CAMINOS Y PUENTES FEDERALES DE INGRESOS Y SERVICIOS CONEXOS

DIRECCIÓN DE ADMINISTRACIÓN Y FINANZAS

CAPUFE

CAMINOS Y PUENTES FEDERALES

MANUAL DE PROCEDIMIENTOS DE SEGURIDAD DE LA INFORMACIÓN

FEBRERO 2026

SUBDIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

ÍNDICE

I. INTRODUCCIÓN

La seguridad de la información es un aspecto fundamental para el funcionamiento y la protección de cualquier organización. En un entorno cada vez más digitalizado y globalizado, las amenazas a la información son más sofisticadas y frecuentes, lo que pone en riesgo la confidencialidad, integridad y disponibilidad de los datos que manejamos.

Con base en el "Acuerdo por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal", publicado en el Diario Oficial de la Federación el 06 de septiembre de 2021, por la entonces Coordinación de la Estrategia Digital Nacional (CEDN), actualmente Agencia de Transformación Digital y Telecomunicaciones (ATDT). El cual establece como directriz que las Instituciones de la Administración Pública Federal deberán contar con un Marco de Gestión de Seguridad de la Información (MGSI), alineado a la política general de Seguridad de la Información, que cada Institución establezca de conformidad con sus objetivos y dimensionamiento.

En virtud de lo anterior, es imperante proporcionar directrices claras y procedimientos establecidos para proteger la información sensible y garantizar que los sistemas del Organismo operen de manera segura y eficiente, de tal manera que sea una guía accesible y comprensible para todo el personal del esta Entidad, independientemente de su rol o nivel técnico. Aquí se describen las mejores prácticas, políticas y procedimientos que el personal debe seguir para mitigar riesgos, prevenir incidentes de seguridad y responder adecuadamente en caso de una brecha de seguridad.

Es responsabilidad de todo el personal del Organismo implementar y seguir procedimientos para garantizar que la información se gestione de forma segura, ética y conforme a las leyes y regulaciones vigentes. Además, es fundamental que los procedimientos sean revisados y actualizados regularmente para adaptarse a los nuevos retos y avances tecnológicos en el ámbito de la ciberseguridad.

Este manual de procedimientos se basa en el principio de seguridad de la información como una responsabilidad compartida que involucra a todo el personal Organismo, y no solo como una tarea del área de Tecnologías de Información.

II. OBJETIVO GENERAL

Establecer acciones para la detección de incidentes cibernéticos, así como la respuesta, contención y recuperación de los servicios informáticos, a fin de mantener niveles de riesgo aceptables protegiendo la información sensible y garantizando que los sistemas del Organismo operen de manera segura y eficiente.

III. FUNDAMENTO LEGAL

- Constitución Política de los Estados Unidos Mexicanos.

  D.O.F. 05/02/1917 y sus últimas reformas.

- Ley Orgánica de la Administración Pública Federal.

  D.O.F. 29/12/1976 y sus últimas reformas.

- Ley General de Responsabilidades Administrativas.

  D.O.F. 18/07/2016 y sus últimas reformas.

- Ley General de Transparencia y Acceso a la Información Pública.

  D.O.F. 20/03/2025.

- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.

  D.O.F. 20/03/2025.

- Ley General de Archivos.

  D.O.F. 15/06/2018 y sus últimas reformas.

- ACUERDO por el que se emiten las políticas y disposiciones para impulsar el uso y aprovechamiento de la informática, el gobierno digital, las tecnologías de la información y comunicación, y la seguridad de la información en la Administración Pública Federal.

  D.O.F. 06/09/2021.

- Estatuto Orgánico de Caminos y Puentes Federales de Ingresos y Servicios Conexos.

  D.O.F. 30/04/2021 y su última modificación.

- Manual de Organización General de Caminos y Puentes Federales de Ingresos y Servicios Conexos.

  D.O.F. 11/10/2024.

- Política de Seguridad de la Información.

  Normateca Interna: 06/12/2024.

- Estándar Técnico de Controles Mínimos de Seguridad de la Información.

  https://wikiguias.atencion.gob.mx/es/seguridad-de-la-informacion/estandar-tecnico-de-controles-minimos-de-seguridad-de-la-informacion

- Protocolo Nacional Homologado de Gestión de Incidentes Cibernéticos.

  Guardia Nacional CERT-MX, 19 de junio de 2023.

  https://www.gob.mx/gncertmx/articulos/protocolo-283239

IV. ÁMBITO DE APLICACIÓN

La aplicación del presente Manual es de observancia general y obligatoria para todo el personal de CAPUFE, así como colaboradores y terceros externos que tengan acceso, manejo o administración de los recursos informáticos, sistemas, aplicaciones, datos y redes dentro del Organismo. Su alcance de manera enunciativa, más no limitativa, abarca todas las actividades, procesos y sistemas de información y tecnologías que involucran la gestión, acceso a datos y recursos, protección y transmisión de información, tanto en medios electrónicos como físicos.

V. DEFINICIONES

- **Árbol de Llamadas:** Es un diagrama o lista jerárquica que define la ruta de comunicación en situaciones críticas, con el objetivo de garantizar que el personal o los integrantes clave reciban información e instrucciones de manera eficiente, confiable y sin duplicidad, especialmente durante emergencias, crisis o interrupciones operativas (Ver Anexo 1).

- **ATDT:** Agencia de Transformación Digital y Telecomunicaciones.

- **Business Continuity Plan (BCP) / Plan de Continuidad del Negocio:** Establece procesos y procedimientos de gestión de riesgos que tienen como objetivo evitar interrupciones en los servicios de misión crítica y restablecer la función completa de la organización de la forma más rápida y sencilla posible.

- **Business Impact Analysis (BIA) / Análisis de Impacto al Negocio:** Proceso de análisis de la actividad y el efecto que puede tener en una interrupción a la Institución.

- **CAPUFE u Organismo:** Caminos y Puentes Federales de Ingresos y Servicios Conexos.

- **Centro de Datos Primario / Centro de Datos Principal**: Es la instalación central donde una organización alberga su infraestructura tecnológica más importante, incluyendo servidores, sistemas de almacenamiento, redes y aplicaciones críticas para el negocio.

- **Centro de Datos Secundario / Centro de Datos Alterno**: Diseñado para garantizar la continuidad operativa de una organización en caso de que el centro de datos principal falle o quede inoperativo. Es el sitio donde se replican los sistemas, datos y aplicaciones críticas del centro primario, permitiendo que la organización pueda restablecer sus operaciones rápidamente ante incidentes como desastres naturales, fallas eléctricas, ataques cibernéticos o errores humanos.

- **Contingencia**: Situación eventual y no necesariamente previsible, que puede suceder o no, y que tiene el potencial de causar daños. Se utiliza para describir riesgos o eventos que pueden requerir un plan de acción.

- **Continuidad de las Operaciones**: Capacidad de CAPUFE para continuar con la entrega de productos o servicios a niveles aceptables predefinidos tras un incidente perjudicial.

- **Desastre:** Situación que da lugar a la perdida de activos o recursos de CAPUFE o que los inutiliza en un corto periodo de tiempo y que puede causar un impacto significativo en las finanzas o reputación del Organismo.

- **Disaster Recovery Plan (DRP) / Plan de Recuperación de Desastres:** Contiene los pasos requeridos para operar con los procedimientos de Recuperación en cuyo caso tendrán que utilizar su Centro de Datos Secundario para que puedan reiniciar sus servicios más importantes, y tendrán que regresar al Centro de Datos Primario una vez superados los problemas que ocasionaron la activación del Plan.

- **ERISC**: Equipo de Respuesta a Incidentes de Seguridad en TIC.

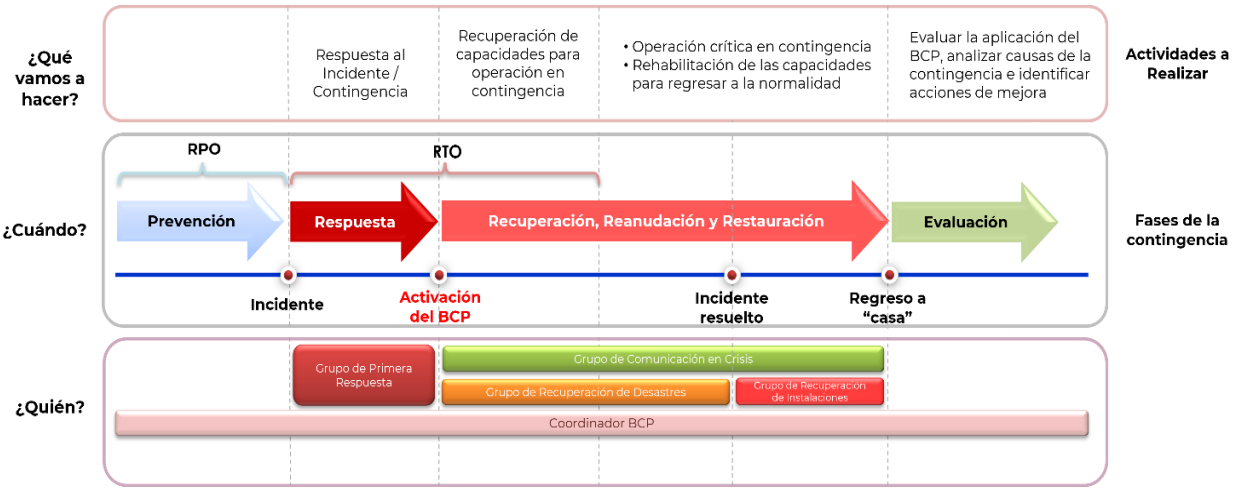
- **Estructura de Gobierno:** Integrada por el Grupo Directivo, la Persona Coordinadora BCP, el Grupo de Manejo de Crisis, el Grupo de Trabajo de Procesos Críticos, el Grupo de Primera Respuesta, el Grupo de Recuperación de Desastres, el Grupo de Comunicación en Crisis, el Grupo de Recuperación de Instalaciones y el Personal Crítico de CAPUFE, es responsable de la gestión de la Continuidad del Negocio y de la asignación de roles y responsabilidades a cada grupo de trabajo. Esta estructura asiste a la Dirección General para garantizar la existencia de medidas de control y procesos de continuidad adecuados, asegurando una respuesta eficiente y efectiva ante la ocurrencia de cualquier contingencia, ya sea desastres naturales, sociales, tecnológicos, interrupciones de servicios o proveedores, pandemias, entre otros, con el objetivo de minimizar los impactos sobre CAPUFE.

- **Evento**: Ocurrencia o cambio de estado en uno o más elementos. Cualquier suceso detectable o medible que tiene relevancia para la gestión de servicios o la seguridad.

- **Evento de Emergencia**: Situación imprevista que requiere atención inmediata y puede poner en peligro la vida, los bienes o el medio ambiente.

- **Fases para la Gestión de Continuidad del Negocio:** Son un conjunto de etapas estructuradas que permiten a CAPUFE prepararse, responder y recuperarse ante interrupciones que puedan afectar sus operaciones críticas, e incluyen las siguientes fases:
  - **Prevención:** Orientada a todas las actividades de prevención, planeación, definición, preparación, pruebas y evaluación para hacer frente a contingencias operativas.
  - **Respuesta:** Inicia cuando se presenta un incidente; el Grupo de Manejo de Crisis identifica y contiene el incidente y evalúa los impactos. Los responsables de los procesos críticos de cada área deben evaluar la situación y decidir sobre la activación del BCP de su área, comunicando la decisión al Grupo Directivo y al Coordinador BCP. El Área de Sistemas evalúa el incidente y decide sobre la activación de la estrategia de recuperación de aplicaciones. Estas actividades buscan salvaguardar la integridad física de las personas, instalaciones, equipos, activos tecnológicos, recursos materiales, insumos e información, así como contener los efectos de la contingencia.
  - **Recuperación:** Se realizan las acciones necesarias para recuperar la capacidad mínima requerida para operar los procesos críticos en un tiempo y nivel predefinido, una vez activado el BCP o la estrategia de recuperación de aplicaciones. Esta fase se centra en recuperar: personal crítico y suplentes; tecnología, incluyendo aplicaciones, sistemas, redes de comunicación, equipos y centros de datos alternos; información física y electrónica; e instalaciones y sitios alternos de operación.
  - **Reanudación:** Comprende las actividades necesarias para reanudar las operaciones de los procesos críticos bajo un ambiente de contingencia. El Coordinador BCP y los responsables de los procesos críticos gestionan y supervisan las acciones del personal crítico, dan seguimiento a las operaciones y notifican su estatus, incluyendo la reanudación de procesos críticos y la rehabilitación de capacidades y activos afectados.

- **Restauración:** Se realizan las actividades necesarias para retornar a la operación normal de todos los procesos de CAPUFE, priorizando los procesos críticos, habilitando instalaciones, infraestructura tecnológica, activos, insumos y servicios básicos para recuperar el nivel de funcionalidad previo a la contingencia. Una vez restablecidos y validados los servicios y condiciones normales, se declara la conclusión de la contingencia.
- **Evaluación:** Comprende la recopilación y análisis de información relevante sobre el desarrollo de las contingencias y de las acciones y procedimientos aplicados para su prevención, contención y restauración, con el objetivo de efectuar los ajustes necesarios al Plan de Continuidad del Negocio.



– **Grupo de Comunicación en Crisis:** Conformado por las personas titulares de la Subgerencia de Telecomunicaciones, Subgerencia de Atención a Usuarios, Subgerencia de Administración de Sistemas de Peaje y el personal operativo de la STI con Rol de Seguridad de la Información, es el responsable de coordinar la comunicación interna y externa durante una contingencia, definiendo, implementando, manteniendo y probando los procedimientos de comunicación; estableciendo las audiencias y herramientas de difusión; desarrollando y validando los mensajes para los distintos canales; designando voceros y autorizando los comunicados oficiales; notificando el estatus al Grupo de Manejo de Crisis a través del Coordinador BCP; y comunicando oportunamente las actualizaciones del evento a todas las partes interesadas con la autorización de la Dirección General.

- **Grupo Directivo:** Integrado por las personas titulares de la Dirección General de CAPUFE, la Dirección de Operación, la Dirección de Administración y Finanzas, la Dirección Técnica y la Dirección Jurídica, es responsable de asegurar el cumplimiento de los procesos de continuidad y de la correcta implementación del Proceso de Administración de Continuidad del Negocio en todas las áreas de la institución, garantizando la observancia de estrategias, políticas, planes y regulaciones en la materia; fungiendo como responsables finales de la continuidad de las operaciones críticas y de la existencia del proceso correspondiente; aprobando su estructura y componentes; impulsando la concientización y capacitación organizacional; asignando el presupuesto y recursos necesarios; y tomando decisiones de alto nivel durante una contingencia.

- **Grupo de Manejo de Crisis:** Liderado por la persona Coordinadora BCP, está integrado por quienes son responsables de coordinar y gestionar las crisis derivadas de contingencias que afecten o amenacen la continuidad de la operación crítica de CAPUFE, adoptando las medidas necesarias para proteger al personal, contener o reducir pérdidas financieras, preservar la reputación institucional, recuperar las funciones críticas durante la contingencia y organizar el retorno a la operación normal una vez concluida. Este grupo aprueba los lineamientos generales de las fases de la Administración de Continuidad del Negocio, informa y consulta al Grupo Directivo, identifica oportunidades de mejora en la gestión de crisis, coordina a los grupos de trabajo involucrados, gestiona el aprovisionamiento de recursos para la recuperación, actúa en coordinación con autoridades y servicios de emergencia, y dirige el proceso de restablecimiento de las operaciones habituales.

- **Grupo de Primera Respuesta:** Integrado por las personas titulares de la Subgerencia de Telecomunicaciones, la Subgerencia de Atención a Usuarios y la Subgerencia de Administración de Sistemas de Peaje, constituye la primera línea de acción ante cualquier incidente en CAPUFE, siendo responsable de identificar, atender, evaluar y reportar los eventos que puedan presentarse. Este grupo opera a través de dos equipos principales: Ciberseguridad, para incidentes tecnológicos, y Operación/Seguridad Física, para aquellos que comprometan la integridad de las personas o las instalaciones, y tiene a su cargo identificar

los tipos de incidentes, evaluar su severidad y determinar la necesidad de escalamiento; notificar al Grupo Directivo sobre la ocurrencia de incidentes; desarrollar y validar la eficacia de los procedimientos de atención; y recopilar retroalimentación de las áreas involucradas para mejorar continuamente la gestión de incidentes.

- **Grupo de Recuperación de Desastres:** Integrado por las personas titulares de la Gerencia de Infraestructura de Tecnologías de Información, la Gerencia de Atención a Usuarios de Tecnologías de Información, la Gerencia de Sistemas de Operación y la Gerencia de Seguridad y Operaciones Tecnológicas, es responsable de resguardar los activos tecnológicos de CAPUFE y ejecutar las acciones necesarias para mantener una infraestructura tecnológica adecuada que soporte los procesos institucionales y atienda las prioridades críticas identificadas. Este grupo evalúa los daños derivados de incidentes tecnológicos e implementa medidas inmediatas para controlar la crisis; protege la infraestructura tecnológica, incluyendo hardware, software, sistemas, redes y telecomunicaciones; notifica el estatus al Grupo de Manejo de Crisis por conducto del Coordinador BCP; coordina la recuperación del Centro de Datos Primario y de sus componentes, aplicaciones e infraestructura de telecomunicaciones; gestiona a los proveedores de servicios y productos tecnológicos; administra y da soporte a los servicios de Tecnologías de la Información durante la contingencia; y dirige los trabajos de restablecimiento de la operación tecnológica, incluyendo la actualización de sistemas y datos en producción una vez concluida la contingencia.

- **Grupo de Recuperación de Instalaciones:** Integrado por el personal encargado de los sistemas auxiliares en la STI, es responsable de evaluar los daños en equipos e instalaciones y de implementar acciones inmediatas para controlar la crisis y/o facilitar la evacuación, garantizando en todo momento la salvaguarda de la integridad física de las personas. Este grupo define, implementa, mantiene y prueba los procedimientos de Primera Respuesta; protege al personal; valora los daños y aplica medidas urgentes para mitigar riesgos; coordina y gestiona la atención del incidente, notificando el estatus al Grupo de Manejo de Crisis por medio del Coordinador BCP; y asegura la seguridad física de las personas, los bienes y las instalaciones de CAPUFE.

- **Grupo de Recuperación de Operaciones por Área:** Integrado por las personas titulares de la Dirección de Operación y la Dirección de Administración y Finanzas, es responsable de la operación y continuidad de los procesos críticos de CAPUFE identificados en el Análisis de Impacto al Negocio (BIA), así como de coordinar y ejecutar la recuperación de dichas operaciones en caso de una contingencia, garantizando su restablecimiento oportuno y ordenado.

- **Grupo de Recuperación Tecnológica:** Coordinado por la persona Líder Ejecutiva del DRP e integrado por la persona titular de la Subgerencia de Administración de Sistemas de Peaje, es responsable de rehabilitar las capacidades de la infraestructura tecnológica y de los activos de información afectados durante una contingencia, reemplazándolos o reparándolos según sea necesario y validando su correcto funcionamiento conforme a los procedimientos establecidos en el Plan de Recuperación de Desastres (DRP).

- **Grupo de Trabajo de Procesos Críticos:** Integrado por personal crítico de CAPUFE, es responsable de ejecutar las actividades interdependientes necesarias para recuperar la operatividad institucional en el menor tiempo posible, permitiendo enfrentar un desastre de manera organizada, eficiente y responsable.

- **GSOT:** Gerencia de Seguridad y Operaciones Tecnológicas.

- **Herramienta de Continuidad**: Es una aplicación que solo las personas involucradas en el Plan de Continuidad del Negocio o en Plan de Desastres la deben de tener instaladas en su teléfono. En esta herramienta se dispara el BCP y/o DRP y se le da seguimiento al mismo.

- **Impacto**: Consecuencia evaluado de una interrupción.

- **Incidente**: Situación que puede ser, o puede dar lugar a interrupciones, pérdidas, emergencia o de crisis. Interrupción no planificada o degradación de la calidad de un servicio de TI. Su gestión busca restaurar la operación normal lo antes posible.

- **Matriz de Alertamiento:** Es una herramienta de gestión preventiva que permite definir niveles de alerta, establecer criterios de activación y determinar acciones específicas ante distintos tipos de incidentes o eventos que puedan afectar la operación normal de una organización (Ver anexo 2).

- **Mesa de Servicio de TI:** Herramienta operada por agentes humanos adscritos al Organismo que permite recibir y atender solicitudes de apoyo para el personal de CAPUFE.

- **Persona Colaboradora:** Persona que participa activamente y aporta valor para lograr metas comunes, es decir cuentan con un rol o función asignada en el Plan de Continuidad del Negocio.

- **Persona Coordinadora BCP:** Titular de la Subdirección de Tecnologías de Información, es responsable de organizar y dirigir a los responsables de los Procesos Críticos de las áreas, así como a los Grupos de Primera Respuesta, Recuperación de Desastres, Comunicación en Crisis y Recuperación de Instalaciones, antes, durante y después de una contingencia de la Unidad de Negocio. Esta persona coordina la actualización del Análisis de Impacto al Negocio y del Análisis de Riesgos de Continuidad, promueve la capacitación y concientización sobre el Proceso de Administración de Continuidad del Negocio, supervisa el seguimiento y cumplimiento de las estrategias de continuidad con el Grupo Directivo y de las acciones de manejo de crisis con el Grupo de Manejo de Crisis, conoce los planes relevantes de la Unidad de Negocio y sus roles asignados, da seguimiento a la activación del BCP y DRP, ejecuta las actividades previstas en los planes durante una crisis, asegura una comunicación adecuada con las partes interesadas, proporciona material de capacitación, gestiona la revisión y actualización de los componentes de Continuidad del Negocio, verifica la vigencia del BCP y sus actualizaciones, y propone mejoras al mismo para garantizar su eficacia.

- **Personal Crítico de CAPUFE:** Se refiere al personal cuyas funciones son esenciales para el funcionamiento y la recuperación de los procesos clave del negocio durante una interrupción o emergencia, ya sea por contar con conocimientos o habilidades especializadas indispensables

para la operación, por participar en la toma de decisiones clave durante una crisis o proceso de recuperación, o por tener acceso y control sobre recursos esenciales como sistemas, equipos, información o infraestructura.

- **Plan de Contingencia / Programa de Contingencia:** Conjunto de procedimientos y acciones preestablecidas que una organización implementa ante emergencias o situaciones inesperadas para minimizar el impacto en sus operaciones, personal y personas usuarias. se centra en la respuesta inmediata a un incidente, definiendo los pasos para gestionar y mitigar riesgos específicos.

- **Plan de Manejo de Crisis:** Es un conjunto estructurado de procedimientos, roles y estrategias que una organización utiliza para responder eficazmente ante una situación crítica o evento inesperado que amenaza su funcionamiento, reputación, seguridad o continuidad operativa y tiene como objetivo coordinar la respuesta organizacional ante emergencias graves como desastres naturales, ciberataques, fallas críticas de sistemas, accidentes, o crisis reputacionales para minimizar los impactos y mantener el control de la situación.

- **Políticas de Activación del BCP:** Son el conjunto de criterios, reglas y procedimientos que determinan cuándo, cómo y quién debe activar el plan ante una interrupción o emergencia que afecte las operaciones críticas de la organización, es decir, son las condiciones y pasos formales que deben cumplirse para poner en marcha el BCP.

- **Procesos Críticos:** Son las actividades que son fundamentales para que una organización o empresa funcione y alcance sus objetivos principales. Son aquellos procesos que, de fallar, tendrían un impacto significativo y directo en la operación, los ingresos, la satisfacción del cliente o la continuidad del negocio. Su correcta gestión es prioritaria y deben ser protegidos o restaurados de forma rápida en caso de una interrupción.

- **Programa de Capacitación y Concientización:** El programa de capacitación y concientización tiene como propósito fortalecer en todo el personal de CAPUFE la comprensión y el compromiso respecto a la responsabilidad, el uso adecuado, la importancia y los beneficios de la Seguridad de la Información. Con ello, se busca fomentar una cultura organizacional sólida que contribuya activamente a la Continuidad del Negocio.

- **Programa de Capacitación para la Gestión de Continuidad del Negocio:** Es un plan de Capacitación y Concientización enfocado en temas de Gestión de Continuidad. Está dirigido a todo el personal de CAPUFE que está involucrado en el proceso de continuidad del negocio principalmente a la formación y educación del personal directivo y administrativos de CAPUFE, además de fomentar la toma de conciencia sobre la continuidad de la operación en CAPUFE.

- **Programa de Cultura de Seguridad de la Información**: Es un plan de capacitación en el que se deberán incluir temas de capacitación para el personal adscrito a la STI, a la gestión de continuidad del negocio, así como campañas de concientización de seguridad de la información dirigidas a todo el personal del Organismo. Esta incluido por los siguientes programas: Programa de Capacitación y Concientización y Programa de Capacitación para la Gestión de Continuidad del Negocio.

- **Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos (PNH-GIC):** Es un documento normativo mexicano que establece procedimientos, roles y fases para la gestión coordinada de incidentes cibernéticos de alto impacto en instituciones públicas, privadas, academia y otros actores relevantes.

- **Punto Objetivo de Recuperación (RPO - Recovery Point Objective):** Define la pérdida de datos máxima tolerable que se acepta ante una situación de desastre.

- **Recursos en un BCP:** Los recursos son todos los elementos necesarios para que los procesos críticos del negocio puedan seguir funcionando o recuperarse rápidamente. Incluyen tanto recursos humanos como materiales, tecnológicos y financieros.

- **Tipos de Recurso:**
  - **Recursos de Información y Documentación:** Bases de datos, manuales operativos, contactos de emergencia, planes actualizados.
  - **Recursos Financieros:** Fondos de emergencia, seguros, líneas de crédito, Presupuesto asignado para contingencias.
  - **Recursos Físicos o Materiales:** Instalaciones alternas, oficinas, centros de datos, equipos, vehículos, etc, Suministros esenciales (energía, agua, materiales).
  - **Recursos Humanos:** Personal clave para operar los procesos críticos, Roles y sustitutos designados.
  - **Recursos Tecnológicos:** Sistemas informáticos, software, hardware, redes, copias de seguridad, Accesos remotos y comunicación segura.

- **Regreso a Casa:** Proceso de retorno de la información del Organismo a su lugar de origen.

- **Responsables de Procesos Críticos:** Integrado por personal crítico de CAPUFE, los cuales realizan una serie de actividades interdependientes para recuperar la operatividad de CAPUFE en el menor tiempo posible y así enfrentar un desastre en forma organizada y responsable.

- **STI:** Subdirección de Tecnologías de la Información.

- **TI:** Tecnologías de Información.

- **TIC:** Tecnologías de Información y Comunicación.

- **Tiempo Objetivo de Recuperación (RTO - Recovery Time Objective):** Define el límite de tiempo máximo tolerable dentro del cual se recuperan las capacidades físicas y tecnológicas para operar un proceso en caso de contingencia. Periodo de tiempo después de un incidente en el que el producto o servicio debe ser reanudado, la actividad debe reanudarse y los recursos deben ser recuperados.

PROCEDIMIENTO DE PROTOCOLO DE INCIDENTES

OBJETIVO

Definir una estructura del equipo de respuesta a incidentes que permita desarrollar las actividades necesarias para la atención y el manejo de crisis, permitiendo al personal de CAPUFE identificar eventos que puedan provocar una interrupción parcial o total.

PROCEDIMIENTO DE PROTOCOLO DE INCIDENTES

POLÍTICAS

1. Los reportes por incidentes relacionados con el personal, las instalaciones, tecnología, seguridad de la información o algún otro factor que potencialmente pueda afectar las operaciones de CAPUFE, serán recibidos por la Subgerencia de Atención a Usuarios, a través de la Mesa de Servicio en las Extensiones 3666 o 3999, o al correo electrónico de la persona encargada de la Gerencia de Atención a Usuarios de Tecnologías de Información.

2. La Subgerencia de Atención a Usuarios será la responsable de asignar y registrar dentro de la Mesa de Servicio el número de ticket, para lo cual deberá solicitar al personal que esté reportando el incidente los detalles del mismo, a fin de identificar el tipo de incidente del que se trate de acuerdo a la Matriz de Alertamiento (Anexo 2).

3. Una vez registrado el número de ticket, deberá ser atendido por la Subgerencia de Atención a Usuarios, en caso de que el incidente se solucione, deberá documentarlo en la Mesa de Servicio y cerrar el número de ticket.

4. Si el problema no fue solucionado, la Gerencia de Atención a Usuarios de Tecnologías de Información, deberá evaluar el incidente reportado, y notificar al Grupo de Primera Respuesta.

5. El Grupo de Primera Respuesta, deberá evaluar los impactos derivados del incidente, recabar la información necesaria y notificar a las áreas conforme a la Matriz de Alertamiento (Anexo 2).

6. Una vez que el incidente haya sido resuelto, el Grupo de Primera Respuesta, deberá emitir el reporte y cerrar el ticket en la Mesa de Servicio. En caso de el incidente no haya sido resuelto, deberá emitir recomendación de declarar estado de contingencia.

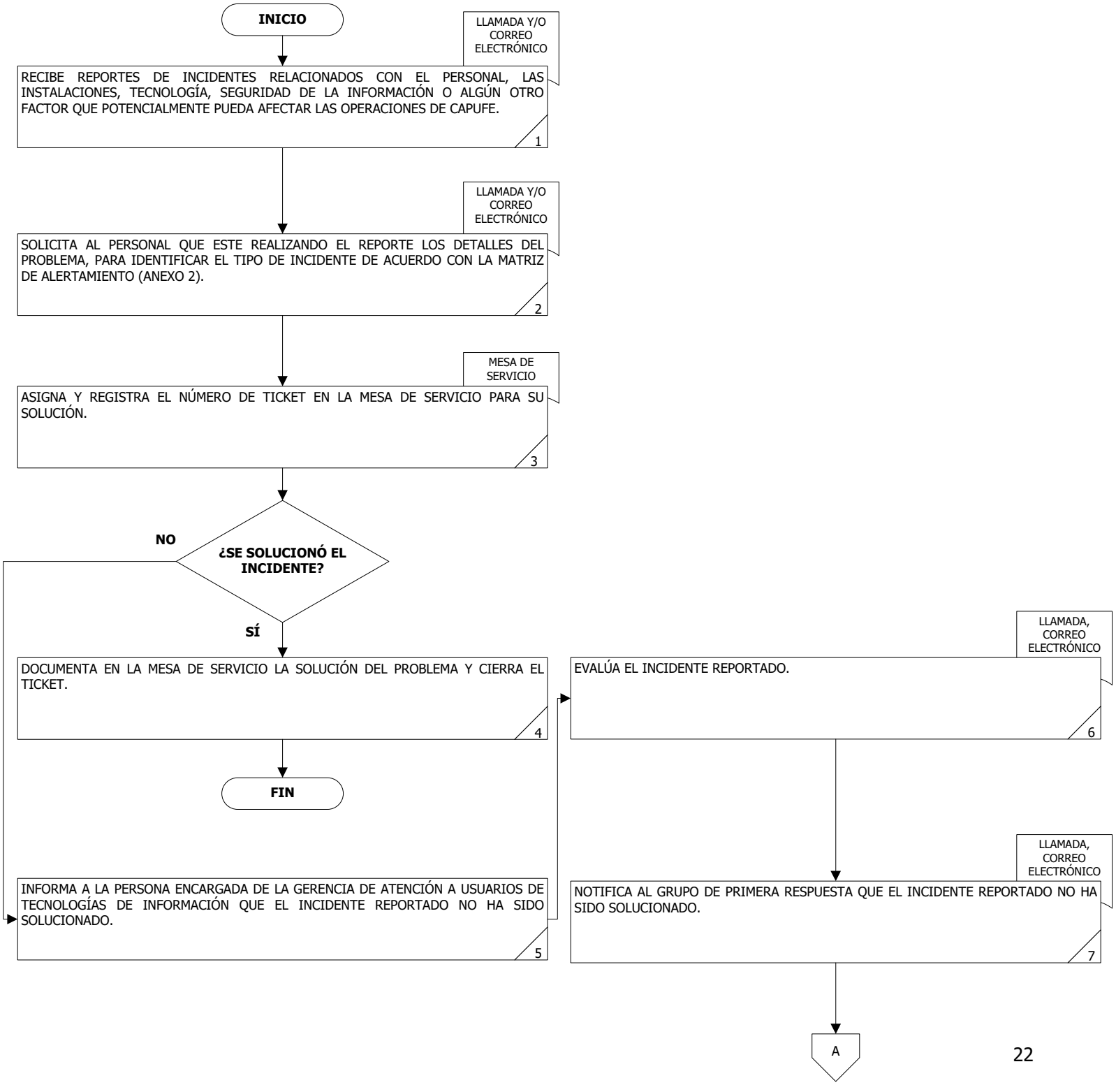
7. La STI deberá convocar a sesión al Equipo de Respuesta a Incidentes de Seguridad de la

Información (ERISC) al menos una vez al año, para revisar el Protocolo de Incidentes y actualizar a las personas integrantes del mismo.

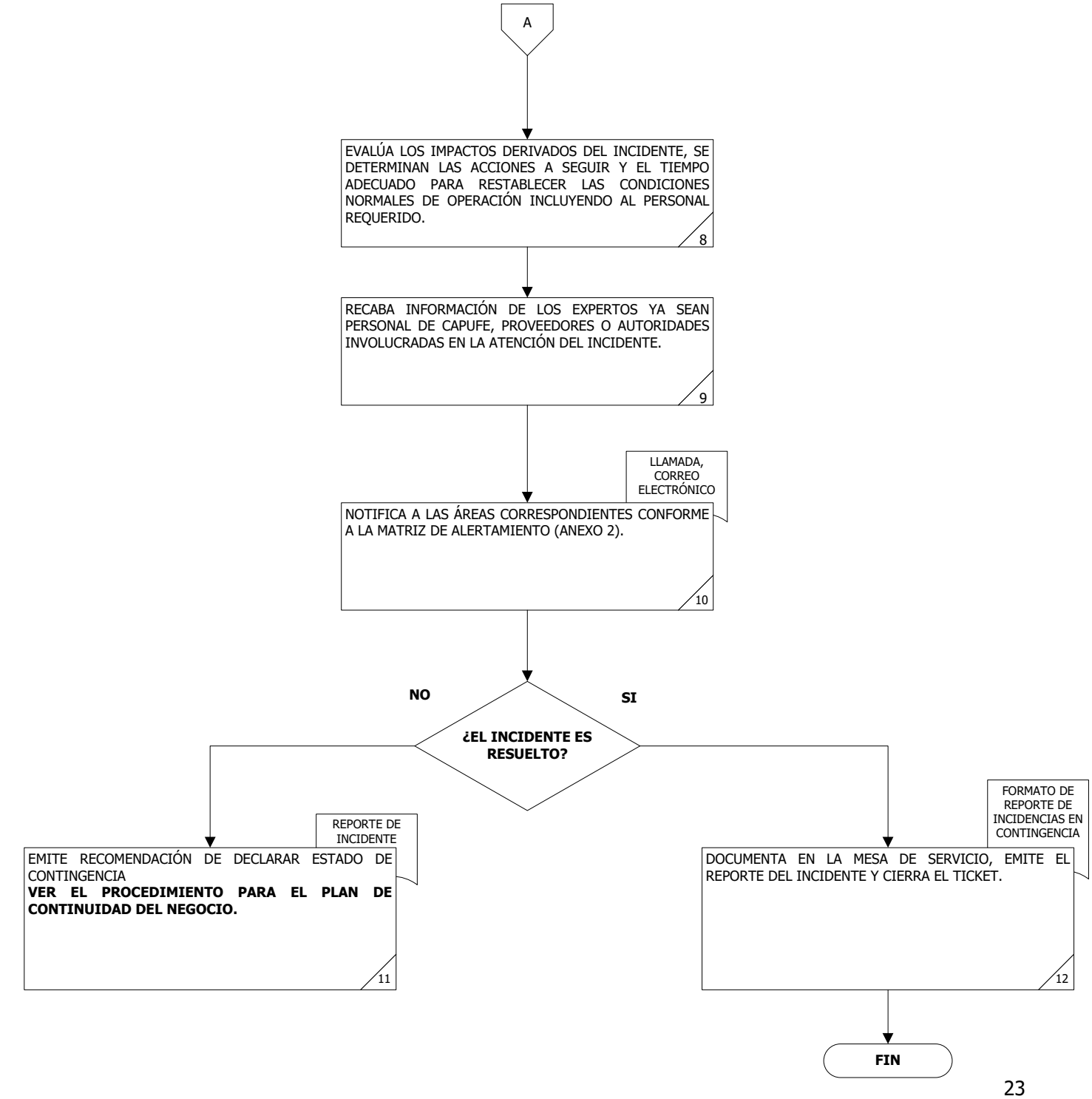
8. La GSOT deberá asegurarse de la alineación al Protocolo Nacional Homologado para la Gestión de Incidentes Cibernéticos.

ÁREA RESPONSABLE	No.	ACTIVIDAD	FORMA O DOCUMENTO
Subgerencia de Atención a Usuarios	1.	Recibe reportes de incidentes relacionados con el personal, las instalaciones, tecnología, seguridad de la información o algún otro factor que potencialmente pueda afectar las operaciones de CAPUFE.	Llamada y/o Correo Electrónico
	2.	Solicita al personal que este realizando el reporte los detalles del problema, para identificar el tipo de incidente de acuerdo con la Matriz de Alertamiento (Anexo 2).	Llamada y/o Correo Electrónico
	3.	Asigna y registra el número de ticket en la Mesa de Servicio para su solución. **¿Se solucionó el incidente?**	Mesa de Servicio
		Sí	
	4.	Documenta en la Mesa de Servicio la solución del problema y cierra el ticket. **Termina procedimiento**	
		No	
	5.	Informa a la persona encargada de la Gerencia de Atención a Usuarios de Tecnologías de Información que el incidente reportado no ha sido solucionado.	
Gerencia de Atención a Usuarios de Tecnologías de Información	6.	Evalúa el incidente reportado.	Llamada, Correo Electrónico
	7.	Notifica al Grupo de Primera Respuesta que el incidente reportado no ha sido solucionado.	Llamada, Correo Electrónico
Subgerencia de Telecomunicaciones, Subgerencia de Atención a Usuarios y Subgerencia de Administración de Sistemas de Peaje (Grupo de Primera Respuesta)	8.	Evalúa los impactos derivados del incidente, se determinan las acciones a seguir y el tiempo adecuado para restablecer las condiciones normales de operación incluyendo al personal requerido.	
	9.	Recaba información de los expertos ya sean personal de CAPUFE, proveedores o autoridades involucradas en la atención del incidente.	
	10.	Notifica a las áreas correspondientes conforme a la Matriz de Alertamiento (Anexo 2). **¿El incidente es resuelto?**	Llamada, Correo Electrónico
		No	
	11.	Emite recomendación de declarar estado de Contingencia **Ver el Procedimiento para el Plan de Continuidad del Negocio.**	Reporte del Incidente
		Sí	
	12.	Documenta en la Mesa de Servicio, emite el reporte del incidente y cierra el ticket. **Termina procedimiento**	Formato de Reporte de Incidencias en Contingencia

SUBGERENCIA DE ATENCIÓN A USUARIOS	GERENCIA DE ATENCIÓN A USUARIOS DE TECNOLOGÍAS DE INFORMACIÓN



SUBGERENCIA DE TELECOMUNICACIONES, SUBGERENCIA DE ATENCIÓN A USUARIOS Y SUBGERENCIA DE ADMINISTRACIÓN DE SISTEMAS DE PEAJE
(GRUPO DE PRIMERA RESPUESTA)



PROCEDIMIENTO PARA EL PLAN DE CONTINUIDAD DEL NEGOCIO

OBJETIVO

Establecer los lineamientos, políticas, responsabilidades y actividades que seguirán las personas involucradas en los grupos de trabajo, de acuerdo con la Estructura de Gobierno definida en el Plan de Continuidad del Negocio, a fin de responder de manera oportuna y eficaz ante una contingencia y/o desastres mayores manteniendo un nivel aceptable en la operación después de un incidente disruptivo o contingencia mejorando el actuar de las personas responsables involucradas.

PROCEDIMIENTO PARA EL PLAN DE CONTINUIDAD DEL NEGOCIO

POLITICAS

CAPUFE se compromete a que todos los procesos críticos del negocio operen adecuadamente, bajo los principios de universalidad, continuidad, oportunidad, calidad y confiabilidad, cumpliendo con los objetivos de continuidad establecidos, para asegurar la operación del tramo carretero, de una manera fácil y sencilla, mediante la implementación de un Plan de Continuidad del Negocio.

Los incidentes que pudieran llevar a una interrupción de los procesos críticos se consideran tales como: sismos, inundaciones, enfermedades infecciosas, incendios, ciberataques, disturbios sociales, etc.

I. POLÍTICAS GENERALES

1. La Dirección General de CAPUFE deberá contar con programas de contingencia y seguridad que permitan la continuidad de las operaciones mismos que deberán mantenerse actualizados.

2. El Plan de Continuidad del Negocio (BCP) deberá ser comunicado a las personas colaboradoras, con la finalidad de llevar a cabo los procedimientos de recuperación de las operaciones.

3. Mantener las obligaciones legales y contractuales con las entidades gubernamentales ante un evento de interrupción, mediante la recuperación de los procesos críticos con base en los resultados del Análisis de Impacto al Negocio (BIA) por sus siglas en inglés.

4. Mantener los procedimientos en funcionamiento durante un período de contingencia, apegándose a los planes del BCP y de la estrategia actual de recuperación de las aplicaciones previamente establecidos.

5. Las personas colaboradoras deberán cumplir y dar seguimiento a los lineamientos establecidos por la STI en los Planes de Contingencia.

6. La persona Coordinadora del BCP, deberá definir la estrategia general de capacitación, para brindar al Personal Crítico y sus suplentes los conceptos fundamentales de continuidad del negocio, el manejo, planeación y mantenimiento de los planes, así como los componentes de continuidad específicos desarrollados e implementados en CAPUFE.

7. La persona responsable de cada proceso crítico debe capacitar al Personal Crítico de su área para asegurar una respuesta oportuna y eficaz en caso de verse afectados por alguna contingencia.

8. La persona responsable de cada proceso crítico deberá generar evidencia de la capacitación impartida, así como de las lecciones aprendidas en caso de realizarse la activación del BCP producto de una contingencia real.

9. La Dirección General de CAPUFE y las personas responsables de los procesos críticos deberá mantener las obligaciones contractuales con las personas usuarias, proveedoras y/o entidades gubernamentales. Así mismo, deberán asegurar la disponibilidad de los siguientes elementos:
    a. La operación de sus procesos críticos.
    b. Cumplimiento de obligaciones legales y contractuales.
    c. Cumplimiento con la normatividad y regulaciones vigentes.
    d. Accesos remotos a sistemas y aplicaciones requeridos para la operación de sus procesos críticos.

10. La Dirección General de CAPUFE y las personas responsables de los procesos críticos deberán informar al Coordinador BCP cuando se presente alguno de los siguientes cambios para mantener actualizados los componentes de continuidad y asegurar su vigencia:
    a. Cambios de personal crítico y suplentes.
    b. Cambios en la información de contacto del personal crítico y suplentes.
    c. Cambios en procesos críticos.

d. Cambios en aplicaciones críticas.
e. Cambios en proveedores críticos.
f. Cambios en sitios de operación.
g. Criticidad de los procesos por juicio experto.

11. La Dirección General de CAPUFE y las personas responsables de los procesos críticos deberán asegurar que las empresas proveedoras que contraten cuenten con Planes de Continuidad del Negocio y Planes de Recuperación de Desastres.

12. La Dirección General de CAPUFE y las personas responsables de los procesos críticos, deberán gestionar los acuerdos contractuales relacionados con la prestación de servicios por terceros, asegurando que se cuenten con garantías de continuidad del servicio con las empresas proveedoras y en su caso serán responsables de aplicar las penalizaciones correspondientes a través de las áreas administrativas y legales de CAPUFE.

13. Las personas responsables de los procesos críticos deberán mantener actualizados, sus planes de continuidad por área como parte de un proceso continuo de revisión y adecuación a las condiciones cambiantes del entorno, incorporando aquellos temas y conceptos requeridos para cada circunstancia.

14. Los colaboradores identificados como personal crítico, así como sus suplentes, deberán contar con equipo de cómputo necesarios para la ejecución de sus funciones y el cual debe ser gestionado por su supervisor directo.

15. El Plan de Continuidad del Negocio y sus componentes deberán ser evaluados por lo menos una vez al año para identificar oportunidades de mejora o posibles fallas en su planeación, documentación y/o implementación. La periodicidad y el alcance de las pruebas puede variar como resultado de la decisión del Grupo de Directivo o como resultado de requerimientos normativos.

II. POLÍTICAS PARA LA COORDINACIÓN Y EJECUCIÓN DEL BCP

1. Todas las personas participantes en el proceso de continuidad del negocio deberán estar capacitadas en conceptos generales de continuidad del negocio, así como en los componentes específicos de continuidad que se están implementados dentro de CAPUFE, de acuerdo con su rol y sus responsabilidades.

2. Las personas responsables de los procesos críticos deberán contar con los recursos físicos, humanos y tecnológicos definidos en cada uno de los planes, en caso de declararse una contingencia.

3. La STI debe establecer un mecanismo de respaldo de información que pueda ser utilizado en casos de contingencia, así como ejecutar pruebas de estos en los periodos de tiempo adecuados para la operación de acuerdo con el Punto Objetivo de Recuperación (RPO) identificado para cada proceso y para cada sistema identificado dentro del Análisis de Impacto al Negocio (BIA).

III. POLÍTICAS PARA LA RECUPERACIÓN DE PROCESOS CRÍTICOS

1. Las personas responsables de los procesos críticos deberán monitorear los límites y parámetros de riesgo establecidos para la operación y recuperación de las áreas y procesos de negocio.

2. El Tiempo Objetivo de Recuperación (RTO) de los procesos críticos deberán ser definidos por los responsables de los procesos críticos con base en lo establecido en el BIA.

3. Las personas responsables de los procesos críticos deberán asegurar la recuperación de sus procesos críticos apegándose a los RTO definidos en la fase de BIA, para evitar la materialización de los impactos previamente identificados.

4. Las personas responsables de los procesos críticos deberán evaluar el impacto al negocio al término de la contingencia a fin de analizar las lecciones aprendidas y lograr la mejora continua e informar a la persona Coordinadora del BCP sobre los resultados para su comunicación.

IV. POLÍTICAS PARA EL PLAN DE PRUEBAS

1. La persona Coordinadora del BCP debe validar que CAPUFE cuente con un programa de pruebas de efectividad y funcionamiento de los planes de contingencia y seguridad establecidos.

2. La persona Coordinadora del BCP debe elaborar un programa de pruebas para validar la efectividad del BCP, este plan debe de contemplar diferentes tipos de pruebas como son: aisladas, de escritorio e integrales. Estas deberán ser realizadas al menos una vez al año.

3. Las personas responsables de los procesos críticos deberán desarrollar y ejecutar un programa de rotación de personal en los distintos puestos, con la finalidad de estar en posibilidad de cubrir al personal en casos de contingencia.

4. Las personas responsables de los procesos críticos deberán implementar en tiempo y forma las acciones correctivas definidas para el cierre de hallazgos y/o recomendaciones derivadas de cada prueba e informar la persona Coordinadora del BCP sobre el resultado de este.

5. El seguimiento de los hallazgos y las áreas de oportunidad de las pruebas del BCP, deberá ser atendido por las áreas responsables de los procesos críticos, mediante la elaboración de planes de acción.

6. Las pruebas de las Estrategias y Planes de Continuidad del Negocio podrán tener los siguientes objetivos, en el entendido que la siguiente es una guía efectuada de manera enunciativa más no limitativa:
    a. Verificar la adecuada planeación, implementación y capacidad de las Estrategias y Planes de Continuidad del Negocio.

b. Verificar el funcionamiento de los Árboles de Llamada en contingencia.
c. Verificar el nivel de capacitación del personal crítico.
d. Verificar el nivel de concientización de las personas colaboradoras.
e. Verificar la disponibilidad de requerimientos mínimos y registros vitales.
f. Verificar la capacidad de recuperación para uno o varios escenarios de interrupción.
g. Demostrar el cumplimiento con regulaciones de autoridades y entes normativos.

7. Todas las pruebas deberán ser documentadas en un reporte por parte de la persona Coordinadora del BCP para identificar las lecciones aprendidas y/o áreas de oportunidad que permitan entrar en un proceso de mejora continua y con esto perfeccionar la efectividad de las Estrategias y Planes de Continuidad del Negocio.

8. La persona Coordinadora del BCP debe planear, definir objetivos, alcance, plan de trabajo, coordinación y documentación de las pruebas realizadas a las Estrategias y Planes de Continuidad del Negocio y sus componentes, notificando por escrito los resultados obtenidos al Grupo Directivo.

9. Las personas responsables de los procesos críticos deberán ejecutar las pruebas de sus planes, confirmando que cumplen los objetivos de recuperación y cuentan con el alcance suficiente para probar todos los elementos que los componen.

10. La persona Coordinadora del BCP debe definir qué áreas participaran en las diferentes pruebas de continuidad de acuerdo con lo establecido en el presente documento.

V. PLAN DE CONTINUIDAD DEL NEGOCIO

El Plan de Continuidad del Negocio se divide en cinco fases:

I. FASE DE RESPUESTA

1. Es responsabilidad del Grupo de Primera Respuesta de atender el incidente de acuerdo al protocolo de cada área, clasificar la situación del evento con base en la Matriz de Alertamiento (Anexo 2), ejecutar las actividades necesarias para contener el incidente, e informar en todo momento al Grupo de Manejo de Crisis si el incidente ha sido o no resuelto.

2. En caso de que no se cuente con los recursos necesarios para activar el BCP, el Grupo de Manejo de Crisis, deberá coordinar al Grupo de Primera Respuesta para contener el incidente, o en su caso, informar y recomendar a la persona Coordinadora del BCP la gravedad del incidente y recomendar la activación del BCP.

3. Es responsabilidad del Grupo Directivo declarar la activación del BCP, e informar al Grupo de Manejo de Crisis y a la persona Coordinadora del BCP, quienes deberán de comunicar a los Grupos de Trabajo la activación de acuerdo al Árbol de Llamadas (Anexo 1). Así mismo, deberá informar al Grupo de Manejo de Crisis y a la persona Coordinadora del BCP, cuando no sea activado el BCP y asignar los recursos necesarios para que el incidente sea atendido.

II. FASE DE RECUPERACIÓN

1. Es responsabilidad del Grupo de Manejo de Crisis, evaluar la contingencia con base a lo establecido en el Plan de Manejo de Crisis, y determinar si cuenta, o no, con los recursos necesarios para recuperar capacidades, y en su caso, validar y administrar los recursos que sean asignados por el Grupo Directivo para contener la contingencia, así como de coordinar al Grupo de Recuperación de Instalaciones, y al Grupo de Recuperación Tecnológica, a fin de que realicen las actividades necesarias para recuperar capacidades para operar en estado de Contingencia.

2. La Persona Coordinadora del BCP, deberá comunicarse en todo momento con el Grupo de Comunicación en Crisis para que lleve a cabo los comunicados correspondientes internos y externos, con las personas Responsables de Procesos Críticos a efecto de iniciar con las actividades de recuperación de procesos, así como de informar al Grupo Directivo cuando se hallan recuperado los procesos críticos.

3. Responsables de Procesos Críticos, deberán comunicar y coordinar al Personal Critico de los procesos afectados para que inicien las actividades de recuperación de los Procesos Críticos, y notificar a la persona Coordinadora del BCP cuando se hayan recuperado.

III. FASE DE REANUDACIÓN

1. De existir incidentes durante la operación en Contingencia, las personas Responsables de Procesos Críticos deberán coordinar al personal de CAPUFE y al Grupo de Recuperación Tecnológica las actividades para mantener la operación en Contingencia, así como de mantener informado al Grupo Directivo sobre el estatus de la Contingencia.

2. Es responsabilidad del Personal Critico mantener informados a las personas Responsables de Procesos Críticos sobre cualquier eventualidad presentada en los Procesos Críticos.

IV. FASE DE RESTAURACIÓN

1. El Grupo de Manejo de Crisis, deberá coordinar al Grupo de Recuperación de Instalaciones y al Grupo de Recuperación Tecnológica, para rehabilitar las capacidades de infraestructura y tecnología, e informar al Grupo de Manejo de Crisis cuando ya se encuentren rehabilitadas estas capacidades.

2. Las personas Responsables de Procesos Críticos y el Personal Crítico, serán responsables de realizar las actividades correspondientes para el Regreso a Casa, así como de informar a la Persona Coordinadora de BCP cuando se pueda operar con normalidad.

3. Es responsabilidad de Grupo Directivo declarar el término de la contingencia, e informar a la persona Coordinadora BCP.

V. FASE DE EVALUACIÓN

1. La Persona Coordinadora BCP, será responsable de recopilar la información generada durante la contingencia con el fin de evaluar la aplicación del BCP, analizar las causas, determinar las afectaciones al Organismo en términos cualitativos y cuantitativos, e identificar las acciones de mejora que se deben implementar para minimizar el daño en situaciones similares subsecuentes.

ÁREA RESPONSABLE	No.	ACTIVIDAD	FORMA O DOCUMENTO
		FASE DE RESPUESTA	
Subgerencia de Telecomunicaciones, Subgerencia de Atención a Usuarios y Subgerencia de Administración de Sistemas de Peaje (Grupo de Primera Respuesta)	1.	Recibe notificación por parte de la Gerencia de Atención a Usuarios del evento de emergencia.	Llamada, Correo Electrónico
	2.	Atiende el incidente de acuerdo al protocolo de cada área.	
	3.	Clasifica la situación del evento con base en la Matriz de Alertamiento (Anexo 2), para determinar si recomienda o no la activación del BCP dependiendo del nivel de alerta, y ejecuta las actividades necesarias para contener el incidente.	
		¿El incidente fue resuelto?	
		Sí	
	4.	Comunica al Grupo de Manejo de Crisis que el incidente fue resuelto.	
		Termina Procedimiento (Evento tratado como Incidente).	
		No	
	5.	Comunica al Grupo de Manejo de Crisis que el incidente no ha sido resuelto.	Llamada, Correo Electrónico
Grupo de Manejo de Crisis	6.	Evalúa y verifica si cuenta con recursos para atender el incidente sin necesidad de la activación del BCP.	
		¿Cuenta con recursos para contener el incidente sin activar el BCP?	
		No	
	7.	Coordina al Grupo de Primera Respuesta para contener el evento sin necesidad de activar el BCP. Regresa a actividad 2.	
		Sí	
	8.	Notifica a la persona Coordinadora BCP la gravedad del evento y en su caso recomienda la activación del BCP.	Llamada, Correo Electrónico
Subdirección de Tecnologías de Información (Persona Coordinadora del BCP)	9.	Informa al Grupo Directivo correspondiente la situación del evento, para que evalúen la situación y decidan si se activa el BCP. **Nota: A partir de esta actividad comienzan las notificaciones de contingencia a través de la herramienta de continuidad.**	Llamada, Correo Electrónico, Formato de Reporte de Incidentes en Contingencia
Dirección General de CAPUFE, Dirección de Operación, Dirección de Administración y Finanzas, Dirección Técnica y Dirección Jurídica (Grupo Directivo)		**¿Activa el BCP?**	Herramienta de Continuidad
		No	
	10.	Notifica al Grupo de Manejo de Crisis y a la persona Coordinadora del BCP, que no se declara la activación del BCP, para que el evento sea gestionado como un incidente normal, y asigna recursos necesarios. Regresa a actividad 2.	

ÁREA RESPONSABLE	No.	ACTIVIDAD	FORMA O DOCUMENTO
		Sí	
	11.	Declara la activación de la contingencia notificando al Grupo de Manejo de Crisis y a la persona Coordinadora del BCP.	Llamada, Correo Electrónico, App
Grupo de Manejo de Crisis, Subdirección de Tecnologías de Información (Persona Coordinadora Del BCP)	12.	Comunican a los Grupos de Trabajo la activación del BCP, de acuerdo con el Árbol de llamadas definido en el BCP de CAPUFE (Anexo 1).	Llamada, Correo Electrónico, App
		FASE DE RECUPERACIÓN	
Grupo de Manejo de Crisis	13.	Evalúa la contingencia con base en lo establecido en el Plan de Manejo de Crisis, para poder determinar el alcance de esta y determinar si se cuenta con recursos para recuperar capacidades. **¿Cuenta con los recursos necesarios?**	
		Sí	
	14.	Notifica a la persona Coordinadora del BCP la gravedad de la contingencia para que notifique al Grupo de Comunicación en Crisis y a las personas Responsables de Procesos Críticos. Continua con la actividad 21.	Llamada, Correo Electrónico, App
		No	
	15.	Solicita los recursos al Grupo Directivo correspondiente.	Llamada, Correo Electrónico, App
Dirección General de CAPUFE, Dirección de Operación, Dirección de Administración y Finanzas, Dirección Técnica y Dirección Jurídica (Grupo Directivo)	16.	Asigna al Grupo de Manejo de Crisis los recursos necesarios para contener la contingencia.	
Grupo de Manejo de Crisis	17.	Valida y administra los recursos asignados, coordina al Grupo de Recuperación de Instalaciones y al Grupo de Recuperación Tecnológica para recuperar capacidades de infraestructura y tecnológica.	
Grupo de Recuperación de Instalaciones	18.	Realiza las actividades necesarias para recuperar las capacidades de infraestructura física, mobiliarios y equipos para operar en contingencia.	
	19.	Notifica a las personas Responsables de Procesos Críticos afectados y al Grupo de Manejo de Crisis, que ya se encuentran recuperadas las capacidades de infraestructura física, mobiliarios y equipos para operar la contingencia.	Llamada, Correo Electrónico, App

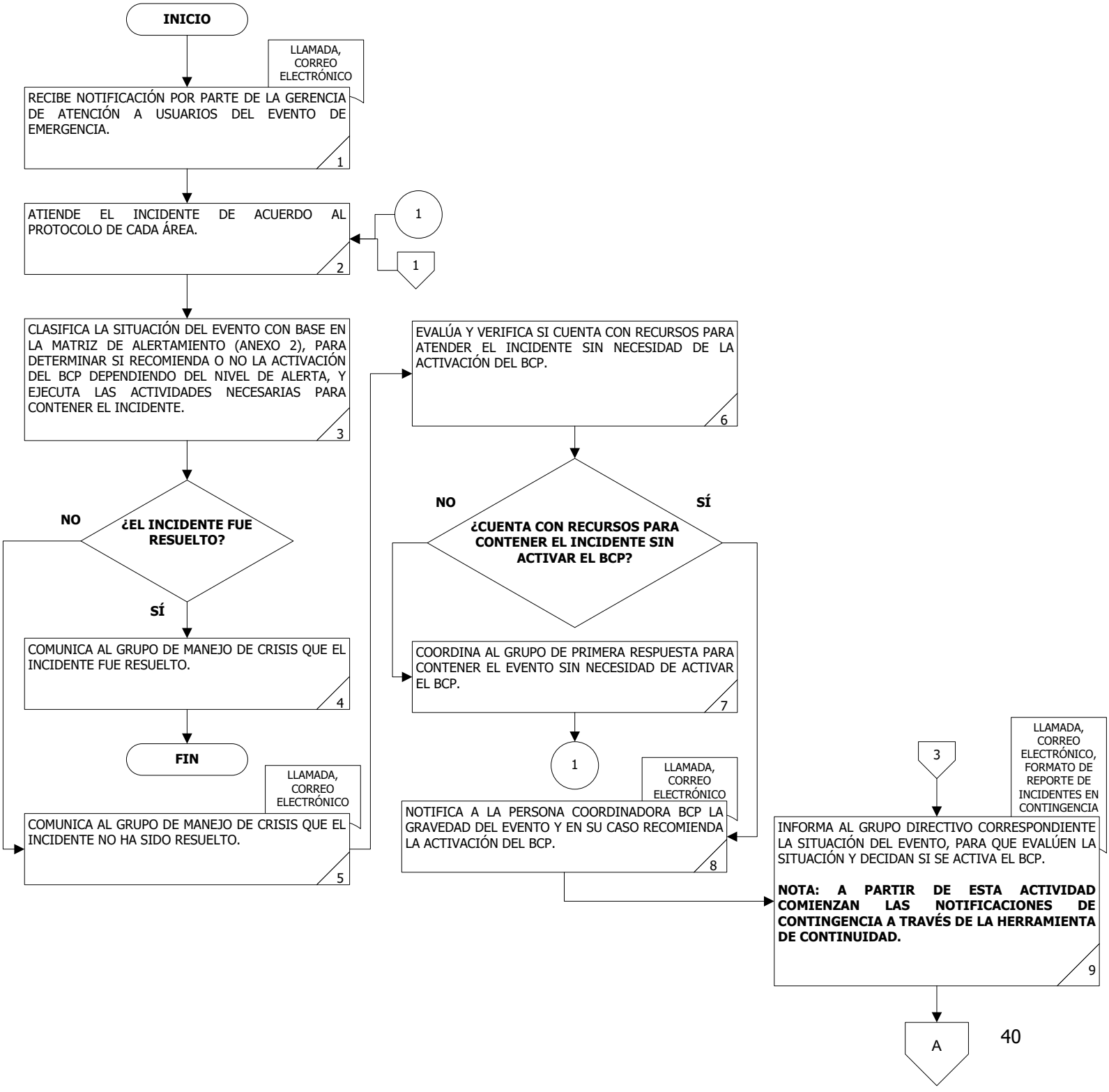
ÁREA RESPONSABLE	No.	ACTIVIDAD	FORMA O DOCUMENTO
Subgerencia de Administración de Sistemas de Peaje (Grupo de Recuperación de Tecnológica)	20.	Determina la necesidad de activar o no el DRP, de acuerdo con los procedimientos propios de TI y ejecuta las actividades necesarias para recuperar las capacidades tecnológicas para operar en contingencia.	
	21.	Notifica a las personas Responsables de Procesos Críticos afectados y al Grupo de Manejo de Crisis, que ya se encuentran recuperadas las capacidades tecnológicas para operar la contingencia.	Llamada, Correo Electrónico, App
Subdirección de Tecnologías de Información (Persona Coordinadora Del BCP)	22.	Notifica al Grupo de Comunicación en Crisis para que lleve a cabo los comunicados correspondientes internos y externos, e informa a las personas Responsables de Procesos Críticos la activación del BCP, para que detonen el Árbol de Llamadas (Anexo 1) de los procesos críticos afectados.	Llamada, Correo Electrónico, App
Subgerencia de Telecomunicaciones, Subgerencia de Atención a Usuarios, Subgerencia de Administración de Sistemas de Peaje (Grupo de Comunicación en Crisis)	23.	Lleva a cabo la comunicación interna y/o externa de acuerdo al nivel de gravedad y alcance de la contingencia y con base en lo establecido en el Plan de Activación y Comunicación del BCP.	Llamada
Subdirección de Tecnologías de Información (Persona Coordinadora Del BCP)	24.	Comunica la activación del BCP oficialmente a las personas Responsables de Procesos Críticos para que estos detonen los árboles de llamadas de los procesos críticos afectados.	Llamada, Correo Electrónico, App
Responsables de Procesos Críticos	25.	Detonan los árboles de llamadas correspondientes para comunicar al Personal Crítico de los procesos afectados para que inicien las actividades de recuperación de procesos.	
Personal Crítico	26.	Coordina las actividades de recuperación de los procesos críticos.	
Responsables de Procesos Críticos	27.	Lleva a cabo las actividades de recuperación de los procesos críticos afectados por la contingencia, con base en la estrategia y los planes de recuperación de operaciones por área.	
	28.	Notifican a la persona Coordinadora del BCP, la recuperación de los procesos críticos.	
Subdirección de Tecnologías de Información (Persona Coordinadora del BCP)	29.	Notifica al Grupo Directivo correspondiente.	Llamada, Correo Electrónico

ÁREA RESPONSABLE	No.	ACTIVIDAD	FORMA O DOCUMENTO
		FASE DE REANUDACIÓN	
Personal Crítico	30.	Lleva a cabo la operación de los Procesos Críticos durante la contingencia. **¿Hay incidentes durante la operación de los Procesos Críticos en contingencia?** **Sí**	
	31.	Comunica a las personas Responsables de Procesos Críticos que ya se encuentran operando los procesos críticos y reportan el incidente.	Llamada, Correo Electrónico
Responsables de Procesos Críticos	32.	Coordinan las actividades para resolver el incidente con personal de CAPUFE y con el Grupo de Recuperación de Tecnológica (DRP), según corresponda.	
Personal de CAPUFE	33.	Atiende a sus actividades de acuerdo con sus procedimientos internos y mantiene el soporte a la operación en contingencia. Regresa a la actividad 9.	
Subgerencia de Administración de Sistemas de Peaje (Grupo de Recuperación de Tecnológica)	34.	Atiende sus actividades de acuerdo con sus procedimientos internos.	
	35.	Mantiene soporte a la operación en contingencia.	
		No	
Personal Crítico	36.	Comunica a las personas Responsables de Procesos Críticos que continúan operando los procesos críticos, así como sobre cualquier eventualidad.	Llamada, Correo Electrónico, App
Responsables de Procesos Críticos	37.	Notifican el estatus de operación al Grupo de Manejo de Crisis y a la persona Coordinadora del BCP.	Llamada, Correo Electrónico, App
	38.	Mantiene informado sobre la situación actual al Grupo Directivo correspondiente.	
		FASE DE RESTAURACIÓN	
Grupo de Manejo de Crisis	39.	Coordina las actividades correspondientes para rehabilitar las capacidades de infraestructura y tecnológicas para el proceso de Regreso a Casa.	
Grupo de Recuperación de Instalaciones, Subgerencia de Administración de Sistemas de Peaje	40.	Comienzan a rehabilitar las capacidades de las instalaciones, infraestructura y tecnológicas, según corresponda, y mantienen soporte a la operación en contingencia.	
	41.	Notifican al Grupo de Manejo de Crisis que ya se encuentran rehabilitadas las capacidades de infraestructura física.	Llamada, Correo Electrónico, App
Grupo de Manejo de Crisis	42.	Notifica a la persona Coordinadora del BCP la rehabilitación de las capacidades para iniciar el Regreso a Casa.	Llamada, Correo Electrónico, App

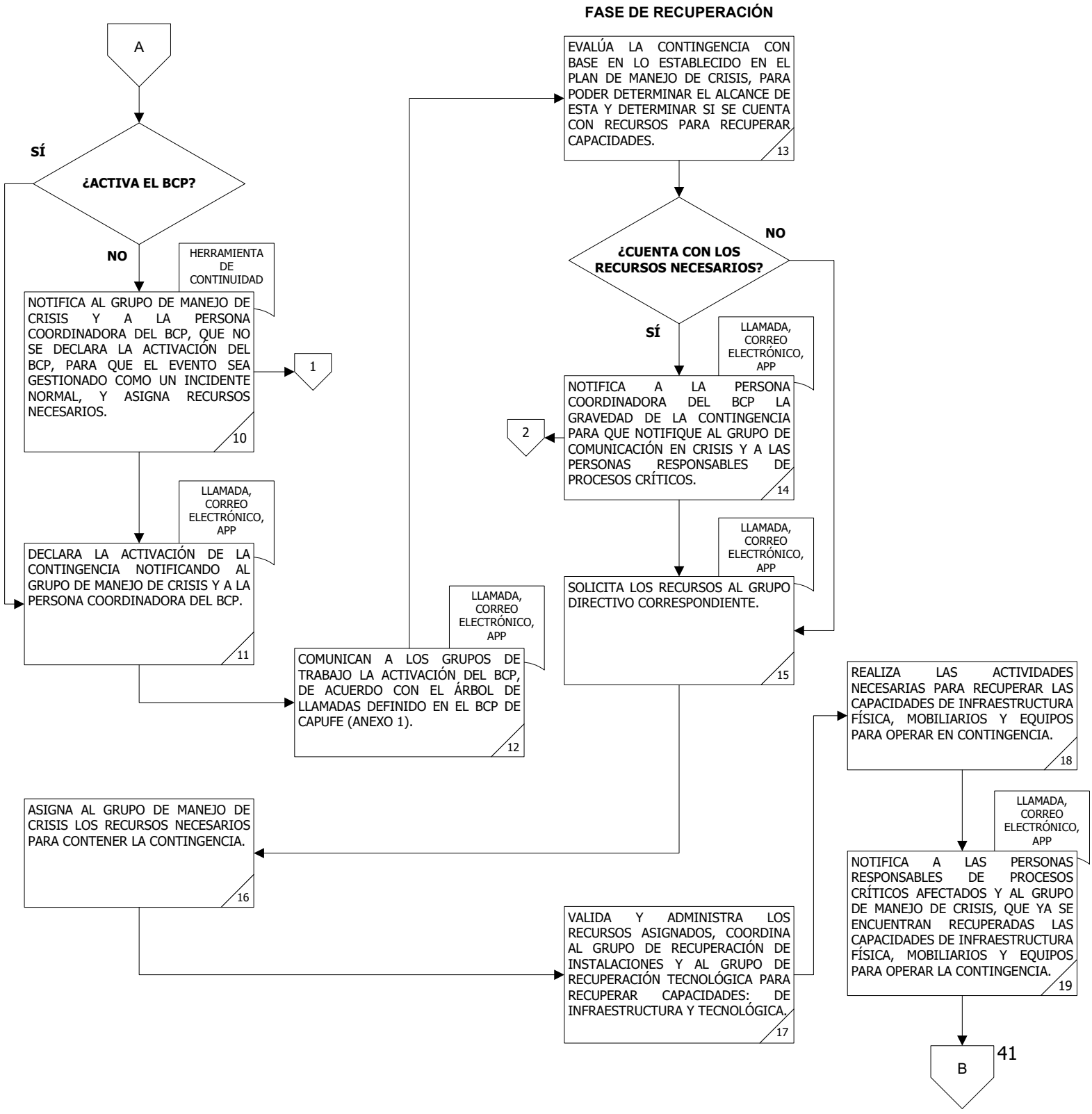
ÁREA RESPONSABLE	No.	ACTIVIDAD	FORMA O DOCUMENTO
Subdirección de Tecnologías de Información (Persona Coordinadora del BCP)	43.	Recibe la notificación de la rehabilitación de capacidades, y comunica a las personas Responsables de Procesos Críticos el inicio del proceso de Regreso a Casa.	Llamada, Correo Electrónico, App
Responsables de Procesos Críticos, Personal Crítico	44.	Realizan actividades correspondientes para el Regreso a Casa e inician operaciones con normalidad.	
	45.	Notifican el inicio de la operación normal a la persona Coordinadora del BCP.	Llamada, Correo Electrónico, App
Subdirección de Tecnologías de Información (Persona Coordinadora del BCP)	46.	Mantiene informado al Grupo de Directivo correspondiente sobre el proceso de Regreso a Casa.	Llamada, Correo Electrónico, App
	47.	Notifica al Grupo Directivo correspondiente que los procesos ya se encuentran operando normalmente.	Llamada, correo Electrónico, App
Dirección General de CAPUFE, Dirección de Operación, Dirección de Administración y Finanzas, Dirección Técnica y Dirección Jurídica (Grupo Directivo)	48.	Da por terminada la contingencia y lo comunica a la persona Coordinadora del BCP.	
Subdirección de Tecnologías de Información (Persona Coordinadora del BCP)	49.	Comunica al Grupo de Comunicación en Crisis la terminación de la contingencia.	Llamada, Correo Electrónico, App
Grupo de Comunicación en Crisis	50.	Notifica el Fin de la contingencia a las partes interesadas internas y/o externas.	Llamada, Correo Electrónico, App
		FASE DE EVALUACIÓN	
Subdirección de Tecnologías de Información (Persona Coordinadora del BCP)	51.	Recopila la información relevante durante el desarrollo de la contingencia.	Minuta
	52.	Da seguimiento a las acciones de mejora establecidas para mejorar el Plan de Continuidad de Negocio y los Planes de Recuperación de Operación Crítica de cada Área.	
	53.	Analiza y evalúa las causas e impactos de la contingencia con el apoyo de otras áreas y direcciones.	

ÁREA RESPONSABLE	No.	ACTIVIDAD	FORMA O DOCUMENTO
	54.	Genera el reporte para el Grupo de Dirección con las Lecciones Aprendidas derivado de la contingencia que incluirá las acciones que se implementarán en los Planes de Continuidad del Negocio y el tiempo estimado para ello.	Reporte Ejecutivo
Personas Responsables de Procesos Críticos, Personal Critico	55.	Registra los incidentes que se presenten y que afecten la operación de los procesos durante la contingencia.	Formato de Reporte de Incidentes en Contingencia
	56.	Implementa acciones de mejora a los Planes de Recuperación de Operación Crítica de cada Área, en conjunto con la persona Coordinadora BCP.	
		Termina Procedimiento	

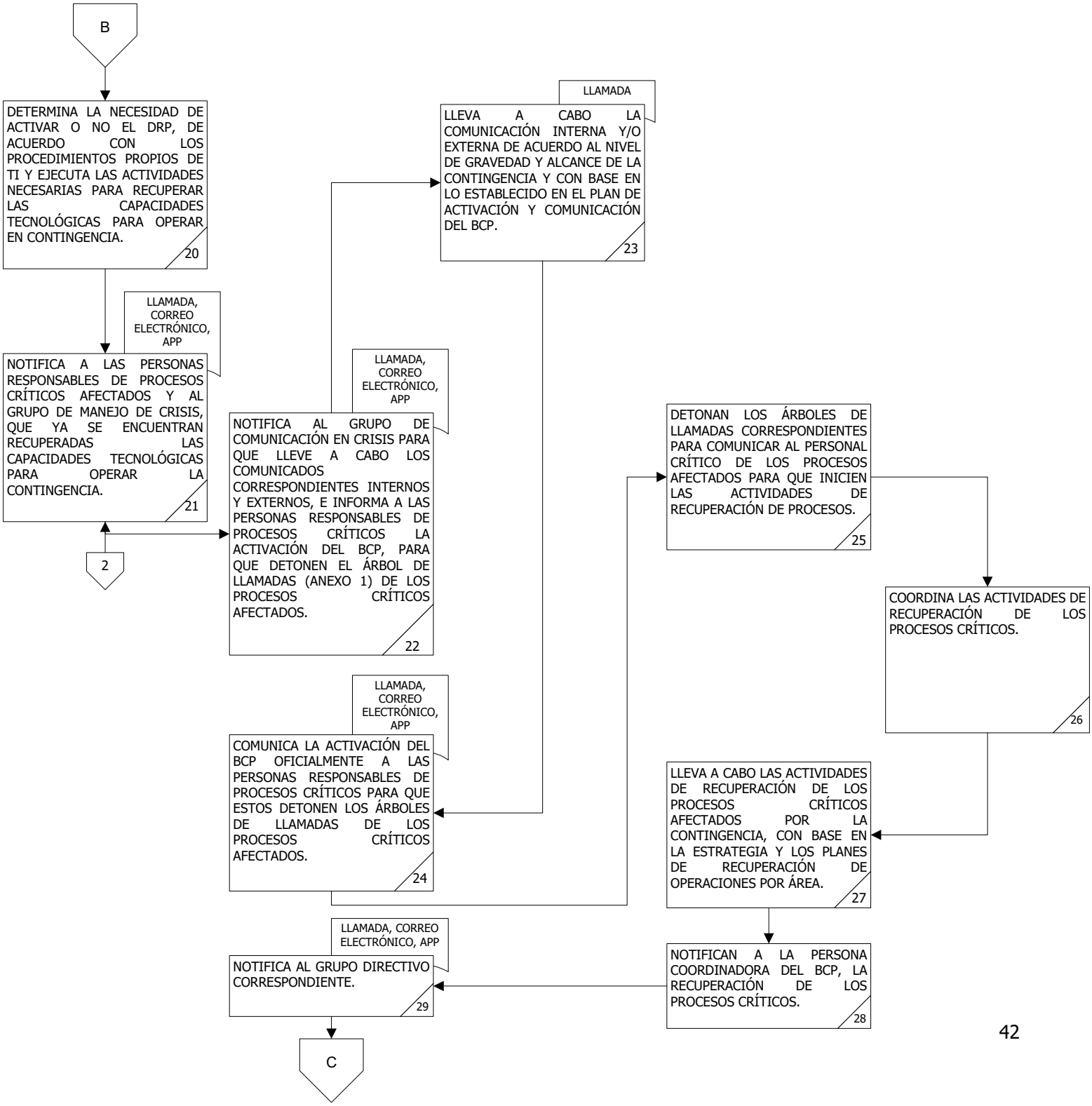
SUBGERENCIA DE TELECOMUNICACIONES, SUBGERENCIA DE ATENCIÓN A USUARIOS Y SUBGERENCIA DE ADMINISTRACIÓN DE SISTEMAS DE PEAJE (GRUPO DE PRIMERA RESPUESTA)	**GRUPO DE MANEJO DE CRISIS**	**SUBDIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN (PERSONA COORDINADORA DEL BCP)**

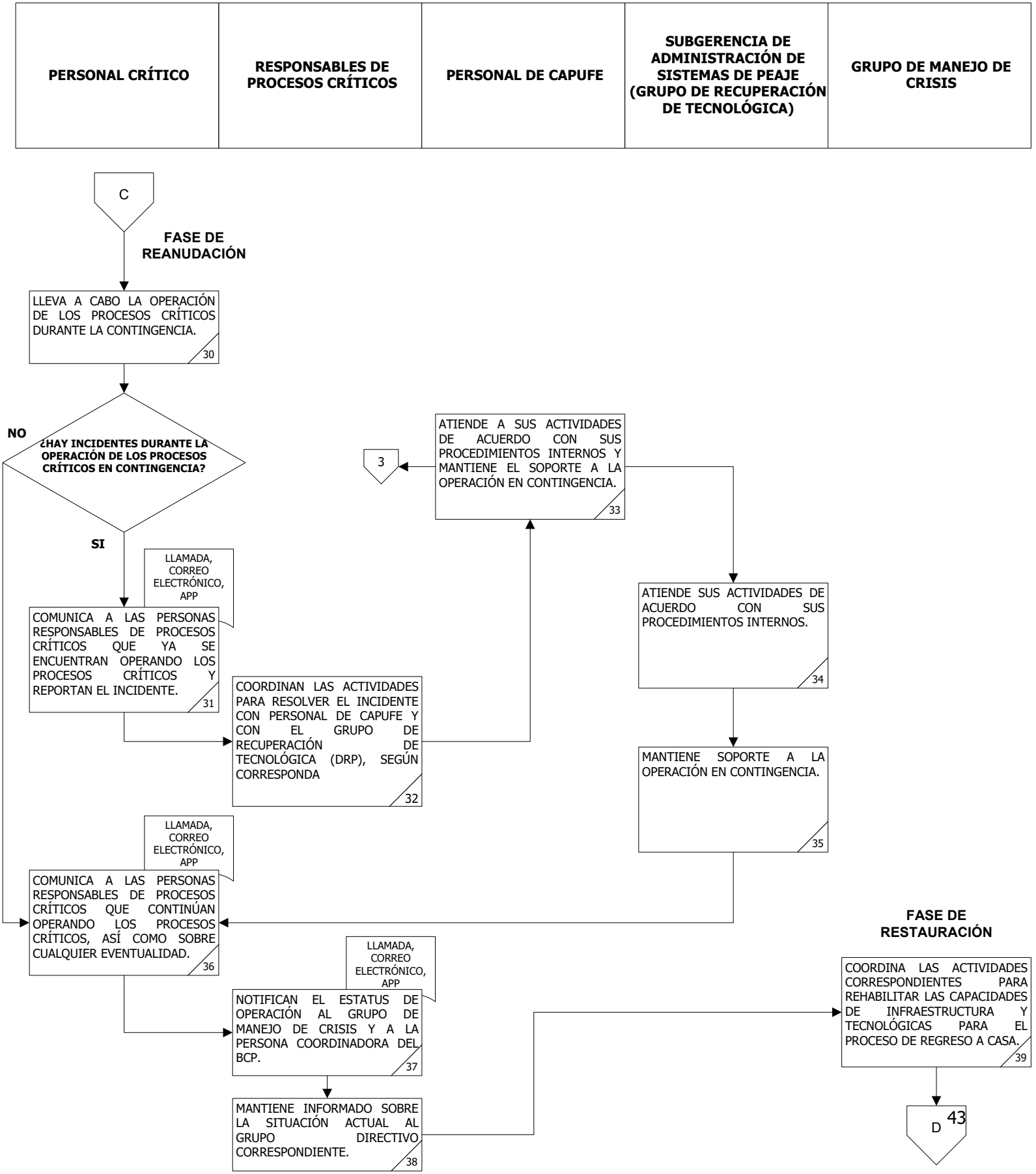


DIRECCIÓN GENERAL DE CAPUFE, DIRECCIÓN DE OPERACIÓN, DIRECCIÓN DE ADMINISTRACIÓN Y FINANZAS, DIRECCIÓN TÉCNICA Y DIRECCIÓN JURÍDICA (GRUPO DIRECTIVO)	GRUPO DE MANEJO DE CRISIS, SUBDIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN (PERSONA COORDINADORA DEL BCP)	GRUPO DE MANEJO DE CRISIS	GRUPO DE RECUPERACIÓN DE INSTALACIONES

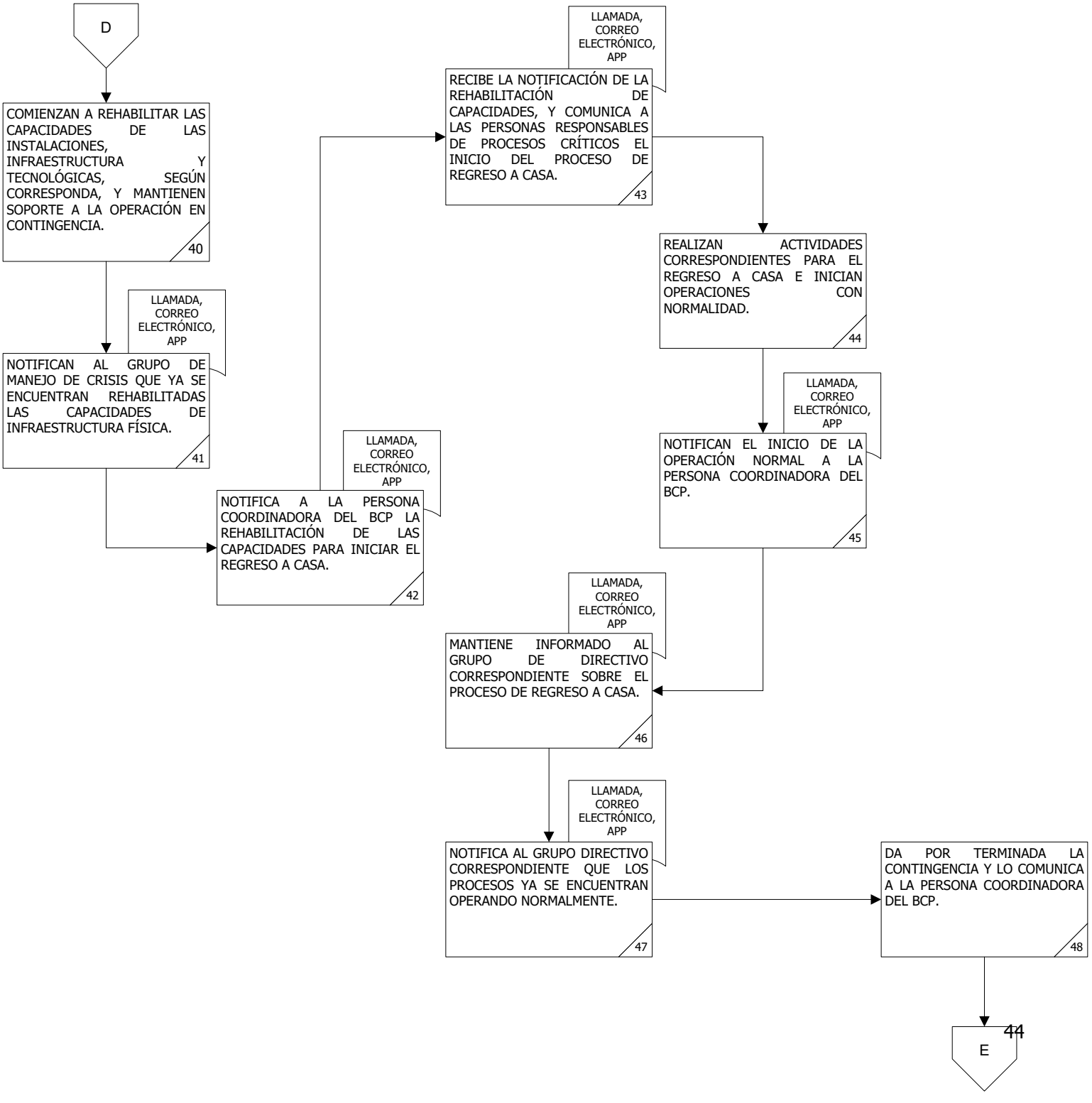


SUBGERENCIA DE ADMINISTRACIÓN DE SISTEMAS DE PEAJE (GRUPO DE RECUPERACIÓN DE TECNOLÓGICA)	SUBDIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN (PERSONA COORDINADORA DEL BCP)	SUBGERENCIA DE TELECOMUNICACIONES, SUBGERENCIA DE ATENCIÓN A USUARIOS, SUBGERENCIA DE ADMINISTRACIÓN DE SISTEMAS DE PEAJE (GRUPO DE COMUNICACIÓN EN CRISIS)	RESPONSABLES DE PROCESOS CRÍTICOS	PERSONAL CRÍTICO

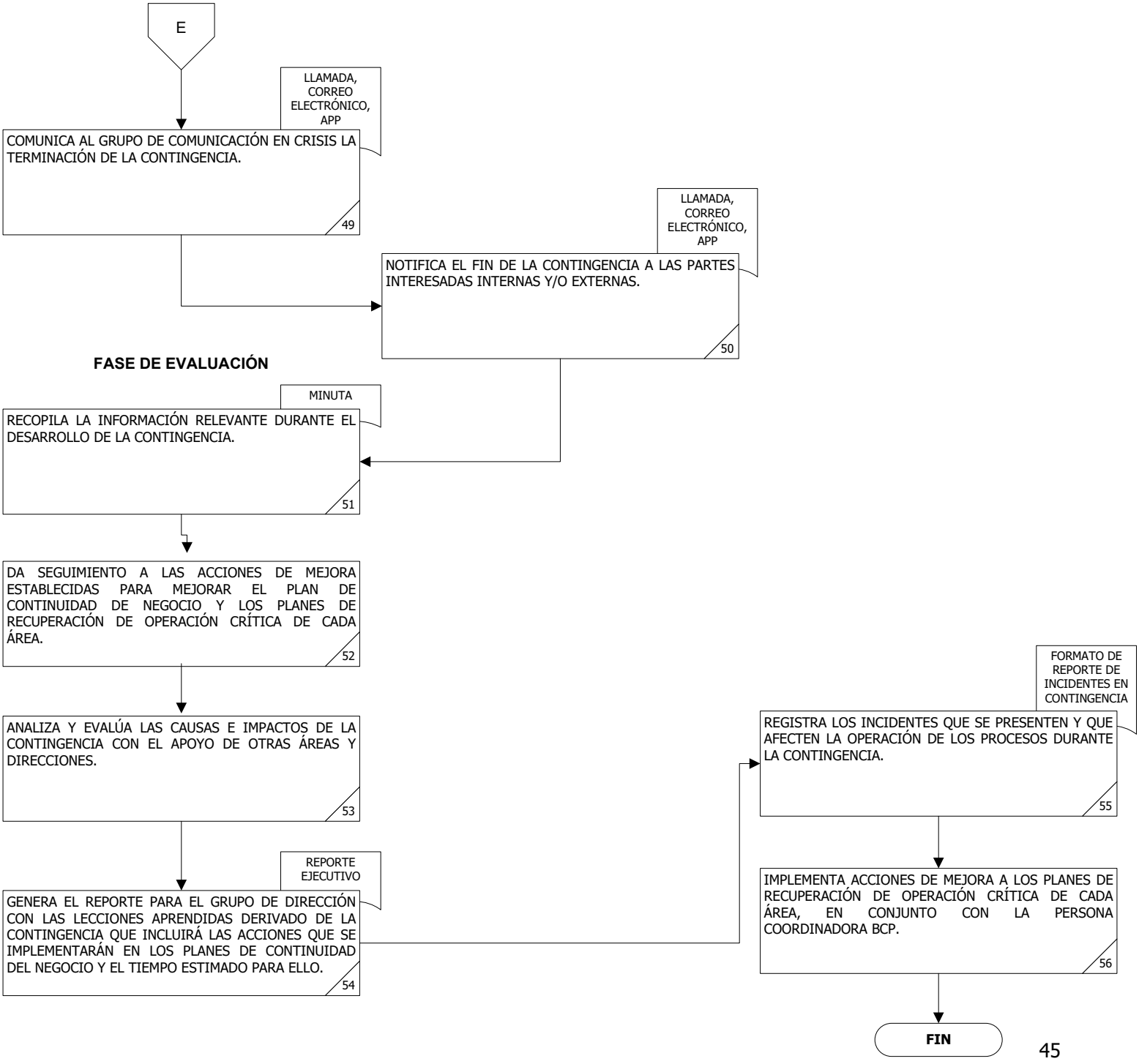



PERSONAL CRÍTICO
RESPONSABLES DE PROCESOS CRÍTICOS
PERSONAL DE CAPUFE
SUBGERENCIA DE ADMINISTRACIÓN DE SISTEMAS DE PEAJE (GRUPO DE RECUPERACIÓN DE TECNOLÓGICA)
GRUPO DE MANEJO DE CRISIS
C
FASE DE REANUDACIÓN
LLEVA A CABO LA OPERACIÓN DE LOS PROCESOS CRÍTICOS DURANTE LA CONTINGENCIA.
30
¿HAY INCIDENTES DURANTE LA OPERACIÓN DE LOS PROCESOS CRÍTICOS EN CONTINGENCIA?
NO
SI
LLAMADA, CORREO ELECTRÓNICO, APP
COMUNICA A LAS PERSONAS RESPONSABLES DE PROCESOS CRÍTICOS QUE YA SE ENCUENTRAN OPERANDO LOS PROCESOS CRÍTICOS Y REPORTAN EL INCIDENTE.
31
COORDINAN LAS ACTIVIDADES PARA RESOLVER EL INCIDENTE CON PERSONAL DE CAPUFE Y CON EL GRUPO DE RECUPERACIÓN DE TECNOLÓGICA (DRP), SEGÚN CORRESPONDA
32
ATIENDE A SUS ACTIVIDADES DE ACUERDO CON SUS PROCEDIMIENTOS INTERNOS Y MANTIENE EL SOPORTE A LA OPERACIÓN EN CONTINGENCIA.
33
3
ATIENDE SUS ACTIVIDADES DE ACUERDO CON SUS PROCEDIMIENTOS INTERNOS.
34
MANTIENE SOPORTE A LA OPERACIÓN EN CONTINGENCIA.
35
LLAMADA, CORREO ELECTRÓNICO, APP
COMUNICA A LAS PERSONAS RESPONSABLES DE PROCESOS CRÍTICOS QUE CONTINÚAN OPERANDO LOS PROCESOS CRÍTICOS, ASÍ COMO SOBRE CUALQUIER EVENTUALIDAD.
36
LLAMADA, CORREO ELECTRÓNICO, APP
NOTIFICAN EL ESTATUS DE OPERACIÓN AL GRUPO DE MANEJO DE CRISIS Y A LA PERSONA COORDINADORA DEL BCP.
37
MANTIENE INFORMADO SOBRE LA SITUACIÓN ACTUAL AL GRUPO DIRECTIVO CORRESPONDIENTE.
38
FASE DE RESTAURACIÓN
COORDINA LAS ACTIVIDADES CORRESPONDIENTES PARA REHABILITAR LAS CAPACIDADES DE INFRAESTRUCTURA Y TECNOLÓGICAS PARA EL PROCESO DE REGRESO A CASA.
39
D
43

GRUPO DE RECUPERACIÓN DE INSTALACIONES, SUBGERENCIA DE ADMINISTRACIÓN DE SISTEMAS DE PEAJE	GRUPO DE MANEJO DE CRISIS	SUBDIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN (PERSONA COORDINADORA DEL BCP)	RESPONSABLES DE PROCESOS CRÍTICOS, PERSONAL CRÍTICO	DIRECCIÓN GENERAL DE CAPUFE, DIRECCIÓN DE OPERACIÓN, DIRECCIÓN DE ADMINISTRACIÓN Y FINANZAS, DIRECCIÓN TÉCNICA Y DIRECCIÓN JURÍDICA (GRUPO DIRECTIVO)



SUBDIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN (PERSONA COORDINADORA DEL BCP)	GRUPO DE COMUNICACIÓN EN CRISIS	PERSONAS RESPONSABLES DE PROCESOS CRÍTICOS, PERSONAL CRITICO



PROCEDIMIENTO PARA EL PROGRAMA DE CULTURA DE SEGURIDAD DE LA INFORMACIÓN

OBJETIVO

Generar y fomentar una cultura organizacional orientada a la seguridad de la información, con el fin de proteger los activos informáticos, la privacidad de los datos y reducir los riesgos asociados con incidentes de seguridad, integrando tanto al personal directamente involucrado con los procesos y servicios críticos, como al resto del personal siendo participantes activos que actúen proactivamente para proteger los recursos del Organismo y la información confidencial.

PROCEDIMIENTO PARA EL PROGRAMA DE CULTURA DE SEGURIDAD DE LA INFORMACIÓN

POLÍTICAS

1. La STI, a través de la GSOT, será la responsable de elaborar anualmente el Programa de Cultura de Seguridad de la Información, en el que se deberán incluir temas de capacitación para el personal adscrito a la STI, a la gestión de continuidad del negocio, así como campañas de concientización de seguridad de la información dirigidas a todo el personal del Organismo.

   - Programa de Capacitación y Concientización, tendrá el objetivo de crear conciencia y sensibilización de la importancia que esto conlleva al logro de los objetivos estratégicos de CAPUFE.

   Consideraciones para el desarrollo de las sesiones de capacitación:

   a. Las sesiones de capacitación para las áreas de CAPUFE se pueden distribuir dependiendo del público objetivo al que vaya dirigido la capacitación, así como la disponibilidad del personal. Es importante considerar que al realizar la asignación del personal no se vea afectada la operación normal de las actividades de las áreas.
   b. Las sesiones de capacitación para las áreas se pueden llevar a cabo a través de sesiones remotas.
   c. Se estima que la sesión de capacitación tenga una duración aproximada entre 1 y 2 horas. Mínimo 2 capacitaciones al año y máximo 4.
   d. Se debe llevar el registro y control de los asistentes a las capacitaciones, a través del cual se identifique claramente el medio (remoto, presencial).
   e. Se debe realizar una evaluación de conocimientos sobre la sesión de la capacitación impartida.

En el momento de llevar a cabo el desarrollo de las campañas de concientización, es importante considerar:

a. Desarrollar un mensaje sencillo y concreto, indicando qué debe hacer y por qué.
b. Difundir el mensaje que se desea por medio de un lenguaje claro.
c. Definir parámetros de seguimiento y evaluación de la campaña, con el propósito de medir la efectividad de ésta, para lo cual se pueden realizar encuestas, observación de actitudes, estadísticas, etc.
d. Incluir sucesos recientes de alto impacto que se hayan presentado al interior o exterior de CAPUFE.
e. Promover que el contenido de la campaña en gran medida sea gráfico.
f. La campaña se difundirá mensualmente de manera electrónica a través de los medios de comunicación oficiales establecidos (correo electrónico, intranet, entre otros), así como físicos (impresiones ubicadas en sitios estratégicos de las instalaciones), dirigidas a todo el personal del Organismo.

- Programa de Capacitación para la Gestión de Continuidad del Negocio las capacitaciones deben ser diseñadas conforme a las necesidades y cambios de estrategias, regulaciones, operación entre otros, considerando los riesgos actuales, los incidentes con mayor recurrencia, los recursos humanos y materiales que sean requeridos, así como los temas específicos relacionados con la Gestión de Continuidad del Negocio requerida por CAPUFE.

Consideraciones para el desarrollo de la capacitación:

a. Las sesiones de capacitación para las áreas de CAPUFE se pueden distribuir dependiendo del público objetivo al que vaya dirigido la capacitación, así como la disponibilidad del personal. Es importante considerar que al realizar la asignación del personal no se vea afectada la operación normal de las actividades de las áreas.
b. Las sesiones de capacitación para las áreas se pueden llevar a cabo a través de sesiones remotas.

c. Se estima que la sesión de capacitación tenga una duración aproximada entre 1 y 2 horas.
d. Se debe llevar el registro y control de los asistentes a las capacitaciones, a través del cual se identifique claramente el medio (remoto, presencial).
e. Se debe realizar una evaluación de conocimientos sobre la sesión de la capacitación impartida.

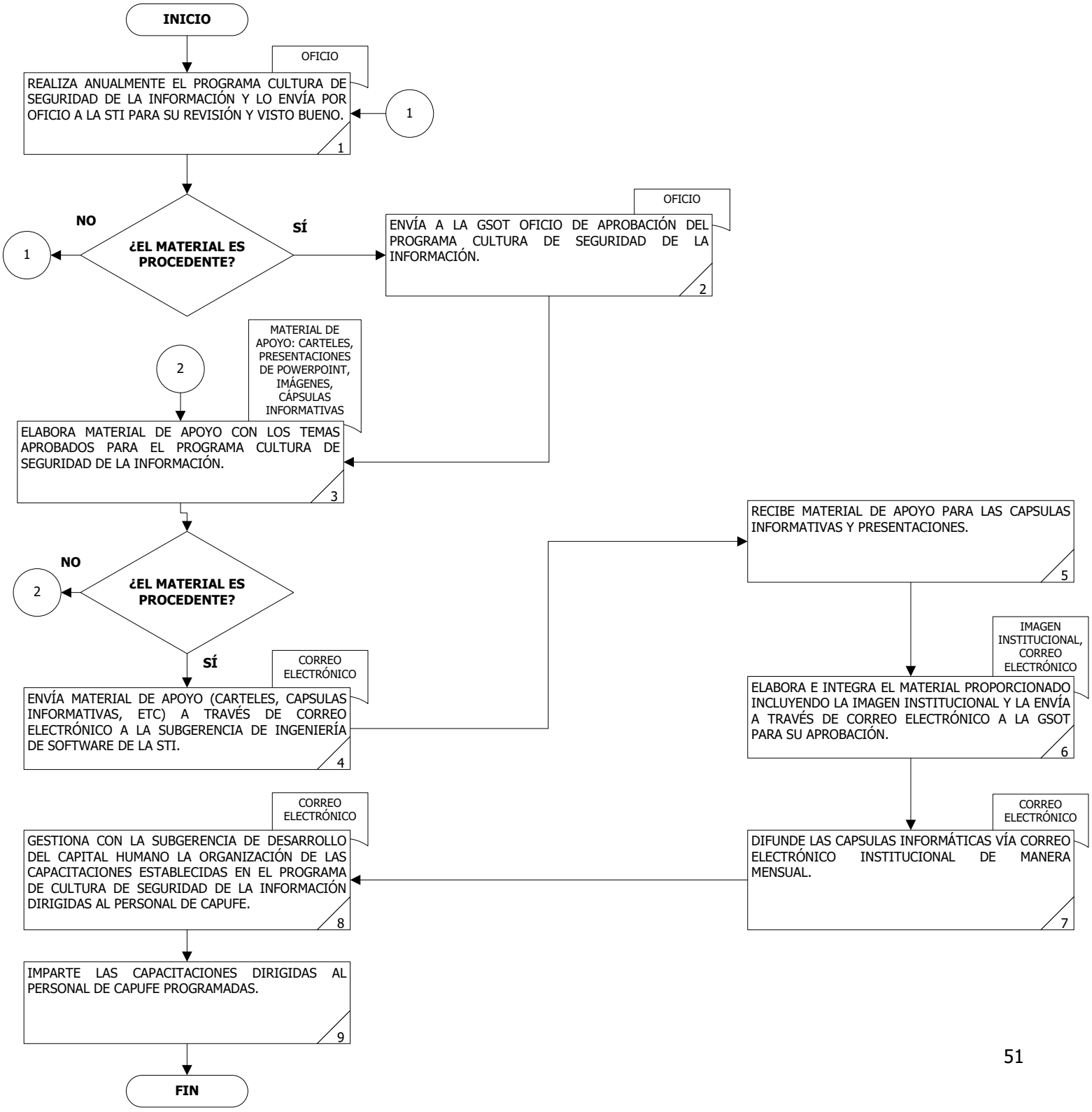
2. Una vez que el Programa de Cultura de Seguridad de la Información, sea aprobado por la STI, la GSOT elaborará el material de apoyo (carteles, capsulas informativas, etc.) mismo que también deberá ser aprobado por la STI.

3. El material de apoyo será difundido mediante el correo electrónico institucional del Organismo de manera mensual, por la Subgerencia de Ingeniería de Software.

4. La GSOT, gestionará con la Subgerencia de Desarrollo del Capital Humano la organización de las capacitaciones establecidas en el Programa de Cultura de Seguridad de la Información dirigidas al personal de CAPUFE.

ÁREA RESPONSABLE	No.	ACTIVIDAD	FORMA O DOCUMENTO
Gerencia de Seguridad y Operaciones Tecnológicas	1.	Realiza anualmente el Programa Cultura de Seguridad de la Información y lo envía por oficio a la STI para su revisión y visto bueno. **¿El material es procedente?** **No** Regresa a la actividad 1. **Sí**	Oficio
STI	2.	Envía a la GSOT oficio de aprobación del Programa Cultura de Seguridad de la Información.	Oficio
Gerencia de Seguridad y Operaciones Tecnológicas	3.	Elabora material de apoyo con los temas aprobados para el Programa Cultura de Seguridad de la Información. **¿El material es procedente?** **No** Regresa a la actividad 3. **Sí**	Material de Apoyo: Carteles, Presentaciones de Power Point, Imágenes, Cápsulas Informativas
	4.	Envía material de apoyo (carteles, capsulas informativas, etc) a través de correo electrónico a la Subgerencia de Ingeniería de Software de la STI.	Correo Electrónico
Subgerencia de Ingeniería de Software	5.	Recibe material de apoyo para las capsulas informativas y presentaciones.	
	6.	Elabora e integra el material proporcionado incluyendo la imagen institucional y la envía a través de correo electrónico a la GSOT para su aprobación.	Imagen Institucional, Correo Electrónico
	7.	Difunde las capsulas informáticas vía correo electrónico institucional de manera mensual.	Correo Electrónico
Gerencia de Seguridad y Operaciones Tecnológicas	8.	Gestiona con la Subgerencia de Desarrollo del Capital Humano la organización de las capacitaciones establecidas en el Programa de Cultura de Seguridad de la Información dirigidas al personal de CAPUFE.	Correo Electrónico
	9.	Imparte las capacitaciones dirigidas al personal de CAPUFE programadas. **Termina procedimiento**	

GERENCIA DE SEGURIDAD Y OPERACIONES TECNOLÓGICAS	STI	SUBGERENCIA DE INGENIERÍA DE SOFTWARE



ANEXO 1

ÁRBOL DE LLAMADAS

Una vez que el Grupo Directivo en conjunto con el Grupo de Manejo de Crisis active el Plan de Continuidad del Negocio derivado de una contingencia, el Coordinador BCP se encarga de notificar al Responsable BCP por área (contacto de 1º nivel), o en caso de ser necesario a su suplente; el Responsable BCP por área debe de iniciar el árbol de llamadas de su área correspondiente e informar al contacto de 2° nivel o a su suplente; a su vez el contacto de 2º nivel debe informar al contacto de 3º nivel o a su suplente. Al final de la contingencia el árbol de llamadas se vuelve a activar con el mensaje oficial y las instrucciones para el regreso a la operación normal.

El árbol de llamadas será activado con base en lo establecido en cada uno de los procesos críticos de CAPUFE, los datos de contacto del personal crítico se consideran de carácter confidencial para el uso interno de CAPUFE.

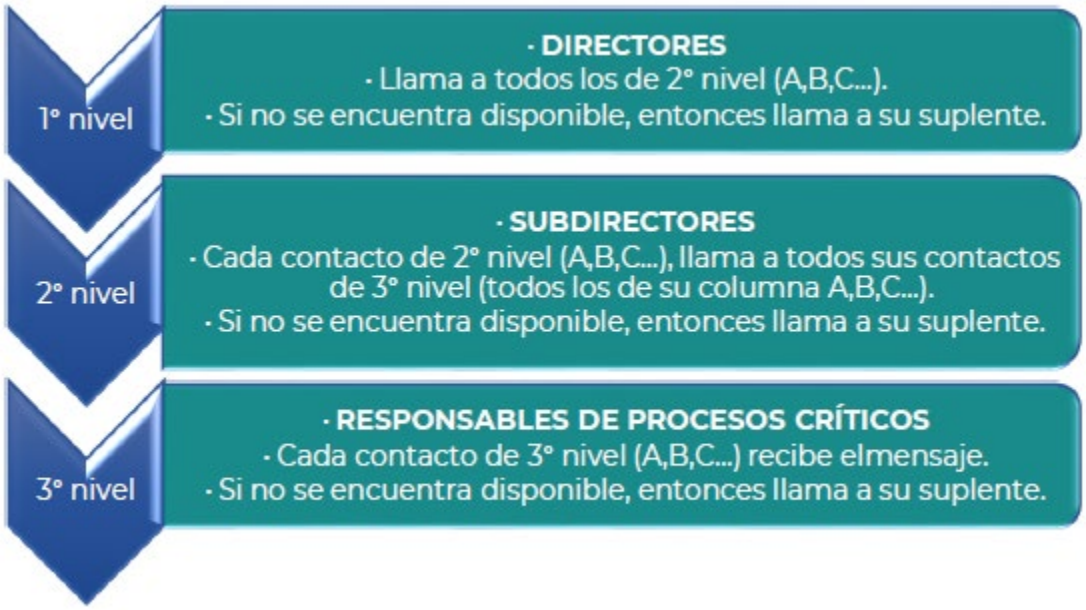
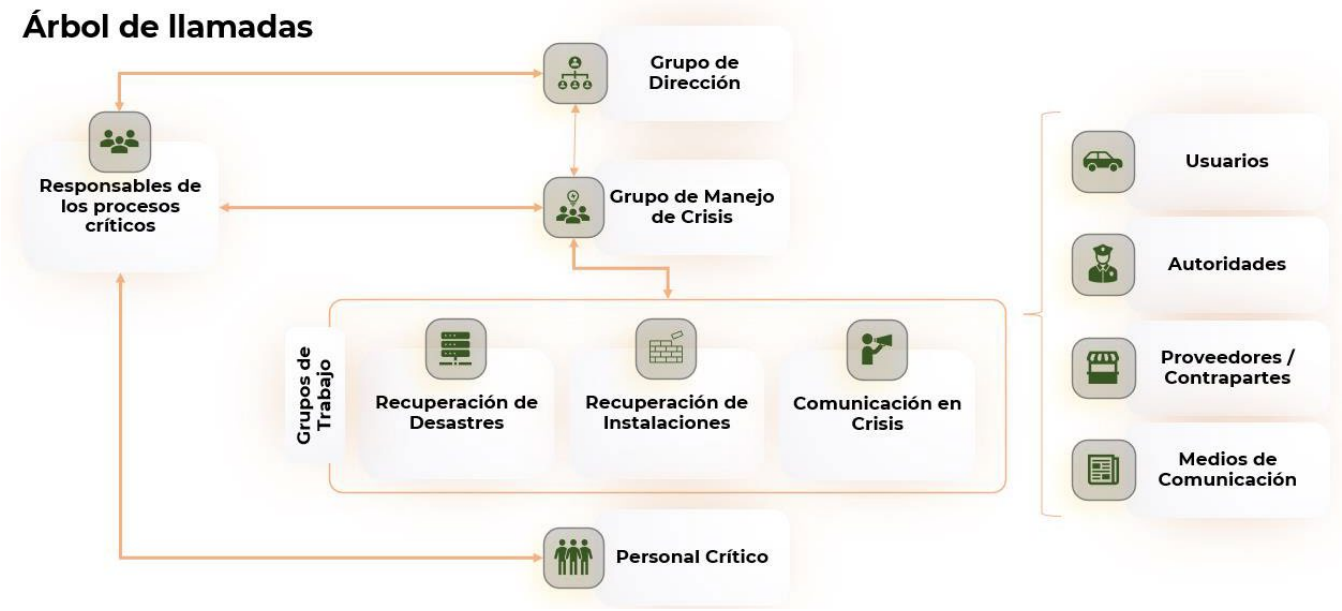


DIAGRAMA DE ÁRBOL DE LLAMADAS JERARQUICO



PRINCIPALES ESCENARIOS DE INTERRUPCIÓN

Como resultado del Análisis de Riesgo y para cubrir los eventos disruptivos que pudieran llevar a una interrupción de los procesos críticos de CAPUFE, tales como, sismos, inundaciones, enfermedades infecciosas, incendios, ciberataques, disturbios sociales, etc., se definieron 5 principales escenarios de interrupción que se muestran a continuación:

ANEXO 2

MATRIZ DE ALERTAMIENTO

El manejo de incidentes debe ser atendido de acuerdo con un nivel de alerta preestablecido que deriva en acciones que van de la contención y resolución de estos a través del Programa Interno de Protección Civil y a los Protocolos de Seguridad Física y Tecnológica establecidos para la atención de incidentes en CAPUFE, hasta la detonación del BCP por parte del Grupo Directivo.

A continuación, se presenta una tabla de alerta con los niveles de mayor a menor para el manejo de los incidentes. Cabe aclarar que los incidentes presentados son enunciativos y de ninguna manera limitativos y pretenden dar una guía de actuación al Grupo de Primera Respuesta para la identificación de contingencias mayores y toma de decisiones.

Nivel de alerta 1. Recomendación de activación BCP con carácter urgente

SE RECOMIENDA LA ACTIVACIÓN DEL BCP CON CARÁCTER URGENTE	
TIPO DE INCIDENTE	**DESCRIPCIÓN DE AFECTACIÓN**
Relacionado con el personal	• Huelgas del personal que impidan el ingreso a las instalaciones. • Incidentes graves del personal por secuestro masivo, toma de rehenes en las instalaciones de CAPUFE. • Bloqueo indefinido de accesos a las instalaciones por grupos externos a CAPUFE. • Declaración de Pandemia por autoridades Federales. • Indisponibilidad del 100% del personal de CAPUFE debido a enfermedades, pandemia o situaciones extraordinarias. • Disturbios sociales de impacto nacional o estatal. • Cualquier incidente relacionado con Personal Crítico de los procesos críticos y altos establecidos en el BIA (considerando los RTOs de cada proceso).
Relacionado con las Instalaciones	• Incendio sin control que implique la pérdida parcial o total de las instalaciones. • Afectación estructural a las instalaciones. • Daños mayores a las plantas de energía eléctrica, acometidas de la CFE, unidades de respaldo de energía (UPS) durante apagones o cortes en los suministros de electricidad de las instalaciones. • Fallas en UPS y plantas de emergencia durante un corte de energía eléctrica prolongado. • Cualquier desastre natural que provoque daños mayores en las instalaciones. • Afectación por amenaza natural con daños y afectación a las instalaciones y/o personal de CAPUFE. • Cualquier incidente que afecte las instalaciones donde se operen alguno de los procesos críticos o altos establecidos en el BIA (considerando los RTOs de cada proceso).
Relacionado con Incidentes Tecnológicos	• Caída de enlaces de comunicación. • Falla de servidores de producción que alojan aplicaciones críticas o componentes que las soportan. • Incidente de seguridad de la información que cause interrupción a los servicios. • Ciberataques. • Daños accidentales o intencionales a la infraestructura tecnológica y de telecomunicaciones. • Cualquier incidente que afecte la infraestructura tecnológica que soporte alguno de los procesos críticos o altos establecidos en el BIA (considerando los RTOs de cada proceso).

SE RECOMIENDA LA ACTIVACIÓN DEL BCP CON CARÁCTER URGENTE	
TIPO DE INCIDENTE	**DESCRIPCIÓN DE AFECTACIÓN**
Tiempo de solución	• Si el Grupo de Primera Respuesta determina que la solución del incidente le va a tomar más de 2 horas. • Si el Grupo de Primera Respuesta identifica que el incidente afecta directamente la operación de algún proceso critico o alto y la solución de este le va a tomar más del tiempo RTO establecido para dicho proceso.
Horario	• Si el Incidente ocurre dentro del horario laboral y el tiempo de solución cumple con las características mencionadas en el cuadro anterior.

Nivel de alerta 2. Recomendación de activación BCP bajo reserva

SE RECOMIENDA LA ACTIVACIÓN DEL BCP BAJO RESERVA DEL GRUPO DE MANEJO DE CRISIS	
INCIDENTE	**DESCRIPCIÓN DE AFECTACIÓN**
Relacionado con el personal	• Accidente grave de personal que ocasione afectaciones en la operación en una o más áreas de CAPUFE. • Daños a la salud que genere gravedad en gran parte del Personal Crítico de CAPUFE. • Indisponibilidad de hasta un 80% del personal de CAPUFE debido a enfermedades, pandemia o situaciones extraordinarias. • Emergencia sanitaria con afectación local. • Cualquier incidente relacionado con Personal Crítico de los procesos críticos y altos establecidos en el BIA (considerando los RTOs de cada proceso).
Relacionado con las Instalaciones	• Incendio controlado con daños o pérdidas parciales en las instalaciones. • Daño o interrupción de la instalación eléctrica. • Problemas graves de alcantarillado en la zona. • Inundaciones graves. • Fallas prolongadas en el suministro de servicios básicos (agua y electricidad). • Amenaza natural con daños, pero sin afectación estructural de las instalaciones. • Cualquier incidente que afecte las instalaciones donde se operen alguno de los procesos críticos o altos establecidos en el BIA (considerando los RTOs de cada proceso).
Relacionado con Incidentes Tecnológicos	• Reporte de 2 o más áreas de negocio sobre fallas de una o varias aplicaciones críticas. • Ataques de negación de servicios no recuperable. • Incidente de seguridad de la información que cause interrupción a los servicios. • Infección de virus diseminada por la red sin antivirus disponible. • Caída prolongada de la red de área local. • Cualquier incidente que afecte la infraestructura tecnológica que soporte alguno de los procesos críticos o altos establecidos en el BIA (considerando los RTOs de cada proceso).
Tiempo de solución	• Si el Grupo de Primera Respuesta determina que la solución del incidente le va a tomar entre 1 y 2 horas. • Si el Grupo de Primera Respuesta identifica que el incidente afecta directamente la operación de algún proceso critico o alto y la solución de este le va a tomar más del tiempo RTO establecido para dicho proceso.
Horario	• Si el Incidente ocurre dentro del horario laboral y el tiempo de solución cumple con las características mencionadas en el cuadro anterior.

Nivel de alerta 3. No se recomienda la activación del BCP

NO SE RECOMIENDA LA ACTIVACIÓN DEL BCP, SIN EMBARGO, SE PONE A DISPOSICIÓN DEL GRUPO DE MANEJO DE CRISIS	
INCIDENTE	**DESCRIPCIÓN DE AFECTACIÓN**
Relacionado con el personal	• Incidentes del personal de CAPUFE que cause una interrupción en el lugar de trabajo y que no afecte Personal Crítico. • Problemas de salud que provoque inasistencias del personal no crítico. • Llamadas de extorsión o amenazas vía telefónica. • Indisponibilidad de hasta un 50% del personal de CAPUFE debido a enfermedades, pandemia o situaciones extraordinarias. • Cualquier incidente relacionado con personal de los procesos críticos y altos establecidos en el BIA (considerando los RTOs de cada proceso).
Relacionado con las Instalaciones	• Incendio con daños menores y limitados. • Corte de energía en instalaciones sin afectación de voz y datos. • Falla prolongada en suministros de agua, alcantarillado. • Clausura temporal del acceso a las instalaciones por granizo, inundación o tormentas sin que afecte los procesos críticos y altos. • Interrupción prolongada en las vías de acceso a las instalaciones de CAPUFE (considerando los RTOs de cada proceso). • Cualquier incidente que afecte las instalaciones que no afecte la operación de los procesos críticos o altos establecidos en el BIA (considerando los RTOs de cada proceso).
Relacionado con Incidentes Tecnológicos	• Reporte de problemas prolongados en el acceso a la red sin afectación a procesos críticos y altos. • Reporte de problemas en el acceso a una aplicación sin afectación a procesos críticos y altos. • Reporte de problemas relacionados con infección de virus sin afectación a Personal Crítico. • Incidente de seguridad de la información que no cause una interrupción a los procesos críticos y altos. • Sobrecarga de capacidad de infraestructura o telecomunicaciones. • Incidentes operativos que pudieran afectar la integridad de la información crítica de CAPUFE. • Cualquier incidente que afecte la infraestructura tecnológica que o soporte alguno de los procesos críticos o altos establecidos en el BIA. *Nota: Estos casos se atenderían mediante proceso de atención de incidentes.*
Tiempo de solución	• Si el Grupo de Primera Respuesta identifica que el incidente no afecta directamente la operación de algún proceso crítico o alto y determina que la solución del incidente le va a tomar menos de 1 hora.
Horario	• Si el Incidente ocurre fuera del horario laboral y el tiempo de solución cumple con las características mencionadas en el cuadro anterior.

Nivel de alerta 4. Sin recomendación de activación BCP

NO SE RECOMIENDA LA ACTIVACIÓN DEL BCP	
INCIDENTE	**DESCRIPCIÓN DE AFECTACIÓN**
Relacionado con el personal	• Accidentes del personal de CAPUFE con lesiones menores. • Robo o pérdida de bienes no relacionados con la operación. • Incidentes menores del personal de CAPUFE que origine una distracción en el lugar de trabajo (discusiones, riñas).

NO SE RECOMIENDA LA ACTIVACIÓN DEL BCP	
INCIDENTE	**DESCRIPCIÓN DE AFECTACIÓN**
	• Indisponibilidad del 30% del personal debido a enfermedades, pandemia o situaciones extraordinarias, sin afectación a Personal Crítico. • Cualquier incidente relacionado con personal que no sea crítico para los procesos críticos y altos establecidos en el BIA.
Relacionado con las Instalaciones	• Cierre temporal de vías de acceso aledañas a las instalaciones o tráfico intenso. • Cierre temporal de accesos a las instalaciones por granizo, lluvia o tormentas sin afectación a procesos críticos y altos. • Falsas alarmas de incendio, humo, o conato de fuego. • Corte de energía sin problemas en el funcionamiento de equipos o fuera del horario de labores. • Falla temporal en suministros de agua. • Manifestaciones, marchas o mítines de personas ajenas a CAPUFE que no afecten el acceso al edificio corporativo. • Cualquier incidente que no afecte las instalaciones donde se operen alguno de los procesos críticos o altos establecidos en el BIA.
Relacionado con Incidentes Tecnológicos	• Reporte de problemas intermitentes en el acceso a una aplicación. • Reporte de pérdida de datos en aplicaciones o archivos almacenados en la red sin afectación a procesos críticos y altos. • Incidente de seguridad de la información que se pueda controlar mediante el procedimiento interno de gestión de incidentes. • Cualquier incidente que afecte la infraestructura tecnológica que no soporte alguno de los procesos críticos o altos establecidos en el BIA.
Tiempo de solución	• Si el Grupo de Primera Respuesta identifica que el incidente no afecta directamente la operación de algún proceso crítico o alto y determina que la solución del incidente le va a tomar menos de 1 hora.
Horario	• Si el Incidente ocurre fuera del horario laboral y el tiempo de solución cumple con las características mencionadas en el cuadro anterior.

Narrativa del procedimiento de primera respuesta
La siguiente tabla muestra la narrativa general del Procedimiento de Primera Respuesta:

PROCESO DE PRIMERA RESPUESTA Y ACTIVACIÓN BCP			
ID	**ACTIVIDAD**	**RESPONSABLE**	**DESCRIPCIÓN**
1	Identifica y notifica Incidente al área correspondiente.	Personal de CAPUFE.	Cualquier persona o colaborador de CAPUFE o el Grupo de Primera Respuesta notifican un evento de emergencia en el momento de que se percaten del incidente. **Nota:** Dependiendo de la naturaleza y características del incidente, es decir, si afecta a instalaciones, personas, tecnología o seguridad de la información, debe ser notificado al área correspondiente: **Primera respuesta personas e instalaciones:** Integrado por Protección civil y Seguridad física. **Primera respuesta tecnológica:** Integrado por personas del área de TI y Seguridad de la Información.

PROCESO DE PRIMERA RESPUESTA Y ACTIVACIÓN BCP			
ID	**ACTIVIDAD**	**RESPONSABLE**	**DESCRIPCIÓN**
2	Recibe notificación y activa el protocolo correspondiente.	Grupo de Primera Respuesta (Protección Civil, Seguridad Física Y Seguridad de la Información).	El Grupo de Primera Respuesta del Área correspondiente recibe la notificación y atiende el incidente de acuerdo con los protocolos existentes para cada tipo de incidente. **Documentación asociada:** Listado de Protocolos de Seguridad Físicas y/o Protección Civil y Seguridad de la Información.
3	Atiende el incidente de acuerdo con el protocolo.	Grupo de Primera Respuesta (Protección Civil, Seguridad Física Y Seguridad de la Información).	El Grupo que reciba la notificación debe atender y contener el incidente de acuerdo con los protocolos propios de cada área.
4	Evalúa la gravedad del incidente.	Grupo de Primera Respuesta (Protección Civil, Seguridad Física Y Seguridad de la Información).	Una vez analizado y contenido el incidente, el Grupo correspondiente debe evaluar la situación con base en la Matriz de Alertamiento, para determinar si recomienda o no la activación del BCP. **¿Se trata de un incidente Nivel 1 y 2?** **Si:** Continúa en actividad 5. **No:** Continúa en actividad 8. **Documentación asociada**: Matriz de Alertamiento.
5	Informa al Grupo de Manejo de crisis.	Grupo de Primera Respuesta (Protección Civil, Seguridad Física Y Seguridad de la Información).	El Grupo de Primera Respuesta que está atendiendo el incidente, informa al Grupo de Manejo de Crisis de al área correspondiente, sobre la gravedad del evento para que se evalué la activación o no del BCP.
6	Evalúa reporte de impacto del evento.	Grupo de Manejo de Crisis	El Grupo de Manejo de Crisis del Área correspondiente, evalúa la situación y verifica si cuenta con recursos para atender el evento sin necesidad de activar BCP. **¿Cuenta con los recursos para contener el incidente sin activar el BCP?** **Si:** Continúa en actividad 7. **No:** Continúa en actividad 10.
7	Asigna recursos necesarios y coordina para contener evento.	Grupo de Manejo de Crisis	El Grupo de Manejo de Crisis del Área correspondiente, gestiona, asigna los recursos necesarios y coordina al Grupo de Primera Respuesta para contener el evento sin necesidad de activar el BCP.
8	Ejecuta actividades para contener incidente.	Grupo de Primera Respuesta (Protección Civil, Seguridad Física Y Seguridad de la Información).	El Grupo de Primera Respuesta ejecuta las actividades necesarias para contener el incidente. El evento es atendido como un incidente normal. **¿El incidente está resuelto?** **Si:** Continúa en actividad 9. **No:** Continúa en actividad 4.

PROCESO DE PRIMERA RESPUESTA Y ACTIVACIÓN BCP			
ID	**ACTIVIDAD**	**RESPONSABLE**	**DESCRIPCIÓN**
9	Comunica al Grupo de Manejo de Crisis.	Grupo de Primera Respuesta (Protección Civil, Seguridad Física Y Seguridad de la Información).	El Grupo de Primera Respuesta comunica al Grupo de Manejo de Crisis que el incidente ha sido resuelto. **Fin (Evento tratado como Incidente).**
10	Notifica al Coordinador BCP recomendación de activación del BCP.	Grupo de Manejo de Crisis.	El Grupo de Manejo de Crisis notifica al Coordinador BCP la gravedad del evento y recomienda activar el BCP.
11	Informa a Grupo de Dirección y notifica recomendación de activación del BCP.	Coordinador BCP.	El Coordinador BCP informa al Grupo de Dirección del área afectada la situación del evento para que evalúen la situación y decidan si se activa o no el BCP.
12	Recibe recomendación y evalúa la situación.	Grupo Directivo.	El Grupo de Dirección del área afectada recibe la notificación, evalúa la situación y decide si se activa o no el BCP, de acuerdo con las políticas de activación del BCP. **¿Se activa el BCP?** **Si:** Continúa en actividad 14. **No:** Continúa en actividad 13.
13	Notifica a Grupo de manejo de crisis para que gestione incidente sin activación BCP.	Grupo Directivo.	Notifica al Grupo de Manejo de Crisis del Área correspondiente y al Coordinador BCP, que no se declara la activación del BCP, para que el evento sea gestionado como un incidente normal y gestiona y asigna recursos necesarios. **Regresa a la actividad 8**.
14	Declara contingencia y notifica al Grupo de Manejo de Crisis y al Coordinador BCP.	Grupo Directivo.	El Grupo Directivo correspondiente declara la activación de la contingencia notificando al Grupo de Manejo de Crisis del área correspondiente y al Coordinador BCP.
15	Recibe comunicado de activación del BCP.	Grupo de Manejo de Crisis.	El Grupo de Manejo de Crisis recibe la notificación de activación del BCP.
16	Comunica a los Grupos de trabajo de acuerdo con el árbol de llamadas de manejo de crisis.	Grupo de Manejo de Crisis.	El Grupo de Manejo de Crisis comunica al área correspondiente la activación del BCP de acuerdo con el Árbol de llamadas de manejo de crisis. **Artefactos:** Árbol de llamadas de manejo de crisis. **Fin del proceso de primera respuesta y activación del BCP.**