Protocolo de Gestión de Crisis del Sector Bancario Ante la Materialización de Riesgos No Financieros.

11 de agosto de 2021
Bogotá, D.C, Colombia
Versión 0.4

Control de versiones

Versión	Fecha (dd/mm/aaaa)	Responsable	Descripción
0.2	05/05/2021	Asobancaria	Especificación niveles de alerta
0.3	07/06/2021	Asobancaria	Ajustes a la Especificación niveles de alerta y evento de ciberseguridad
04	08/03/2021	Asobancaria	Revisión Jaime Rincón
05	11/08/2021	Asobancaria	Cambios estructura de gobierno, definiciones de glosario.

Asociación Bancaria y de Entidades Financieras de Colombia – Asobancaria

Hernando Jose Gomez Restrepo
Presidente

Alejandro Vera Sandoval
Vicepresidente Técnico

Elaboración del documento:

Jaime Andres Rincon
Director de Operaciones y Seguridad

Sergio Andres Silva
Profesional Junior
Dirección de Operaciones y Seguridad

Grupo de Trabajo de Centro de Comando:

Omar Gutiérrez
Director de Continuidad del Negocio
Banco Popular

Tatiana Lorena Sarria
Gerencia de Estrategia de Continuidad del Negocio
Bancolombia

Andrés Quijano
Profesional Senior
Asobancaria - Dirección de Operaciones y Seguridad

Diana Rocio Castiblanco Nieto
Profesional III
Banco Davivienda

Alexandra Vera Casallas
Jefe de Continuidad de negocio
Banco de Bogotá

Gerson Méndez
Analista PCN
Banco Avvillas

Diana Carolina Ceballos
Continuidad de Negocio
Banco de la República

Walter Wilches Jimenez
Profesional Universitario de Continuidad del Negocio
Banco Agrario

Contenido

GLOSARIO

ALERTA: Estado que se declara con anterioridad a la manifestación de un evento peligroso, con base en el monitoreo del comportamiento del respectivo fenómeno, con el fin de que las entidades bancarias activen procedimientos de acción previamente establecidos o definir estrategias de acción.

CENIT: El sistema CENIT – Compensación Electrónica Nacional Interbancaria, es una Cámara de Compensación Automatizada (conocida por sus siglas en inglés como ACH) operada por el Banco de la República, que provee el servicio de procesamiento de órdenes de pago o recaudo electrónicas de bajo valor, originadas por las entidades vinculadas a nombre propio o de sus clientes, personas naturales o jurídicas con cuenta corriente o de ahorros. Participan en el CENIT, además de todas las Entidades Bancarias, la Dirección General de Crédito Público y del Tesoro Nacional que canaliza los giros y pagos efectuados por la Nación a los entes territoriales; los Operadores de Información que tramitan el pago de los Aportes del Sistema General de Seguridad Social mediante la Planilla Unificada de Recaudo; DECEVAL que atiende el servicio de deuda de sus depositantes; y el Banco de la República para la realización de sus propios pagos y recaudos.

COMITÉ DE GESTIÓN DE CRISIS: Es una instancia de trabajo colaborativo entre las diferentes entidades bancarias para fortalecer la articulación del sector financiero en momento de crisis.

CIBERATAQUE O ATAQUE CIBERNÉTICO: Ataque cibernético que afecte a más de una de las entidades del sector financiero.

CRISIS: Situación de desastre o emergencia de riesgo no financiero que impacta el desarrollo de los procesos críticos del sector bancario, originando incertidumbre dentro de los Stakeholders, por lo que requiere una capacidad de respuesta inmediata, un manejo adecuado de comunicaciones y una administración oportuna de la situación.

DCV: Depósito Central de Valores. Es un sistema computarizado diseñado para el manejo, mediante registros electrónicos, de los títulos valores que emite o administra el Banco de la República; tiene como objetivos eliminar el riesgo que para los tenedores representa el manejo de títulos físicos, agilizar

las transacciones en el mercado secundario y facilitar el cobro de rendimientos de capital e intereses

DECEVAL: El Depósito Centralizado de Valores de Colombia -DECEVAL S.A.-, una entidad facultada para recibir en depósito títulos valores, instrumentos financieros y valores que se encuentren o no inscritos en el Registro Nacional de Valores e Intermediarios, sean emitidos en Colombia o en el exterior, para que mediante un sistema computarizado de alta tecnología y seguridad, administrarlos mitigando los riesgos asociados a su manejo físico en transferencias, registros, ejercicio de derechos patrimoniales etc.

DISTURBIOS CIVILES, GUERRA Y TERRORISMO: Eventos que impidan el acceso a las instalaciones o que afecten al personal de más de una entidad del sector financiero.

ESCENARIO: Conjunto de circunstancias de tiempo, lugar, modo que está influenciada por una situación ocasional que rodean un suceso.

EPIDEMIA Y/O PANDEMIA: Ocurrencia de un número de casos con daño particular en un área y en un tiempo dado, mayor que el número de casos esperados. Generalmente de amplia difusión en un territorio. (Ministerio de Salud y Protección Social de Colombia, s.f.)

ROCESOS CRÍTICOS: Hacen referencia a aquellos que por su interrupción causa mayores impactos en el sector financiero, se basan en la atención a clientes, oficinas, cajeros automáticos y los servicios comunes.

PROVEEDORES ESTRATÉGICOS: Aliado de las entidades bancarias que suministra o distribuye productos y servicios en el sector bancario, cualquiera que sea el título o contrato en virtud del cual realice dicha distribución o prestación.

PÓLIZA GLOBAL BANCARIA: Seguro global bancario como forma de mitigar el impacto del riesgo. Cubre las necesidades del sector específico y tiene dos características principales que la identifican. La primera, es que normalmente opera sobre la base del descubrimiento del siniestro. La segunda, es que es global y de amparos múltiples.

SEBRA: Servicios Electrónicos del Banco de la República. El objetivo del Sistema SEBRA es permitir el acceso seguro a los servicios electrónicos que permiten efectuar las transacciones y las comunicaciones entre el Banco de la República y el Sector Financiero, de una manera ágil, eficiente y segura.

SIMULACRO: Ejercicios prácticos que representan una situación de emergencia lo más cercano a lo que sería en la realidad, basados siempre en el análisis del riesgo municipal, en consecuencia, una simulación es una forma de poner a prueba la Estrategia de Respuesta y sus protocolos (UNGRD, s.f.) . Unidad Nacional para la Gestión del Riesgo de Desastres (UNGRD).

1. GENERALIDADES

1.1 Introducción:

Este documento incluye las estrategias y los lineamientos a seguir por Asobancaria y sus entidades afiliadas ante un Evento de Crisis como respuesta a situaciones excepcionales que afecten los Procesos Críticos del sector bancario, así como la respuesta gremial a requerimientos de autoridades, medios de comunicación frente a la crisis y atención a Proveedores Críticos en medio de la Crisis.

1.2 OBJETIVOS

1.2.1 Objetivo General:

- Establecer una estructura de gobierno y planes de acción que permitan articular acciones y lineamientos generales de forma gremial para administrar y gestionar Eventos de Crisis que afecten la continuidad en la prestación de los Procesos Críticos del sector bancario de manera conjunta entre Asobancaria y sus entidades agremiadas.

1.2.2 Objetivos Específicos:

- Recuperación del servicio y operación de Procesos Críticos. Definir las estrategias, procedimientos y herramientas para minimizar el impacto sistémico del sector bancario, garantizando la recuperación de los procesos gremiales definidos como críticos, que no puedan ser gestionados de manera individual.

- Atención de la crisis ante Proveedores Estratégicos del sector bancario que requieran atención gremial.

- Coordinación técnica de la respuesta ante autoridades y medios de comunicación: Proporcionar ante medios de comunicación y autoridades una respuesta técnica coordinada, rápida y efectiva ante algún evento gremial de crisis que impacte al sector financiero. En todo caso, para la comunicación gremial, se deben seguir los lineamientos del Manual de Comunicaciones en Crisis, elaborado por Asobancaria.

1.3 ALCANCE

- Incluye una estructura organizativa gremial para gestionar Eventos de Crisis que puedan generar afectación del servicio (clientes y usuarios), de conformidad con los niveles de alerta descritos en el capítulo 2 del presente documento.

- Incluye la gestión gremial de proveedores críticos y aliados estratégicos trasversales al sector financiero, que por la materialización de eventos de crisis puedan impactar el funcionamiento de la banca.

- Define estrategias de comunicación en crisis que involucra las partes interesadas.

- Contempla los lineamientos para la ejecución de simulacros que permitan asegurar la vigencia del protocolo y la identificación de oportunidades de mejora.

1.3.1 ESTE PROTOCOLO NO REGULA

- Crisis financiera y Eventos de interrupción en la continuidad operativa y tecnológica de las entidades financieras y los Proveedores Estratégicos del sector financiero que no se consideren como Eventos de Crisis o aquellos, enmarcados en el ámbito individual.

- A pesar de lo dispuesto en este documento, se entiende que cada entidad afiliada a Asobancaria y Proveedor Estratégico del Sector Financiero afectado aplicará sus planes internos de continuidad de negocio o crisis, según lo dispuesto en la normatividad vigente.

1.4 ESCENARIOS/ EVENTOS DE CRISIS DEL SECTOR BANCARIO

Este Protocolo será aplicable en los siguientes escenarios/eventos cuando ocurran situaciones excepcionales que afecten o impidan la continuidad normal de los procesos críticos del numeral 1.5 del presente documento:

1.4.1 Ciberataque o Ataque Cibernético: Ataque cibernético que afecte a más de una de las entidades del sector financiero.

1.4.2 Epidemia /Pandemia: Declaración de Pandemia por parte de las entidades autorizadas tanto globales como locales (Organización Mundial para la Salud, Ministerio de Salud y Protección Social o Secretarías de Salud) que afecté le funcionamiento normal del sector.

1.4.3 Disturbios civiles, guerra y terrorismo: Eventos que impidan el acceso a las instalaciones o que afecten al personal de más de una entidad del sector financiero.

1.4.4 Desastre Natural: Evento inesperado y catastrófico que afecta de manera grave la infraestructura física, tecnológica, humana, etc. de la ciudad o país. Ej. Terremoto (entre otros).

1.4.5 Eventos emergentes de Riesgos no Financieros: Son todos los eventos ajenos a los definidos que tengan impacto o afecte la operatividad bancaria de riesgo no financiero.

1.5 PROCESOS CRÍTICOS DEL SECTOR BANCARIO:

Este documento se enfocará en las actuaciones que deberá seguir el gremio sobre los Procesos Críticos que afectan la operación bancaria en caso de crisis

Los procesos críticos definidos por las entidades agremiadas a Asobancaria son los siguientes:

- Proceso de gestión, distribución y acceso a efectivo
- Proceso de Canje (compensación de cheques CEDEC)
- Proceso transaccional en redes (ACH, Credibanco, Redaban)
- Proceso Compensación electrónica interbancaria
- Proceso Cuentas de Depósito Banco de la República CUD
- Proceso DECEVAL Custodia de títulos valores desmaterializados
- Negociación y custodia de títulos del estado - DCV
- Proceso Negociación y Cumplimiento de Operaciones con BVC
- Proceso de administración de pagos y transferencia en moneda extranjera – Swift
- Realización de operaciones de expansión y contracción transitoria o permanente e intervención cambiaria (subastas de liquidez) Banco de la República.
- Proceso de compensación de PILA
- Recaudo de Impuestos
- Reporte autoridades
- Comunicados a medios de comunicación
- Distribución por servicio bancario digital
- Distribución por servicio bancario físico

2. NIVELES DE ALERTA

Para efectos de la aplicación del presente Protocolo:

- Los niveles de alerta son: Amarillo y Rojo, de acuerdo con la gravedad de los Eventos de Crisis que se presenten. El nivel de alerta amarillo activara los órganos de gobierno del nivel táctico y el nivel rojo activara los órganos de gobierno del nivel estratégico, así como las estrategias a tomar en cada caso.

- Luego de la declaratoria de crisis, cada entidad debe evaluar y determinar el nivel de alerta en el que se encuentra, de forma individual e informar al equipo coordinador.

- Conforme la información recibida, el equipo coordinador evaluará la situación para informar sus resultados al comité de gestión de crisis quien definirá el nivel de alerta, de igual forma este comité tomará las medidas que estime necesarias para estabilizar la operación afectada en las Entidades Financieras y minimizar el impacto desfavorable del Evento.

2.1 DEFINICIÓN DE LAS ALERTAS

A continuación, la gráfica 1. Muestra los criterios de activación por niveles de alerta sobre los procesos críticos definidos en el numeral "1.7 PROCESOS CRÍTICOS DEL SECTOR BANCARIO" que deberán atender las entidades financieras al momento de la materialización de alguno de los eventos de crisis definidos "1.5 ESCENARIOS/ EVENTOS DE CRISIS DEL SECTOR BANCARIO.

Tabla 1. criterios de activación por niveles de alerta [1]sobre procesos críticos del sector bancario.

PROCESOS CRITICOS		**CRITERIOS DE ACTIVACION POR ALERTAS**	
		AMARILLA	**ROJA**
1	Proceso de gestión, distribución y acceso a efectivo	Entre 50% y 75% disminución del inventario en las bóvedas = 1 mes	Mayor al 75% disminución del inventario en las bóvedas = 15 días
2	Proceso de Canje (compensación de cheques CEDEC)	Entre 24 y 36 horas sin compensación	Mayor a 36 horas sin compensación
3	Proceso transaccional en redes (ACH, Credibanco, Redeban)	Entre 24 y 48 horas sin transaccionalidad	Mayor a 48 horas por fuera sin transaccionalidad
4	Proceso Compensación electrónica interbancaria (CENIT o ACH)	No pudo gestionarse un (1) ciclo interbancario	No pudieron gestionarse dos (2) ciclos interbancarios
5	Proceso Cuentas de Depósito Banco de la República CUD	Si el Banco de la República excede sus tiempos de uso de contingencia y alerto al gremio sobre el evento presentado.	El Banco de la República declara al gremio que esta en crisis.

[1] Estos criterios fueron definidos por la mesa de trabajo para garantizar la operación de los bancos de acuerdo a cada nivel alerta.

6	Proceso DECEVAL Custodia de títulos valores desmaterializados	Entre 1 a 3 horas sin custodia	Mayor a 3 horas sin custodia
7	Negociación y custodia de títulos del estado - DCV	Si el Banco de la República excede sus tiempos de uso de contingencia y alerto al gremio sobre el evento.	Declaración de crisis por pate del banco de la República
8	Proceso Negociación y Cumplimiento de Operaciones con BVC	De 30 minutos a 2 horas sin cumplimiento de operaciones	A partir de 2 horas sin cumplimiento de operaciones
9	Proceso de administración de pagos y transferencia en moneda extranjera – Swift	Indisponibilidad del servicio por (1) día	Indisponibilidad del servicio por (2) días
10	Realización de operaciones de expansión y contracción transitoria o permanente e intervención cambiaria (subastas de liquidez) Banco de la República.	Indisponibilidad del servicio (1) día	Indisponibilidad del servició (2) días
11	Proceso de compensación de PILA	Indisponibilidad del servicio por (1) día	Indisponibilidad del servicio por (2) días
12	Recaudo de Impuestos	Indisponibilidad del servicio por (1) día	Indisponibilidad del servicio por (2) días
13	Reporte autoridades	Imposibilidad de hacer reporte por (1) día	Imposibilidad de hacer reporte por (2) día
14	Comunicados a medios de comunicación	Según lo definido por el protocolo de comunicaciones	
15	Distribución por servicio bancario digital	Afectación en los canalés digitales por más de (24) horas*.	Afectación en los canalés digitales por más de (48) horas
16	Distribución por servicio bancario físico	Afectación física de las sucursales bancarias por más de (24) horas sin posibilidad de hacer el 10% de operaciones en otros canales en una ciudad con presencia de 3 o más bancos.	Afectación física de las sucursales bancarias por más de (48) horas sin posibilidad de hacer el 10% de operaciones en otros canales en una ciudad con presencia de 3 o más bancos.

- No obstante, se considerará una **Alerta Amarilla** cuando una o más entidades bancarias durante (12) horas sobrelleven la materialización de los siguientes

eventos y por lo menos una entidad financiera considere necesaria la intervención del gremio:

- Una interrupción de su operación.
- Fallas o imposibilidad de activación de su plan de Continuidad del Negocio, donde su aplicación de contingencia no sea exitosa, y no pueda estabilizar su operatividad.

- No obstante, se considera una **Alerta Roja** cuando una o más entidades bancarias durante (24) horas sobrelleven la materialización de alguno de los siguientes eventos y por lo menos una entidad financiera considere necesaria la intervención del gremio:

  - Se presenten fallas o imposibilidades de activar sus planes de Continuidad del Negocio individuales o su activación no sea exitosa.

  - Cuando las medidas de mitigación de impacto de un incidente de Alerta amarilla no hayan sido efectivas.

2.2 Probabilidad de nivel de impacto de los escenarios en los recursos del sector.

Ante la materialización de alguno de los eventos de crisis definidos en el numeral 1.5 ESCENARIOS / EVENTOS DE CRISIS DEL SECTOR BANCARIO la respuesta del sector financiero ante un escenario / evento de crisis deberá enfocarse en los efectos de la crisis en los siguientes recursos: personas, tecnología e infraestructura de acuerdo con la siguiente tabla de priorización. A continuación, se relaciona la potencial afectación de estos recursos de acuerdo a los Eventos de Crisis

Tabla 2[2]. Niveles de alerta de los escenarios definidos para este protocolo

ESCENARIO		PERSONAS	TECNOLOGÍA	INFRAESTRUCTURA
1	**DESASTRE NATURAL**	ALTO	ALTO	ALTO
2	**PANDEMIA**	ALTO	MEDIO	MEDIO
3	**CIBERATAQUE O ATAQUE CIBERNÉTICO**	**N/A**	ALTO	**N/A**
4	**DISTURBIOS CIVILES, GUERRA O TERRORISMO**	MEDIO	BAJO	MEDIO

2.3 Niveles de impacto por procesos críticos

[2] la tabla 2. Muestra la probabilidad de impacto definido en: alto, medio, bajo sobre la relación entre los escenarios y las variables de indisponibilidad al interior de las entidades financieras por los niveles de alerta.

Ante la materialización de alguno de los eventos de crisis definidos en el numeral 1.5 ESCENARIOS / EVENTOS DE CRISIS DEL SECTOR BANCARIO la respuesta del sector financiero ante un escenario / evento de crisis deberá enfocarse en la recuperación de los Procesos Críticos según la probabilidad por nivel de impacto ante la materialización de uno de los eventos de crisis definidos en el numeral 1.7 de acuerdo con la siguiente tabla de potenciales impactos en los procesos críticos:

Tabla 3. Nivel de impacto[3] por procesos críticos de acuerdo con fuente de riesgo afectada.

	Procesos criticos /Escenarios	Desastre Natural y Antrópico	Epidemia /Pandemia	Ciberataque o Ataque Cibernético	Disturbios civiles, guerra y terrorismo
1	Proceso de gestión, distribución y acceso a efectivo	ALTO	MEDIO	MEDIO	MEDIO
2	Proceso de Canje (compensación de cheques CEDEC)	ALTO	MEDIO	MEDIO	MEDIO
3	Proceso transaccional en redes (ACH, Credibanco, Redeban)	ALTO	BAJO	MEDIO	BAJO
4	Proceso Compensación electrónica interbancaria	ALTO	BAJO	ALTO	BAJO
5	Proceso Cuentas de Depósito Banco de la República CUD	MEDIO	BAJO	MEDIO	BAJO
6	Proceso DECEVAL Custodia de títulos valores desmaterializados	MEDIO	BAJO	MEDIO	BAJO
7	Negociación y custodia de títulos del estado - DCV	ALTO	BAJO	MEDIO	BAJO
8	Proceso Negociación y Cumplimiento de Operaciones con BVC	ALTO	BAJO	ALTO	BAJO
9	Proceso de administración de pagos y transferencia en moneda extranjera – Swift	MEDIO	BAJO	ALTO	BAJO

[3] Estos criterios fueron definidos por la mesa de trabajo de acuerdo con en análisis que se realizo frente al impacto de los procesos críticos para cada uno de los eventos de crisis definidos.

10	Realización de operaciones de expansión y contracción transitoria o permanente e intervención cambiaria (subastas de liquidez) Banco de la República.	MEDIO	BAJO	MEDIO	BAJO
11	Proceso de compensación de PILA	MEDIO	BAJO	MEDIO	BAJO
12	Recaudo de Impuestos	ALTO	BAJO	MEDIO	MEDIO
13	Reporte autoridades	ALTO	BAJO	MEDIO	BAJO
14	Comunicados a medios de comunicación	MEDIO	BAJO	MEDIO	BAJO
15	Distribución por servicio bancario digital	MEDIO	BAJO	ALTO	BAJO
16	Distribución por servicio bancario físico	ALTO	ALTO	MEDIO	ALTO

2.4 INICIO DE LAS ACTUACIONES ANTE UN VENTO DE CRISIS:

La Dirección de Gestión Operativa y Seguridad – DGOS de Asobancaria, comunicará y convocará al Nivel Táctico, en un plazo máximo de 1 día calendario, cuando se presente alguna de las siguientes situaciones generales:

- Un miembro del Comité de Gestión de crisis lo haya solicitado.
- Uno de los presidentes de una entidad agremiada a la Asociación haya informado sobre la materialización del evento de crisis o cualquier instancia directiva de Asobancaria.
- Uno de los vicepresidentes miembros de algún comité o junta de Asobancaria haya informado sobre la materialización del evento de crisis o cualquier instancia directiva de Asobancaria.
- Cuando las directivas de Asobancaria lo consideren.
- Circule en 2 o más medios de comunicación la noticia sobre la materialización de un Evento de Crisis.

2.5 Declaración de la Crisis e inicio de actuaciones.

Una vez citado el Comité de Crisis de Asobancaria, este deberá evaluar el Nivel de Alerta en que se encuentra el sector y decretar la Crisis a nivel Gremial. En caso de que se defina que se encuentra en una Nivel de Alerta Roja, se procederá a citar a la Junta Directiva de Asobancaria, de acuerdo a lo dispuesto por este documento.

3. ESTRUCTURA DE GOBIERNO

Con el fin de responder adecuadamente ante los eventos/ escenarios de una crisis, se definen a continuación los órganos de Gobierno de atención a la crisis. Cada uno de estos órganos de Gobierno tendrán funciones antes, durante y después de la Crisis.

3.1 ESTRUCTURA

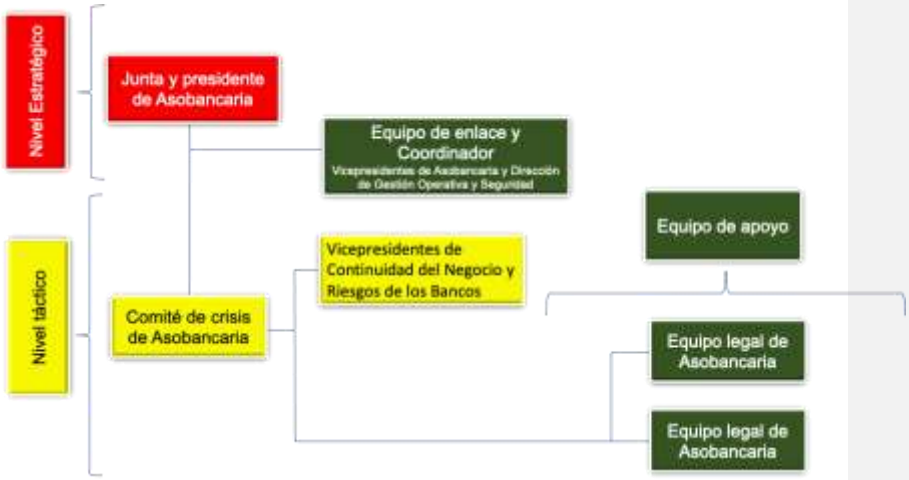
En los órganos de gobierno donde participan los funcionarios designados por cada uno de las Entidades Financieras, según lo estimen necesario o conveniente, podrán invitar a personas externas, asesores, o representantes de terceros, incluyendo a los proveedores estratégicos.

El diseño, activación y ejecución de las actividades establecidas en el Protocolo de Crisis del sector financiero estarán a cargo de los siguientes órganos de gobierno:

- **Nivel estratégico:**
  - Junta de Asobancaria – Presidentes Bancos[4] y presidente de Asobancaria
- **Nivel Táctico:**
  - Comité de Crisis Asobancaria
  - Equipo legal - vicepresidente legal Asobancaria
  - Equipo táctico - vicepresidente técnico de Asobancaria y dirección de gestión operativa y seguridad
  - Equipo de Comunicaciones - vicepresidente de asuntos corporativos de Asobancaria
- **Equipo de enlace:**
  - Vicepresidente Técnico junto con la dirección de gestión operativa y seguridad.

[4] Hace referencia a los presidentes de los bancos que son miembros de la junta de Asobancaria.

Gráfico 1 – Estructura de Gobierno.



3.2 Funciones y Responsabilidades de los Niveles:

Este capitulo 3.2 se refiere a la generalidad de las funciones y responsabilidades de los diferentes niveles de gobierno del presente protocolo. No obstante, en cada uno de los eventos de crisis se definen unas funciones y responsabilidad adicionales de acuerdo al evento específico.

3.2.1 Nivel Estratégico

Este nivel será el encargado de tomar las decisiones dentro de su ámbito de responsabilidad como máxima instancia en la gestión de crisis del sector

bancario además de apalancar decisiones de nivel táctico. Los mecanismos para la toma de decisiones deberán seguir los lineamientos del ser l gobierno corporativo de Asobancaria .

3.2.1.1 Estructura

El Nivel Estratégico está integrado por la Junta Directiva de Asobancaria la cual está compuesta por los siguientes órganos:

- Presidentes de las Entidades Agremiadas Miembros de junta
- Presidente de Asobancaria

3.2.1.2 Funciones y responsabilidades de los Miembros

- **Antes de la crisis:**

  - Aprobar el protocolo de crisis
  - Participar de las pruebas estratégicas
  - Retroalimentación a nivel de protocolo y pruebas
  - Promover la efectividad del protocolo

- **Durante la Crisis:**

  - Tomar las decisiones y avalar los diferentes planes de acción frente a los eventos de crisis propuestos en este documento.

  - Transmitir al Equipo de Comunicaciones la información que debe ser divulgada de manera coordinada y definir la línea general de los mensajes a comunicar.

  - Recibir informes de las acciones definidas durante la crisis por el equipo de enlace.

- **Después la Crisis:**

  - Monitorear la atención oportuna de las necesidades que surjan como consecuencia de un Evento de Crisis.

  - Promover la actualización del protocolo de crisis con las lecciones aprendidas

3.2.1.3 Equipo de coordinador y de enlace con nivel estratégico:

El Equipo enlace estará integrado por el Vicepresidente Técnico y la dirección de gestión operativa y seguridad.

El equipo enlace es el órgano de gobierno de carácter operativo que deberá estar en constante comunicación y coordinación con el Comité de Crisis y los demás equipos. Tiene las siguientes funciones y responsabilidades delegadas por el Nivel estratégico:

- **Antes de la crisis:**

  - Identificar mejoras a las acciones existentes y nuevas acciones como mecanismos para responder ante un Evento de Crisis.

  - Propender por implementar las actividades incorporadas en el Protocolo.

  - Coordinar la actualización de los datos de contactos de los integrantes de los comités.

  - Diseñar, implementar y mantener actualizado el presente Protocolo de Crisis.

  - Indagar y profundizar sobre la materialización de posibles eventos de crisis.

  - Mantener actualizado los Integrantes y Datos de Contacto de los integrantes del comité de gestión de crisis y su suplente a través de una encuesta periódica.

  - Solicitar información y mantener comunicación periódica con aliados estratégicos del sector sobre la gestión de crisis.

  - Liderar la construcción del protocolo de gestión de crisis y propender por su actualización de acuerdo con la retroalimentación de los otros niveles.

  - Gestionar recursos tecnológicos y humanos al interior de la Asobancaria para atender la crisis.

- **Durante la crisis:**

  - Mantener comunicación constante con el regulador para coordinar acciones en pro de minimizar los impactos al sector.

- En ausencia de titular o su delegado de alguno de los miembros de los órganos de gobierno deberá buscar y asignar el reemplazo, siguiendo en todo caso, las definiciones del Gobierno Corporativo de Asobancaria. .

- Convocar al nivel táctico y/o estratégico de acuerdo con el Nivel de Alerta materializado.

- Activar canales de comunicación necesarios para informar a entes reguladores y/o entidades de gobiernos

- Ser canal de comunicación entre el nivel estratégico y nivel táctico.

- Solicitar la información a las entidades financieras afectadas en el momento que se requiera sobre el número de cajeros y/o sucursales físicas – oficina a nivel nacional de acuerdo con los criterios definidos por la Asobancaria.

- Dependiendo de los niveles de alerta se activarán las estrategias definidas en este documento

- Identificar y analizar el impacto que se materializó sobre el evento de crisis y notificar (por e-mail, comunicación telefónica, WhatsApp, correo en la nube, mensaje de texto, telefonía satelital) a todos los miembros del Comité de Crisis para su activación.

- Mantener comunicación permanente con los integrantes y/o respectico suplente del nivel táctico incluyendo a los aliados estratégicos.

- Ser canal entre las entidades financieras y aliados estratégicos frente a las estrategias sobre los eventos de crisis materializados.

- **Después de la crisis:**

  - Propender por la implementación de las acciones definidas durante la crisis por el nivel táctico de este protocolo.

  - Informar a todos los integrantes del comité de gestión de crisis sobre el retorno a la normalidad.

  - Realizar seguimiento al cumplimiento de las estrategias y retroalimentar el proceso de manejo de información (contactos, oficinas, cajeros, etc.) de ser necesario a los diferentes comités.

3.2.1.4 Nivel Táctico

El Equipo táctico estará integrado por los siguientes órganos:

- Comité de Gestión de Crisis: Integrado por representantes de Bancos. Cada banco Titulares del Comité de Gestión de Crisis de Asobancaria .
- Equipo de comunicaciones: Vicepresidencia de asuntos corporativos de la Asociación
- Equipo Coordinador: Dirección de Operaciones y de Seguridad de la Asociación.
- Equipo legal: Vicepresidencia jurídica de la Asociación.

3.2.1.5 Comité de crisis:

El Comité de Crisis de las Entidades Financieras estará integrado por un representante de cada uno de los bancos agremiados a la Asociación Bancaria de Entidades Financieras de Colombia, de acuerdo a lo definido por el Gobierno Corporativo de la entidad.

El presidente de las entidades agremiadas podrá reemplazar en cualquier momento al representante designado para integrar el Comité y la persona designada deberá:

- Asegurar la implantación de todos los aspectos relacionados con el Plan de Continuidad respecto a su entidad o competencia.
- Gestionar la información de crisis a proveedores o terceros, afectados operativamente.
- Comunicar al interior de su entidad a la Alta Dirección sobre las decisiones tomadas en el Comité Táctico y Operativo, así como también informar el plan de trabajo.

- **Antes de la Crisis:**
  - Revisar al menos dos veces al año este Protocolo, en caso tal que no se haya actualizado después de la ejecución de una prueba del mismo o un evento de crisis.
  - Participar activamente de las pruebas definidas del protocolo establecido.
  - Revisar la definición de estrategias de recuperación ante posibles eventos de interrupción de alto impacto en el gremio, incluidos los riesgos emergentes.

- Actualizar y/o validar de manera anual los procesos críticos definidos en el numeral "*1.7 PROCESOS CRÍTICOS DEL SECTOR BANCARIO"*

- Definir las estrategias para cualquier tipo de alerta (amarilla, o roja) que se pueda presentar para minimizar el impacto sistémico del sector bancario

- Promover una política de permanente comunicación de incidentes en el sector bancario.

- **Durante la Crisis:**

  - Recopilar información relevante respecto a la afectación de la tecnología, las personas y la infraestructura física las Entidades Financieras importantes y realizar un diagnóstico de la situación para determinar el nivel de alerta del evento

  - De acuerdo con la información presentada por el equipo coordinador según lo informado por los bancos deberá decretar la crisis y su nivel de alerta.

  - Proponer en función de la situación de crisis que se origine, la activación del plan de acción o de las medidas de actuación a seguir. Suministrar la información para la construcción del comunicado a transmitir a la opinión pública.

  - Monitorear los reportes sobre el estado de las actividades de recuperación y retorno a la operación normal.

  - Establecer las afectaciones de cada uno de los Procesos Críticos de acuerdo a la probabilidad de impacto de cada Escenario y poner en marcha su plan de recuperación.

  - Establecer las afectaciones de cada uno de los Recursos del Sector (infraestructura, personas, tecnología) de acuerdo a la probabilidad de impacto de cada Escenario y poner en marcha su plan de recuperación.

  - Ejecutar los protocolos de comunicación a los principales interesados

  - Definir las estrategias de acción que no preestablezca este protocolo

  - Revisar la póliza global bancaria

  - Gestionar la atención de las alertas amarillas o rojas, según lo establecido en este documento

- Estar al tanto de la situación actual de la crisis, transmitir la información al interior de su entidad
- Tomar decisiones en representación de su entidad en pro de gestionar la crisis gremial.
- Escalar la propuesta de activación del Nivel Estratégico a través del equipo de enlace de acuerdo con el evento presentado
- De acuerdo con el tipo de alerta accionar las estrategias definidas
- Monitorear las estrategias activadas
- Sugerir la declaración de terminación de la crisis al comité estratégico.
- Activar las estrategias definidas en este protocolo ante los eventos de crisis

- **Después de la Crisis:**
  - Evaluar la gestión realizada durante la crisis con el fin de optimizar las estrategias asociadas a este protocolo, en caso de que estas no existieran o correspondiera a un evento no contemplado.
  - Actualizar las estrategias definidas en el documento para manejo de crisis, con las buenas prácticas implementadas durante la misma.
  - Retroalimentar las estrategias frente a las partes interesadas.

4. Canales de comunicación:

Los siguientes canales de comunicación están listados de acuerdo a su prioridad y deberán ser utilizados en orden según el estado de la Crisis y su disponibilidad al momento de la Crisis.

1. **Correos electrónicos institucionales:** El canal principal para las comunicaciones en crisis será el correo electrónico. Si no hubo afectación a los servidores, son un canal seguro de comunicación entre los bancos y proveedores críticos.
2. **WhatsApp:** El canal secundario para las comunicaciones será WhatsApp. Ofrece comunicación de disponibilidad media-alta. Aunque depende de los proveedores de datos y comunicaciones, está demostrado que la comunicación por datos tiene mayor cobertura y disponibilidad que la comunicación por voz o mensaje de texto en eventos

de gran magnitud. Permite la comunicación directa a un usuario o grupo específico.

3. **Comunicación telefónica:** Como tercer canal, su disponibilidad varía dependiendo del escenario. Permite hacer conferencias telefónicas entre los proveedores o convocar a reuniones presenciales o virtuales.
4.
5. **Mensajes de texto (SMS):** Como cuarto canal, se recomienda su uso para transmisión de mensajes uno a uno, cortos y concretos con referencia a un evento ocurrido, decisión tomada o instrucción.

6. **Comunicación satelital:** como quinto canal, su disponibilidad varía dependiendo del escenario. Permite llamadas satelitales entres las entidades que cuenten con el servicio.

Reuniones presenciales o virtuales: el punto de reunión principal será en las Instalaciones de la Asociación Bancaria y de Entidades Financieras de Colombia, Asobancaria, el alterno deberá ser el centro de efectivo del Banco de la República Calle 24 Bis # 66-90, Bogotá, (Carolina Ceballos – jefe de Sección – Continuidad o Diego Mauricio Vásquez – Director Departamento de Gestión de Riesgos y Procesos). En caso de que no sea posible o conveniente utilizar ninguna de estas instalaciones, quien convoque los equipos definirá lugar y horario de reunión presencial o virtual. En caso de reunión virtual, se optará por los medios disponibles (WhatsApp, Microsoft Teams, Meet, Zoom, Skype, Webex, etc.).

5. Actividades del Nivel táctico asociados a cada proceso crítico afectado:

Comentado [JA1]: Revisar que este capitulo tenga sentido por favor!!

De acuerdo con los Procesos críticos definidos en el numeral 1.5 PROCESOS CRÍTICOS DEL SECTOR BANCARIO, los numerales 1, 2, 5, y 10 son propios del Banco de la República.

El equipo de coordinador y de enlace deberá comunicarse con las infraestructura critica (Banco de la República – Banrep) para obtener más información del incidente (Sistema de pagos de alto valor CUD y bajo valor CENIT).

El equipo de coordinador y de enlace debe velar porque el Banco de la República presente la siguiente información:

5.1 Nivel de afectación modificación en tiempos definidos:

- ¿En cuánto tiene estimado el Banco de la República el Tiempo Objetivo de Recuperación?
  RTA: 2 Horas para el Banco de la República.
- ¿En cuánto tiene estimado el punto de Objetivo de recuperación

- RTA = 0 (Sin perdidas de información en los datos de los servicios)
- Verificar que los planes de continuidad del negocio de las entidades estén acordes con el plan del Banco de la República

5.2 El Nivel Táctico debe construir un informe con la siguiente información:

- La cantidad de transacciones afectadas de todos los actores involucrados.
- El monto de las transacciones afectadas.
- Definir un plan de trabajo conjunto que contenga: plan de trabajo conjunto entre nivel táctico, Banco República o los involucrados en la afectación del proceso critico
- Actividades
- Responsable
- Tiempo
- Indicador esperado frente a los procesos críticos definidos 2.1 DEFINICIÓN DE LAS ALERTAS
- Procesos críticos 3, 4, 11, 9. Redes procesadoras de pagos.
- El equipo coordinador deberá comunicarse con las redes procesadoras de pagos o SWIFT, de acuerdo con su nivel de afectación, para obtener más información del incidente.

5.3 El comité de crisis deberá velar porque las redes presenten al comité si Nivel de afectación de acuerdo con las siguientes preguntas:

- ¿En cuánto tiene estimado el Tiempo Objetivo de Recuperación (RTO)?
  RTA: 2 Horas para el Banco de la República.
- ¿En cuánto tiene estimado el punto de Objetivo de recuperación (RPO)?
  RTA = 0 (Sin perdidas de información en los datos de los servicios)

5.4 El equipo coordinador y de enlace debe construir un informe con la siguiente información:

- Cantidad de transacciones comprometidas
- Inventario de información comprometida
- Cantidad de comercios afectados
- Cantidad de productos financieros comprometidos
- Proponer realizar una investigación forense con una QSA que pertenezca al PCI Council con el fin de obtener un diagnóstico real del incidente (no aplica para el proceso crítico 9).
- Definir un plan de trabajo conjunto que contenga
- Actividades

- Responsable
- Tiempo
- Indicador esperado
- En caso de que el incidente afecte datos de tarjetas de crédito el comité deberá evaluar la pertinencia de invitar autoridades o entidades de investigación como Incocrédito para lograr la solución de la crisis
- El equipo coordinador deberá comunicarse con la BVC y/o DECEVAL para obtener más información del incidente.

5.5 El equipo coordinador y de enlace debe velar porque la BVC o DECEVAL presenten:

- Nivel de afectación
- ¿En cuánto tiene estimado el Tiempo Objetivo de Recuperación (RTO)?
- ¿En cuánto tiene estimado el punto de Objetivo de recuperación (RPO)?
- El comité debe verificar:
- La información relevante respecto a la afectación de la tecnología, las personas y la infraestructura física de los proveedores de infraestructura sistémicamente importantes y realizar un diagnóstico de la situación para determinar el nivel de afectación.
- La disponibilidad de servicios transaccionales.
- La disponibilidad de recursos del sector bancario (inversiones) en el mercado de capitales, a efecto de liquidez y solvencia de los bancos.
- La disponibilidad de sistema de proveedores de liquidez (Miembros Liquidadores de la CCRC y otros).
- La Información comprometida.
- La cantidad y monto de transacciones afectadas.
- La preparación de los sistemas de información para el retorno, mediante conciliación y arqueo de operaciones teniendo en cuenta lo definido en las Reglas de Operación de la BVC.
- La activación del Protocolo de Crisis de las Infraestructuras del Mercado de Valores Y Divisas
- Definir un plan de trabajo conjunto que contenga.
- Actividades
- Responsable
- Tiempo
- Indicador esperado

Proceso crítico 12 – DIAN

El equipo coordinador y de enlace deberá comunicarse con la DIAN para obtener más información del incidente.

Por lo anterior, el equipo coordinador y de enlace debe velar porque la DIAN presente:

- Nivel de afectación
- ¿En cuánto tiene estimado el Tiempo Objetivo de Recuperación (RTO)?
- ¿En cuánto tiene estimado el punto de Objetivo de recuperación (RPO)?
- El nivel táctico debe verificar:
- La disponibilidad de aduanas
- La disponibilidad de información fiscal
- La contingencia (plan) para el envío o intercambio de información.
- Definir plan de trabajo conjunto que contenga:
- Actividades
- Responsable
- Tiempo
- Indicador esperado

6. Modelo de actuación del protocolo frente a cada uno de los eventos de crisis.

6.1 Evento de ciberataque o ataque cibernético.

Este capítulo va dirigido tanto al responsable de seguridad de la información y ciberseguridad como al conjunto del equipo directivo a nivel táctico.

Lo establecido en el siguiente capítulo busca definir las directrices generales que permitan hacer un seguimiento, análisis y evaluación de las amenazas cibernéticas con el potencial de afectar al sector bancario, así como, la puesta en marcha de acciones y la coordinación de los agentes del sistema en una situación de crisis cibernética.

Según el numeral 2.5 del presente protocolo, el Comité de Crisis es el responsable de decretar el estado de crisis cibernética.

6.2 Declaración de la Crisis e inicio de actuaciones.

Adicional debe tenerse en cuenta que de acuerdo con las partes descritas en el numeral 5.1 de este documento, la crisis para el presente evento se decreta con la colaboración con el CSIRT Financiero, quienes comunican y convocan al comité táctico, cuando se presente alguna de las siguientes situaciones específicas para este evento:

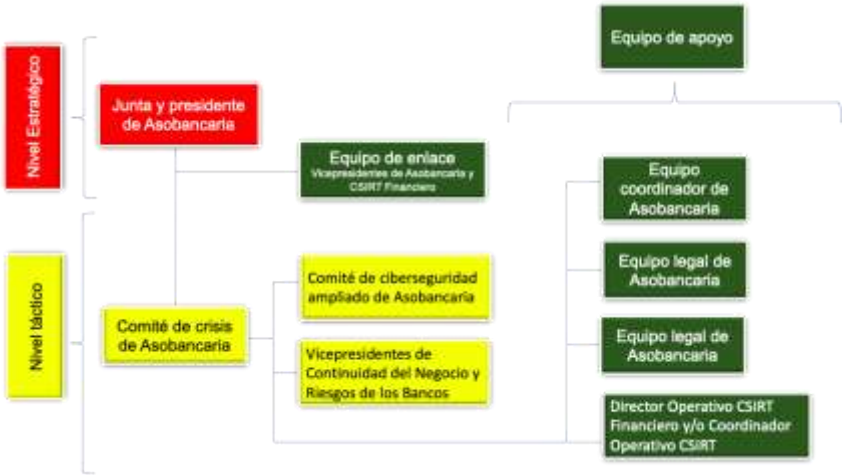
- Un miembro del Comité de ciberseguridad lo haya solicitado.
- Uno de los presidentes de una entidad agremiada a la Asociación le haya informado un escenario de ataque cibernético al CSIRT financiero o cualquier instancia directiva de la Asociación.
- La(s) entidad(es) bancaria(s) que sufrieron el ciberataque requieren de ayuda externa (proveedores o terceros involucrados) y así lo manifiesten al CSIRT o alguna instancia directiva de la Asociación (Comité o Junta).

6.3.2 Estructura de Gobierno

Con el fin de responder adecuadamente a situaciones de crisis cibernética, se requiere conformar comités que lideren la estrategia sectorial para el manejo de esta, así como desarrollar planes de respuesta y comunicación, que protejan la reputación del sector bancario.

El diseño, activación y ejecución de las actividades establecidas en el Protocolo de Crisis cibernética del sector bancario estarán a cargo de los siguientes órganos de gobierno5:

Adicional a los miembros definidos en el numeral 3.1 a nivel estratégico se invitará a:



Adicional a las funciones y responsabilidades del nivel estratégico, definidas en el numeral 3.2.1. 2, se incluye lo siguiente:

---

[5] Regla general: el flujo de información debe ser universal o general, la toma de decisiones debe ser cerrada.

- **Antes de la crisis:**

    - Participar en las pruebas de los planes de gestión de crisis, al menos una vez al año.

Adicional a las funciones y responsabilidades del nivel táctico, definidas en el numeral 3.2.1.4, se incluye lo siguiente:

- **Antes de la crisis:**

    - Propender por crear nuevos grupos de intercambio de información con otros sectores6.
    - Debe propender por realizar pruebas de penetración a infraestructura críticas cibernéticas del sector bancario (con su respectiva remediación), involucrando a todos los actores críticos internos y externos (del ecosistema financiero): propietarios de sistemas, continuidad del negocio y equipos de respuesta a incidentes y crisis.
    - Debe propender por seguir lineamientos de seguridad para definir criterios de privacidad, integridad y confidencialidad de la información.
    - Participar en las pruebas de simulación de crisis cibernética que defina Asobancaria.

- **Durante la crisis:**

    - Evaluar la criticidad del incidente y determinar y analizar si este debe clasificarse como una alerta amarilla o roja de acuerdo con los parámetros del presente protocolo, o aplicable a otros sistemas de estandarización. (Por ejemplo: CSIRT, MISP, FIRST).
    - Definir el o los procesos críticos afectados según la tabla 2.
    - Contactar al proveedor o terceros involucrados en la crisis para establecer vectores de ataque.
    - Recopilar información relevante asociada al o los proceso(s) crítico(s) afectado(s).
    - Invitar al proveedor crítico o entidad afectada para presentar su plan de recuperación y respuesta ante el incidente.
    - Recaudar información para determinar la activación del plan de comunicaciones de Asobancaria.
    - Recopilar la información del incidente para realizar una contextualización de los hechos para informar al comité técnico definido en el Plan de Protección Sectorial de Protección y Defensa para la Infraestructura Crítica Cibernética.

[6] Aquellos sectores de servicios esenciales definidos en la Guía de Infraestructura Crítica Cibernética.

- Revisar los requerimientos de las autoridades y definir planes de acción frente a estos con el propósito de lograr establecer una posición del gremio.
- Evaluar la pertinencia de invitar a las aseguradoras con las que se tienen pólizas de riesgo cibernético contratadas.
- Definir una periodicidad de convocatoria del comité durante el periodo de crisis.
- Decretar la terminación y vuelta a la normalidad una vez superada la crisis.

- **Después de la crisis:**

  Realizar un análisis post -crisis, registro de la solución y seguimiento de la cadena de ataque y la detección de IoC, esto con el propósito de generar alertas que deberán ser documentadas y compartidas entre las entidades.
  Construir base de datos de eventos conocidos y soluciones, para mejorar la gestión de crisis.

6.3.3 Criterios de activación

- **Alerta Amarilla:**

  Adicional a lo dispuesto en el numeral 2.1 “definición de las alertas” Se considera una Alerta Amarrilla cuando una o más entidades bancarias durante (12) horas sobrelleven la materialización de un ataque cibernético o cuando ocurra alguna de las siguientes situaciones:

  - Afectación a procesos críticos de acuerdo a matriz de criticidad...

  - Fuga masiva de datos de usuarios del sistema financiero desde las infraestructuras críticas cibernéticas del sector bancario (incluyendo aquellas que hacen parte de la cadena de suministro).

  - Denegación del servicio (DDoS) entre 6 y 12 horas.

  - Si se presentan incidentes cibernéticos relacionados con algún tipo de malware, troyano, puerta trasera o APT dirigida al sector financiero, los cuales no puedan ser gestionados directamente por las entidades.

- **Alerta Roja:**

- Fuga masiva de datos que afecte de forma critica la operación de usuarios del sistema financiero desde las infraestructuras críticas cibernéticas del sector bancario.

Adicional a lo dispuesto en el numeral 2.1 “definición de las alertas” Se considera una Alerta roja cuando una o más entidades bancarias durante (24) horas sobrelleven la materialización de alguno de los siguientes eventos o cuando ocurra alguna de las siguientes situaciones:

- Afectación a procesos críticos de acuerdo a matriz de criticidad.
- Fuga de información sujeta a reserva bancaria
- La(s) entidad(es) bancaria(s) no logre(n) volver a la normalidad por si sola(s) por mas de (12) horas.
- Si se presentan incidentes cibernéticos relacionados con algún tipo de malware, troyano, puerta trasera o APT dirigida al sector financiero, los cuales no puedan ser gestionados directamente por las entidades el equipo de respuesta no puede contenerlo mas de un día.
- Se afectan más de 2 interdependencias sectoriales (intermediarios financieros, seguros y aseguradoras, bolsa de valores e intermediarios, DIAN, Banrep).
- Pérdida de confianza de los consumidores en la seguridad y la solidez del sistema financiero debido a ataques cibernéticos de gran impacto o ataques de menor escala masivos que tengan como consecuencia el retiro masivo de recursos en cuentas de ahorro y corriente.

7. Evento de epidemia/pandemia

Este capítulo busca definir las directrices generales que permitan hacer un seguimiento, análisis y evaluación de impacto ante la materialización de un evento de pandemia que afecten al sector bancario, así como, la puesta en marcha de acciones y la coordinación de los diversos actores para atender la crisis.

7.1 Declaración de la Crisis e inicio de actuaciones.

La Declaratoria de la OMS o del gobierno nacional activara el protocolo y el comité de gestión de crisis decretara la crisis sobre el sector financiero.
Adicional a las funciones y responsabilidades del nivel táctico, definidas en el numeral 3.2.1. 2, se incluye lo siguiente:

- **Antes de la crisis**

- Referenciación o investigación gremial de las actuaciones a nivel global.
- Alistamiento de recursos como medidas de contención ante la pandemia.
- Simulacro del escenario.

- **Durante la Crisis**

  - Evaluar y difundir comunicaciones gremiales.
  - Definir el esquema de entrega de ayudas con el gobierno nacional.
  - Implementación de la normatividad decretada por el gobierno nacional.
  - Revisar y socializar con las entidades financieras la normativa del regulador. (emitida o por emitir).
  - Monitoreo de las estrategias decretadas para los procesos críticos.
  - Monitorear las estrategias de los aliados y/o proveedores críticos del sector financiero.

- **Después de la crisis**

  - Identificar y socializar lecciones aprendidas
  - Ajustar el protocolo de gestión de crisis
  - Monitoreo del gremio post crisis
  - Seguimiento normativo post crisis

8. Evento de Disturbios civiles, guerra y terrorismo:

Este capítulo busca definir las directrices generales que permitan hacer un seguimiento, análisis y evaluación de impacto ante la materialización de un evento de disturbios civiles, guerra y terrorismo que afecten al sector bancario, así como, la puesta en marcha de acciones y la coordinación de los diversos actores para atender la crisis.

Adicional a las funciones y responsabilidades del nivel táctico, definidas en el numeral 3.2.1. 2, se incluye lo siguiente:

Según las recomendaciones descritas en la cartilla de recomendaciones gremiales para la gestión de crisis. Anexo 1.

- **Antes de la crisis:**

  - Asobancaria realizará una reunión previa a la fecha establecida para el paro nacional o marcha con las áreas de las Entidades Financieras de: continuidad del negocio, seguridad, operaciones y riesgos, junto a la Policía Nacional y Secretaria de Seguridad Distrital, con el fin de:

  - Conocer información sobre corredores viales y puntos de concentración de los manifestantes. Así como número de marchas convocadas.

  - Definir un canal de comunicación entre entidades y autoridades, generalmente, un grupo de WhatsApp, para la entrega de información importante en tiempo real.

  - Definir contactos que harán parte del grupo por parte de cada entidad financiera y de las autoridades.

  - Definir las gestiones que debería realizar Asobancaria con otras entidades como Banco de la República, DIAN, Secretaría de Hacienda Distrital y otras que puedan aplicar en el evento.

  - En las ciudades donde Asobancaria cuenta con Frentes de Seguridad Bancarios, las reuniones serán responsabilidad de cada líder y las entidades bancarias deberían definir un contacto único mediante el cual fluirá la información relacionada con la situación de orden público.

- **Durante la crisis:**

  - Asobancaria recopilara información relevante que las entidades financieras deberán enviar una vez sea solicitada por el grupo de WhatsApp o correo electrónico, respecto a la afectación de la tecnología (ATM), las personas y la infraestructura física (Oficinas) de las Entidades Financieras importantes.

  - Asobancaria con la información obtenida realizar un diagnóstico de la situación para determinar el nivel de alerta del evento.

  - Dependiendo del nivel de alerta estimado, Asobancaria gestionara la atención de las alertas amarillas o rojas, según lo establecido en este documento.

- En caso de ser necesario, el equipo coordinador convocara al nivel táctico con el fin de definir estrategias de acción que no preestablezca este protocolo.

- Asobancaria sostendrá dialogo permanente con terceros afectados en procesos críticos de los bancos como lo son el Banco de la República-canje, superintendencia financiera – reportes al igual que con la Dian y secretara de hacienda distrital.

- Asobancaria monitoreara las estrategias activadas.

- Sugerir la declaración de terminación de la crisis al comité estratégico.

- **Después de la crisis:**

  - Evaluar la gestión realizada durante la crisis con el fin de optimizar las estrategias para gestión del evento de disturbios civiles, guerra y terrorismo.

  - Informar a todos los integrantes del Comité de gestión de crisis sobre el retorno a la normalidad de acuerdo.

  - Realizar seguimiento al cumplimiento de las estrategias y retroalimentar el proceso de manejo de información y el nivel de afectación del gremio en lo que respecta a: oficinas, cajeros y recurso humano.

Anexo 1. Recomendaciones para las entidades financieras:

- **Antes de la crisis:**

  - Se recomienda a las entidades bancarias definir oficinas y cajeros por donde posiblemente pasarán las marchas, con el fin de:

  - Darles prioridad en la instalación de protección física y monitoreo.

  - Disminuir el aprovisionamiento de efectivo de las oficinas y ATM.

  - Se recomienda a las entidades bancarias tratar de disponer de otros medios de comunicación alternos como medida de contingencia.

  - Las entidades bancarias deberán tomar las medidas preventivas necesarias para garantizar la seguridad de sus empleados y clientes:

  - Mantener un canal de comunicación activo sobre las situaciones que se puedan presentar.

- **Durante la crisis:**

  - Las fuerzas comerciales de las entidades bancarias deberán restringir o suspender salidas comerciales.

  - Las entidades bancarias si lo consideran necesario notificaran a la Superintendencia Financiera de Colombia y a la Asobancaria la modificación de horarios de atención o cierre de oficinas.

  - Establecer esquemas de comunicación con al área de seguridad o a los teléfonos de emergencia de la ciudad para reportar cualquier novedad de riesgo relacionada con la integridad del empleado.

  - Recomendaciones para las sucursales bancarias durante la situación:

  - En caso de observar situaciones inusuales en el entorno de la oficina, abstenerse de entrar a la oficina y comunicarlo al área de seguridad del banco.

  - En conjunto con el equipo de seguridad tomar las medidas necesarias para salvaguardar la integridad de los empleados, clientes y de las oficinas.

  - En caso de cerrar la oficina, se recomienda levantar todos aquellos elementos contundentes que pueden ser usados posteriormente por vándalos como extintores, organizadores de fila, etc.

  - Conocer el número y mantener contacto con el cuadrante de policía del sector, para consultar las condiciones generales de seguridad del sector.

  - En caso de que el gerente de la sucursal reciba recomendaciones del área de seguridad o advertencias puntuales relacionadas con la seguridad personal o de la oficina, se debe atender e informar inmediatamente al área de seguridad del banco.

  - Validar mediante los canales de comunicación dispuestos toda la información que sea recibida o vista a través de redes sociales y no difundir información sin verificación.

  - Si la situación no es de gravedad, la oficina puede seguir operando normalmente a puerta cerrada mientras pasa la manifestación.

- **Después de la crisis:**

- Las entidades bancarias deberán instaurar la denuncia de los daños y afectaciones que se tuvieron.

9. Desastre Natural y Antrópicos:

Este capítulo busca definir las directrices generales que permitan hacer un seguimiento, análisis y evaluación de impacto ante la materialización de un evento de desastre natural y antrópicos que afecten al sector bancario, así como, la puesta en marcha de acciones y la coordinación de los diversos actores para atender la crisis.

Adicional a las funciones y responsabilidades del nivel táctico, definidas en el numeral 3.2.1. 2, se incluye lo siguiente:

- **Ante de la crisis:**
  - El comité de gestión de crisis deberá conocer el listado de centros alternos de las entidades y de sus proveedores, que permita restablecer el capital tecnológico y humano de las entidades bancarias y sus aliados.
  - El comité de gestión de crisis deberá coordinar los planes de contingencia de las entidades financieras junto con los grupos de interés, como empresas transportadoras, entidades del Gobierno Nacional, entidades bancarias y financieras, entre otros, que faciliten la articulación y la respuesta rápida, segura y organizada respondiendo a las siguientes necesidades: ¿Cómo gestionar la comunicación? ¿Cómo recibir y entregar las ayudas? ¿Quién debe llegar primero y en compañía de qué entidades? ¿Cómo llegar a los clientes?
  - Realizar Pruebas de escritorio respecto a las estrategias y proveedores definidos en este protocolo sobre todas las estrategias diseñadas, para identificar a tiempo ajustes de mejora, y verificar que en efecto funcionarían de manera adecuada en caso de una crisis.
  - El comité de gestión de crisis deberá hacer una encuesta respecto a las recomendaciones propuestas en el anexo 2 del presente documento con el fin de conocer el nivel de madurez frente a recomendaciones definidas para las entidades en el numeral 9.1 de este documento.
  - Establecer y estandarizar formatos para entrega de efectivo de transportadoras a bancos durante la crisis.
  - El comité de crisis deberá instar porque cada entidad defina oficinas principales o puntos de pago para recibir el efectivo para distribuir.
  - Establecer con las fuerzas militares acuerdos de apoyo de seguridad en los puntos de distribución y en las zonas aledañas.

- Establecer acuerdos con terceros, por ejemplo: registraduría civil para la identificación para la entrega de efectivo, empresas de telecomunicaciones, entre otros.
- Definir un protocolo de entrega de efectivo a través de transportadoras.
- Designar un Comité de riesgo de liquidez junto con la Superfinanciera para definir los montos que van a ser entregados.

- **Durante la crisis:**
  - El comité de gestión de crisis deberá evaluar el estado de las oficinas afectadas acompañados de la defensa civil para determinar si se puede acceder al efectivo de las bóvedas y cajeros.
  - El comité de crisis deberá solicitar la información a entidades sobre las existencias de efectivo en oficinas a las que se pueda acceder con el necesario acompañamiento de fuerzas de seguridad nacionales.
  - Evaluar y reportar la situación de las transportadoras de valores en la ciudad de impacto.
  - El comité de gestión de crisis deberá propender por que se conozca la disponibilidad de efectivo del Banco de la República
  - El comité de gestión de crisis deberá propender por conocer la logística de las transportadoras de valores y banco para traslado de efectivo.
  - El comité de gestión de crisis deberá velar por conocer los puntos de pago y/o los gremiales de acuerdo con indicaciones de la Superfinanciera, IDIGER, UNGRD.
  - Se deberá Informar a través de los medios de comunicación disponibles los puntos de pago, horarios y montos de entrega.

- **Después de la crisis:**
  - El comité deberá velar por conocer la fecha de reanudación de las operaciones con ayuda del Banco de la República para suplir la totalidad de las necesidades por un periodo determinado de tiempo.
  - Definir junto con las autoridades un plazo para recuperar al 100% las operaciones.

Anexo 2. Recomendaciones para las entidades financieras para el proceso de manejo del efectivo.

- **Antes de la crisis**

¿Cuanto efectivo tiene la entidad?

- Identificar por entidad los recursos mínimos para operar en contingencia.
- Definir periodicidad del cuadre contable de los fondos de efectivo y de los fondos de oficinas
- Conocer y detallar la calidad del efectivo existente en las bóvedas de las transportadoras.
- Conocer por oficina el porcentaje que representan los pasivos sobre el efectivo que registran.
- Definir planes de contingencia para cada uno de los canales. (oficinas, digitales, CNB y ATM, entre otros)
- Asegurar la actualización del número de token brindado por el Banco de la República para poder realizar transacciones
- Desarrollar un plan de contingencia para la negociación del efectivo en caso de una crisis, centro alterno ubicado en otra ciudad de acuerdo con el Banco de la República ante la estrategia de provisión de efectivo a los establecimientos de crédito en un evento de desastre en Bogotá.

Cuánto efectivo necesita la entidad:

- Identificar por entidad los recursos mínimos para operar en contingencia.
- Conocer la estrategia de provisión de efectivo a los establecimientos de crédito en un evento de desastre en Bogotá del Banco de la República, su objetivo de tiempo de recuperación y sus centros de distribución alternos a Bogotá.
- Definir sitios alternos de efectivo fuera de la ciudad.
- Definir sitios alternos para la ubicación física los servidores con back up de la información y el acceso desde otras ciudades (descentralizar de Bogotá)
- Definir con las autoridades competentes el plan de zonificación para entrega y distribución de efectivo dependiendo de la magnitud del terremoto, teniendo en cuenta los recursos mínimos para operar en contingencia.
- Asegurar la actualización del número de token brindado por el Banco de la República para poder realizar transacciones
- Realizar preacuerdos de negociación con otras entidades para compensar efectivo

- Realizar acuerdos nacionales de servicio con entidades externas, por ejemplo: IDIGER[7]8, Banco de la República y la UNGRD

A dónde se lleva el efectivo:

- Alinear las pruebas gremiales de los PCN de las entidades y el Banco de la República para alcanzar un nivel de madurez
- Participar en las pruebas y ejercicios de protocolos establecidos por el Banco de la República de tecnología y procesos.
- Definir el inventario y cupo de almacenamiento de efectivo físico.
- Validar vías de transporte y rutas de tránsito del efectivo.
- Definir medio de transporte del efectivo (terrestre o aéreo)

Dónde se entrega el efectivo:

- Definir los sitios de distribución donde se ubicarán todos los bancos, como un sitio gremial de crisis, con coordinación del IDIGER - UNGRD
- Establecer roles y responsabilidades de los funcionarios que atenderán en los sitios alternos del efectivo.
- Definir puntos de encuentro de los funcionarios disponibles que atenderán en puntos de entrega de efectivo.
- Fortalecer la infraestructura de las oficinas principales y alternas[9]
- Estructurar los procedimientos de entrega en los sitios donde se lleve el efectivo.

A quién se entrega el efectivo:

- Utilizar mecanismos de autenticación con sus correspondientes esquemas alternos.
- Definir entregas prioritarias de efectivo.
- Definir procesos de excepción. Por ejemplo, pago a familiares.
- Respaldar la información: saldos, datos básicos, infraestructura mínima transaccional.
- Contratar y revisar pólizas de seguros: solicitud de cláusulas, cobertura, exclusividad, pólizas de seguros.
- Definir mecanismos de entrega para usuarios.
- Capacitar al personal asociado al proceso del banco, por ejemplo, en: grafología, dactiloscopia, sellos secos, verificación de la veracidad de otros documentos: licencia de conducción, pasaportes, registros

[7] Instituto Distrital de Gestión de Riesgos y Cambio Climático

[9] Estrategia de conocimiento y reducción del riesgo de afectación a las edificaciones de las entidades financieras. Para esto, es importante contar con infraestructura construida bajo las normas de construcción antisísmica.

Cómo se entrega el efectivo:

- Tener plan de comunicación alterna como números de teléfono satelitales.
- Capacitar a personal de otras ciudades en el procedimiento de entrega de efectivo.
- Incluir convenios de servicio en crisis con canales alternativos como corresponsales bancarios y definir puntos autorizados
- Organizar la entrega del efectivo por zonas. Definir horarios de atención.

Cuánto efectivo se entrega:

- Definir puntos alternos de centralización para la información de saldos
- Definir forma de actualización de saldos por cliente.

- **Durante la crisis**

Estas acciones se concretan en una estrategia de activación del plan de continuidad y dar respuesta en los primeros días luego de la catástrofe. Van dirigidas a resolver temas logísticos, de recursos, comunicaciones y soporte, con el fin de contemplar soluciones gremiales para facilitar la experiencia de los usuarios.

Procesos para el manejo del efectivo

Cuánto efectivo tiene la entidad:

- Evaluar y reportar la situación de las transportadoras de valores en la ciudad de impacto
- Controlar inventario de efectivo en bóveda por periodos determinados para planear la demanda
- Evaluar la demanda de efectivo de acuerdo con la necesidad localizada en la ciudad de Bogotá
- Consultar la disponibilidad de las denominaciones de efectivo que se van a entregar por el Banco de la República
- Ubicar el personal en el sitio alterno
- Evaluar el estado de las oficinas afectadas acompañados de la defensa civil para determinar si se puede acceder al efectivo de las bóvedas y cajeros
- Validar detalle de existencias de efectivo en oficinas a las que se pueda acceder con el necesario acompañamiento de fuerzas de seguridad nacionales
- Evaluar y reportar la situación de las transportadoras de valores en la ciudad de impacto
- Controlar inventario de efectivo en bóveda por periodos determinados para planear la demanda

A dónde se lleva el efectivo:

- Activar los centros de acopio definidos para guardar con seguridad el efectivo
- Activar protocolo de rutas según la magnitud del evento
- Diligenciar los formatos preestablecidos con transportadoras
- Designar actividades y turnos del personal disponible
- Aislar el efectivo

Dónde se entrega el efectivo:

- Transportar e instalar las herramientas tecnológicas para atender al público
- Asignar el personal disponible a los sitios donde se activará la contingencia
- Establecer conexión con la plataforma del banco

A quién se entrega el efectivo:

- Usar los mecanismos de autenticación para usuarios definidos por el banco
- Controlar el almacenamiento y custodia de formatos únicos físicos de transacciones aprobadas.
- Formalizar el pago de los siniestros por parte de las aseguradoras concerniente al negocio del Banco y las pólizas contratadas por los clientes a través de las entidades financieras.

Cómo se entrega el efectivo:

- Entregar el efectivo a las transportadoras y sitios de entrega de efectivo
- Usar oficinas y cajeros móviles disponibles
- Teniendo en cuenta la gravedad de la emergencia, el efectivo disponible y los topes definidos con anterioridad, es discreción de las autoridades y los bancos establecer cuánto efectivo se entrega a los clientes y usuarios.

- **Después de la Crisis:**

En este momento, la estrategia va enfocada a la recuperación y vuelta a la normalidad del servicio luego de la segunda semana y hasta dos meses después de la emergencia, acompañada de la actualización de la información sobre las operaciones que se realizaron manualmente, y, por último, la documentación de lo sucedido antes y durante la crisis, con el fin de evaluar la efectividad de los planes

previstos, para realizar las mejoras que se consideren necesarias de acuerdo con la experiencia.

Procesos para el manejo del efectivo

Cuánto efectivo tengo:

- Hacer uso del efectivo que se encontraba en bóvedas a las que no se tenía acceso por la afectación.
- Coordinar con transportadoras de valores el traslado del efectivo sobrante.

Cuánto efectivo necesito:

- Verificar qué disponibilidad de efectivo quedó en Bogotá
- Realizar el control contable de la cuenta de efectivo del banco y contabilizar los saldos de centros de efectivo
- Hacer proyecciones de demanda del efectivo

Adónde se lleva el efectivo:

- Retomar las actividades de redistribución de efectivo
- Transportar los formatos únicos físicos de transacciones aprobadas al lugar donde se va a digitalizar la información.

Dónde se entrega el efectivo:

- Notificar y comunicar con clientes dónde se entregará el efectivo, pasada la emergencia
- Atender quejas y solicitudes

A quién se entrega el efectivo:

- Digitalizar o ingresar al sistema de la entidad las operaciones realizadas en físico
- Actualizar la información de saldos de los clientes
- Analizar la información sobre los movimientos de efectivo realizados para su posterior estudio

Cómo se entrega el efectivo:

- Restablecer la conexión a las plataformas de las entidades, progresivamente se reanudan operaciones en oficinas
- Avalar el uso de tarjetas para efectuar los retiros

Cuánto efectivo se entrega:

- Revisar las proyecciones de demanda de efectivo para ir ajustándolas de acuerdo con las necesidades reales

Anexo 3. Comunicación a medios.

El nivel táctico debe implementar lo establecido en el protocolo de comunicaciones de Asobancaria y tendrá la responsabilidad de generar materiales para el vocero a medios de comunicación.

Formato Mensajes en caso de que sea un solo banco el afectado:

"Fuimos notificados del ciberataque que sufrió uno de nuestros agremiados, el banco [XXX]. El ataque cibernético ocurrió a las [XXX] a través de [XXX] (explicar brevemente los hechos, sin entrar en mayor detalle)."

" Desde Asobancaria repudiamos estos hechos de vandalismo que afectan no solo al sistema financiero sino a los usuarios que hacen parte de él. De modo que trabajaremos de la mano con las autoridades competentes para encontrar a los responsables de lo sucedido y tomar las acciones legales pertinentes."

"En Colombia, como cualquier país del mundo, el sistema financiero no está exento de recibir un ciberataque.

"Desde Asobancaria y el banco [XXX], queremos pedirles disculpas a todos los usuarios financieros que fueron víctimas del ciberataque del [XXX]. Nos encontramos trabajando junto a [XXX] para tomar las medidas necesarias que garanticen no solo la seguridad de la red, sino que evite que esta situación se repita".

Mensajes en caso de que sea más de un banco afectado:

"El día de hoy hemos fuimos notificados del ciberataque que sufrieron varios de nuestros agremiados, los bancos [XXX]. El ataque cibernético ocurrió a las [XXX] a través de [XXX] (explicar brevemente los hechos, sin entrar en mayor detalle)."

" Desde Asobancaria repudiamos estos hechos de vandalismo que afectan no solo al sistema financiero sino a los usuarios que hacen parte de él. De modo que trabajaremos de la mano con las autoridades competentes para encontrar a los responsables de lo sucedido y tomar las acciones legales pertinentes."

"En Colombia, como cualquier país del mundo, el sistema financiero no está exento de recibir un ciberataque"

“Desde Asobancaria y los bancos [XXX], queremos pedirles disculpas a todos los usuarios financieros que fueron víctimas del ciberataque del [XXX]. Nos encontramos trabajando junto a [XXX] para tomar las medidas necesarias que garanticen no solo la seguridad de la red, sino que evite que esta situación se repita”.