jefe de Servidores
Manuales digitales de los servidores, aplicativos y bases de datos	Almacenado en un repositorio/server con seguridades	1	Inmediatamente después de ocurrido el incidente disruptivo	Representante legal de la Empresa IBM
Paquete instalador de los gestores de bases de datos utilizados en la institución	Almacenados en un Servidor del Centro de Computo bajo seguridades informáticas	2	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo	Jefe de Servidores
Instaladores de los sistemas	Almacenados en un Servidor del Centro de	2	Inmediatamente después de 1 hora de ocurrido el incidente	Jefe de Servidores

operativos manejados en la institución y de las herramientas administrativas, financieras y tecnológicas de gestión de aplicaciones	Computo bajo seguridades informáticas		disruptivo	
Datos almacenados en papel:				
Arquitectura de conexiones IT	Archivador de Jefatura y Administrador de Servidores	2	Inmediatamente después de ocurrido el incidente disruptivo	Jefe de Servidores
Manuales impresos para la configuración de servidores, aplicaciones y	Archivador de Jefaturas de Servidores y Soporte Técnico	2	Inmediatamente después de ocurrido el incidente disruptivo	Jefe de Servidores

bases de datos				
Contactos internos y externos para la gestión de TI	Archivador de Jefaturas de Mesa de Servicios y Analista de Soluciones	2	Inmediatamente después de ocurrido el incidente disruptivo	Jefe de Servidores
Equipos de TI y comunicaciones:				
PCs de escritorio	AllOne Core i7 2.4 GHz, 8 GB de memoria ram, disco duro sata de 1TB, 2 monitores LCD, teclado completo y mouse.	16	Inmediatamente después de ocurrido el incidente disruptivo	Jefe Administrativo
Laptop	AllOne Core i5 3.0 GHz, 8 GB de memoria ram, disco duro de 500 GB	2	Inmediatamente después de ocurrido el incidente disruptivo	Jefe Administrativo
Servidor de Monitoreo	Servidor físico Lenovo i7, 2.4 GHz, 8 GB de memoria ram, disco duro sata de 500 GB.	4	Inmediatamente después de 4 horas de ocurrido el incidente disruptivo	Jefe Administrativo
Servidor de Aplicaciones	Servidor virtual ubicado en el Data Center, Intel	30	Inmediatamente después de ocurrido el incidente disruptivo	Representante legal de la Empresa IBM

	Xeon 2.9 GHz, 8 GB de memoria ram, disco duro SCSI de 500 GB, Windows server 2008 R2			
Impresora	Xerox workcentre	3	Después de 24 horas de ocurrido el incidente disruptivo	Jefe Administrativo
Teléfono	Teléfono IP Alcatel 4038	16	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo	Jefe Administrativo
Teléfono Celular	BlackBerry Curve, con paquete de datos	10	Inmediatamente después de ocurrido el incidente disruptivo	Jefe Administrativo
Canales de comunicación:				
Líneas fijas de teléfono	Líneas habilitadas de telefonía fija con salida a celulares	6	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo	Jefe Administrativo
Líneas celulares	Teléfonos celulares habilitados con paquetes de voz, datos y salida internacional	10	Inmediatamente después de ocurrido el incidente disruptivo	Jefe Administrativo

Acceso a internet	Enlace dedicado fibra óptica de 35Mbps	2	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo	Jefe de Comunicaciones
Correo electrónico	Servidor de correo con cuentas habilitadas, con capacidad de 5 MB	4	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo	Jefe de Servidores
Otros equipos:				
Televisor	Televisor Panasonic de 42"	1	Inmediatamente después de 4 horas de ocurrido el incidente disruptivo	Jefe Administrativo
Instalaciones e infraestructura:				
Puntos de Red de computadoras	Red LAN de cableado vertical y horizontal categoría 6a	16	Inmediatamente después de 1 hora de ocurrido el incidente disruptivo	Jefe de Comunicaciones
BackBone de equipos de Core Bancario	Red LAN, SAN de cableado de Fibra Óptica	50	Inmediatamente después de ocurrido el incidente disruptivo	Jefe de Comunicaciones
Muebles de oficina	Sillas y escritorios individuales para uso del	20	Inmediatamente después de 1 hora de ocurrido el incidente	Jefe Administrativo

	personal técnico		disruptivo	
Servicios externos:				
Electricidad	Alimentación eléctrica de la red pública	2	Inmediatamente después de ocurrido el incidente disruptivo	Jefe Administrativo
Agua potable	Servicio de agua potable	1	Inmediatamente después de ocurrido el incidente disruptivo	Jefe Administrativo
Oficinas	Renta de Oficinas para uso del personal de Comunicaciones	1	Inmediatamente después de ocurrido el incidente disruptivo	Jefe Administrativo
Servicios de soporte del proveedor correspondiente	Servicio de soporte de las empresas proveedoras de los aplicativos	1	Inmediatamente después de ocurrido el incidente disruptivo	Jefe de Servidores

Adaptado de: (Kosutic, 2015).

Pasos de recuperación para la actividad

Esta actividad se debe recuperar de la siguiente forma:

Tabla 105. Pasos de recuperación - Disponibilidad de los Aplicativos Administrativos, Financieros y Tecnológicos.

Procedimientos de recuperación (pasos principales / tareas individuales)	Personas responsables de la implementación	Comunicación (contenido, destinatario)	Registro de implementación (fecha / hora)
1. Reunión del equipo en la ubicación alternativa			
1.1 Verificar si todos los miembros del equipo se encuentran presentes	Auxiliar de recuperación	Verificación realizada con éxito por medio de la toma de asistencia, Gerente de recuperación	ND
1.2 Informar a los miembros del equipo del incidente disruptivo ocurrido	Gerente de recuperación	Comunicación publicada con éxito, Gabinete de crisis	
1.3 Dar directrices puntuales necesarias a los miembros del equipo	Coordinador de recuperación	Comunicación de directrices, Gabinete de crisis	
2. Verificación y recuperación de la infraestructura y muebles básicos			
2.1 Verificar si se cuenta con la infraestructura necesaria para iniciar la	Supervisor de recuperación	Verificación de infraestructura realizada con éxito,	

recuperación de la actividad		Coordinador de recuperación	
2.2 Levantar un informe de la infraestructura disponible y de la infraestructura faltante necesaria	Supervisor de recuperación	Informe de infraestructura realizado con éxito, Coordinador de recuperación	
2.3 Instalación de muebles básicos necesarios para iniciar la recuperación	Auxiliar de recuperación	Instalación de muebles realizada con éxito, Supervisor de recuperación	
3. Verificación y recuperación de los equipos y vínculos de TIC			
3.1 Verificar si se cuenta con los equipos y vínculos necesarios para iniciar la recuperación de la actividad	Operador de recuperación	Verificación de equipos y vínculos realizada con éxito, Supervisor de recuperación	
3.2 Levantar un informe sobre los equipos faltantes (si los hubiera) y de cuál es la capacidad operativa con los equipos actuales	Operador de recuperación	Informe de equipos realizado con éxito, Supervisor de recuperación	
3.3 Poner operativos los equipos necesarios para	Supervisor de recuperación	Equipos puestos en	

iniciar la recuperación de la actividad		operación, Coordinador de recuperación	
4. Verificación y recuperación de aplicaciones			
4.1 Verificar si se cuenta con las aplicaciones y los instaladores de estas para iniciar la recuperación de la actividad	Operador de recuperación	Verificación de las aplicaciones e instaladores realizada con éxito, Supervisor de recuperación	
4.2 Poner en marcha las aplicaciones necesarias para la recuperación de la actividad	Supervisor de recuperación	Puesta en marcha de aplicaciones necesarias, Coordinador de recuperación	
4.3 Levantar un informe sobre el funcionamiento de las aplicaciones puestas en marcha y la carga de trabajo que pueden soportar	Supervisor de recuperación	Informe sobre funcionamiento de aplicaciones realizado con éxito, Coordinador de recuperación	
5. Verificación y recuperación de datos y documentos (en formato electrónico o papel)			

5.1 Verificar si se cuenta con los datos y documentos necesarios para iniciar la recuperación de la actividad	Operador de recuperación	Verificación de datos y documentos realizado con éxito, Supervisor de recuperación	
5.2 Poner a disposición de las personas correspondientes los datos y los documentos necesarios para iniciar la recuperación de la actividad	Operador de recuperación	Datos y documentos entregados al personal correspondiente, Supervisor de recuperación	

Adaptado de: (Kosutic, 2015).

Gestión de registros guardados en base a este documento

Tabla 106. Registros guardados de las principales características del documento - Disponibilidad de los Aplicativos Administrativos, Financieros y Tecnológicos.

Nombre del registro	Ubicación de archivo	Persona responsable del archivo	Controles para la protección del registro	Tiempo de retención
Registro de implementación de pasos de recuperación (registro en papel)	Archivo del Gerente de recuperación	Gerente Nacional de Tecnología	Los registros se guardan en un gabinete con llave	3 años

Validez y gestión de documentos

Este documento es válido desde el 03 de Agosto del 2015.

Este documento, junto con todos los documentos adicionales, es archivado de la siguiente forma:

- El documento en papel se archiva en las siguientes ubicaciones: Centro de crisis y todas las ubicaciones alternativas para actividades
- El documento en formato electrónico se archiva en la siguiente ruta: \\SRVTECH\SGCN\PLAN_DE_RESPUESTA_A_INCIDENTES\Anexo 6.6 Apendice_6c_Plan de recuperación para la disponibilidad de Aplicaciones Financieras, Administrativas y Tecnológicas.

El propietario de este documento es el Gerente Nacional de Tecnología, que debe verificar, y si es necesario actualizar, el documento por lo menos una vez al año.

Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- Cantidad de medidas correctivas de acuerdo a los ejercicios realizados.
- Cantidad de medidas correctivas en base a la implementación del plan en una crisis.
- En caso de crisis, si la recuperación se consiguió dentro de los objetivos de tiempo de recuperación.

Documentos adicionales

- Documentación técnica de los equipos para los Aplicativos Financieros, Administrativos y Tecnológicos (Servidores, bases de datos, Switches, routers, firewalls, IPs).
- Planes de recuperación detallados para los sistemas individuales de TIC.

- Instrucciones de funcionamiento de los equipos utilizados para Aplicativos Financieros, Administrativos y Tecnológicos, hardware en general.

Gerente Nacional de Tecnología

Ing. Santiago Pazmiño

_____

Firma

ANEXO 7

Historial de modificaciones

Anexo 7: Plan de prueba y verificación

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
03/08/2015	1.0	Vinicio Sarabia	Creación de la primera versión del documento

Tabla de contenido

Objetivo, alcance y usuarios

El objetivo de este Plan es determinar la frecuencia y los métodos de verificación para evaluar la factibilidad de las medidas y de los arreglos para la gestión de la Continuidad del Negocio, como también para establecer las acciones correctivas necesarias.

Este Plan se aplica a todos los elementos que se encuentran dentro del alcance del SGCN, incluyendo los arreglos con los proveedores y socios.

Los usuarios de este documento son todas las personas que cumplen una función en el SGCN.

Implementación de pruebas y verificaciones

La prueba y verificación de Continuidad del Negocio se implementará en el Banco KLM de la siguiente manera:

- Plazo: desde el 05 de Septiembre hasta el 07 de Septiembre del 2015.
- El Gerente de Producción y Servicios es la persona responsable de la coordinación e implementación de la prueba y verificación.
- Los objetivos de la prueba y verificación son los siguientes:
    - Verificar si los planes y recursos son precisos para:
    - Implementar planes de recuperación para cada actividad.
    - Verificar si los empleados responsables de la recuperación están familiarizados con los detalles del plan.
    - Verificar la implementación de todos los pasos especificados en los planes.
    - Cumplir con todas las obligaciones dentro de los plazos predefinidos.
    - Activar procedimientos alternativos en caso que sea necesario.
    - Asegurar todos los recursos necesarios (incluyendo la recuperación de datos).
    - Permitir los procedimientos de comunicación y aviso entre miembros de un equipo determinado, con otros equipos de recuperación, con el Gabinete de crisis y con otras partes interesadas
    - Lograr la armonización con los planes de recuperación de otras actividades.

- Generar comentarios o sugerencias para mejorar los planes.

- Alcance de la prueba y verificación: Se validará el funcionamiento de los servicios de:
    - Comunicaciones
    - Aplicativos de Core Bancario y Negocios
    - Aplicativos Financieros, Administrativos y Tecnológicos

- La operatividad de los servicios y actividades incluyen también a los proveedores del Banco KLM:
    - Telconet
    - Cnt
    - Level3
    - AT&T
    - Claro
    - Empresa eléctrica
    - Todouno
    - IBM
    - Kruger
    - TATA
    - Qmatic
    - IBM
    - Desca
    - Teradata

- Método de prueba y verificación:
    - Chequeo de escritorio: chequeo de los planes con técnicas de auditoría, validación y verificación; realizado por el autor del plan y un moderador.
    - Repaso de los planes: chequeo de los planes a través de interacción de equipos; realizada por los principales participantes

del plan y por el moderador, cuya interacción se verifica en una reunión conjunta.

- Simulación: verificación de todos los planes relacionados (incluyendo los procedimientos de proveedores) con recursos de información reales pero sin necesidad de relocalización en la ubicación alternativa; realizado por todos los empleados necesarios, proveedores y por el moderador.

- Prueba funcional: se reubican las actividades en la ubicación alternativa bajo un ejercicio controlado (anunciado); participan todos los empleados necesarios, proveedores, el moderador y observadores.

- Prueba completa: se trasladan todas las actividades desde la ubicación original a la alternativa (anunciado o no); participan todos los empleados necesarios, proveedores, el moderador, observadores y auditores.

- Reducción del riesgo de que la prueba y verificación interfieran con las actividades comerciales habituales, para ello se basará en una capacitación adecuada al personal y la confirmación del funcionamiento de los sistemas tecnológicos críticos en alta disponibilidad.

  - ¿Se anunciarán las pruebas y verificaciones? [SÍ/NO]

  - Escenario sobre el que se basará la prueba y verificación

  - Proceso de verificación detallado en el informe de prueba y verificación

Revisión de resultados

El Gerente de Producción y Servicios debe controlar los resultados de las pruebas y debe preparar un Informe de prueba y verificación.

En el Informe se deben incluir las acciones correctivas correspondientes, como también otras recomendaciones de mejora.

Gestión de registros guardados en base a este documento

Tabla 107. Registros guardados de la revisión de resultados.

Nombre del registro	Ubicación de archivo	Persona responsable del archivo	Controles para la protección del registro	Tiempo de retención
Informe de prueba y verificación (en formato electrónico)	Ordenador del Gerente de Producción y Servicios	Gerente de Producción y Servicios	Solamente el Gerente de Producción y Servicios puede editar la lista	3 años

Validez y gestión de documentos

Este documento es válido desde el 03 de Agosto del 2015.

El propietario de este documento es el Gerente de Producción y Servicios.

Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- Cantidad de acciones correctivas encontradas.
- Efecto negativo sobre las actividades comerciales habituales debido a la prueba y verificación.
- ¿La prueba y verificación abarca todo el alcance del SGCN?
- Porcentaje de personal involucrado en la prueba y verificación.

Apéndice

Formulario: Informe de prueba y verificación

Gerente de Producción y Servicios

Ing. Luis Arevalo

_____

Firma

ANEXO 7.1

Formulario para Informe de prueba y verificación

Anexo 7.1: Plan de prueba y verificación

Apéndice 1: Formulario para Informe de prueba y verificación

La prueba y verificación se realizó de la siguiente manera:

- Plazo: desde el 05 de Septiembre del 2015 hasta el 07 de Septiembre del 2015.
- Persona responsable de la coordinación e implementación de la prueba y verificación: Gerente de Producción y Servicios
- Alcance de la prueba y verificación: La prueba se enfocó en el Área de Infraestructura Tecnológica, actuando el Gerente de Producción y Servicios y todos los empleados de esta Área. Además intervino los proveedores de datos Todouno y de Software de Seguridad IBM
- Método de prueba y verificación: Simulacro piloto
- ¿Se anunció la prueba y verificación? SÍ
- Proceso de verificación:

Escenario: Ataque de código malicioso

Siguiendo el plan de respuesta a los incidentes el personal realizó lo siguiente:

- Paso 1: Un empleado de TIC recibe información sobre el incidente.
    - Problema encontrado: ninguno.
- Paso 2: Como se trataba de un código malicioso desconocido, se notificó al Subgerente de Control Tecnológico.
    - Problema encontrado: ninguno.
- Paso 3: Se notificó al fabricante del software antivirus y proveedor del antivirus.

    - Problema encontrado: no se obtiene respuesta del proveedor del software antivirus.

- Paso 4: Se notificó a los empleados que intercambiaron mensajes con el sistema infectado.

    - Problema encontrado: ninguno.

- Paso 5: Se consultó a ciertos proveedores de servicios de TI y proveedores de software.

    - Problema encontrado: ninguno.

- Paso 6: Se dispuso a todos los empleados que poseen sus computadores infectados que desconecten físicamente la red, desactiven las redes inalámbricas, bluetooth, etc.

    - Problema encontrado: usuarios gerenciales resistentes a desconectarse

- Paso 7: El personal de TIC consideró necesario restringir todo el tráfico de datos/red para los usuarios con computadores infectados

    - Problema encontrado: los usuarios se vieron afectados, por la restricción y bloqueo a la red corporativa

- Paso 8: Los ordenadores que todavía no habían sido desconectados de la red, los empleados de la TIC se encargaron de evaluar si lo desconectaban para evitar mayor infección, además de desactivar las conexiones inalámbricas.

    - Problema encontrado: ninguno.

- Paso 9: Los empleados de TIC consideraron necesario notificar a los usuarios de los sistemas informáticos sobre la gravedad de la infección.

    - Problema encontrado: ninguno

-

- Paso 10: Los empleados de TIC consiguieron información (internet, proveedores) sobre códigos maliciosos muy parecidos que dieron pauta mediante los pasos necesarios a su erradicación, lo cuáles fueron ejecutados en todos los computadores infectados, incluso en los servidores.

    - Problema encontrado: ninguno.

Logro de los objetivos de prueba:

Tabla 108. Datos principales de prueba piloto – Ataque de código malicioso.

Objetivos de prueba:	Logro de objetivos (1: objetivo no alcanzado; 2: objetivo alcanzado parcialmente; 3: objetivo alcanzado)
Probar la preparación de los empleados de TIC y los usuarios finales ante infecciones de software	Objetivo alcanzado
Adquirir conocimientos mediante la investigación sobre como erradicar códigos maliciosos	Objetivo alcanzado

En base a los resultados de la prueba, se iniciaron las siguientes medidas correctivas:

Se realiza el trámite para la renovación de las licencias del software antivirus.

Recomendaciones:

Colocar los usuarios informáticos inalámbricos en un servidor aislado, para evitar infecciones que ingresen vía inalámbrica por PCs contaminadas en otro sitio.

Escenario: Falla en Telecomunicaciones

Siguiendo el plan de respuesta a los incidentes el personal realizó lo siguiente:

- Paso 1: Verifica si todos los equipos de comunicación se encuentran encendidos.
    - Problema encontrado: ninguno.
- Paso 2: Verifica si los cables se encuentran conectados y en los sitios correctos.
    - Problema encontrado: faltan etiquetas en algunos de los cables (temporales), lo que dificulta la tarea de revisión.
- Paso 3: Reinicia los equipos de comunicación por si se han inhibido.
    - Problema encontrado: algunos equipos mantienen su alta disponibilidad de servicios sobre el mismo hardware.
- Paso 4: Verifica la configuración de los equipos de comunicación para identificar y corregir posibles problemas.
    - Problema encontrado: el servidor de monitoreo se encuentra en estado intermitente, posiblemente tiene un daño en la tarjeta de video, lo cual ocasiona intermitencias de video continuas y un monitoreo ineficiente.
- Paso 5: Si es necesario, coordina el proceso con proveedores de servicios de TI.
    - Problema encontrado: ninguno.
- Paso 6: Los usuarios de este servicio usan medios de comunicación alternativos.

- Problema encontrado: las comunicaciones para algunos servicios son inevitablemente suspendidas mientras se reinicia el equipo.

Logro de los objetivos de prueba:

Tabla 109. Datos principales de prueba piloto – Falla en Telecomunicaciones.

Objetivos de prueba:	Logro de objetivos (1: objetivo no alcanzado; 2: objetivo alcanzado parcialmente; 3: objetivo alcanzado)
Identificar problemas al detectar fallas en los equipos de Comunicaciones	Objetivo alcanzado
Diagnosticar y dar respuesta o solución inmediata a las fallas encontradas para restablecer los servicios de Comunicaciones	Objetivo alcanzado
Probar la disponibilidad de personal calificado por la empresa proveedora de servicios de TI, en caso de que el personal interno no encuentre solución a la falla del servicio	Objetivo alcanzado parcialmente
Detectar problemas en el uso de las vías alternativas de Comunicaciones	Objetivo alcanzado

En base a los resultados de la prueba, se iniciaron las siguientes medidas correctivas:

- Etiquetar los cables de conexiones temporales, que no contienen su respectiva descripción.
- Enlistar medios de comunicaciones alternativos, y servicios afectados por cada appliance

Recomendaciones:

- Adquisición de nuevos equipos de monitoreo

En Quito, 07 de Septiembre del 2015.

Gerente de Producción y Servicios

Ing. Luis Arevalo

_____

Firma

ANEXO 8

Formulario de revisión post incidente

Anexo 8: Formulario de revisión post incidente

Tabla 110. Formulario de revisión post incidente.

Fecha del incidente:	
Número de incidente en el Registro de incidentes:	
Tipo de incidente:	
Descripción del incidente:	
Causa del incidente:	
Adecuación de respuesta de la dirección al incidente: (1: la dirección no respondió o respondió insatisfactoriamente; 2: la dirección respondió pero no respetó los planes en su totalidad; 3: la dirección respondió completamente de acuerdo a los planes)	
¿Qué planes de recuperación se activaron?	
¿Hasta qué punto se alcanzaron los objetivos de tiempo de recuperación? (1: para ninguna de las actividades; 2: sólo para algunas actividades; 3: para todas las actividades)	
Nivel de preparación de los empleados para el incidente: (1: completamente sin preparación, 2: parcialmente preparados, 3: totalmente preparados)	
Mejoras necesarias: Referencia al Formulario para acciones correctivas y preventivas	

Tomado de: (Kosutic, 2015).

Gerente de Producción y Servicios

Ing. Luis Arévalo

_____

Firma

ANEXO 9

Plan de mantenimiento y revisión del SGCN

Anexo 9: Plan de mantenimiento y revisión del SGCN

Para mantener la exactitud y utilidad de todos los elementos del SGCN, es necesario revisarlos y actualizarlos de acuerdo a las siguientes frecuencias:

Tabla 111. Plan de mantenimiento y revisión.

Elemento del SGCN	Enero	Febrero	Marzo	Abril	Mayo	Junio	Julio	Agosto	Septiembre	Octubre	Noviembre	Diciembre
Actualización de software, IOS de equipos de Comunicaciones		X						X				
Limpieza de equipos de Comunicaciones				X						X		
Actualización de	X						X					

software, SO de equipos de Servidores, bases de datos												
Limpieza de equipos de Servidores, bases de datos			X						X			

Nota: El Gerente de Producción y Servicios es el responsable de este plan, archivado en la ruta \\SRVTECH\SGCN\PLAN_DE_MANTENIMIENTO_Y_REVISION; y esa persona tiene un derecho exclusivo para editar y modificar el documento; este registro se debe guardar por 3 años.

ANEXO 10

Procedimiento para Auditoría Interna

Banco KLM

Banco KLM Compañía Anónima

Anexo 10: Procedimiento para Auditoría Interna

Código:	PRO-TI-2015-08
Versión:	1.0
Fecha de la versión:	3 de Agosto del 2015
Creado por:	Ing. Vinicio Sarabia
Aprobado por:	Ing. Santiago Pazmiño
Nivel de confidencialidad:	Medio

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
03/08/2015	1.0	Vinicio Sarabia	Creación de la primera versión del documento

Tabla de contenido

Objetivo, alcance y usuarios

El objetivo de este procedimiento es describir todas las actividades relacionadas con la auditoría: redacción del programa de auditoría, selección del auditor, realización de auditorías individuales e informes.

Este procedimiento se aplica a todas las actividades realizadas dentro del Sistema de Gestión de Continuidad del Negocio (SGCN).

Los usuarios de este documento son los miembros de la alta gerencia del Banco KLM y los auditores internos.

Documentos de referencia

- Norma ISO/IEC 27001, clausula 6, punto A.6.1.8
- Norma ISO 22301, punto 9.2
- Política del sistema de gestión de seguridad de la información
- Política de la gestión de Continuidad del Negocio
- Procedimiento para acciones correctivas y preventivas

Auditoría interna

Objetivo de la auditoría interna

El objetivo de la auditoría interna es determinar si los procedimientos, controles, procesos, acuerdos y demás actividades dentro del SGCN concuerdan con las normas ISO 27001 e ISO 22301, con las regulaciones correspondientes y con la documentación interna de la organización; como

también verificar si son implementados y sostenidos y si cumplen requisitos de políticas y establecen objetivos.

Planificación de la auditoría interna

El Gerente Nacional del Centro de Servicios aprueba un programa anual de auditorías internas, redactado como se detalla en el formulario del Apéndice 1 (ver Anexo 10.1).

Se deben realizar una o más auditorías internas en el transcurso de un año, asegurando una cobertura acumulativa de todo el alcance del SGCN. Las auditorías internas son planificadas en base a la evaluación de riesgos, como también por los resultados de auditorías anteriores. Generalmente son realizadas antes de la revisión por parte de la gerencia.

El Programa anual de auditoría interna debe incluir la siguiente información sobre cada auditoría interna individual:

- Momento de la auditoría: El mes de Septiembre 2015
- Alcance de la auditoría: Área de Infraestructura Tecnológica
- Criterio de auditoría: Normas ISO 22301 e ISO 27001.
- Métodos de la auditoría: Revisión de documentación, entrevistas con empleados, revisión de registros, de sistemas informáticos, etc.
- Quién realizará la auditoría: Auditor interno del Banco KLM.

Se debe llevar un registro de las auditorías realizadas en el Programa anual de auditoría interna.

Designación de auditores internos

El Gerente Nacional del Riesgos debe designar a los auditores internos.

Un auditor interno puede ser alguien de la organización o una persona externa a la misma. Los criterios para la designación de los auditores son:

- Que conozca las normas ISO/IEC 27001 e ISO 22301.
- Que esté familiarizado sobre técnicas de auditoría sobre sistemas de gestión.
- Que sepa cómo funcionan las tecnologías de la información y de la comunicación como para estar familiarizado con el objetivo de los sistemas individuales y también con los impactos sobre procedimientos de seguridad y/o Continuidad del Negocio.

Se debe seleccionar a los auditores internos de tal forma de garantizar objetividad e imparcialidad; es decir, de evitar el conflicto de intereses, ya que los auditores no pueden auditar su propio trabajo.

Se recomienda que los auditores internos realicen un curso para auditores internos según la norma ISO/IEC 27001 e ISO 22301.

Realización de auditorías internas individuales

Las personas responsables de las auditorías internas individuales están identificadas en el Programa anual de auditoría interna. Si una auditoría es realizada por un equipo de varios auditores, la persona responsable de la auditoría es aquella que está indicada como Líder de equipo de auditoría.

Durante la realización de una auditoría interna se deben tener en cuenta los siguientes puntos:

- El criterio establecido en el Programa anual de auditoría interna.
- Los resultados de auditorías internas o externas anteriores.
- Los resultados de la evaluación de riesgos, de la implementación de controles, del análisis de impacto en los negocios, etc.

Se deben documentar los siguientes elementos como resultado de la auditoría interna:

- Informe de auditoría interna, debe ser enviado al Gerente Nacional de Riesgos

- Las posibles acciones correctivas deben ser documentadas en el Formulario para acciones correctivas o preventivas, de acuerdo a lo establecido en el Procedimiento para acciones correctivas y preventivas.

Actividades de seguimiento

La persona responsable de la auditoría debe monitorear la implementación de las acciones correctivas identificadas durante la auditoría, debe verificar que esas acciones se hayan implementado adecuadamente y dentro de los plazos establecidos y debe informar los resultados al Gerente Nacional de Riesgos.

Gestión de registros guardados en base a este documento

Tabla 112. Gestión de registros guardados en base a este documento de Auditoría Interna.

Nombre del registro	Ubicación de archivo	Persona responsable del archivo	Controles para la protección del registro	Tiempo de retención
Programa anual de auditoría interna (en formato electrónico)	Ordenador del Gerente Nacional de Riesgos	Gerente Nacional de Riesgos	Solamente el Gerente Nacional de Riesgos y el auditor interno pueden ingresar datos y modificaciones al Programa anual de auditoría interna.	Los programas son almacenados por el plazo de 3 años.
Informe de auditoría interna (en	Ordenador del auditor interno y	Auditor interno	Los informes son almacenados en versiones de sólo	Los informes son

formato electrónico)	del Gerente Nacional de Riesgos		lectura en formato PDF.	almacenados por el plazo de 3 años.

Tomado de: (Kosutic, 2015).

Solamente el Gerente Nacional de Riesgos puede otorgar a otros empleados el derecho de acceso al Programa anual de auditoría interna y al Informe de auditoría interna.

Validez y gestión de documentos

Este documento es válido desde el 03 de Agosto del 2015.

El propietario de este documento es el Gerente Nacional de Riesgos, que debe verificar, y si es necesario actualizar, el documento por lo menos una vez al año.

Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- Cantidad de acciones correctivas identificadas durante la auditoría.
- Cantidad de acciones correctivas identificadas durante la auditoría de certificación realizada luego de la auditoría interna.
- Si la frecuencia de auditorías internas coincide con el Programa anual de auditoría interna.

Apéndices

Apéndice 1: Programa anual de auditoría interna

Apéndice 2: Informe de auditoría interna

Gerente Nacional de Riesgos

Ing. Elba Espinoza

_____

Firma

ANEXO 10.1

Programa anual de auditoría interna

Anexo 10.1: Procedimiento para Auditoría Interna

Apéndice 1: Programa anual de auditoría interna

Se redacta este programa anual para el período comprendido desde el..... hasta el.....

Las auditorías internas en el marco de las normas ISO/IEC 27001 e ISO 22301 serán realizadas de la siguiente forma:

Tabla 113. Principales datos del programa anual de auditoría para la evaluación del DRP en el Banco KLM.

Período de la auditoría	Alcance de la auditoría	Criterios de la auditoría	Método de la auditoría	Auditores	Registro de implementación de la auditoría

Tomado de: (Kosutic, 2015).

Auditor General Interno

Ing. Nicolás Ocampos

_____

Firma

ANEXO 10.2

Informe de auditoría interna

Anexo 10.2: Procedimiento para Auditoría Interna

Apéndice 2: Informe de auditoría interna

Tabla 114. Formato de informe de auditoría interna.

Fecha del informe:		
Período de la auditoría interna:		
Quién realizó la auditoría interna:		
Criterios de la auditoría:		
Alcance de la auditoría:		
Seguimiento de la auditoría:		
Recomendaciones de mejora:		
Resultados: Cantidad total de no-conformidades		
No-conformidades identificadas	Referencia cruzada con el Formulario para acciones correctivas	Acción correctiva implementada en

Tomado de: (Kosutic, 2015).

Auditor General Interno

Ing. Nicolás Ocampos

_____

Firma

ANEXO 11

Minutas de Revisión por parte de la dirección

Anexo 11: Minutas de Revisión por parte de la dirección

La reunión del Comité fue realizada el..... y asistieron las siguientes personas:

- .....

El objetivo de la reunión fue revisar la conveniencia, adecuación y eficacia del Sistema de Gestión de Continuidad del Negocio.

Los materiales o información revisados en la reunión fueron los siguientes:

1. [Nombre y fecha del informe de auditoría interna], [nombre y fecha del informe de auditoría externa], [nombres y fechas de otras revisiones internas, como también de revisiones sobre proveedores o socios]
2. [Documento o descripción del feedback recibido de las partes involucradas]
3. [Documento o descripción de los métodos, productos o procedimientos, como también de las nuevas buenas prácticas y lineamientos, que se pueden utilizar para mejorar la eficacia del SGCN]
4. [Información sobre el nivel de riesgo residual y nivel de riesgo aceptable]
5. Estado de las acciones preventivas y correctivas
6. [Documento o descripción de las amenazas y vulnerabilidades que no fueron tenidas en cuenta durante la evaluación de riesgos]
7. [Documento o descripción del control y evaluación de medición de resultados]
8. Estado de las actividades de seguimiento que deberían haberse tomado luego de la revisión por parte de la dirección

9. [Documento o descripción de modificaciones en temas internos y externos que podrían haber afectado al SGCN]
10. [Documento o descripción de recomendaciones de mejora, incluidos cambios sobre la Política y objetivos del SGCN]
11. [Nombre y fecha del informe sobre realización y prueba de resultados]
12. [Descripción de nuevas buenas prácticas que hayan surgido]
13. [Nombre y fecha del informe o documento sobre la revisión realizada luego de un incidente disruptivo]
14. [Resultados de los programas de capacitación y concienciación]

En la reunión se tomaron las siguientes decisiones:

1. [Descripción de modificaciones en el alcance del SGCN]
2. [Descripción de acciones para la mejora de la eficacia del SGCN]
3. [Descripción de cómo se deben actualizar la evaluación de riesgos, el análisis del impacto en el negocio, los planes de Continuidad del Negocio y el plan de tratamiento del riesgo]
4. [Descripción de modificaciones realizadas a la documentación y/o controles que fueron necesarios a raíz de cambios internos o externos]
5. [Descripción de los recursos aprobados para la implementación]
6. [Necesidades de financiación o de elaboración de un presupuesto]
7. [Descripción de cómo se deben mejorar las mediciones de eficacia]
8. [Detalle de las partes interesadas a las que es necesario comunicar las decisiones tomadas sobre esta reunión de Revisión por parte de la dirección]

Auditor General Interno

Ing. Nicolás Ocampos

_____

Firma

ANEXO 12

Procedimiento para acciones Correctivas y Preventivas

Banco KLM

Banco KLM Compañía Anónima

Anexo 12: Procedimiento para acciones Correctivas y Preventivas

Código:	PRO-TI-02-2015-08
Versión:	1.0
Fecha de la versión:	3 de Agosto del 2015
Creado por:	Ing. Vinicio Sarabia
Aprobado por:	Ing. Santiago Pazmiño
Nivel de confidencialidad:	Alto

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación
03/08/2015	1.0	Vinicio Sarabia	Creación de la primera versión del documento

Tabla de contenido

Objetivo, alcance y usuarios

El objetivo de este procedimiento es describir todas las actividades relacionadas con la iniciación, implementación y mantenimiento de registros correcciones y de acciones correctivas y preventivas.

Este procedimiento se aplica a todas las actividades implementadas dentro del Sistema de Gestión de Continuidad del Negocio (SGCN).

Los usuarios de este documento son todos los empleados del Banco KLM.

Documentos de referencia

- Norma ISO/IEC 27001, clausula 8
- Norma ISO 22301, punto 10.1
- Política de la gestión de Continuidad del Negocio
- Procedimiento para auditoría interna
- Procedimiento para gestión de incidentes

Correcciones y acciones correctivas

No conformidades y correcciones

Una no-conformidad es todo incumplimiento de los requerimientos de las normas, documentación interna, reglamentos, obligaciones contractuales y de otra clase dentro del SGCN. Las no conformidades pueden ser identificadas durante una auditoría interna o externa, en base a resultados de la revisión por parte de la dirección, luego de incidentes, durante el transcurso normal de las operaciones de negocios o en cualquier otra situación.

Un empleado que detecta una no conformidad debe tomar acciones inmediatamente para controlarla, contenerla y corregirla y para contener sus consecuencias. Si un empleado no es responsable de esa no conformidad debe transmitir la información sobre ella a la persona responsable que pueda corregirla.

Acciones correctivas

La persona responsable debe evaluar la necesidad de eliminar el origen de la no conformidad y evitar su recurrencia tomando acciones correctivas.

Una acción correctiva puede ser iniciada por cualquier empleado o, cuando sea pertinente, por cualquier cliente, proveedor o socio de la organización. Una acción correctiva puede demandar cambios sobre cualquier documento, proceso o acuerdo dentro del marco del SGCN.

Implementación de acciones correctivas

Una acción correctiva se implementa de la siguiente forma:

Tabla 115. Pasos para la implementación de una acción correctiva.

Pasos	Persona responsable de la implementación
1. Revisión de la no conformidad	Cualquiera con una función dentro del SGCN
2. Determinación de la causa de la no-conformidad	Persona responsable del área donde se ha identificado la no-conformidad
3. Identificar si la no conformidad	Persona responsable del área donde

ya existía	se ha identificado la no-conformidad
4. Evaluación de la necesidad de tomar acciones para eliminar la no-conformidad	Persona responsable del área donde se ha identificado la no-conformidad
5. Determinación de las acciones necesarias para eliminar las causas de la no-conformidad y para asegurar que no se produzca nuevamente	Persona responsable del área donde se ha identificado la no-conformidad
6. Implementación de las acciones planificadas	Persona a cargo de la implementación, designada por la persona responsable
7. Revisión para determinar si la acción tomada logró eliminar las causas de la no-conformidad	Subgerente de Control Tecnológico
8. Informar a todas las personas involucradas que se ha implementado la acción correctiva	Persona a cargo de la implementación, designada por la persona responsable

Tomado de: (Kosutic, 2015).

Cada uno de los pasos anteriores debe quedar registrado en el formulario de acciones correctivas o preventivas.

Acciones preventivas

Introducción

El objetivo de la acción preventiva es evitar los efectos no deseados determinando las actividades orientadas a eliminar la causa de potenciales no-conformidades para evitar su ocurrencia.

Implementación de acciones preventivas

Las acciones preventivas que son identificadas durante la evaluación de riesgos y el análisis del impacto en el negocio generalmente son detalladas en el Plan de tratamiento del riesgo y en el Plan de preparación para Continuidad del Negocio.

Las acciones preventivas no atendidas en los documentos mencionados anteriormente se implementan de la misma forma que la detallada para las acciones correctivas.

Gestión de registros guardados en base a este documento

Tabla 116. Gestión de registros guardados para acciones correctivas y preventivas.

Nombre del registro	Ubicación de archivo	Persona responsable del archivo	Controles para la protección del registro	Tiempo de retención
Procedimiento para acciones correctivas y preventivas	\\SRVTECH\SGCN\PROCEDIMIENTO_PARA_ACCIONES_CORRECTIVAS_Y_PREVENTIVAS	Subgerente de Control Tecnológico	Una vez que se han registrado todos los datos, se debe evitar cualquier ampliación	3 años

Validez y gestión de documentos

Este documento es válido desde el 03 de Agosto del 2015.

El propietario de este documento es el Subgerente de Control Tecnológico, que debe verificar, y si es necesario actualizar, el documento por lo menos una vez al año.

Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- Cantidad de acciones correctivas y preventivas iniciadas
- Cantidad de acciones correctivas y preventivas incompletas
- Cantidad de acciones correctivas y preventivas tomadas sin haber sido registradas en un formulario designado

Apéndices

Apéndice: Formulario para acciones correctivas y preventivas

Subgerente de Control Tecnológico

Msc. Jorge Montenegro

_____

Firma

ANEXO 12.1

Formulario para acciones correctivas y preventivas

Anexo 12.1: Procedimiento para acciones Correctivas y Preventivas

Apéndice 1: Formulario para acciones correctivas y preventivas

Tabla 117. Formulario para el registro de medidas correctivas detectadas durante incidentes disruptivos.

<table>
<tr><td colspan="2">Acción correctiva/preventiva N°.____</td><td>Acción correctiva / Acción preventiva (marcar con un círculo)</td></tr>
<tr><td colspan="3">Descripción de la no-conformidad:</td></tr>
<tr><td>No-conformidad identificada en:</td><td>Nombre de la persona que identificó la no-conformidad</td><td>Firma</td></tr>
<tr><td colspan="3">Causa de la no-conformidad:</td></tr>
<tr><td colspan="3">Si ya existe una no conformidad similar, indique aquí su Acción correctiva N°.</td></tr>
<tr><td colspan="3">Es necesario tomar acciones correctivas/preventivas: SÍ - NO (marcar con un círculo)</td></tr>
<tr><td colspan="3">Acción correctiva/preventiva a implementar:</td></tr>
</table>

¿Quién debe estar informado sobre la acción implementada?:		
Aprobado por	Fecha límite para la implementación	Persona responsable de la implementación
Acción correctiva/preventiva implementada en:		Firma
Efectividad de la acción implementada revisada en:		Firma

Tomado de: (Kosutic, 2015).