Universidad Nacional de Panamá

Universidad Carlos III de Madrid

Vicerrectoría de Investigación y Postgrado de la Universidad de Panamá

MASTER EN GESTIÓN Y TECNOLOGÍA DEL CONOCIMIENTO

PROYECTO

GUÍA DE RECUPERACIÓN ANTE DESASTRES (DRP) PARA UN BANCO EN PANAMÁ ORIENTADO A LOS ATM (CAJEROS AUTOMÁTICOS)

Autor: ENRIQUE GUADAMUZ NÚÑEZ

Cédula: 8-229-2508

Profesor Guía: Doctora Almudena Alcaide Raya
Profesor Titular: Benjamín Ramos

TESIS PRESENTADA COMO UNO DE LOS REQUISITOS PARA OBTENER EL GRADO DE MASTER EN GESTIÓN Y TECNOLOGÍA DEL CONOCIMIENTO

Panamá, República de Panamá
2012

ÍNDICE

CAPÍTULO III

PROCEDIMIENTOS DE RECUPERACIÓN EN LOS SITIOS ALTERNOS

CAPÍTULO IV.
MANTENIMIENTO DEL PLAN DE RECUPERACIÓN DE DESASTRES

LISTADO DE ABREVIATURAS Y TÉRMINOS

Abreviaturas	Descripción y términos
BCP	Sigla en inglés del término "Plan de Continuidad del Negocio" (*Business Continuity Planning*).
DRP	Sigla en inglés del término plan de "Administración de Desastres" (*Disaster Recovery Plan*).
BRP	Sigla en Inglés del término "Plan de Recuperación del Negocio" (*Business Recovery Planning*).
BIA	Sigla en inglés del término "Análisis de Impacto del Negocio" (*Bussiness Impact Analysis*).
TI	Sigla en Inglés del término "Tecnología de la Información" (*Information technology*).
ATM	Sigla en Inglés del término "Cajeros Automáticos" (*Automatic Teller Machine*).
POS	Sigla en inglés del término "Puntos de Ventas" (*Point of Sale*).
RTO	Sigla en inglés del término "Objetivo de Punto de Recuperación" (*Recovery Point Objective*).
Telered	Red privada de cajeros automáticos en Panamá, la cual brinda servicio a todos los bancos como un *switch* de transacciones.
ACH	Sigla en inglés del término "Sistema de Transferencias Electrónicas" (*Automatic Clearing House*).

IDC	Sigla en inglés del término "Infraestructura de Centro de Datos" (*Infrastructure, Data Center*).
FIBRA ÓPTICA	Es un medio de transmisión empleado habitualmente en redes de datos, hilo muy fino de material transparente, vidrio o materiales plásticos.
SLA	Sigla en inglés del término "Acuerdo de Niveles de Servicio" (*Service Level Agreements*).
SPOOL	Sigla en inglés del término que se refiere al proceso mediante el cual la computadora introduce trabajos en un área especial de memoria o un disco (*Simultaneous Peripheral Operations On-Line).*
ADSL	Sigla en inglés del término "Línea Asimétrica de Suscripción Digital" (*Asymmetrical Digital Subscriber Line*).
NETWORKING	Generalmente el término Networking se aplica a la integración de dos sistemas de redes completas.
TAPES BACKUP	Son unidades de respaldo de información.
URL's	Sigla en inglés del término "Localizador Uniforme de Recursos"; se refiere la forma de organizar la información en la Web (*Uniform Resource Locator*).

DNS	Sigla en inglés del término "Nombres del Dominio". Es una asignación en forma jerárquica de una nomenclatura; es utilizada para la conexión de un ordenador a una Red Privada a un Servicio determinado; o bien, para una conexión a Internet.

RESUMEN EJECUTIVO.

El término desastre se define como una desgracia grande, suceso infeliz y lamentable. En el ámbito de la tecnología cuando hablamos de desastre lo definimos de modo más específico, como la interrupción del negocio debido a la pérdida o incapacidad de acceso a los elementos que contienen la información necesaria para la operación normal de la organización.

Para mitigar las consecuencias que podría causar un desastre, nacen los planes de recuperación por desastre; los cuales consisten básicamente en las acciones para recuperarse en caso de que se presente un desastre. Incluye la planeación de pasos para evitar riesgos, mitigarlos o transferirlos a alguien más por medios seguros. El DRP es aplicable a todos los aspectos de un negocio; sin embargo, se utiliza normalmente en el contexto de operaciones para el procesamiento de datos.

La actividad de transacciones a través de los ATM en Panamá mueve una cantidad importante de dinero; por tal motivo, se requiere una alta disponibilidad de los sistemas informáticos que soporten esta operación. Un fallo en los sistemas que soportan estas redes o estas conexiones a la red de ATM o Telered, puede significar pérdidas importantes tanto económicas como de imagen de las instituciones bancarias. Por lo anterior, es importante para los bancos contar con un plan de contingencias, que les permita continuar con el negocio en caso de que se presente un imprevisto que impacte los sistemas que soportan el normal funcionamiento del banco.

El objetivo principal de este proyecto es mostrar a los bancos en Panamá cómo se puede preparar y mantener una guía actualizada de manera dinámica, que permita la creación y activación de un procedimiento de recuperación del sistema informático que soporta las transacciones solicitadas por Telered, donde se encuentran conectados sus ATM, cuando se presente un desastre; ya sea natural o inducido.

EXECUTIVE SUMMARY.

The term disaster is defined as a great misfortune, unhappy and unfortunate event. In the area of technology, when we refer to disaster, we define it specifically as the interruption of business due to the loss of inability to access elements with the necessary information for the regular operation of the organization.

To mitigate the consequences that could cause a disaster, recovery plans were born which consist basically in the steps to be taken in order to recover in the event of a disaster. Includes planning steps to avoid risks, diminish or transfer them to someone else by secure means. DRP is applicable to all aspects of a business, but is normally used in the context of Data processing operations."

The transactions through ATMs in Panama move a significant amount of money, for this reason, a high availability of computer systems to support this operation is required. A failure in the systems that support these networks or these connections to the ATM network or Telered, could mean significant losses both financial and reputational for the banking institutions. Therefore, it is important for banks to have contingency plans that allow them to continue business in the event of an unexpected situation that could impact the systems that support the normal functioning of the bank.

The main objective of this project is to show the banks in Panama how to prepare and maintain a dynamically updated guide that allows the creation and activation of a recovery procedure of the computer systems that support transactions requested by Telered, where their ATMs are connected, given a disaster, either natural or induced.

INTRODUCCIÓN.

Hoy en día las organizaciones están expuestas a múltiples eventos o desastres, que son causantes de interrupciones en la prestación normal del servicio y afectan en forma negativa la imagen y reputación de una organización. Estos eventos tienen múltiples facetas y se pueden presentar de diferentes formas: desastres naturales, provocados por el hombre, pandémicos o tecnológicos.

Los bancos en Panamá están conscientes de la necesidad de mantener la continuidad de los servicios y productos suministrados a sus clientes; para esto, se les ha preparado una guía para implementar y probar un DRP que les permita responder ante eventos de interrupción que afecten la plataforma tecnológica de los ATM, crítica para soportar las operaciones de los bancos.

Igualmente el proyecto contempla la documentación de los planes y procedimientos necesarios para responder, recuperar y retornar a la normalidad luego de una interrupción. Con el fin de validar su efectividad y encontrar los ajustes pertinentes, esta guía y procedimientos serán sometidos a una prueba de escritorio, y en la medida de lo posible, a una prueba real.

Este documento tiene como finalidad definir los objetivos y alcances del proyecto; así como, la definición del programa detallado, el equipo de trabajo, los factores críticos de éxito y los riesgos visualizados que pueden afectar el logro de los objetivos establecidos.

Un banco debe contar con una estrategia de recuperación ante desastres de su plataforma tecnológica, focalizada en la replicación de su infraestructura tecnológica principal a equipos homólogos en centros de cómputo de contingencia o sitio alternos. Dentro de las posibilidades, para garantizar un mejor plan de continuidad de negocios, se recomienda que cuenten con dos sitios de contingencia.

Los planes para darle continuidad a una actividad realmente no son nuevos; diariamente se convive mucho con ellos, lo cual hace imperceptible su utilización. Sea cual sea la medida que se tome para afrontar un riesgo, las acciones buscan siempre mitigar, evitar o transferir el riesgo identificado.

Continuidad del negocio también lo podemos definir:

"Conjunto de políticas y procedimientos usados para minimizar el impacto de los eventos negativos para la operación normal del negocio, manteniéndose las pérdidas operativas y financieras en un nivel aceptable" (Bonilla)

¿Qué es un desastre en tecnología?

"Evento de interrupción que causa que los sistemas o servicios tecnológicos no estén disponibles por un periodo de tiempo en el cual las pérdidas operacionales o financieras para la organización son inaceptables". (Bonilla)

En este trabajo mantendremos la tendencia global de las organizaciones, al dirigir nuestro enfoque hacia el fortalecimiento de las estructuras de liderazgo en situaciones de crisis, garantizando una mejor alineación entre el Plan de Continuidad del Negocio (BCP)

y el Plan de Recuperación de Desastres (DRP), y la gestión de la continuidad de terceros, orientado hacia los ATM de un banco en Panamá.

Un DRP es la estrategia que se seguirá para restablecer los servicios de TI (Hardware y Software) después de haber sufrido una afectación por una catástrofe natural, epidemiológica, falla masiva, caídas planeadas por mantenimiento a la plataforma principal, daño premeditado, ataque de cualquier tipo el cual atente contra la continuidad de las operaciones bancarias en los ATM. Cuando cualquier compañía no cuenta con un DRP implementado y se tiene una eventualidad, estas lo tratan de recuperar a cualquier costo, ya que dependen del funcionamiento de su sistema de información.

El DRP que vamos a desarrollar para un banco en Panamá garantizará a la organización mantenerse un paso adelante ante la expectativas de los cambios en las regulaciones.

Es importante el nivel de interacción que exista con las entidades reguladores en este punto. De igual manera es importante que las organizaciones realicen constantemente ejercicios de pruebas del DRP. Más del 80% de las organizaciones no cuentan con una política estricta al llevar cabo ejercicios en vivo con transacciones reales, esto presenta desafío de alto nivel en la entrega efectiva de las iniciativas del DRP de TI de una organización. El mantenimiento de la calidad de datos se considera un riesgo durante los ejercicios de pruebas. Por ejemplo, las transacciones procesadas durante estos ejercicios de DRP de TI no siempre se consideran transacciones comercialmente

válidas y no se utiliza el ambiente de producción cuando se mueve el recurso a la ubicación de contingencia.

Para que un banco pueda mantener la continuidad de los servicios para los **ATM** a sus clientes, se ha desarrollado, implementado y probado en esta tesis un **DRP orientada hacia los ATM.** Utilizando este **DRP** se podrá responder ante los eventos de interrupción que afecten la plataforma tecnológica crítica para el soporte de las operaciones de un banco; se cumplirá con las disposiciones legales; y además, se renovara la imagen y confianza ante los usuarios (clientes).

Con este trabajo se proyecta crear una guía que permita establecer un procedimiento o plan de recuperación a seguir, en caso de que se presente un desastre (natural o inducido) en el sistema que atiende las solicitudes de los ATM; de manera que, los procesos se puedan habilitar en un sitio alterno y la atención a clientes continúe.

Finalmente es importante mencionar que en un banco el sistema informático es muy amplio, y las aplicaciones alrededor de este son enormemente numerosas; que es muy difícil que se contemplen todas en la primera fase del proyecto DRP. Este proyecto se concentra únicamente en el sistema que responde a las transacciones de ATM.

Por lo tanto, el objetivo general del proyecto es:

- Diseñar una guía que permita crear un procedimiento ante desastre, natural o inducido, para el sistema informático que atiende las transacciones de los ATM; de tal manera que pueda ser ejecutado por el personal técnico del banco; y que en

un tiempo previamente definido, se pueda volver a brindar el servicio brindando de atención a los ATM.

MARCO TÉORICO.

"El término desastre, de acuerdo a la ISO 22301 que reemplaza a la BS25999 significa la interrupción del negocio debido a la pérdida o incapacidad de acceder a los activos que contienen la información requerida para la operación normal. Se refieren en este contexto a la pérdida o interrupción de las funciones que procesan los datos de las compañías, bancos o una pérdida en sí de los datos. La pérdida puede presentarse debido a borrados accidentales o intencionales o por la destrucción de los medios de almacenamiento. Esta pérdida puede ser causada por fenómenos naturales o inducidos por el factor humano". (Villalobos, 2008)

"Un riesgo se define como un evento o condición que, si se produce, tiene un efecto positivo o negativo sobre al menos un objetivo del proyecto, como tiempo, costo, alcance o calidad". (Villalobos, 2008)

"Se considera una amenaza para las organizaciones, aquellos eventos o situaciones que podrían impactar directa o indirectamente a la compañía, afectando total o parcialmente la razón de ser de la misma. Las potenciales amenazas que puede causar un desastre en una organización se clasifican en cuatro grandes categorías". (Villalobos, 2008)

Accidental: Por ejemplo, pérdida de electricidad, accidente de transporte, contaminación química, humo tóxico, otros.

Natural: Inundaciones, terremotos, huracanes, tornados y otros.

Internas: Sabotaje, robo, violencia de empleados o ex empleados, otros.

Conflicto Armado: Secuestro, terrorismo y otros.

"Para mitigar el efecto o impacto de un riesgo, el cual representa una amenaza para la organización, las compañías desarrollan planes de contingencia que son en pocas palabras respuestas para superar o mitigar el impacto de situaciones inesperadas". (Villalobos, 2008)

CAPÍTULO I

OBJETIVOS Y ALCANCES DEL PLAN DE RECUPERACIÓN DE DESASTRES (DRP).

1.1. Objetivos y Alcances.

Identificar los riesgos que pueden afectar la continuidad de la plataforma tecnológica que soporta los productos y servicios de los ATM en la plataforma de cualquier banco en Panamá.

Establecer el conjunto de estrategias, procedimientos, roles y responsabilidades requeridos, para reanudar los servicios de tecnología de un banco para los ATM en caso de que ocurriera un evento de desastre, mantenimiento, pruebas o alguna otra interrupción mayor que afecte la plataforma tecnológica principal de un banco.

Este plan tiene los siguientes objetivos específicos:

Recuperar la plataforma tecnológica de ATM que soporta los servicios críticos de un banco en Panamá. Este procedimiento debe aplicar para desastres naturales en el sitio principal, mantenimientos al sitio principal, pruebas en el sitio principal o una interrupción mayor que afecte la plataforma tecnológica del Banco.

Definir los elementos y procedimientos necesarios que le permitan al banco soportar la recuperación efectiva y eficiente de los ATM (Cajeros Automáticos).

Reducir los tiempos de recuperación mediante la estructuración de las acciones a seguir antes, durante y después del evento que se presente.

Alinear los diferentes procedimientos de contingencia documentados en la gerencia de área de tecnología.

Preparar un análisis de impacto (BIA).

El Análisis de Impacto en el Negocio (BIA) es una actividad específica dentro de la Gestión de la Continuidad de Negocio que tiene por objetivo la cuantificación y cualificación de los impactos negativos que puede ocasionar una interrupción no planeada o no esperada en el negocio.

El BIA es la fuente de información para dar respuesta a preguntas como:

¿Cuánto debo invertir en estrategias de continuidad de negocio y recuperación ante desastres?

¿Cuánto tiempo tengo para detener la interrupción y evitar un impacto mayor para el negocio?

En caso de una interrupción, ¿cuáles y cuántos recursos destinados a restablecer la continuidad de los servicios se deben tener para mantener al menos, un nivel de atención mínimo aceptable por el cliente?

¿Cuál debería ser la estrategia para proteger la información o los recursos críticos necesarios para mantener la operación y la prestación básica del servicio?

La información mínima necesaria para un resultado del análisis de impacto de aplicaciones de un banco se presentan bajo los siguientes tres aspectos:

1. **Impacto Cuantitativo:** Corresponde al impacto financiero que se produce con el banco por una interrupción en los servicios y operaciones a causa de una no disponibilidad de la plataforma tecnológica en los ATM.

Pérdida de ingresos por no prestación de servicios	En miles de dólares diarios.

2. **Impacto Cualitativo:** Corresponde al impacto no cuantificable; ya sea operacional, legal, reputación, financiero, que se produce en el banco por una interrupción en los servicios y operaciones a causa de una no disponibilidad de la plataforma tecnológica en los ATM. Quiere decir que los impactos cualitativos son aquellos que tienen un efecto negativo sobre la organización y que no son fáciles de cuantificar.

Área más importantes investigadas por la Gerencia de Canales.

Aplicación o Plataforma	ATM (Cajeros Automáticos)
Impacto Financiero	Identificar el Impacto financieros
Impacto Operacional	Identificar el Impacto Operacional
Impacto Legal	Identificar el Impacto Legal
Impacto en la Reputación	Identificar el impacto en la Reputación

Estas investigaciones se realizan mediante entrevistas con las diferentes áreas de canales.

3. **Tiempos críticos (RTO):** Corresponde al análisis de los tiempos de interrupción de la plataforma tecnológica tolerables por las áreas, y también a los puntos objetivos de recuperación para la definición de estrategias de respaldo.

Tiempo máximo permitido de no disponibilidad, sin impactar los procesos.	Este tiempo se estable con las áreas de canales dependiendo de las entrevistas. El tiempo normal permitido está entre 0 y 2 horas.

Para alcanzar con éxito el plan de recuperación de la plataforma tecnológica de los ATM, es necesario que el DRP describa lo siguiente:

- La estructura organizacional; los roles y responsabilidades del personal para dar respuesta a un desastre o interrupción mayor.

- Las estrategias de recuperación y contingencia establecidas por el banco para la plataforma tecnológica de los ATM.

- El conjunto de procedimientos que serán utilizados para responder a un desastre o interrupción mayor en los ATM.

El cuadro de los elementos en que se enmarca el DRP para los ATM. Recuperación de las plataformas tecnológicas de los ATM críticas administradas por la Gerencia de Área de Tecnología, en el tiempo objetivo de recuperación para esta Plataforma.	RTO (Diurno)	RTO (Nocturno)

Plataforma de los ATM contingencias.	0-30 minutos	2 horas

1.2. Entendimiento de la Situación Actual para un Banco.

El entendimiento de la situación actual, parte del conocimiento e identificación de los siguientes elementos:

Los ATM son uno de los servicios más importantes para cualquier banco; ya que es un frente de servicios que atiende siete días a la semana, 24 horas al día. Además es parte significativa de la imagen del banco; pues cada día se orienta más a los usuarios a utilizar estos servicios y no las taquillas bancarias. Normalmente los clientes de cada banco, que mantienen cuentas corrientes o cuentas de ahorros, tienen una tarjeta del banco para realizar transacciones en los ATM.

Por lo anterior, los ATM se han convertido en un producto tan sensitivo como principal en un banco.

Los bancos en Panamá están conectados a Telered o Sistema Clave.

(Telered.com.pa)

¿Quién es Telered?.

Es una empresa de capital panameño, con más de 20 años de experiencia en el mercado, que provee soluciones a instituciones financieras que facilitan el intercambio de transacciones de forma electrónica.

La junta de accionistas de Telered está conformada por Bancos cuya solidez y experiencia aportan a la empresa un gran respaldo y confiabilidad en los servicios que brinda.

Telered posee una infraestructura soportada por tecnología de punta que tiene la capacidad y velocidad necesarias para implementar nuevas aplicaciones que generen economía de escala a sus miembros.

De igual forma, Telered mantiene conexión con varias entidades, tanto privadas (nacionales e internacionales) como públicas, a través de una infraestructura de comunicaciones que trasmite de forma segura y confiable la información entre las entidades y las instituciones financieras afiliadas.

Los servicios que ofrece Telered se pueden agrupar en tres líneas de negocios:

1. **SISTEMA Clave:** Red de cajeros automáticos, puntos de venta y tarjetas de débito.

2. **ACH Directo:** Transferencias ACH local y con los Estados Unidos.

3. **CPD:** Centro de procesamiento de cheques y documentos.

Estas líneas de negocios ofrecen diferentes opciones de servicio tanto al sector comercial y financiero, como al sector personal.

La marca **Sistema Clave** brinda un servicio, puesto a disposición de las instituciones financieras con licencia general, que consiste en una red interbancaria de cajeros automáticos y puntos de venta operados por Telered, S.A.

Sistema Clave ofrece el servicio de procesamiento de transacciones electrónicas realizadas a través de tarjetas de débito, accediendo las cuentas que mantienen los clientes consumidores en las diferentes instituciones financieras afiliadas a la red.

Actualmente, el **Sistema Clave** cuenta con más de 40 instituciones financieras (Bancos y Cooperativas) afiliadas a la red, los cuales en su conjunto han emitido más de 1,000,000 (un millón) de tarjetas de débito clave. La red cuenta con más de 1,153 cajeros automáticos instalados en todo el territorio de la República de Panamá

(Telered.com.pa) (Sociedades, 2011)

El SISTEMA CLAVE O TELERED.

Posee un millón de tarjetas emitidas.

En censo 2010 refleja que uno de cada tres habitantes tiene una tarjeta débito Sistema Clave.

La red cuenta con más de 1,150 cajeros automáticos; de los cuales el 70 por ciento se encuentra en localidades del área metropolitana.

Tiene más de 20 mil terminales de puntos de ventas ubicados en más de 11 mil comercios a lo largo de la República de Panamá.

La red procesa un promedio de **siete millones de transacciones cada mes.**

El Sistema Clave mantiene conexión internacional con las redes de VISA y MasterCard a través de más de un millón de cajeros automáticos alrededor del mundo en aproximadamente 200 países.

En el 2011 el registro de nuevos tarjetahabientes creció un 11% en comparación con el 2010 y se espera que en el 2012 haya un incremento de 16% en nuevos tarjetahabientes.

De esta forma Telered es el *switch* establecido en Panamá para procesar transacciones de ATM, POS, ACH, e imágenes de cheques para compensación.

En Telered actualmente están conectados todos los ATM de los bancos en Panamá; y Telered a su vez, tiene una conexión con el sistema principal de cada banco donde se autorizan las transacciones en línea realizadas en los diferentes ATM y POS. Normalmente las transacciones procesadas en los ATM propios tienen un costo más bajo que transacciones procesadas en otros ATM, en los cuales, el cuenta habiente no es miembro; estas transacciones usualmente son llamadas transacciones cruzadas.

Todas las conexiones primarias de Telered a cada Banco, generalmente tienen una conexión de contingecia, esto garantiza que si la línea principal falla pueda utilizarse la línea de contingencia.

Además cada banco cuenta con una conexión a un sitio de contingencia; ya que, todos los bancos tienen sistemas redundantes como contingencia. Igualmente, este sitio también cuenta con una conexión de contingencias para garantizar el servicio.

Imagen 1. Diagrama de conexión estándar de Telered a un Banco.

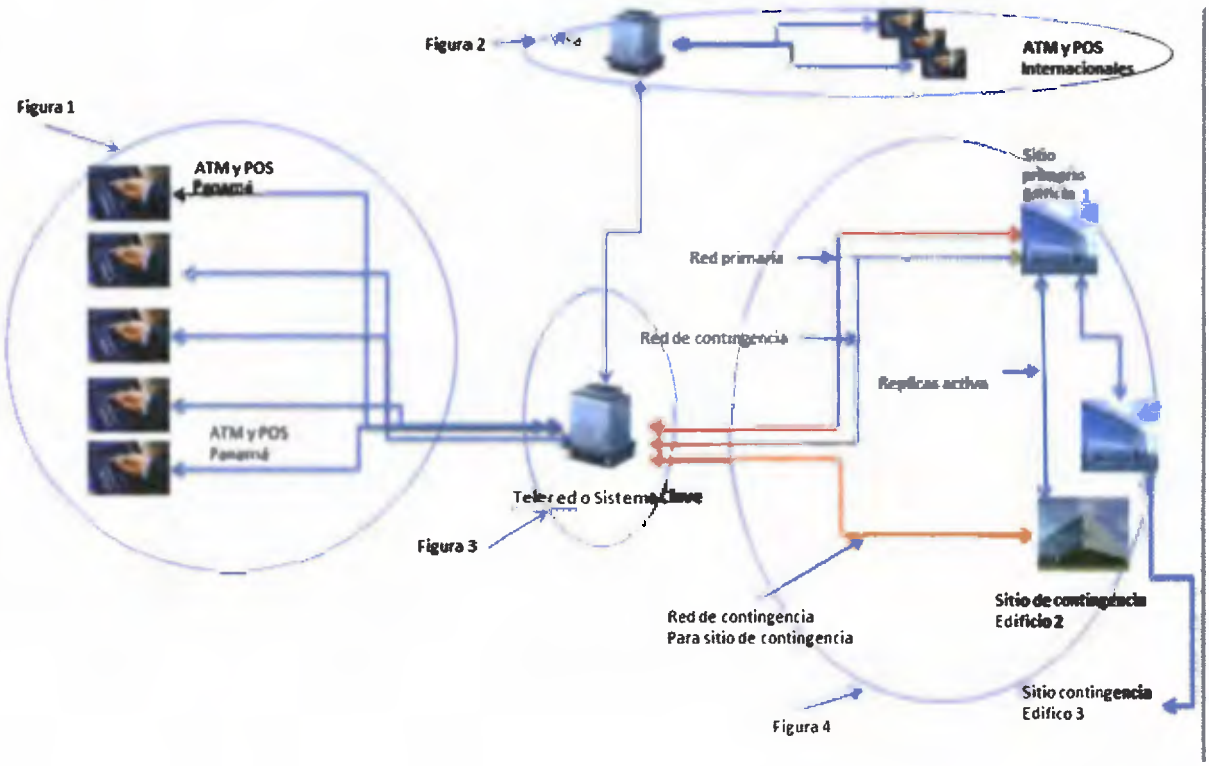


Figura 1.

Muestra la conexión de ATM y POS a Telered o Sistema Clave (figura 3). De esta forma clientes del banco puedan realizar sus transacciones y Telered o Sistema Clave (figura 3). Dirige las transacciones al banco dueño de la transacción para autorizarla (figura 4).

Figura 2.

Muestra la conexión de ATM y POS a Visa Internacional (figura 2). También pude estar conectado a otra red Internacional; de esta forma, cuando clientes de Panamá realicen sus transacciones internacionales, el sistema VISA la dirige a Telered y este a su vez las dirige a su banco dueño para autorizar la transacción (figura 4).

Figura 3.

El Sistema Clave o Telered, donde se encuentran conectados todos los cajeros Automáticos instalados en Panamá; mantiene conexiones con los Bancos dueños de los ATM para solicitar la autorización de las transacciones.

Figura 4.

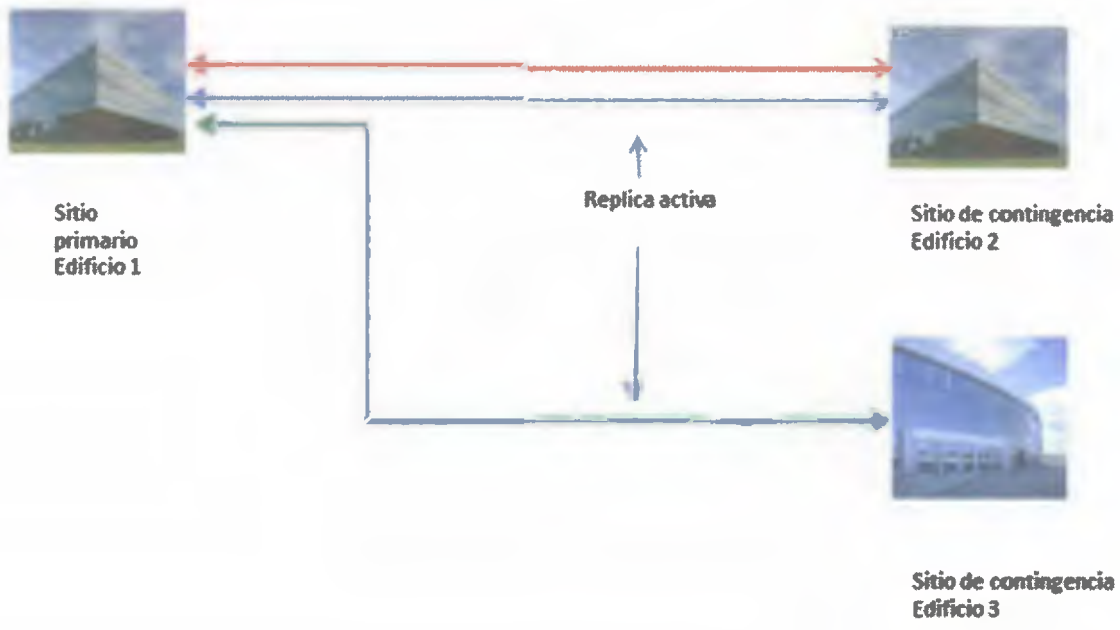
En la (figura 4) se muestra la conexión estándar de Telered o sistema clave a un Banco (sitio primario o principal). Se identifica en **color rojo** la conexión primaria del banco por una fibra óptica de alta velocidad

La fibra de contingencia del Banco (sitio primario o principal) se muestra en **color verde**; esta fibra se conecta en caso que la primaria falle.

En **color chocolate** se muestra una fibra conectada al sitio de contingencia del banco; la cual se activa en caso de un desastre natural, falla planeada o activación del DRP. La Contingencia en un banco, es un requisito solicitado por Telered o Sistema Clave; esto es para reforzar el valor de contar con un sitio de contingencia o redundante en cada banco.

Es una recomendación importante que cada banco cuente con 2 sitios de contingencia donde se esté replicando la información del sistema que está atendiendo en línea a los clientes; ya sea, principal o sitio de contingencia. Redunda en beneficio que, al estar realizando pruebas o mantenimientos al sitio principal, el sitio de contingencia esté replicando las transacciones que están ocurriendo al segundo sitio de contingencia. En la imagen 2 se muestra como sería esta configuración.

Imagen 2. Conexión a sitio de contingencia desde el sitio primario de cada banco.



La línea roja es la conexión primaria al primer sitio de contingencia, la fibra debe ser de alta velocidad.

La línea azul de contingencia; igualmente, fibra de alta velocidad.

La línea verde es la conexión al segundo sitio de contingencia, la fibra debe ser de alta velocidad.

1.2.1. Mapa transaccional estándar en los ATM.

Entendimiento de los productos y/o servicios que presta los ATM en un banco en Panamá.



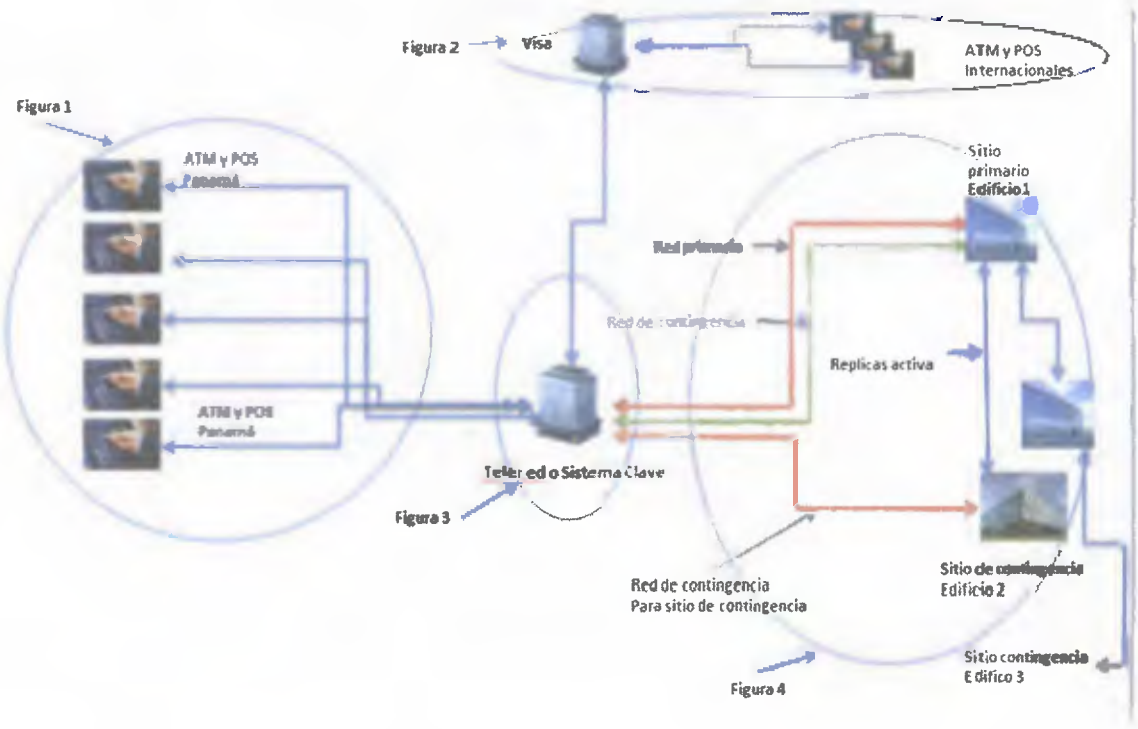
Las transacciones normales soportadas en ATM son:

- Retiros de cuentas corrientes y cuentas de ahorros.
- Consultas de saldos de cuentas corrientes y cuentas de ahorros.
- Transferencias entre cuentas corrientes y cuentas de ahorros.
- Pagos de servicios públicos con débitos a cuentas.
- Compra de pines para teléfonos.
- Pago de préstamos.
- Recarga de celulares.

1.2.2. Mapa Tecnológico.

Requerimiento mínimo que debe tener las plataformas tecnológicas que soportan el servicio para operación de ATM.

Imagen 3. Mapa tecnológico de cómo debe ser la conexión con el sistema de Telered en Panamá.



En la imagen 3 se muestra mapa tecnológico de los ATM que se encuentran conectados a Telered y a un banco para la realización de las transacciones, operaciones y servicios.

Plataforma de Telered requerida para todas las operaciones de Cajero Automáticos, Puntos de Ventas y transacciones de ACH de cada banco en Panamá, Telered a su vez se conecta con el computador principal de cada Banco.

En Panamá los centros de cómputo están alojados en los IDC de Telecarrier, Cable&Wireless y KIO Networek. Estos son los 3 únicos proveedores que prestan este servicio de IDC, que cumplen con todos los estándares requeridos para un centro de cómputo.

1.2.3. Infraestructura física.

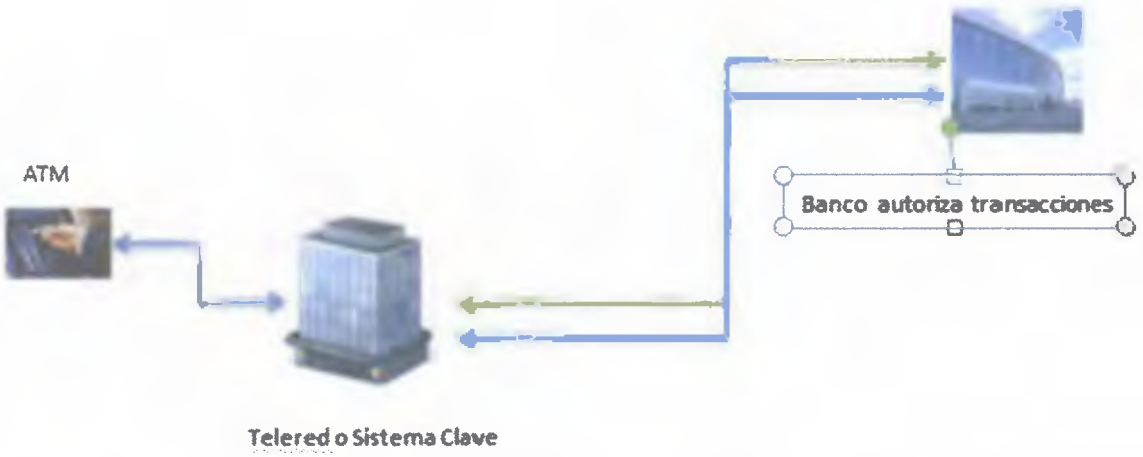
Se refiere a la identificación y evaluación de las condiciones físicas de los centros de cómputo donde se encuentran las plataformas críticas para el manejo de los ATM.

Los bancos deben disponer, como mínimo, de una infraestructura con los siguientes elementos:

Sitio principal del banco: Son las instalaciones principales del banco donde se autorizan las transacciones de los cuentahabientes que utilizan los diferentes ATM del país. En la Imagen 4 se muestra como los ATM se conectan a Telered y este, a su vez, al banco para solicitar la autorización de la transacción que realiza el usuario.

Sitios de contingencia: Normalmente los sitios de contingencia de los bancos se encuentran en centro de cómputo de Cable & Wireless, Telecarrier o Kio NetWork. En estas instalaciones se encuentras los equipos de contingencia para las plataformas que soportan los equipos de los bancos necesarios para poder continuar con el servicio que están prestando en caso de un desastre.

Imagen 4. Conexión de Telered con el Banco para autorizar las transaccones que son solicitadas de los diferentes ATM.



1.2.4. Respaldo de la Información.

Iniciativa de contingencia adicional que deben realizan los bancos. Se debe identificar las diferentes estrategias e iniciativas del banco para mantener la disponibilidad de la plataforma tecnológica para ATM.

Los bancos deben haber diseñado e implementado una serie de elementos de contingencia a nivel de su plataforma tecnológica, entre los que se encuentran los siguientes:

- Respaldo de información de servidores en doble cinta con almacenamiento externo en bóvedas del banco.
- Alta disponibilidad de la información; los servidores deben estar listos y utilizar los más avanzados sistemas de replicación de información.
- Debe mantener un sistema redundante en las comunicaciones entre su sitio principal y su sitio de contingencia.

1.2.5. Escenarios y estrategias de recuperación.

Los escenarios de desastre o interrupción mayor y las estrategias de recuperación implementadas para un banco se enmarcan en los siguientes estándares:

Escenario de Interrupción o Falla	**Eventos factibles**	**Estrategia de Recuperación**
No disponibilidad del centro de cómputo o sitio principal donde se encuentran conectados los ATM.	Desastre Natural. Incendio, Sabotaje, Fallas eléctricas o aires acondicionados, Fallas en las comunicaciones.	Recuperación en el Sitio Alterno donde está el servidor de contingencia principal y donde se puede atender las solicitudes de Telered.

No disponibilidad del sistema en sitio principal, base fundamental principal de los ATM.	Falla de los servidores de producción, Fallas en los sistema de almacenamiento, Fallas en el servidor de entrada al sistema, Mantenimiento a los computadores principales por instalación de nuevas versiones, Pruebas del sitio de contingencia por normativas de la Súper Intendencia de Bancos.	Recuperación en el Sitio Alterno donde está el servidor de contingencia principal y se puede atender las solicitudes de Telered.

La plataforma tecnológica establecida en los centros de cómputo alterno deberán sostener las operaciones para los ATM de forma indefinida, al igual que las operaciones normales del banco.

Es recomendable que los bancos cuenten con un tercer sitio de contingencia conectado al servidor principal donde su principal participación sea para cuando se realizan pruebas en el sitio de contingencia.

Supuestos.

La aplicabilidad y efectividad del Plan de Recuperación ante Desastres para ATM (CAJEROS AUTOMÁTICOS) y sus procedimientos se fundamenta en los siguientes supuestos:

La implementación de las estrategias de recuperación y contingencia que se recomiendan deben estar actualizadas con base en los cambios realizados en la plataforma tecnológica para ATM y en los servidores principales, que están conectados con los sistemas de Telered.

El evento de interrupción no afectó al mismo tiempo los centros de cómputo principal (producción) y alterno (contingencia).

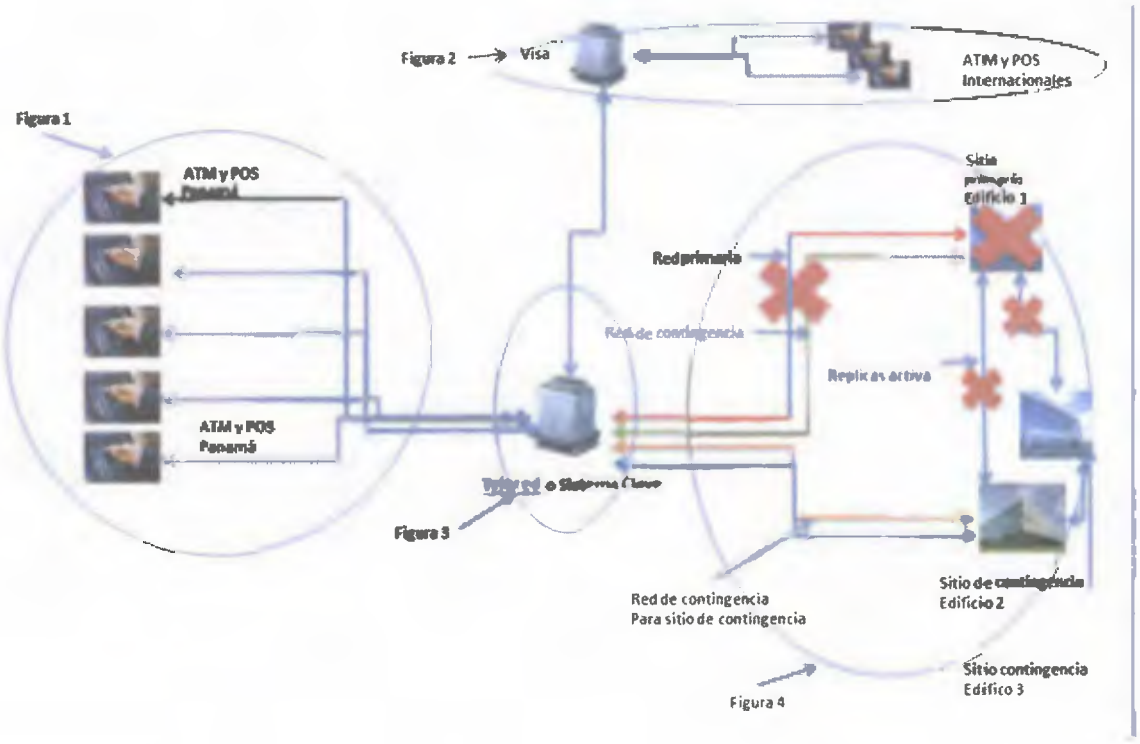
Se deben haber realizado las pruebas periódicas de este plan de recuperación ante desastres para ATM, efectuando simulaciones que apuntan a contingencia y luego pasan a producción; y también, se deben haber realizado los ajustes correspondientes.

Por otro lado, se deben haber llevado a cabo pruebas por supuestos; ya sean, mantenimiento a la plataforma principal o a la de contingencia, donde se necesiten direccionar los servicios según sea el caso.

El plan de recuperación ante desastres ha sido activado de acuerdo a los procedimientos establecidos y por el personal indicado en los roles y responsabilidades.

Se tiene establecido un SLA (Acuerdo de Nivel de Servicios) con la empresa Telered para las transacciones que llegan de los diferentes ATM a nivel nacional y mundial; para establecer hacia donde se van a direccionar estas transacciones de ocurrir un evento.

Imagen 5. Muestra la desconexión con el sitio principal del banco y de que modo el sitio de contingencia del banco toma el control para aprobar las transacciones que están siendo solicitadas por Telered. También se puede ver que el sitio de contingencia 2 comienza a replicar la información con el sitio de contingencia 3.

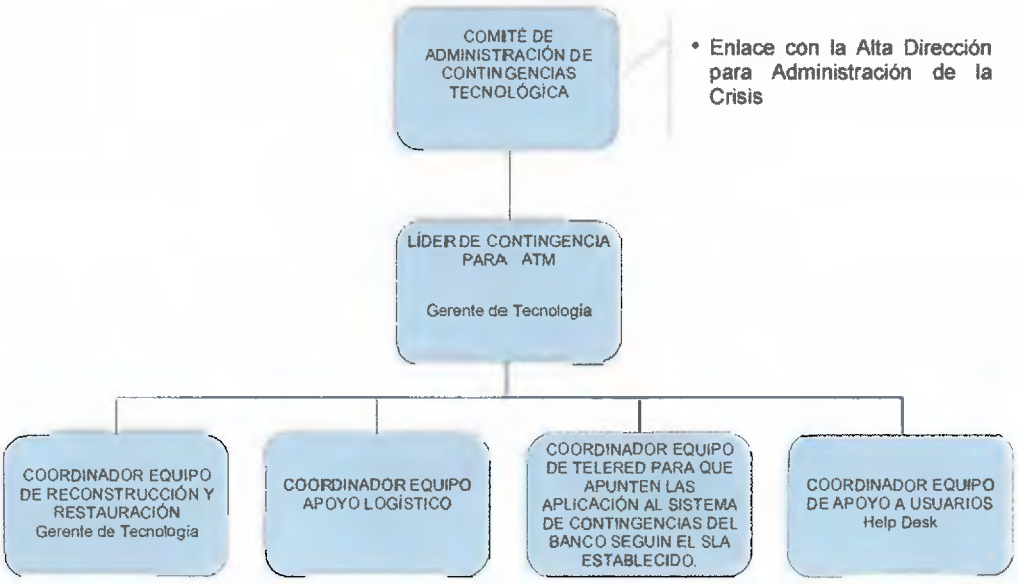


CAPÍTULO II

ESTRUCTURA DE RESPUESTAS ANTE DESASTRES

2.1. Estructura de respuesta.

La siguiente es la estructura mínima recomendada a nivel organizacional, definida para responder ante eventos de interrupción en la plataforma tecnológica para los ATM.



Equipos, Roles y Responsabilidades del Plan de Recuperación de Desastres.

En el **Anexo 1 Directorio de Continuidad**, se detallan las personas que deben asumir un rol en cada una de las estructuras definidas.

Comité de Administración de Contingencias de Tecnología

Comité encargado de realizar la evaluación de incidentes, desastres o interrupciones mayores, que afectan la operación de los servicios para los ATM de tecnología dentro de

los tiempos de interrupción definidos como críticos. Además, deberá tomar decisiones para afrontar el evento. Este comité está conformado por:

Gerencia General.

Gerente de Tecnología.

Líder del Plan de Recuperación ante Desastres

Y Coordinador de Preparación en Recuperación ante Desastres y Contingencias

Las responsabilidades de este comité contemplan:

RESPONSABILIDADES		
ANTES DEL DESASTRE O INTERRUPCIÓN MAYOR	**DURANTE EL DESASTRE O INTERRUPCIÓN MAYOR**	**DESPUÉS DEL DESASTRE O INTERRUPCIÓN MAYOR**
Aprobar el presupuesto recursos requeridos para mantener vigente el plan. Aprobar y participar en programas de capacitación y entrenamiento en el plan. Velar por el mantenimiento y pruebas del plan. Involucrar a los diferentes proveedores en las pruebas. Contar con todas las herramientas necesarias para mantener el plan del DRP actualizado de la mejor forma y siguiendo las mejores prácticas.	Estar informado sobre la magnitud y el impacto del desastre, contingencia o interrupción mayor y definir acciones tendientes a mitigar los impactos. Tomar decisiones sobre las acciones a seguir una vez conocido el resultado de la evaluación del evento. Coordinar la comunicación con las áreas del negocio y a las áreas de comunicación del banco.	Observar atentamente el restablecimiento de los servicios del Banco y de los ATM en el sitio principal. Realizar seguimiento a las actividades de restauración de recursos y servicios. Mantener monitoreo permanente de los hechos posteriores al desastre, incidente o interrupción mayor. Identificar lecciones aprendidas y velar por la actualización del plan. Mantener siempre una base de conocimiento sobre todos los eventos.

2.1.1. Equipo de contingencia para ATM.

La función principal de este rol se enmarca en liderar la ejecución de los procedimientos establecidos en el DRP para los ATM y recuperar la disponibilidad de la plataforma tecnológica ante un evento de interrupción.

Este comité está conformado por:

Gerente de Tecnología, Líder del Plan de Recuperación ante Desastres y Coordinador de Proyectos.

Las responsabilidades de este rol contemplan:

RESPONSABILIDADES		
ANTES DEL DESASTRE O INTERRUPCIÓN MAYOR	**DURANTE EL DESASTRE O INTERRUPCIÓN MAYOR**	**DESPUÉS DEL DESASTRE O INTERRUPCIÓN MAYOR**
Gestionar ante la Gerencia la consecución de los recursos para mantener vigente el plan y sus procedimientos. Velar por mantener actualizado y probado el plan. Participar en las capacitaciones, pruebas y entrenamientos en el plan.	Convocar al Comité de Administración de Contingencias de Tecnología establecido por el Banco. Liderar la evaluación de los daños, interrupciones o fallos Liderar las actividades de recuperación ante un desastre. Comunicar al Comité de Administración de Contingencias de Tecnología los inconvenientes y aspectos relevantes de la operación bajo contingencia.	Liderar la restauración de operaciones y el retorno a la normalidad Monitorear el comportamiento, disponibilidad y confiabilidad de las aplicaciones y sistemas. Evaluar la efectividad del plan y sus componentes.

2.1.2. Equipo de Reconstrucción y Restauración

Mantener siempre un equipo que se encarga de coordinar las labores de reconstrucción de las áreas afectadas en el centro de cómputo, según el resultado de la evaluación de daños.

El comité está integrado por:

Coordinador del Equipo de Reconstrucción y Restauración (Gerente de Tecnología),

Coordinador de Obras, Proyectos y Mantenimiento,

Coordinador de Mantenimiento,

Coordinador de Servicios Administrativos (Compra y Seguros),

Coordinador de Planificación y Control (Presupuesto),

Bases de Datos y

Proveedores de los sistemas críticos del Banco.

Las responsabilidades de este equipo contemplan:

RESPONSABILIDADES		
ANTES DEL DESASTRE O INTERRUPCIÓN MAYOR	**DURANTE EL DESASTRE O INTERRUPCIÓN MAYOR**	**DESPUÉS DEL DESASTRE O INTERRUPCIÓN MAYOR**
Participar en la ejecución de las pruebas del plan. Tener identificados todos los periféricos necesarios y proveedores involucrados para la restauración del sitio principal. Tener pensado un sitio alterno para replicar la información del sitio de contingencia mientras dure la restauración de la base principal.	Participar en el Comité de Administración de Contingencias de Tecnología cuando haya sido convocado. Coordinar las labores de reconstrucción de las áreas afectadas, según la evaluación de daños. Mantener comunicación permanente con proveedores **Anexo 2 Lista de Proveedores**.	Reportar las inconveniencias y oportunidades de mejoras del plan.

2.1.3. Equipo de Apoyo Logístico.

Este equipo se encarga de suministrar todos los requerimientos logísticos requeridos para apoyar pruebas, desastre o interrupción mayor.

El comité está integrado por:

Coordinador Equipo de Apoyo Logístico,

Coordinador Equipo Recursos Humanos,

Coordinador de Transporte y Suministro,

Las responsabilidades de este equipo contemplan:

RESPONSABILIDADES

ANTES DEL DESASTRE O INTERRUPCIÓN MAYOR	DURANTE EL DESASTRE O INTERRUPCIÓN MAYOR	DESPUÉS DEL DESASTRE O INTERRUPCIÓN MAYOR
Participar en la ejecución de las pruebas del plan. Es importante el apoyo que este grupo tenga para el desarrollo de pruebas, desastres o interrupciones mayores.	Coordinar todas las actividades de consecución de recursos para la recuperación de la plataforma tecnológica. Coordinar la disponibilidad de alimentos y bebidas cuando sea requerido. Asegurar la comunicación y desplazamiento del personal ejecutor de contingencia a cargo. Apoyar los procesos de selección y contratación de personal para apoyar la respuesta.	Reportar los inconvenientes y oportunidades de mejora del plan.

2.1.4. Equipo de Contingencias de Infraestructura, Comunicaciones y Aplicaciones.

Este equipo se encarga de evaluar los daños ocasionados por el desastre sobre la infraestructura, las aplicaciones del centro de cómputo y la plataforma de red. Debe direccionar la ejecución de los procedimientos y actividades de contingencia para recuperar la plataforma de servidores, almacenamiento, y bases de datos, y coordinar el retorno a la normalidad.

Está integrado por:

Coordinador del Equipo Contingencia, Infraestructura, Comunicaciones y Aplicaciones.

Coordinador de recuperación las diferentes plataformas que usa el banco y sistema de almacenamiento.

Coordinador de recuperación la aplicación de los ATM con Telered.

Las responsabilidades de este equipo contemplan:

RESPONSABILIDADES		
ANTES DEL DESASTRE O INTERRUPCIÓN MAYOR	**DURANTE EL DESASTRE O INTERRUPCIÓN MAYOR**	**DESPUÉS DEL DESASTRE O INTERRUPCIÓN MAYOR**
Participar en la ejecución de las pruebas del plan. Mantener actualizados los procedimientos de contingencia Advertir sobre necesidades de actualización en el plan, por cambios en la plataforma tecnológica.	Participar en el Comité de Administración de Contingencias de Tecnología cuando haya sido convocado. Coordinar la evaluación de daños. Activar las contingencias establecidas ante los escenarios de falla	Reportar los inconvenientes y oportunidades de mejora del plan.

Coordinador del Equipo de TELERED.

Este equipo se apega al SLA establecido con Telered y ejecutado en las diferentes pruebas. En esencia se encarga de llamar o localizar al centro de atención en Telered e informar que se está en contingencia, para que apunten los servidores de Telered hacia los servidores de aplicaciones que se encuentran en el sitio alterno definido por el banco; para que estos servidores pueden atender las operaciones en los ATM hasta poder restablecer el sitio de producción del banco.

El comité está integrado por:

Líder del plan de recuperación de desastres,

Coordinador de Preparación en Recuperación ante Desastres y Contingencias,

Las responsabilidades de este equipo contemplan:

RESPONSABILIDADES		
ANTES DEL DESASTRE O INTERRUPCIÓN MAYOR	**DURANTE EL DESASTRE O INTERRUPCIÓN MAYOR**	**DESPUÉS DEL DESASTRE O INTERRUPCIÓN MAYOR**
Participar en la ejecución de las pruebas del plan. Telered debe participar en las pruebas utilizando el sitio de pruebas como primera fase, y luego, como segunda fase, utilizar el sistema principal.	Participar en el Comité de Administración de Contingencias de Tecnología cuando haya sido convocado. Mantener informados a los usuarios sobre la contingencia.	Reportar los inconvenientes y oportunidades de mejora del plan

Establecer SLA de servicios para el banco por parte de Telered.	Solucionar inconvenientes a usuarios.	

2.1.5. Equipo de Apoyo a Usuarios

Este equipo se encarga de suministrar apoyo a los usuarios ante incidentes e inconvenientes para operar desde los centros de contingencia.

Está integrado por:

Service Desk

Las responsabilidades de este equipo contemplan:

RESPONSABILIDADES		
ANTES DEL DESASTRE O INTERRUPCIÓN MAYOR	**DURANTE EL DESASTRE O INTERRUPCIÓN MAYOR**	**DESPUÉS DEL DESASTRE O INTERRUPCIÓN MAYOR**
Participar en la ejecución de las pruebas del plan.	Participar en el Comité de Administración de Contingencias de Tecnología, cuando haya sido convocado. Mantener informados a los usuarios sobre la contingencia. Solucionar inconvenientes a usuarios.	Reportar los inconvenientes y oportunidades de mejora del plan. Mantener una base de conocimientos para analizar todos los detalles ocurridos en simulaciones y casos reales.

2.2. Árbol de llamadas

A continuación se muestra el árbol de llamadas que se debe seguir y cumplir para notificar un evento y comunicar la activación del plan de recuperación ante desastres a los diferentes integrantes y personal involucrado.

Primer Nivel.

Líder de Plan de Recuperación ante Desastres,

Comité de Administración de Contingencia y Tecnología,

Gerente General y Subgerente,

Gerentes del banco,

Gerencia de Comunicaciones y Telered

Mecanismos de Comunicación

El llamado a los integrantes del plan se debe realizar teniendo en cuenta los siguientes mecanismos y prioridades de comunicación:

Persona a persona: Este medio permite ser más explícito y detallar el evento ocurrido. La comunicación depende de factores socio-ambientales y/o factores de riesgo (catástrofes) que afecten este tipo de comunicación.

Telefonía fija o celular: La comunicación telefónica es un medio facilitador para acortar distancias y tener una conversación interpersonal. Con esta se puede al igual que con la comunicación persona a persona ser más explícito y ahondar dentro de la comunicación del evento.

La utilización de medios de comunicación como chat puede ser utilizada como un mecanismo rápido y grupal para difundir un mensaje.

Correo electrónico: El correo electrónico se ha establecido como un medio efectivo para comunicarse a cualquier distancia y en el menor tiempo. Este tipo de comunicación depende del grado de consulta de los intercomunicadores.

2.3. CENTRO DE COMANDO Y OPERACIÓN ANTE CONTINGENCIAS Y DESASTRES POR ATM.

Es importante establecer varios centros de comando, los cuales deben permitir concentrar la operación de los integrantes del Comité de Administración de Contingencias de Tecnología y deben operar en las siguientes instalaciones:

Centros de Comando y Operación	**Centro de Comando y Operación Prioridad 1**	**Centro de Comando y Operación Prioridad 2**	**Centro de Comando y Operación Prioridad 3**	**Recursos Requeridos**
Centro de Comando de Administración de Contingencias y Desastres	Oficina de Reuniones Número 1	Oficina de Reuniones Número 2	Oficina de Reuniones Número 3	Recomendaciones 1 Mesa con capacidad mínima de 10 personas Por lo menos 2 Líneas telefónicas para (Llamada nacional e internacionales) Tableros Marcadores Conexión a red Acceso a Internet Plan de Recuperación ante Desastres Luces de emergencia. Acceso a todas las instalaciones del centro de comando, (Activación de aires acondicionados, elevadores, cafeterías).

2.3.1. PROCEDIMIENTOS DEL PLAN

- Procedimiento de notificación, evaluación y activación del plan.
- Notificación y evaluación del desastre o interrupción mayor.
- Activación de solución de recuperación.
- A continuación se describe el detalle de las actividades a ejecutar:

#	Actividad ¿Qué hacer?	Descripción ¿Cómo hacer?	Responsable
1. Notificación y Evaluación del desastre o interrupción mayor			
1.1	Notificar el desastre o interrupción mayor al líder del plan de recuperación ante desastres.	Identifican la ocurrencia del desastre o incidente que genera la interrupción sobre la plataforma tecnológica y notifican el evento mediante los medios y el árbol de llamadas establecido. La notificación se debe realizar cuando se presenta alguno o varios de los siguientes escenarios: No disponibilidad del centro principal de cómputo por desastres naturales, incendio, sabotaje, atentados o falta de suministro eléctrico o comunicaciones. Las comunicaciones que van de Telered al sitio principal Tenga en cuenta que si el desastre es evidente, se debe notificar de acuerdo a las prioridades establecidas en los mecanismos de comunicación, sin embargo se debe dejar registro posterior de la notificación en el **Anexo 3 Control de Problemas y Soluciones.**	Operadores y supervisores Coordinador Equipo Contingencia de Infraestructura, Comunicaciones y Aplicaciones Inspector de Seguridad Coordinador de Mantenimiento

1.2	Evaluar el incidente / desastre en forma preliminar	Afectación del Centro de Cómputo Afectación del Recurso(s) humano(s) Afectación de la Plataforma tecnológica (Caracterizar el escenario de interrupción) Tiempos estimados de solución (incluyendo tiempos de desplazamiento, solución y re-establecimiento de la operación). Tiempo transcurrido desde la notificación del incidente hasta el momento de finalizar el diagnóstico. Tenga en cuenta en la evaluación, cuando es requerido apoyarse en el coordinador de reconstrucción y restauración.	Líder del Plan de Recuperación ante Desastres Coordinador Equipo Contingencia de Infraestructura, Comunicaciones y Aplicaciones Coordinador de Reconstrucción y Restauración en caso de ser requerido.
2. Activación de solución de recuperación			

2.1	Establecer el Centro de Comando de Contingencias y Desastres	Asegurar la disponibilidad del Centro de Comando de Contingencias y Desastres seleccionado, mediante la verificación de los siguientes aspectos: – Que no haya sido afectado por el mismo evento de desastre. – Que las rutas de acceso estén despejadas y el sitio sea accesible. – Que los medios de comunicación, voz y datos estén operando. – Que cuente con los recursos y servicios públicos necesarios En el caso que no cumpla con estas condiciones, se debe iniciar la verificación con el siguiente Centro de Comando de Contingencias y Desastres establecido.	Líder del plan de recuperación ante desastres
2.2	Convocar al Comité	Convocar al Comité de Administración de Contingencias de Tecnología, informando la ubicación del Centro de Comando de Contingencias y Desastres	Líder del plan de recuperación ante desastres

2.3	Evaluar y activar el plan	El Líder del plan de recuperación ante desastres reporta la evaluación inicial realizada del evento al Comité de Administración de Contingencias de Tecnología, quien tomará la decisión de activar o no, el plan de recuperación ante desastres , teniendo en cuenta las siguientes consideraciones: – Si es un desastre cuyo escenario de interrupción es conocido y el tiempo de resolución total desde el momento en que se notificó la falla es menor al RTO de la plataforma; solicitar accionar los mecanismos de soporte y atención para solucionar el incidente. – Se debe saber si es un desastre cuyo escenario de interrupción es conocido y el tiempo de solución total desde el momento en que se notificó la falla puede tardar un tiempo superior al requerido para la plataforma. En este caso, si la decisión es no activar el plan de recuperación ante desastres, se deberá monitorear permanentemente la evolución del incidente, y evaluar nuevamente. En caso contrario, si se activa el plan y se continúa con la actividad de recuperación.	Comité de Administración de Contingencias de Tecnología
2.4	Notificar la activación de los planes / procedimientos	Notificar de acuerdo a lo establecido en el árbol de llamadas, la activación del plan de recuperación ante desastres. Igualmente, notificar al personal responsable del servicio de ATM, a fin de que se activen los procedimientos que garanticen la activación de la plataforma en el sitio alterno, en los casos en que se requiera.	Líder del Plan de Contingencia y Recuperación ante Desastre

2.5	Activar Centro de Cómputo Alterno	De acuerdo al escenario que se haya identificado, activar la estrategia de recuperación que corresponda. Comunicar la activación al equipo de Contingencia de Infraestructura, Comunicaciones y Aplicaciones	Coordinador Equipo de Contingencia de Infraestructura, Comunicaciones y Aplicaciones
2.6	Notificar el incidente o desastre al negocio	Suministrar información al negocio sobre el incidente o desastre ocurrido, teniendo en cuenta los siguientes aspectos: La información a proveer contiene: – Fecha y hora del reporte – Incidente presentado – Acciones tomadas – Acciones por desarrollar – Tiempo estimado de solución	Comité de Administración de Contingencias de Tecnología

2.7	Monitorear el incidente o desastre	En el caso en que las estrategias y procedimientos de recuperación hayan sido activados, se debe: Verificar que la activación, alistamiento y disponibilidad de los centros de cómputo alternos se estén llevando a cabo de acuerdo a lo establecido en el plan. Mantener contacto con los diferentes coordinadores de equipo. Tomar decisiones sobre inconvenientes presentados en la activación de los procedimientos y las estrategias de recuperación. El Líder del plan de recuperación ante desastres debe mantener una bitácora o trazabilidad de las decisiones tomadas por el Comité (**Anexo 3 Control de Problemas y Soluciones).** En el caso en que las estrategias y procedimientos de contingencia y recuperación **NO** hayan sido activados, se debe: Monitorear la situación y estar al tanto de las acciones que los coordinadores realizan para mitigar los incidentes presentados. – Si el tiempo de solución esperado se extiende, el Comité debe evaluar nuevamente la necesidad de activación de las distintas estrategias de contingencia y recuperación. – Finalizado el procedimiento de recuperación, el líder del plan de recuperación ante desastres apoyado con los coordinadores de contingencia, formalizan la finalización del procedimiento de recuperación. – Igualmente, el Comité de Administración de Contingencias de Tecnología deberá notificar al negocio la recuperación de la plataforma. La información a proveer contiene: – Fecha de inicio y fin del incidente – Incidente presentado – Acciones tomadas – Estado de la plataforma – Restricciones de la plataforma en contingencia.	Comité de Administración de Contingencias de Tecnología

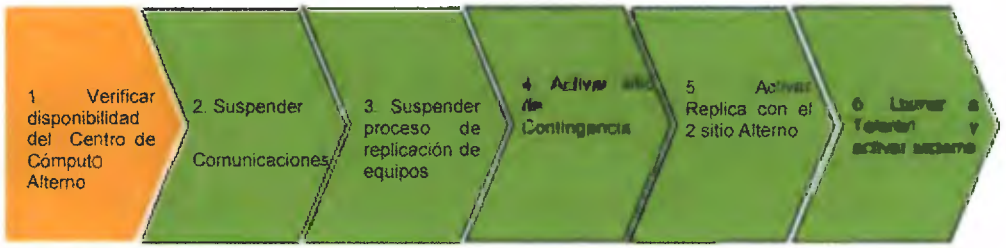
2.8	Iniciar el procedimiento de reconstrucción del Centro de Cómputo Principal	Si el incidente ocasionó daños en el Centro de Cómputo Principal, se deberá iniciar el procedimiento descrito.	Coordinador Equipo de Reconstrucción y Restauración
2.9	Cierre del incidente o desastre	Una vez se hayan ejecutado los procedimientos relacionados con el incidente presentado, el Líder del Plan de Recuperación ante Desastres, deberá dar cierre utilizando el "**Formato: Evaluación de Efectividad del Plan y Cierre**". En este caso se identificaran las lecciones aprendidas del incidente, oportunidades de mejora sobre el DRP y las estrategias, y cualquier aspecto relevante para mejorar la efectividad del DRP.	Líder del plan de Recuperación ante Desastres. Coordinador de preparación en Recuperación ante Desastres y Contingencias

CAPÍTULO III

PROCEDIMIENTOS DE RECUPERACIÓN EN LOS SITIOS ALTERNOS

En este capítulo explicamos el procedimiento para la recuperación en el sitio alterno o de contingencia. Este sitio debe ser una réplica casi exacta del sitio principal con la misma cantidad de equipos y configuraciones para poder soportar todas las transacciones que se realizan en el sitio principal del banco. Es recomendable hacer como mínimo una prueba completa al año, sin embargo realizar pruebas de los equipos de forma separada garantiza la activación del sitio alterno al momento de realizar las pruebas.

Pasos a seguir para la activación del sitio alterno.



3.1. Procedimiento de Recuperación en el Centro de Cómputo Alterno.

El presente procedimiento define el conjunto de recomendaciones o actividades que se deben ejecutar para recuperar la plataforma y aplicaciones críticas que se encuentran en el centro de cómputo alterno.

Verificar la disponibilidad del centro de cómputo alterno.

Verificar las comunicaciones entre Telered y el sitio alterno, revisar la línea principal y de contingencia que se tienen al sitio alterno.

Deshabilitar plataforma de producción (si está dentro de las posibilidades).

Bajar o Deshabilitar las diferentes interfaces o conexiones que existan del sistema de producción (si está dentro de las posibilidades).

Activar Interfaces o conexiones de comunicación en el sitio de contingencia.

Realizar los cambios de roles en los servidores de contingencia.

Verificar los cambios de roles.

Habilitar todos los servicios de las diferentes plataformas en el sitio de contingencia.

Verificar que Telered e interfaces que tengan contingencia activa.

A continuación se describe el detalle de las actividades a ejecutar:

#	Actividad	Descripción	Responsable
1. Verificar disponibilidad del Centro de Cómputo Alterno			
1.1	Comunicar a los proveedores la activación del Centro de Cómputo Alterno	Contactar al proveedores de equipos, sistemas y del sitio de contingencia para comunicar que se ha activado la contingencia implementada en el centro de cómputo alterno, por lo cual deberán estar atentos para prestar cualquier apoyo requerido por el banco, en especial en aspectos relacionados con: Asignar el personal que sea necesario para el correcto y satisfactorio cumplimiento en la prestación del servicio. Disponibilidad de personal en caso de que se requiera servicio de manos remotas, el cual puede contemplar: Reiniciación de servidores en caso de falla. Reiniciación de equipamiento de *networking* Montaje de tapes de *backup* de ser necesario.	Coordinador de Equipo de Infraestructura, Comunicaciones y Aplicaciones

		Montaje de los CD para la instalación remota del software de ser necesario. Verificación de estado de equipos y cableado Recepción o entrega de cintas al personal o proveedor autorizado por el banco, de ser necesario. Oportunidad de acceso al centro de cómputo por el personal del banco designado, según el SLA; esto siempre debe estar actualizado. Disponibilidad de las condiciones ambientales requeridas Oportunidad en la atención y solución de incidentes que afecten la disponibilidad de la plataforma. Oportunidad en los mantenimientos preventivos y correctivos requeridos.	
1.2	Verificar disponibilidad de los recursos en el Centro de Cómputo Alterno	Verificar que todos los recursos requeridos para recuperar los servicios de tecnología críticos se encuentran disponibles en el Centro de Cómputo Alterno. En caso de no estar disponible uno o más recursos, realizar la gestión para asegurar la disponibilidad de los recursos faltantes.	Coordinador de Equipo de Infraestructura Comunicaciones y Aplicaciones

1.3	Movilizar equipo de recuperación hacia sitio alterno	En el caso en que el sitio principal no esté disponible, se debe coordinar con el equipo de apoyo logístico la movilización del equipo de infraestructura, comunicaciones y aplicaciones hacia el sitio alterno desde donde se hará la recuperación de la plataforma del Centro de Cómputo Alterno. Continuar con el paso descrito en la actividad 3: Habilitar comunicaciones en el centro de cómputo alterno.	Coordinador de Equipo de Infraestructura, Comunicaciones y Aplicaciones
2. Habilitar comunicaciones al centro de cómputo alterno			

2.1	Garantizar que Telered esté en comunicación con el sitio de contingencia	Se deberán ejecutar los siguientes pasos, en caso de fallas con el sistema principal; Ajustar el tráfico que ingresa al sitio principal desde Telered y direccionarlo al sitio alterno o de contingencia. En caso de que el sitio principal no está disponible; se deberán ejecutar los siguientes pasos. Movilizar al coordinador de comunicaciones hacia Telered. Activar circuito hacia el sitio Alterno o de contingencia.	Coordinador de Comunicaciones
3. Habilitar servicios y aplicaciones del sitio alterno.			
3.1	Subir aplicación en equipo de contingencia	Se levanta aplicación en sitio de contingencia	Soporte Técnico
3.2	Activar las aplicación para los ATM	Se activan las aplicaciones en los servidores que atienden los sistemas de los ATM.	Soporte Técnico
3.3	Validar disponibilidad de datos	Se verifican que los datos para el funcionamiento de las aplicaciones estén cargados y listos para usarse en los sistemas.	Coordinador de Producción
3.4	Realizar cambio de direcciones	Se hace una revisión de los cambios de dirección necesarios para el funcionamiento de las aplicaciones.	Coordinador de Seguridad
3.5	Validar que la aplicación de la encriptación está trabajando correctamente	Validar que la aplicación de encriptación esté funcionando correctamente, en caso contrario, inhabilitar la aplicación de encriptación. Telered recomienda que todas sus conexiones tengan sistemas de encriptación.	Coordinador de Comunicaciones

4. Verificar disponibilidad del servicio desde el centro de cómputo alterno			
4.1	Verificar disponibilidad del servicio	Verificar que el servicio ya se puede prestar desde el centro de cómputo alterno. Notificar al Líder de Plan de Recuperación ante Desastres la recuperación de la plataforma.	Coordinador Equipo Contingencia de Infraestructura, Comunicaciones y Aplicaciones.
4.2	Monitorear y dar soporte sobre la plataforma del centro de cómputo alterno	Monitorear y realizar las actividades de soporte sobre la plataforma que se encuentra operando en el centro de cómputo alterno. Igualmente se debe monitorear la habilitación del centro de cómputo principal y la plataforma, para iniciar el procedimiento de retorno a la normalidad establecido en este documento.	Coordinador de Soporte Centro de Cómputo

3.2. Procedimiento de Reconstrucción del Centro de Cómputo Principal

Este procedimiento contiene las actividades que se deben realizar para reconstruir el centro de cómputo principal ante un daño parcial o total.

A continuación se presenta la descripción detallada de cada una de las actividades:

#	Actividad	Descripción	Responsable
1. Evaluación detallada de los daños en el centro de cómputo principal			
1.1	Evaluar los daños ocasionados	Evaluar detalladamente los daños ocasionados en el centro de cómputo principal. En este caso se deberá apoyar en los **Anexo 4: "Formato: Evaluación del Incidente", Anexo 5: "Listado de Recursos Para el Sitio Principal"**	Coordinador Equipo de Reconstrucción y Restauración
1.2	Identificar necesidades de infraestructura	Realizar inventario de requerimientos en la infraestructura del centro de cómputo principal, teniendo en cuenta los resultados de la evaluación de datos y la infraestructura requerida para operar las plataformas críticas.	Coordinador Equipo de Reconstrucción y Restauración
1.3	Identificar estado de los equipos	Realizar inventario de equipos/elementos dañados y salvados (Equipos de comunicación computadores, sistemas Swift, baterías).	Coordinador Equipo de Reconstrucción y Restauración
1.4.	Revisar equipos salvados	Coordinar con los proveedores la revisión y el soporte en caso de ser requerido, de los equipos que pudieron salvarse del siniestro.	Coordinador Equipo de Reconstrucción y Restauración
2. Reconstruir el centro de cómputo principal			
2.1	Identificar equivalencia de equipos dañados	Revisar con los proveedores el inventario de los equipos dañados que fueron instalados antes del siniestro para evaluar la equivalencia con equipos disponibles en el mercado, tanto local como internacional.	Coordinador Equipo de Reconstrucción y Restauración
2.2	Revisar nuevo diseño de arquitectura	Si se requiere, revisar nuevo diseño de plataforma o configuración de equipos con proveedores y con el área técnica de sistemas.	Coordinador Equipo de Reconstrucción y Restauración

2.3	Definir servicios y equipos que serán adquiridos	Definir servicios y equipos/elementos que serán adquiridos. Después de analizar las necesidades y evaluados las disponibilidades del mercado.	Coordinador Equipo de Reconstrucción y Restauración Coordinador de Innovación Tecnológica
2.4	Realizar reclamos de equipos/elemento bajo cobertura	Hacer las gestiones para materializar los reclamos a aseguradoras para elementos con cobertura.	Coordinador Equipo de Reconstrucción y Restauración
2.5	Solicitar cotizaciones para los servicios y equipos requeridos	Solicitar a los diferentes proveedores, propuestas de los equipos requeridos para comparar beneficios vs precios.	Coordinador Equipo de Reconstrucción y Restauración Coordinador de Obras Proyectos y Mantenimiento Coordinador de Innovación Tecnológica
•	Comprar equipos/ contratar servicios	Escoger los equipos y/o contrataciones a ser adquiridos tomando en cuenta las necesidades y el presupuesto del banco y luego elaborar la solicitud de compra de tales equipos y/o servicios, según el inventario recolectado por el equipo de reconstrucción y restauración.	Coordinador Equipo de Reconstrucción y Restauración

2.7	Coordinar la recuperación o reconstrucción de la instalación	Coordinar las tareas de reconstrucción del centro de cómputo, incluyendo entre otros, lo siguiente: – Obtener certificación para las instalaciones o áreas reconstruidas en el centro de cómputo principal. – Coordinar la instalación y configuración de los equipos que han sido adquiridos o recuperados. – Definir y realizar las pruebas requeridas para verificar el funcionamiento de los equipos y plataformas adquiridas y/o restauradas, que han sido instaladas y configuradas. – Certificar que los equipos instalados se encuentran disponibles para iniciar el proceso de restauración.	Coordinador Equipo de Reconstrucción y Restauración Coordinador de Obras Proyectos y Mantenimiento Coordinador de Innovación Tecnológica
2.8	Comunicar la finalización de la reconstrucción y recuperación del centro de cómputo principal.	Comunicar al Líder del plan de recuperación ante desastre y al Comité de Administración de Contingencias de Tecnología la finalización de la reconstrucción del centro de cómputo principal del banco, que debe incluir todas las plataformas necesarias para atender al banco como sitio principal.	Coordinador Equipo de Reconstrucción y Restauración
3. Coordinar retorno a la normalidad			
3.1	Planificar ejecución del proceso de restauración del sitio principal	Definir y planificar las condiciones en las que se realizará la restauración del servicio en el centro de cómputo principal. Realizar las pruebas necesarias para certificar que las aplicaciones de Telered pueden comunicarse con el nuevo sitio reconstruido. Revisar que las interfaces que estaban conectadas al sitio principal, estén activadas nuevamente.	Comité de Administración de Contingencias

3.2	Notificar al negocio la activación de los procedimientos de restauración	Suministrar el resumen de la planificación para la restauración del centro de cómputo principal. La información a proveer deberá incluir: – Fecha y hora en el que se realizará el procedimiento de restauración – Tiempo estimado de la interrupción	Líder del Plan de Recuperación ante Desastres
3.3	Notificar la activación de los planes/ procedimientos	Notificar la activación, de acuerdo a lo establecido en el árbol de llamadas, y según lo planificado, al personal responsable de la ejecución de los procedimientos de restauración para del plan de restauración del sitio principal.	Líder del plan de recuperación ante desastres
3.4	Iniciar proceso de restauración	De acuerdo al escenario de falla que se haya identificado, se debe activar la estrategia de restauración que corresponda. Esta activación contempla la ejecución de los procedimientos de recuperación establecidos en el **numeral 3.3 "Procedimiento de Retorno en el centro de cómputo principal"**, según sea el caso.	Coordinador de Equipo de Contingencia de Infraestructura, Comunicaciones y Aplicaciones

3.5	Monitorear ejecución de los procedimientos para el retorno	Durante el monitoreo de la ejecución de los procedimientos para el retorno, se deben realizar las siguientes tareas: Verificar que la activación, alistamiento y disponibilidad del centro de cómputo principal se esté llevando a cabo de acuerdo a lo establecido en el plan. Mantener contacto con los diferentes coordinadores de equipo. Tomar decisiones sobre inconvenientes presentados en la activación de los procedimientos y las estrategias de restauración. El Líder del Plan de recuperación ante desastres debe mantener una bitácora o trazabilidad de las decisiones tomadas por el comité, apoyado en el **Anexo 3: Control de Problemas y Soluciones.** Una vez finalizado el procedimiento de restauración, se procede con el siguiente paso.	Comité de Administración de Contingencias de Tecnología
3.6	Notificar finalización del proceso de restauración y cierre	Suministrar información al negocio acerca del resultado del procedimiento ejecutado, donde se deberá proveer la siguiente información: – Estatus del proceso de ejecución – Fecha y hora en la que se inició y finalizó el procedimiento.	Comité de Administración de Contingencias de Tecnología

3.3. Procedimiento de Restauración del Centro de Cómputo Principal o el Designado como Primario.

Este procedimiento contiene las actividades que se deben realizar para retornar a la normalidad la plataforma principal o el designado como primario, luego de ser superado el desastre.

A continuación se presenta la descripción detallada de cada una de las actividades:

#	Actividad	Descripción	Responsable
1. Definir estrategia de retorno a la normalidad			
1.1	Definir la estrategia de retorno	Definir la estrategia a emplear para el retorno a la normalidad en el centro de cómputo principal o el designado como primario, teniendo en cuenta el escenario de falla presentado.	Comité de Administración de Contingencias de Tecnología
1.2.	Comunicar la estrategia de retorno	Comunicar a los equipos, la información y consideraciones claves a tener en cuenta para el proceso de retorno.	Líder del Plan de Recuperación ante Desastres
1.3	Verificar la disponibilidad de la plataforma en centro de cómputo principal	Asegurar que todos los elementos del ambiente principal, se encuentren con la configuración y estado correctos para recibir toda la operación nuevamente. Se debe tener en cuenta: Que los recursos se encuentren disponibles en el centro de cómputo principal o el designado como primario. Que se haya notificado al Líder del Plan de Recuperación ante Desastres el avance de la reanudación de operaciones en el ambiente principal.	Coordinador de Equipo de Contingencias de Infraestructura, Comunicaciones y Aplicaciones

2. Realizar retorno a la normalidad del sitio principal o el designado como primario.			
2.1	Validar que los servidores se encuentren disponibles y encendidos	Validar que los servidores cuentan con las condiciones necesarias para iniciar la replicación de data hacia el centro de cómputo principal. Una vez hecha la verificación, activar la replicación del sitio de contingencia contra el principal; sin embargo, se debe tener en cuenta que el sitio de contingencia siempre deberá mantener el control hasta que el equipo de producción cuente con toda la información, igual a la del sitio de contingencia, y pueda seguir atendiendo los servicios del banco. Cuando los servicios estén replicados, establecer ante los comités el mejor momento para hacer el cambio al sistema principal y que este tome el control nuevamente.	Soporte Técnico.
2.5	Restaurar datos desde *backup* más reciente	Esta actividad aplica si la falla afectó tanto a producción como a contingencia. Es necesario restaurar desde la última copia en *backups* con que cuente el banco. Se restaura toda la información al sitio reconstruido.	Soporte Técnico
2.6	Activar replicación y esperar sincronía de datos	En este caso se deberá esperar la sincronía correcta de datos para los servidores restaurados en el sitio de producción.	Soporte Técnico

2.8	Bajar los servicios de servidores de contingencia, una vez sincronizada la información de los equipos.	Se deberán desactivar todos los servicios del sistema de contingencia.	Soporte Técnico
2.9	Cambiar los procedimientos de manual a automático para servidores y servicios.	De forma manual activar los procedimientos establecidos para activar los sistemas automáticos que establecerán la sincronización de los datos.	Soporte Técnico
2.10	Realizar cambio de rol para base de datos	De forma automática se deberán activar los procedimientos establecidos para cambiar a la forma automática los servicios.	Soporte Técnico
2.13	Subir servicios en sitio principal	De forma automática activar los procedimientos establecidos para iniciar o activar los servicios del sitio principal.	Soporte Técnico.
2.14	Activar las direcciones del sitio de producción.	Se debe realizar esta actividad en caso de que la falla ocurrida haya sido: De forma automática activar los procedimientos establecidos para cambiar de forma automática las direcciones.	Soporte Técnico
2.15	Direccionamiento de Telered hacia sitio principal	Se deberán ejecutar los siguientes pasos: Direccionar las transacciones al nuevo sitio de producción.	Coordinador de Comunicaciones
2.16	Levantar o activar aplicaciones principales.	Ejecutar los *script* establecidos para cambiar de forma automática los servicios que se van activar.	Soporte Técnico
2.17	Subir aplicación para ATM	Activar la aplicación que atiende ATM.	Soporte Técnico

2.18	Activar replicación desde sitio principal hacia contingencia	En este caso se deberán ejecutar los siguientes pasos: – Ejecutar los *script* establecidos para cambiar de forma automática los servicios. – Activar la replicación a su estado normal; quiere decir. role de producción normal hacia el role de contingencia normal.	Soporte Técnico
2.19	Revisar *URLs*	Se debe validar la disponibilidad de las *URLs*:	Soporte Técnico
2.20	Realizar cambio de DNS manual	Ejecutar los *script* establecidos para cambiar de forma automática los servicios para cambios de DNS. Normalmente es colocar la dirección IP correspondiente a cada servidor que se requiere cambiar.	Coordinador de Seguridad
3.		**Verificar Ambiente de Producción.**	
3.1	Notificar la disponibilidad del ambiente productivo	Comunicar el estatus del proceso de alistamiento del ambiente productivo para reanudar la operación.	Líder del Plan de Recuperación ante Desastres

CAPÍTULO IV

MANTENIMIENTO DEL PLAN DE RECUPERACIÓN DE DESASTRES.

4.1. Mantenimiento del Plan del DRP.

Para lograr que un requerimiento de recuperación sea viable y que su desarrollo se dé de manera precisa y adecuada, el Plan de Recuperación ante Desastres debe mantenerse actualizado y vigente. Para ello, el mantenimiento del mismo debe contar con el esfuerzo continuo de todos los integrantes de la **Gerencia de Tecnología** para que cualquier cambio que pueda afectarlo sea reflejado y documentado oportunamente en el DRP; contar con las herramientas necesarias para que este plan se mantenga de forma actualizada y de la forma más ágil que se pueda.

Responsabilidad del mantenimiento

El mantenimiento del (DRP) será responsabilidad del coordinador de preparación en recuperación ante desastres y contingencias.

Cualquier personal de la Gerencia que tenga conocimiento de un nuevo desarrollo o cambios a los sistemas existentes o cambios en el ambiente actual de procesamiento, debe notificar dicho cambio al coordinador de preparación en recuperación ante desastres y contingencias.

Objetivos y responsabilidades

Responsable	Objetivos	Responsabilidades
Coordinador de preparación en Recuperación ante Desastres y Contingencias.	Reflejar en el DRP todo cambio organizacional o de contexto, que afecte directa o indirectamente al mismo.	Coordinar las reuniones anuales de evaluación de riesgos y revisión general del DRP. Coordinar las pruebas periódicas del DRP y asegurar la documentación de los resultados arrojados por las mismas. Asegurarse que se mantiene actualizada la configuración de los centros de cómputo alternos, de acuerdo con los cambios y/o actualizaciones realizadas a los servidores y aplicaciones del centro de cómputo principal. Asegurarse que la documentación contiene todos los cambios y/o actualizaciones. Luego de ocurrido un desastre, de acuerdo con el impacto del análisis efectuado, proceder a realizar las modificaciones que correspondan. Obtener luego de ocurrido un desastre, los comentarios de los distintos coordinadores de los grupos de recuperación y registrar en la documentación los cambios que se consideren necesarios. Obtener también, el análisis de los incidentes registrados y guardar la documentación de los cambios que se consideren necesarios. Asegurar que se actualice el DRP cuando ocurra cualquier otro cambio que lo afecte directa o indirectamente.

Objetivos y responsabilidades de los equipos de recuperación

Responsable	Objetivos	Responsabilidades
Todos los Equipos de Recuperación	Informar al equipo coordinador correspondiente, todo suceso que pueda afectar el plan. Los equipos coordinadores son: Coordinador Equipo Contingencia de Infraestructura, Comunicaciones y Aplicaciones Coordinador de Recuperación Plataforma del Banco y Sistema de almacenamiento Coordinador de Recuperación de Bases de Datos – Servidores. Coordinador de Telefonía y Cableado de Red	Canalizar, mediante el Equipo de coordinadores, todas las novedades que hayan surgido durante la ejecución y/o revisión del DRP, así como también la solución que se dio al problema. Asistir a la reunión anual de DRP para identificar situaciones que deberán verse reflejadas en el DRP. Mantener actualizada la configuración y/o procedimientos de recuperación en los centros de cómputo alternos, de acuerdo con los cambios y/o actualizaciones realizadas en el centro de cómputo principal. Documentar todos los cambios y/o actualizaciones y/o procedimientos, tanto de los centros de cómputo principales como del centro de cómputo alterno, y transferirlos al coordinador de preparación y recuperación de desastres para actualizar el plan.

	Coordinador de Comunicaciones Proveedores de aplicaciones en caso de ser requeridos. Los que establezca el comité.	

4.1.1. Procedimientos de mantenimiento de plan del DRP.

Se entiende que los cambios podrán ser producidos como consecuencia de fuerzas externas (proveedores, mercado, entre otras), aparición de nuevas necesidades de los usuarios (revisión de especificaciones, incorporación de nuevas funciones).

En todos los casos se realizará un análisis de los costos que involucre cada cambio, antes de que dicho cambio pueda ser aprobado. Así como el análisis de impacto sobre los recursos, tiempos de implementación e interrelación con los servicios existentes.

Se deberá contemplar la planeación y ejecución de pruebas sobre las estrategias y planes de continuidad y recuperación ante desastres que se encuentren documentados, previa autorización del comité de continuidad de negocio y recuperación ante desastres y de acuerdo a los lineamentos establecidos en el Procedimiento de Gestión de Continuidad de Negocio.

CONCLUSIONES.

(Ramos, 2010)

Con la frase de una de las películas de la serie ***Jason Bourne***, uno de los personajes declara: "*Espero siempre lo mejor, pero me preparo para lo peor*". Estamos de acuerdo en adoptar esta frase como una política muy sana; que de seguro llevará a evitar muchas malas sorpresas. Algo similar refleja el lema de Andy Grove; "***Sólo los paranoicos sobreviven***", mismo que usó como título del libro autobiográfico donde reseña su exitosa labor como cofundador de Intel.

Preparar un plan de continuidad de negocios no es algo sencillo; abarca muchas áreas, que implica conocer las actividades de muchos para poder tener un buen plan de acción al momento que se presente la necesidad. Este plan de contingencia o DRP orientado hacia los ATM, está basado en experiencias adquiridas a lo largo de los años; sin embargo, también hemos tomado en cuenta las mejores prácticas del mercado para la implantación de este plan de recuperación de desastres. Además, tratamos de orientar al lector en cuales deben ser las prevenciones a tomar para la implementación o ejecución de un plan de esta envergadura.

Un proyecto como este es muy dinámico; requiere de cambios constantes en el mantenimiento de todas sus áreas. Por eso, es importante que se realicen pruebas cada cierto tiempo; que además, sirvan para generar un grado de confianza alto en la gerencia general, en la junta directiva y en general, en todos los mandos altos de la institución financiera.

Por lo mencionado anteriormente, concluimos que se debe tener un área o departamento dedicado exclusivamente al seguimiento y mejoramiento de este plan, utilizando herramientas para mantener el sistema; y asegurar de esta forma, que siempre estará al día el plan de contingencia en caso que ocurra un desastre.

Recomendaciones:

1. Conseguir el apoyo de la gerencia general y junta directiva del banco para el desarrollo exitoso del proyecto.

2. Formar un comité de contingencia en el banco con los gerentes de cada área con el fin de transmitir la importancia del plan; necesaria al momento de realizar pruebas y tomar decisiones. Todo el personal debe estar actualizado e involucrado en igual grado.

3. Implementar dos sitios alternos de contingencia, por las ventajas que ofrece tener este tipo de redundancia.

BIBLIOGRAFÍA

IS&BCA. (s.f.). *Information Security & Business Continuity Academy*. Obtenido de http://www.iso27001standard.com/es/servicios/Paquete-de-documentos-sobre-BS-25999

Bonilla, S. P. (s.f.). *Bonilla, Sandra Patricia Camacho.* Obtenido de www.acis.org.co/fileadmin/Base.../ConferenciaSandraCamacho.pdf

22301, I. 2. (s.f.). *Recuperación ante desastres vs. Continuidad del negocio.* Obtenido de http://blog.iso27001standard.com/es/tag/recuperacion-ante-desastres/

Revisión, A. B. (s.f.). *Search Data Center En Espanol.* Obtenido de http://searchdatacenter.techtarget.com/es/consejo/Aspectos-basicos-del-plan-de-recuperacion-de-desastres-Actualizacion-y-revision

No.006-2011, República de Panamá Superintendencia de Bancos acuerdo. (s.f.). Obtenido de http://www.superbancos.gob.pa/documentos/leyes_y_regulaciones/leyes_y_regulaciones/acuerdos/Acuerdo_6-2011.pdf

Ramos, A. (4 de octubre de 2010). *Optimismo Crítico - cómo evitar sorpresas y desilusiones en la clusterización.* Obtenido de Clusterizando: http://clusterizando.com/2010/10/04/optimismo-critico-%E2%80%93-como-evitar-sorpresas-y-desilusiones-en-la-clusterizacion/

bsigroup. (s.f.). *Requisitos de la ISO 22301.* Obtenido de bsigroup: http://www.bsigroup.es/es/Formacion/Areas-formacion/Continuidad-de-Negocio-ISO-22301/introduccion-22301/

Villalobos, J. S. (Enero de 2008). *Universidad para la cooperación Internacional.* Obtenido de www.uci.ac.cr/Biblioteca/Tesis/PFGMAP505.pdf

Telered.com.pa, O. . (s.f.). *Organización - Telered.com.pa.* Obtenido de http://www.telered.com.pa/es/org.htm

Sociedades, S. d. (6 de diciembre de 2011). *Guia: Plan de recuperación ante desastres DRP.*

Obtenido de http://www.supersociedades.gov.co/web/Ntrabajo/SISTEMA_INTEGRADO/Documentos%20Infraestructura/DOCUMENTOS/GINF-G-010%20Guia_%20DRP.pdf

ANEXO 1 – Directorio de Continuidad

A continuación se referencian las personas que conforman el Equipo del Plan de recuperación ante desastres, especificando su rol.

Equipo del DRP	Rol / Cargo	Titular	Suplente
Comité de Administración de Contingencias de Tecnología	Gerente Tecnología	Nombre: **Principal 1** Teléfono oficina: Teléfono móvil: Teléfono residencial: Correos electrónico:	Nombre: **Suplente 1** Teléfono oficina: Teléfono móvil: Teléfono residencial: Correos electrónico:
	Sub - Gerente de Tecnología	Nombre: **Principal 2** Teléfono oficina: Teléfono móvil: Teléfono residencial: Correos electrónico:	Nombre: **Suplente 2** Teléfono oficina: Teléfono móvil: Teléfono residencial: Correos electrónico:
	Líder del Plan de Recuperación ante Desastres	Nombre: **Principal 3** Teléfono oficina: Teléfono móvil: Teléfono residencial: Correos electrónico:	Nombre: **Suplente 3** Teléfono oficina: Teléfono móvil Teléfono residencial: Correos electrónico:
	Coordinador de preparación en Recuperación ante Desastres y Contingencias	Nombre: **Principal 4** Teléfono oficina: Teléfono móvil: Teléfono residencial: Correos electrónico:	Nombre: **Suplente 4** Teléfono oficina: Teléfono móvil Teléfono residencial: Correos electrónico:

Equipo de Reconstrucción y Restauración	Coordinador de Equipo de reconstrucción y restauración	Nombre: **Principal 5** Teléfono oficina: Teléfono móvil: Teléfono residencial: Correos electrónico:	Nombre: **Suplente 5** Teléfono oficina: Teléfono móvil Teléfono residencial: Correos electrónico:
	Coordinador de Obras, Proyectos y Mantenimiento (obras, mantenimiento: construcción, UPS elevadores y plantas eléctricas, aires acondicionados)	Coordinador de Mantenimiento: Nombre: **Principal 6** Teléfono oficina: Teléfono móvil: Teléfono residencial: Correos electrónico: Coordinador de Obras y Proyectos Nombre: **Principal 7** Teléfono oficina: Teléfono móvil: Teléfono residencial: Correos electrónico:	Coordinador de Mantenimiento: Nombre: **Suplente 6** Teléfono oficina: Teléfono móvil Teléfono residencial: Correos electrónico: Coordinador de Obras y Proyectos Nombre: **Suplente 7** Teléfono oficina: Teléfono móvil: Teléfono residencial: Correos electrónico:
	Coordinador de Servicios Administrativos (servicios generales, adquisición de bienes y servicios, seguros y seguimiento, soporte administrativo y mantenimiento)	Nombre: **Principal 8** Teléfono oficina: Teléfono móvil: Teléfono residencial: Correos electrónico:	Nombre: **Suplente 8** Teléfono oficina: Teléfono móvil Teléfono residencial: Correos electrónico:
	Coordinador de Equipo Tecnología (Bases de Datos, Comunicaciones Telefonía y Cableadores, Servidores, proveedores críticos	Nombre: **Principal 9** Teléfono oficina: Teléfono móvil: Teléfono residencial: Correos electrónico:	Nombre: **Suplente 9** Teléfono oficina: Teléfono móvil: Teléfono residencial: Correos electrónico:

Equipo Apoyo Logístico	Coordinador de Equipo de Apoyo Logístico	Nombre: **Principal 10** Teléfono oficina: Teléfono móvil: Teléfono residencial: Correos electrónico:	Nombre: **Suplente 10** Teléfono oficina: Teléfono móvil: Teléfono residencial: Correos electrónico:
	Coordinador Transporte y Logística	Nombre: **Principal 11** Teléfono oficina: Teléfono móvil: Teléfono residencial: Correos electrónico:	Nombre: **Suplente 11** Teléfono oficina: Teléfono móvil Teléfono residencial: Correos electrónico:
Equipo Recuperación de Infraestructura Comunicaciones y Aplicaciones	Coordinador Equipo de Infraestructura, Comunicaciones y Aplicaciones	Nombre: **Principal 12** Teléfono oficina: Teléfono móvil: Teléfono residencial: Correos electrónico:	Nombre: **Suplente 12** Teléfono oficina: Teléfono móvil: Teléfono residencial: Correos electrónico:
	Equipo de Recuperación de Servidores	Nombre: **Principal 13** Teléfono oficina: Teléfono móvil: Teléfono residencial: Correos electrónico:	Nombre: **Suplente 13** Teléfono oficina: Teléfono móvil Teléfono residencial: Correos electrónico:
	Equipo de Recuperación Plataforma de almacenamiento	Nombre: **Principal 14** Teléfono oficina: Teléfono móvil: Teléfono residencial: Correos electrónico:	Nombre: **Suplente 14** Teléfono oficina: Teléfono móvil: Teléfono residencial: Correos electrónico:
	Equipo de Recuperación de Bases de Datos	Nombre: **Principal 15** Teléfono oficina: Teléfono móvil: Teléfono residencial: Correos electrónico:	Nombre: **Suplente 15** Teléfono oficina: Teléfono móvil Teléfono residencial: Correos electrónico:
	Equipo de Recuperación Cableado	Nombre: **Principal 16** Teléfono oficina:	Nombre: **Suplente 16** Teléfono oficina:

	y Telefonía	Teléfono móvil: Teléfono residencial: Correos electrónico:	Teléfono móvil: Teléfono residencial: Correos electrónico:
	Coordinador Equipo de Contingencias de redes y Telecomunicaciones	Nombre: **Principal 17** Teléfono oficina: Teléfono móvil: Teléfono residencial: Correos electrónico:	Nombre: **Suplente 17** Teléfono oficina: Teléfono móvil Teléfono residencial: Correos electrónico:
	Coordinador de Soporte Centro de Cómputo Alterno	Nombre: **Principal 18** Teléfono oficina: Teléfono móvil: Teléfono residencial: Correos electrónico:	Nombre: **Suplente 18** Teléfono oficina: Teléfono móvil: Teléfono residencial: Correos electrónico:
	Coordinador de Producción	Nombre: **Principal 19** Teléfono oficina: Teléfono móvil: Teléfono residencial: Correos electrónico:	Nombre: **Suplente 19** Teléfono oficina: Teléfono móvil Teléfono residencial: Correos electrónico:
	Coordinador de Seguridad	Nombre: **Principal 20** Teléfono oficina: Teléfono móvil: Teléfono residencial: Correos electrónico:	Nombre: **Suplente 20** Teléfono oficina: Teléfono móvil Teléfono residencial: Correos electrónico:
	Coordinador de Apoyo a Usuarios	Nombre: **Principal 21** Teléfono oficina: Teléfono móvil: Teléfono residencial: Correos electrónico:	Nombre: **Suplente 21** Teléfono oficina: Teléfono móvil Teléfono residencial: Correos electrónico:

ANEXO 2 – Listado de Proveedores

Proveedor	Servicio	Contacto Principal	Contacto Alterno
Proveedor 1	Producto 1 Producto 2 Producto 3 Producto 4	Nombre: Cargo: Teléfono oficina: Teléfono móvil: Correos electrónico:	Nombre: Teléfono oficina: Teléfono móvil Teléfono residencial: Correos electrónico:
Proveedor 2	Producto 1 Producto 2 Producto 3 Producto 4	Nombre: Cargo: Teléfono oficina: Teléfono celular: Correos electrónico:	Nombre: Teléfono oficina: Teléfono móvil Teléfono residencial: : Correos electrónico:
Proveedor 3	Producto 1 Producto 2 Producto 3 Producto 4	Nombre: Cargo: Teléfono oficina: Teléfono celular: Correos electrónico:	Nombre: Teléfono oficina: Teléfono móvil Teléfono residencial: : Correos electrónico:
Proveedor 4	Producto 1 Producto 2 Producto 3 Producto 4	Nombre: Cargo: Teléfono oficina: Teléfono celular: Correos electrónico:	Nombre: Teléfono oficina: Teléfono móvil Teléfono residencial: : Correos electrónico:

ANEXO 3 – Control de Problemas y Soluciones

Este formato de control tiene como objetivo registrar los inconvenientes presentados **durante la activación, operación y retorno a la normalidad luego de ocurrido el desastre, contingencia o interrupción mayor**

No	Problema	Fecha	Hora	Solución	Tiempo de Solución	Solucionado por:

ANEXO 2 – Evaluación del Incidente

Este formato tiene como objetivo apoyar el proceso de evaluación del incidente.

No	Nombre	Departamento	Área
1			
2			
3			
4			

2. FECHA Y HORA DE LA EVALUACIÓN DEL INCIDENTE	
Fecha de evaluación :	
Hora inicio de la evaluación:	
Hora final de la evaluación:	
3. DESCRIPCIÓN DEL INCIDENTE	
Fecha de inicio:	
Hora de inicio :	
Descripción del incidente:	
Notificado por:	

4. Evaluación de Plataforma de ATM	
Sistemas o plataformas afectadas:	
Tiempo estimado de solución del incidente:	
5. OBSERVACIONES ADICIONALES	
6.Registro de Firmas	
Firma:	
Cargo y área :	
Nombre:	

ANEXO 5 – Listado de Recursos Para el sitio Principal.

Este formato tiene como objetivo verificar que todos los recursos requeridos para recuperar los servicios de tecnología críticos se encuentran disponibles en el centro de cómputo alterno con los que cuenta el banco.

1. REALIZADORES DE LA EVALUACIÓN

No	Nombre	Cargo	Área
1			
2			
3			
4			

2. FECHA Y HORA DE LA EVALUACIÓN

Fecha de evaluación :		
Hora inicio de la evaluación:		
Hora final de la evaluación:		
Características de los equipos afectados:	Están Disponible (Si / No)	
	a)	
	b)	

3. OBSERVACIONES ADICIONALES DETALLAR

4. REGISTRO DE FIRMAS	
Firma: **Nombre:** **Cargo**	**Firma:** **Nombre:** **Cargo:**