Protocolo de Manejo de Incidentes e Identificación de Crisis

Proceso: Planeación, Estrategia y Control
Subproceso: Administración del Sistema de Gestión
Versión 03
Código OD-PEC-0003
Año 2025

El contenido de este documento corresponde a Información Pública

Contenido

INTRODUCCIÓN 3
1. Objetivos 3
2. Alcance 3
3. ESCENARIOS DE CONTINUIDAD DEL NEGOCIO 4
3.1. Emergencia Social 4
3.2. Desastre Tecnológico 4
3.3. Fuga de Información: 4
3.4. Desastre Natural y Colapso de la Infraestructura 4
3.5. Incapacidad de la Operación de los Procesos 4
4. ACTIVIDADES PARA LA ATENCIÓN DEL INCIDENTE 5
4.1. Reportar el Incidente 6
4.2. Confirmar y detallar el incidente 7
4.3. Activar la Mesa de Incidentes o quien haga sus veces 7
4.3.1 Activación 7
4.3.2 Intengrantes de la Mesa de Incidentes 8
4.3.3 Tareas de los integrantes de la Mesa de Incidentes 8
4.4. Valorar el incidente 9
4.4.1 Criterios para evaluar el incidente 9
4.4.2 Criterios para escalar el incidente a PMU: 10
4.5. Diseñar el Plan de Acción 11
4.6. Implementar el Plan de Acción 12
4.7. Realizar monitoreo y seguimiento 12
4.8. Preparar los requisitos para escalar a PMU 12
4.9. Decretar el cierre del incidente 13
5. Definiciones y siglas 14
6. Control de Cambios 15

INTRODUCCIÓN

La entidad está expuesta a eventos disruptivos o incidentes que pueden o podrían conducir a una interrupción, pérdida, emergencia o crisis, que afecten la continuidad de la operación. Para ello, es necesario contar con un protocolo que dé los lineamientos para actuar de manera ordenada, eficiente y oportuna frente a estos eventos, de forma tal que permita restablecer en el menor tiempo la prestación de los servicios y mitigar el impacto negativo de la pérdida de recursos.

Este protocolo va dirigido a los servidores públicos, especialmente a quienes ocupan cargos directivos, y tiene como propósito la atención de eventos que comprometan la continuidad del negocio, estableciendo lineamientos prácticos para responder ante la no disponibilidad de la operación normal, criterios para valorar la magnitud del incidente y, en caso de ser necesario, su escalamiento a una situación de crisis, en cuyo caso se aplicaría el Protocolo de Manejo de Crisis OD-PEC-0004.

1. Objetivos

Contención y mitigación oportuna: Diseñar, implementar y coordinar acciones inmediatas para contener y mitigar los incidentes dentro del ámbito de competencia de las áreas involucradas, minimizando su impacto en la operación y el cumplimiento de los objetivos institucionales.

Coordinación de recursos: Movilizar de manera eficiente los recursos internos, contratistas y terceros para ejecutar acciones de respuesta y recuperación ante incidentes.

Reducción del tiempo de interrupción: Disminuir el tiempo de afectación de los procesos críticos, garantizando la continuidad de las funciones esenciales de la Entidad.

Protección de las personas: Salvaguardar la integridad de los servidores públicos, contratistas y visitantes dentro de las instalaciones de la Entidad.

Fortalecimiento de capacidades: Mejorar continuamente las capacidades institucionales para gestionar incidentes de forma eficaz, reduciendo o eliminando sus efectos adversos sobre la operación y la reputación de la Entidad.

Comunicación efectiva: Informar de manera oportuna y transparente sobre los incidentes a las partes interesadas internas y externas, conforme al protocolo OD-PEC-0002, fortaleciendo la confianza en la capacidad institucional de respuesta.

Escalamiento a crisis: Establecer criterios claros para escalar un incidente a nivel de crisis, activando el PMU o la instancia correspondiente, para su atención de acuerdo con el protocolo de manejo de crisis OD-PEC-0004.

2. Alcance

Este protocolo comprende desde la identificación y confirmación de un incidente, pasando por la convocatoria de la Mesa de Incidentes, la valoración del evento, la implementación del plan de acción, su monitoreo y seguimiento, hasta el cierre del incidente y el balance post-incidente (si no escaló a crisis). En caso de que se cumplan los criterios establecidos, el incidente podrá ser escalado al PMU o a la instancia que haga sus veces.

Aplica para la gestión de incidentes o eventos disruptivos que puedan afectar negativamente a los activos de información, procesos críticos, personal interno o externo, servicios tecnológicos o la

reputación de la UAE DIAN y que esten relacionados con algún escenario de continuidad del negocio.

3. ESCENARIOS DE CONTINUIDAD DEL NEGOCIO

3.1. Emergencia Social

- **Amenazas:** Situaciones de violencia o inseguridad que pueden poner en riesgo la seguridad de los empleados y las operaciones de la Entidad.
- **Paros:** Huelgas o manifestaciones que interrumpen el acceso a las instalaciones o el funcionamiento normal de la entidad.
- **Pandemias:** Brotes de enfermedades contagiosas que afectan la salud de los empleados y la capacidad operativa de la entidad.

3.2. Desastre Tecnológico

- **Infraestructura:** Fallos en la infraestructura tecnológica, como cortes de energía o daños en los servidores, que interrumpen las operaciones.
- **Software:** Incidentes tecnológicos relacionados con las soluciones y servicios críticos que atenten contra la esencia misional de la entidad como errores o fallos en las actualizaciones y cambios, ausencia de desarrollo seguro que afectan la funcionalidad de los sistemas críticos.
- **Ciberataque:** Ataques maliciosos que comprometen las soluciones y servicios tecnológicos de la entidad.

3.3. Fuga de Información

- **Perdida de confidencialidad:** Pérdida o robo de datos sensibles que pueden dañar la reputación y la confianza de los ciudadanos o contribuyentes**.**
- **Ciberataque:** Ataques maliciosos que comprometen la seguridad de los datos e información de la entidad.

3.4. Desastre Natural y Colapso de la Infraestructura

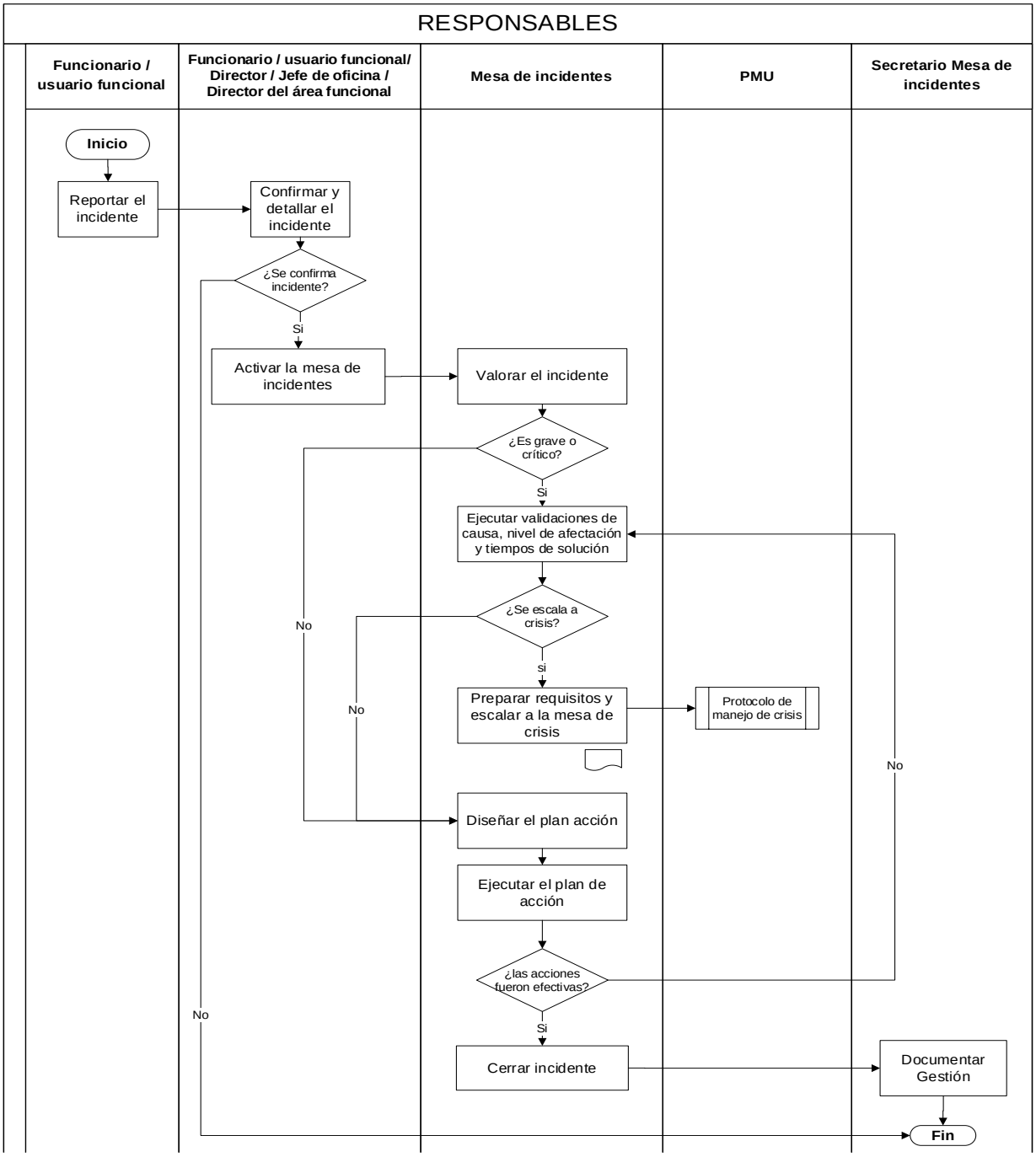
- **Desastres Naturales:** Eventos como terremotos, inundaciones, vendavales, huracanes o incendios que pueden causar daños significativos a las instalaciones físicas de la entidad.
- **Colapso de la Infraestructura:** Fallos estructurales en los edificios o instalaciones que pueden interrumpir las operaciones y poner en riesgo la seguridad de los funcionarios.

3.5. Incapacidad de la Operación de los Procesos

- **Interrupción No Planificada:** Fallos en los procesos operativos que reducen la calidad y eficiencia, limitando la capacidad de entregar productos y servicios a los clientes internos, ciudadanos o contribuyentes.
- **Impacto en la Calidad:** Problemas que afectan la consistencia y calidad de los productos o servicios, lo que puede llevar a la insatisfacción del ciudadano o contribuyente.

Afectación de Imagen reputacional: La materialización de un incidente/ evento disruptivo, en cualquiera de los escenarios mencionados, puede generar un impacto negativo en la imagen y reputación institucional.

4. ACTIVIDADES PARA LA ATENCIÓN DEL INCIDENTE



Grafica. Actividades para la atención del incidente

4.1. Reportar el Incidente

Para que se considere un incidente, se debe presentar de manera clara y concreta situaciones que puedan eventualmente afectar negativamente el cumplimiento de los objetivos o la imagen reputacional de la Entidad, o que podría conducir a una interrupción, degradación, pérdida, emergencia o crisis. Para ello se debe reportar según la ubicación del incidente:

- En el nivel local, al Director Seccional respectivo,
- En el nivel central, dependiendo al escenario que este asociado el incidente, así:

Asociado al Escenario	Evidencia / Identificación	Reportar a	Acción Inicial (posterior al reporte)
Emergencias sociales	Alertas sobre alteraciones del orden público en la zona de la sede DIAN, información en redes sociales o medios de comunicación.	Director de Gestión Corporativa	Confirmar la información con fuentes oficiales como alcaldías, gobernaciones o la Policía Nacional.
Desastre natural o Colapso de la Infraestructura	Observación directa o reporte de testigos sobre eventos como sismos, inundaciones, incendios, entre otros.	Director de Gestión Corporativa	Verificar el alcance y nivel de riesgo conforme a los procedimientos establecidos en las dependencias.
Desastre tecnológico	Alertas generadas por parte de un área de la Dirección de Gestión de Innovación y de Tecnología PQRS relacionadas con el incidente tecnológico. Correos dirigidos a los Directivos de la DIAN Alertas generadas a través de los diferentes canales institucionales como callcenter, chatbot, atención presencial en puntos contanto, entre otros, los cuales se direccionan	Al usuario funcional o Coordinación de Servicios y Administración Técnica.	Confirmar el alcance, Tipificación del incidente, si es masivo, determinar si afecta el objeto misional de la entidad y verificar si existe una obligación legal relacionada con la prestación de los servicios TAC. (calendario tributario, términos de actuaciones administrativas)
Fuga de información	Alertas provenientes de usuarios de los servicios tecnológicos, áreas de la Dirección de Gestión de Innovación y de Tecnología, Oficina de Seguridad de la Información, o Enlace de seguridad de la información	Jefe de la Oficina de Seguridad de la Información.	Confirmar el alcance de la situación y su nivel de riesgo, según los procedimientos formalizados en las dependencias.
Incapacidad de la operación de los procesos	Alerta o Interrupción generada durante la operación normal de los procesos y reportada por servidores públicos o partes interesadas	Al responsable de los procesos afectados según sea, Jefe de Oficina, Director de Gestión respectivo o Director Operativo	Confirmar el alcance de la situación y su nivel de riesgo, según los procedimientos formalizados en las dependencias
Afectación imagen reputacional	Publicaciones en redes sociales o medios de comunicación de tipo político-reputacional	Jefe de la Oficina de Comunicaciones Institucionales	Analizar el monitero de redes sociales y medios de comunicación

En todo caso para incidentes tecnológicos, se debe reportar de acuerdo con el procedimiento PR-IIT-0458 Gestión de Incidentes.

4.2. Confirmar y detallar el incidente

Responsable: Si es incidente tecnológico el responsable de confirmar y detallarlo será al usuario funcional y la Coordinación de Servicios y Administración Técnica, de acuerdo con lo estipulado en el procedimiento PR-IIT-0458 Gestión de Incidentes. Si es otro tipo de incidente será el Director Seccional, Director de Gestión, Jefe de Oficina, Director Operativo.

Confirmar el incidente Verificar ubicación, actores involucrados, impacto actual y potencial, causas preliminares y servicios afectados, posibles alternativas de contención del incidente.

Nota: La confirmación del incidente se realizará con base en la experiencia y juicio técnico del área funcional y del área técnica hasta tanto se definan criterios según el nivel de afectación a productos, servicios y trámites institucionales, personas, infraestructura y demás factores que puedan ser descritos.

Criterios para activar la mesa de incidentes

- **Si el incidente afecta la continuidad de las operaciones críticas de la Entidad, definidas en el BIA:**
    - Si el incidente afecta negativamente la continuidad de las operaciones de la Entidad se activa la Mesa de Incidentes o la instancia que haga sus veces.
    - En caso contrario, el Director Seccional, Director de Gestión, Jefe de Oficina o Director Operativo, gestiona el tratamiento que requiera la situación presentada y da por finalizado el incidente.

- Si el incidente implica una de crisis reputacional institucional de nivel grave o crítico de acuerdo con el protocolo OD-PEC-002.

4.3. Activar la Mesa de Incidentes o quien haga sus veces

4.3.1 Activación

El Director Seccional, Director de Gestión, Jefe de Oficina, Director Operativo, convoca por el medio oportuno o disponible (teams, personal, llamada, whatsapp, etc), la Mesa de Incidentes o la instancia que haga sus veces para gestionar la atención del incidente identificado.

Los integrantes de la Mesa de Incidentes o la instancia que haga sus veces deberán:

- Dar prioridad a este asunto frente a cualquier otra situación,
- Permanecer en contacto permanente con el fin de brindar el reporte de estado de las acciones ejecutadas para la gestión de los incidentes.

4.3.2 Integrantes de la Mesa de Incidentes

Líder del incidente	Director Seccional, Director de Gestión, Jefe de Oficina o Director Operativo, según sea la localización del incidente
Integrantes	Los integrantes serán definidos según lo requerido para la atención del incidente: En el nivel seccional: • Jefe de División Administrativa y Financiera o quien haga sus veces, el responsable del activo afectado y los demás que el Director Seccional determine. En el nivel central: • Subdirectores de la Dirección de Gestión o de la Dirección Operativa afectada que estén relacionados directamente con el incidente, el responsable del activo afectado y los demás servidores públicos que el Líder de Incidentes determine.
Invitados	El Líder del Incidente puede invitar a directivos y/o asesores de comunicaciones, servidores públicos de otras dependencias de acuerdo con la naturaleza del incidente.
Secretario	Designado por el líder del incidente.

Para incidentes tecnológicos

Líder del incidente	Director de Gestión del área de Negocio afectada
Integrantes	Los integrantes serán definidos según lo requerido para la atención del incidente: Director de Gestión de Innovación y Tecnológia-DGIT Director de Gestión de Impuestos o Director de Gestión de aduanas, Jefe de la Oficina de Seguridad de la Información y/o delegados Subdirectores de la DGIT de acuerdo con la naturaleza del incidente. Oficina de Comunicaciones Institucionales
Invitados	Los demás servidores públicos que el Líder de Incidentes determine de acuerdo con la naturaleza del incidente Director de Gestión de Estrategia y Análitica – Como garante de los protocolos
Secretario	Designado por el líder del incidente.

4.3.3 Tareas de los integrantes de la Mesa de Incidentes

Líder del Incidente

a. Convoca la Mesa de Incidentes o a la instancia que haga sus veces.
b. Coordina la implementación del Plan de Acción.
c. Valida el seguimiento al cumplimiento del Plan de Acción y del monitoreo del incidente.
d. Comunica la información sobre el incidente, el Plan de Acción y su ejecución al interior de la

entidad.

e. Tanto en el nivel central como en el nivel local, podrá ser el vocero ante medios de comunicación de acuerdo con los lineamientos del protocolo OD-PEC-002 numeral 4.3.1.
f. Cierra el incidente cuando la alerta haya bajado.
g. Escala el incidente al PMU o a la instancia que haga sus veces, cuando se cumplan los requisitos de escalamiento.
h. Liderar el balance post-incidente (si no escaló a crisis).

Integrantes

a. Aportar su conocimiento y experiencia en la gestión oportuna del incidente, con propuestas para el Plan de Acción, y mejoras que se puedan implementar.
b. Desarrollar, directamente o a través de las dependencias a su cargo, el Plan de Acción definido para la gestión del incidente, conforme a sus competencias.
c. De acuerdo con sus competencias funcionales, restablecer la prestación de servicios a condiciones normales una vez superada la situación del incidente.
d. Identificar y proponer acciones de mejora que permitan afrontar futuros incidentes.
e. Evaluar la información generada durante el incidente, para establecer si está sujeta a las excepciones de acceso a la información establecidas en las disposiciones legales, tales como la Ley 1712 de 2014 y el Artículo 130 de Ley 2010 de 2019, entre otras. En caso de corresponder a alguna de las excepciones se debe mantener las reservas de acceso a la información de forma permanente.
f. Realizar el el balance post-incidente (si no escaló a crisis)

NOTA: Los invitados participan de la Mesa de Incidentes con voz, pero sin voto.

Secretario

a. Documentar las decisiones de la Mesa de Incidentes o la instancia que haga sus veces, de la forma que considere más adecuada.
b. Recopilar la información de los análisis del incidente presentado en la Mesa de Incidentes o en la instancia que haga sus veces.
c. Consolidar el seguimiento a la ejecución de las tareas del Plan de Acción.
d. Preparar la información que se debe adjuntar cuando se escale el incidente al PMU o quien haga sus veces, documentándolo en el formato FT-PEC-2843 Reporte de incidentes
e. Ejercer como Secretario en el PMU, si así lo decide la mencionada mesa.
f. Consolidar el balance post-incidente (si no escaló a crisis).

4.4. Valorar el incidente

La Mesa de Incidentes debe valorarlo, en un plazo máximo de 2 horas desde el momento en que se recibe el incidente, tiempo en el cual deben evaluarse los siguientes criterios y determinar si se escala a crisis.

4.4.1 Criterios para evaluar el incidente

El incidente presentado se debe evaluar según los criterios de evaluación presentados en la siguiente tabla:

Impacto	Criterio de evaluación			
	Afectación servidores públicos	**Afectación reputacional**	**Afectación legal**	**Afectación en el servicio**
Ninguno	No hay impacto	No hay impacto	No hay impacto	No hay impacto
Leve	Afectación en la disponibilidad de los servidores públicos: • Menor o igual al 1 % del total nacional, o • Menor o igual al 5 % del total local.	Incidente latente: Se detecta internamente una situación anómala que podría comprometer la imagen de la DIAN. La falla aún no es de dominio público.	Incumplimiento de reglamentos internos	Disminución menor o igual al 1 % de declaraciones presentadas con relación al año anterior y, 20 casos o menos registrados en 1 hora.
Moderado	Afectación en la disponibilidad de los servidores públicos: • Mayor que el 1 % y menor o igual al 3 % del total nacional, o • Mayor que el 5 % y menor o igual al 10 % del total local.	Filtración inicial: Circulan rumores o comentarios en redes, medios de comunicación o entre actores clave (sindicatos, gremios, terceros). La información no ha sido validada, pero empieza a generar inquietud.	Sanciones disciplinarias internas / incumplimientos legales	Disminución mayor que el 1 % y menor o igual al 2 % de declaraciones presentadas con relación al año anterior y, entre 21- 40 casos registrados en 1 hora.
Grave	Afectación en la disponibilidad de los servidores públicos: • Mayor que el 3 % y menor o igual al 5 % del total nacional, o • Mayor que el 10 % y menor o igual al 20 % del total local.	Reacción pública inicial: El incidente comienza a tener efectos visibles: indignación ciudadana, impacto en usuarios, cobertura inicial en medios con carácter informativo y no de opinión; el tema se instala en la conversación pública.	Sanciones externas/ multas /Demandas para la entidad	Disminución mayor que el 2 % y menor o igual al 5 % de declaraciones presentadas con relación al año anterior y, entre 41- 60 casos registrados en 1 hora.
Crítico	Afectación en la disponibilidad de los servidores públicos: • Mayor que el 5 % del total nacional, o • Mayor que el 20 % total local.	Opinión desbordada y testimonios sensibles: Se multiplican las versiones, juicios y especulaciones. Surgen expertos, influenciadores y figuras públicas opinando sin base clara, además, los medios de comunicación empiezan a visibilizar los testimonios de personas presuntamente afectadas por el incidente, generando empatía y amplificando la indignación, se posiciona un rostro humano del impacto. El relato se sale de control.	Además de lo anterior, Reportes a entes de Control/ Investigaciones penales	Disminución mayor que el 5% de declaraciones presentadas con relación al año anterior y, más de 60 casos registrados en 1 hora.

Nota: Los criterios de Afectación del Servicio relacionados en la tabla anterior corresponden a la presentación de la declaración de renta personas naturales; para otros incidentes en los que haya afectación del servicio, la valoración se realizará con base en la experiencia y juicio técnico del área funcional y del área técnica, entre tanto se actualicen los criterios para estos incidentes.

Si el resultado de la evaluación de alguno de los criterios fue crítico, se evalua lo dispuesto en el numeral 4.4.2. De lo contrario si fue leve, moderado o grave el inicidente no se escala a crisis y se debe diseñar Plan de Acción de cuerdo con el numeral 4.5.

4.4.2 Criterios para escalar el incidente al PMU:

El incidente debe escalarse al PMU o a la instancia correspondiente cuando ocurra alguna de las

siguientes situaciones:

i. Si, tras la evaluación del incidente, algún criterio se clasifica como crítico y la respuesta a alguna de las siguientes preguntas es "No":

- ¿Puede continuar prestándose el servicio de manera alterna, o si la afectación es reputacional o legal, el incidente puede resolverse dentro de los RTO definidos en el BIA?
- ¿Se puede solucionar el incidente sin la gestión del PMU?

Si la respuesta es "Sí", continúa con el numeral 4.5.

ii. Si la implementación del plan de acción no ha dado como resultado la mitigación del incidente o es posible el incremento de las consecuencias negativas.

4.5. Diseñar el Plan de Acción

El Plan de Acción se define según la naturaleza del incidente, la competencia y autonomía de la dependencia afectada, con el objetivo de disminuir su impacto en las personas, la operación de la Entidad, la información, la tecnología y la reputación institucional.

El plan incluye las tareas a realizar, sus responsables, tiempos de ejecución y recursos requeridos, así:

- Las tareas que se ejecutarán para mantener la operación de los procesos institucionales en el periodo de afectación del incidente,
- La posible activación de planes como:
  - Planes de emergencia relacionados con el sistema de seguridad y salud en el trabajo,
  - Planes de manejo ambiental relacionados con el sistema de gestión ambiental,
  - Plan de continuidad o de recuperación tecnológica determinados por la Dirección de Gestión de Innovación y Tecnología,
  - Políticas de comunicaciones definidas por la Oficina de Comunicaciones Institucionales y en el protocolo de Gestión de Comunicaciones en momento de crisis, documento OD-PEC-0002.
  - Los demás planes de acción que considere la Mesa de Incidentes o quien haga sus veces.
- Establecer medidas de protección al usuario, de acuerdo con el procedimiento PR-IIT-0454.
- Las tareas de gobernabilidad de los integrantes de la Mesa de Incidentes o quien haga sus veces para resolver las consecuencias del incidente sobre la Entidad.

Cuando se requieran tareas cuyo responsable sea otra dependencia que no forme parte de la Mesa de Incidentes o quien haga sus veces, el Líder de Incidentes deberá realizar las gestiones pertinentes para comunicar dicha responsabilidad a esa dependencia y para que la misma ejecute las tareas.

En el Plan de Acción se deben establecer los recursos necesarios para su implementación, pudiendo incluir los siguientes, sin perjuicio de los demás que considere la Mesa de Incidentes o quien haga sus veces:

- Talento Humano,
- Información como datos, expedientes, archivos, etc.
- Instalaciones físicas,
- Elementos de trabajo como equipos de cómputo, consumibles, formatos,
- Servicios informáticos,

- Recursos financieros,
- Proveedores y contratistas.

Para la recuperación de la operación normal de la Entidad se pueden considerar diferentes alternativas de acuerdo con el impacto del incidente. Entre ellas se destacan, sin limitarse a:

- Recuperación utilizando las mismas instalaciones de la entidad con recursos propios, es decir otras dependencias, otras sedes.
- Recuperación utilizando el trabajo en casa para los servidores públicos afectados.
- Recuperación de la actividad en las instalaciones o con los recursos de un proveedor independiente, como por ejemplo centros de cómputo alternos o infraestructura de nube.
- Combinando diferentes alternativas.

El Plan de Acción se debe consolidar por parte del Secretario de la Mesa de Incidentes o quien haga sus veces; según se presenten los hechos, se puede documentar posteriormente al cierre del incidente.

4.6. Implementar el Plan de Acción

La implementación del Plan de Acción estará a cargo de cada responsable definido en el mismo.

Las responsabilidades se establecen de forma expresa en el Plan de Acción y obedeciendo a la naturaleza de la dependencia, sus funciones y competencias, en el marco legal establecido.

4.7. Realizar monitoreo y seguimiento

Los integrantes de la Mesa de Incidentes deben monitorear permanente el avance de las tareas a su cargo dentro del plan de acción, con el propósito de:

- Asegurar el cumplimiento de las tareas definidas, de acuerdo con los tiempos establecidos en el Plan de Acción
- Evaluar la posibilidad de ajustar el plan,
- Solicitar que se escale la situación al PMU o a la instancia que haga sus veces.

Como resultado del monitoreo y seguimiento se debe determinar la efectividad de las acciones del plan así:

- Si se ha controlado el incidente, el Secretario debe informar al Líder del Incidente para su cierre, Continua con el numeral 4.9.
- Si no ha dado como resultado la mitigación de los incidentes o es posible el incremento de las consecuencias negativas, la Mesa de Incidentes debe evaluar:
    - sí ajusta el Plan de Acción o
    - sí se escala el incidente a PMU, numeral 4.8.

4.8. Preparar los requisitos para escalar a PMU

Para realizar el escalamiento del incidente es necesario presentar al PMU, como mínimo, los siguientes elementos, los cuales deben ser debidamente diligenciados y presentados por el secretario de la mesa

de incidentes en el formato FT-PEC-2843 Reporte de incidentes:

i. La identificación clara y concreta del incidente (ver numeral 4.2.).
ii. Breve recuento de las acciones realizadas en la Mesa de Incidentes que no fueron suficientes para mitigar el incidente o sus efectos negativos.
iii. La valoración del incidente, en los factores de afectación (ver numeral 4.4.).
iv. Plan de Acción estimado, en especial de lo que sea de gobernabilidad del Director General y/o directores de gestión (ver numeral 4.5).
v. Propuesta de integrantes del PMU.
vi. Propuesta de Secretario para el PMU, el cual puede ser el mismo de la Mesa de Incidentes.

Una vez esté diligenciado el formato con la información requerida, se debe remitir al Director General o su delegado por el medio digital o de comunicación disponible para que, en su calidad de gerente del PMU, active esta instancia según lo dispuesto en el protocolo OD-PEC-0004.

4.9. Decretar el cierre del incidente

Cuando el incidente ha sido controlado, el Líder de la Mesa de Incidentes (Director Seccional, Director de Gestión, Jefe de Oficina o Director Operativo) comunica por los medios digitales o de comunicación, a los integrantes de la mesa, a los servidores públicos involucrados y a las partes interesadas el cierre del incidente, de acuerdo con el protocolo OD-PEC-002.

4.10 Balance post-incidente

Una vez declarado el cierre del incidente,si no se escaló a crisis, la Mesa de Incidentes hará el seguimiento final,documentación y registros de esta.

Para tal fin se tendrá en cuenta lo siguiente:

a. Si no se realizó durante la gestión del incidente, documentar las acciones realizadas y el seguimiento de la misma.
b. Analizar los hechos ocurridos, las acciones realizadas y las lecciones aprendidas.
c. Identificar posibles acciones de mejora para la organización, disminuyendo la probabilidad de ocurrencia del incidente.
d. Identificar si requiere el creación o ajuste de mapas de riesgos, con la identificación o ajustes de nuevos riesgos o controles,
e. Idenficar si se requiere la creación o ajustes de procedimientos u otros documentos,
f. Retroalimentar a las dependencias involucradas en posibles acciones de mejora y/o lecciones aprendidas.
g. Hacer el análisis de las coberturas frente al evento, y hacer las reclamaciones a que haya lugar.
h. Identificar si se requiere actualizar o mejorar el presente protocolo.

La información será documentada por el Secretario de la Mesa de Incidentes en la sección correspondiente al balance post incidente del formato FT-PEC-2843 Reporte de incidentes.

5. Definiciones y siglas

Actividad priorizada: actividad a la que se le da urgencia con el fin de evitar impactos indeseables para el negocio durante una interrupción. Fuente NTC-ISO 22301 de 2019.

Amenazas: causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. Fuente ISO/IEC 27000 de 2013.

Crisis: materialización de un incidente, que sale de control y que afecta negativamente las personas en las sedes, la prestación del servicio, la información, la tecnología y la reputación de la Entidad. Fuente: Subdirección de Procesos.

Escalamiento: trasladar o subir la gestión de un incidente desde la Mesa de Incidentes (o quien haga sus veces) al PMU o la instancia que haga sus veces. Fuente: Subdirección de Procesos.

Interrupción: incidente bien sea esperado o no, que causa una alteración negativa y no planeada de la oferta esperada de los productos y servicios de acuerdo con los objetivos de la organización. Fuente NTC-ISO 22301 de 2019.

Incidente: evento que puede ser, o podría conducir a una interrupción, pérdida, emergencia o crisis. Fuente NTC-ISO 22301 de 2019.

Incidente crítico tecnológico: Incidente Masivo que afecte los sistemas de información catalogados como críticos en el BIA, con alta Tendencia en redes sociales o medios de comunicación,

Impacto: resultado de una interrupción que afecta los objetivos. Fuente NTC-ISO 22301 de 2019.

Mesa de Incidentes: Instancia de coordinación donde se analiza el incidente y se toman decisiones para su atención inmediata. Puede realizarse por medios digitales o presenciales (Teams, llamadas, WhatsApp, reuniones físicas, entre otros). Es liderada por el Director Seccional, Director de Gestión, , Jefe de Oficina o Director Operativo, según corresponda. Fuente: Subdirección de Procesos – Oficina de Seguridad de la Información.

Monitoreo: determina el estado de un sistema, un proceso o una actividad. Fuente NTC-ISO 22301 de 2019.

PMU Puesto de Mando Unificado o Instancia que haga sus veces: equipo de trabajo convocado por el Director General o su delegado para gestionar la atención de una crisis con un nivel de impacto crítico, o que requiere de la gobernabilidad de la Dirección General. Puede realizarse por medios digitales o presenciales (Teams, llamadas, WhatsApp, reuniones físicas, entre otros). Fuente: Subdirección de Procesos

Parte interesada: persona u organización que puede afectar, verse afectada o percibirse como afectada por una decisión o actividad. Fuente NTC-ISO 22301 de 2019.

Reputación: el buen nombre y prestigio de la DIAN producto de las percepciones agregadas de las partes interesadas sobre la satisfacción de las expectativas. Fuente: Subdirección de Procesos.

Plan de continuidad del negocio: información documentada que orienta a una organización para responder una interrupción y reanudar, recuperar y restaurar la oferta de productos y servicios de acuerdo con sus objetivos de continuidad de negocio. Fuente NTC-ISO 22301de 2019.

Protocolo: documento que establece una serie de acciones, instrucciones y reglas que se consideran adecuadas ante una situación específica. Fuente: Subdirección de Procesos.

Riesgo: efecto de la incertidumbre en los objetivos. Fuente NTC-ISO 22301de 2019.

Recursos: todos los activos (incluyendo planta y equipo), personas, habilidades, tecnología, instalaciones, provisiones, suministros e información (bien sea electrónica o no) que una organización posee y que tienen que tener disponibilidad para usarse cuando sea necesario, con el fin de operar y lograr su objetivo. Fuente NTC-ISO 22301 de 2019.

Terceros: consultores, pasantes, proveedores de bienes y servicios, contribuyentes, ciudadanos y otros terceros que desempeñen alguna actividad en las instalaciones de la entidad o a nombre de ésta. Fuente: DIAN – Oficina de Seguridad de la Información.

6. Control de Cambios

Versión	Vigencia		Descripción de los cambios	Tipo de información
	Desde	Hasta		
1	27/10/2021	27/02/2022	Versión 1 de la cartilla que reemplaza lo establecido en la versión inicial de documento denominado Protocolo de PreCrisis y Crisis aprobado por la Alta Dirección en 2019. Se generaron ajustes en el documento, relacionados con el nombre del proceso de acuerdo con la nueva estructura de procesos establecida en el considerando de la Resolución 060 del 11 de junio del 2020 y el código alfabético del mismo en el numeral 2 (página 1) y 4 (Páginas 1, 2 y 3). Cabe aclarar, que el contenido técnico del documento no presenta cambios respecto a la versión inicial. Por lo tanto, cualquier consulta respecto a los contenidos técnicos de los mismos debe efectuarse a los elaboradores técnicos y revisores de la versión anterior. Se ajustaron las dependencias de acuerdo con la nueva estructura establecida en el Decreto 1742 del 22 de diciembre de 2020.	

2	28/02/2022	12/08/2025	Versión 2 de Otros documentos. Aprobada el día 28 de febrero de 2022 en sesión del Comité Institucional Estratégico -CIE. El presente documento, en conjunto con el documento OD-PEC-0004 protocolo de manejo de crisis, reemplaza lo establecido en la Cartilla de Protocolo de Crisis versión 1.	Pública reservada
3	13/08/2025		Se actualizaron los escenarios de Continuidad del Negocio. Se revisan y ajustan las tablas para reportar incidente (sección 4.1) y para evaluar incidentes (sección 4.4.1) Se invoca el procedimiento PR-IIT-0458 Gestión de Incidentes y al procedimiento PR-IIT-0454 para establecer medidas de protección al usuario, como parte del plan de acción para la atención del incidente. Se describe una conformación de una mesa de incidentes específica para incidentes tecnológicos. Se ajusta “Mesa de crisis” por “Puesto de Mando Unificado PMU”. Se incluye el formato FT-PEC-2843 Reporte de incidentes, para documentar características importantes del incidente y su atención, para escalar al PMU si se convierte en crisis; también para documentar el balance post-incidente, si no se escala a crisis. El secretario de la mesa de incidentes debe preparar esta información. Le alinean criterios de comunicaciones con el protocolo OD-PEC-002. Se ajustan los criterios y requisitos para escalar al PMU.	Información Pública.

Elaboró:	Carlos Javier Ibañez Serna Edgar Fernando Aviles Gómez – Yeni Marcela Arcos Casas Sandra Janette Piedrahita Urueña **Elaboración técnica**	Gestor II Gestor III Gestor IV Gestor IV	Oficina Seguridad de la Información Subdirección de Innovación y Proyectos Oficina Seguridad de la Información
	Tito Alejandro Menjura Murcia Yeimy Liseth Becerra Pita César Augusto Garzón Baquero **Elaboración metodológica**	Gestor II Gestor II Gestor I	Coordinación de Procesos y Riesgos Operacionales
Revisó:	Francisco Andrés Daza Cardona Iván Mauricio Quintero Sosa	Jefe Oficina Seguridad de la Información Subdirector de Procesos	Oficina Seguridad de la Información Subdirección de Procesos
Aprobó:	Comité Institucional Estratégico - CIE.	Comité Institucional Estratégico -CIE.	Comité Institucional Estratégico -CIE.