

## Contenido

### 1. OBJETIVO

Describir la metodología empleada por ICETEX para la atención de los incidentes de continuidad y de contingencia del negocio, donde se establezcan las responsabilidades y actividades a desarrollar para gestionarlo en cada caso.

### 2. ALCANCE

Inicia con la identificación del incidente y va hasta el reporte de gestión del mismo.

En este procedimiento se describen las actividades necesarias para dar una respuesta efectiva a los incidentes que afecten la operación de los procedimientos críticos y la prestación de los servicios y productos.

### 3. DEFINICIONES

- **Colaborador:** Término utilizado para referenciar a un funcionario y contratista de la Entidad
- **Contingencia:** Posibilidad de que algo sucede o no sucede. Evento que no es deliberado y cuya probabilidad no es determinada.
- **Continuidad de negocio:** Capacidad de la organización para la entrega continua de productos o servicios a niveles aceptables predefinidos luego de un incidente disruptivo.
- **Incidente de trabajo:** Es un evento que no es parte de la operación estándar de un servicio y el cual puede causar interrupción o reducción en la calidad del servicio y en la productividad.
- **Plan de Continuidad de Negocio (PCN):** Procedimiento documentado que guía a la organización para responder, recuperar, reanudar y restaurar a un nivel predefinido de operación cuando ocurra una interrupción. Este documento lo conforman los planes de contingencia.
- **Proveedor:** Tercero contratado por ICETEX para la prestación de un servicio o adquisición de un bien.
- **Tiempo de recuperación objetivo (RTO- Recovery Time Objective):** Hace referencia al tiempo máximo, durante el cual debe ser recuperado el procedimiento y sus recursos, posterior a la ocurrencia de un incidente. <sup>[1]</sup>
- **Punto de recuperación objetivo (RPO- Recovery Point Objective):** Hace referencia al estado anterior al que debe ser restaurada la información usada por un proceso de negocio después de una interrupción, para lograr su reanudación. Cada organización deberá definir su "pérdida máxima de información".

### 4. CONDICIONES GENERALES

#### NORMAS EXTERNAS

Aplican las siguientes normas de la Superintendencia Financiera de Colombia:

- **Circular Externa 025 de 2020 de la Superintendencia Financiera de Colombia:** Las entidades deben definir, implementar, probar y mantener un proceso para administrar la continuidad del negocio que incluya la prevención y atención de emergencias, administración de la crisis, planes de contingencia y capacidad de retorno a la operación normal.
- **Circular 038/2009 – Sistema de Control Interno:** Implementar, probar y mantener un proceso para administrar la continuidad de la operación de la entidad para responder a las fallas e interrupciones específicas de un sistema o proceso y capacidad de retorno a la normalidad.

#### NORMAS INTERNAS

- Los incidentes de continuidad son reportados en el Comité SARO – SARLAFT, donde son revisados y de considerar necesario solicitan acciones que se deban emprender para el tratamiento de los riesgos de continuidad.
- El presente procedimiento se deberá revisar y actualizar (si se hace necesario).

Los incidentes de PCN se clasifican de la siguiente manera:

#### Incidentes relacionados con servicios tecnológicos

- Servicio telefónico
- Caída de los sistemas
- Falla de la infraestructura

#### Incidentes relacionados con infraestructura física

- o Falla en el suministro de servicios públicos (agua y luz)
- o No disponibilidad del sitio de trabajo por causas naturales, factores sociales y políticos.
- Cuando el comité SARO-SARLAFT determine la activación de la contingencia se diligenciará el "[Formato de activación y seguimiento de contingencia en sitio](#)" ( F291), el cual será firmado por el Señor Presidente en su rol de Director de Continuidad y/o Jefe de Riesgos en su rol como Directora alterna.
- El Líder de Riesgos registrará en el aplicativo de gestión de riesgos y diligenciará el formato Reporte de Incidentes de Contingencia (F289), los incidentes de Plan de contingencia operativos o del plan de continuidad del negocio que se generen los cuales serán revisados por la Oficina de Riesgos.
- Ante un incidente presentado, el plan de contingencia operativo para los procedimientos críticos se mantendrá hasta que se retorne a la operación normal.
- De acuerdo con el escenario materializado se realiza la activación de los planes de contingencia operativos que se encuentran en el procedimiento escenarios de falla y estrategias de continuidad.

#### Incidentes relacionados con Personas

- Tomando como prioridad el aseguramiento de la integridad de las personas, se siguen las indicaciones definidas en el Plan de Emergencias establecido por el Grupo de Talento Humano de la sede principal del ICETEX, que se encuentra en el publicado en el Sistema de Gestión de Calidad.

#### Incidentes relacionados con Tecnología

- Si el tiempo de recuperación es mayor al tiempo objetivo de recuperación del proceso/procedimiento afectado, el Grupo de Infraestructura de la Dirección de Tecnología solicita la activación de la contingencia tecnológica definida para el tipo de incidente presentado, para lo cual se realizarán las actividades descritas en el plan de recuperación de Desastres de TI, que se encuentra en el publicado en el Sistema de Gestión de Calidad.

#### Incidentes sobre procesos ejecutados por terceros (Proveedores)

- Los proveedores que efectúan procesos de la Entidad deben informar los incidentes de continuidad que se generan de manera oportuna y completa, para lo cual el supervisor del contrato debe asegurarse que los proveedores conozcan de este lineamiento y lo presenten acorde a lo descrito en el presente procedimiento

## 5. DESCRIPCIÓN

### 5.1. DIAGRAMA DE FLUJO

(No aplica)

### 5.2. ACTIVIDADES

¿Es un incidente relacionado con?

- Incidentes Relacionados con Tecnología 5.2.7
- Incidentes Relacionados con Infraestructura Física 5.2.13
- Incidentes Relacionados con Proveedores 5.2.20

#### Proveedor de ICETEX

- 5.2.1. Informa la ocurrencia del incidente al supervisor del contrato indicando los aspectos de fecha, hora de inicio del incidente, situación presentada, plan de contingencia que utilizan para dar continuidad al proceso y mecanismos de recuperación para dar solución a la falla presentada.

#### Colaborador del área

- 5.2.2. Identifica un incidente de continuidad del negocio y lo informa al Líder de procesos de forma verbal, por correo electrónico, teléfono o medio de comunicación que tenga a su alcance, para posteriormente ser registrado en el aplicativo de gestión de riesgos y en el "[formato Reporte de Incidentes de Contingencia](#)" (F289).

#### Líder de Riesgos Área / Procesos ICETEX

- 5.2.3. Verifica si el incidente se está presentando a otros colaboradores de la misma área, determinando el alcance del mismo.

- 5.2.4. Informar a las siguientes áreas acorde al origen del incidente así por correo electrónico:

- o Aspectos relacionados con servicios tecnológicos: Coordinador de Infraestructura y Director de Tecnología siga con la actividad 5.2.7
- o Aspectos relacionados con infraestructura física: Coordinador de Recursos Físicos.

- 5.2.5. Diligencia el formato "[Reporte de incidente PCN](#)" (F289), y remitir a la Oficina de Riesgos, con copia al Líder del Proceso responsable del área afectada, una vez se haya solucionado el incidente.

### Profesional - Oficina de Riesgos- Plan de Continuidad de Negocio

5.2.6. El profesional de la Oficina de Riesgos analiza el reporte de incidentes, especialmente en el desarrollo del plan de contingencia aplicado y de ser necesario, solicita al Líder del Proceso el fortalecimiento mediante un plan de mejoramiento.

### Incidentes Relacionados con Tecnología

#### Coordinador de Infraestructura y/o Director de Tecnología

5.2.7. Con el equipo de Infraestructura analizan la situación presentada, validan técnicamente el incidente, determinan las causas generadoras, procesos y áreas afectadas.

5.2.8. Establecen los procedimientos de recuperación que se tienen para el incidente presentado y el tiempo de recuperación de la falla.

- Si el tiempo de recuperación de la falla es mayor al tiempo objetivo de recuperación (RTO) del proceso/procedimiento afectado, solicita la activación de la contingencia tecnológica y continua con la actividad 5.2.9.
- En caso contrario continua con la actividad 5.2.11

5.2.9. Levanta la contingencia tecnológica y ejecutar el retorno a la normalidad aplicable de acuerdo con el plan de recuperación definido por esta área.

5.2.10. Informa mediante correo electrónico al Jefe de área que reportó el suceso con copia a la Oficina de Riesgos, para que retomen las actividades del proceso afectado, continua con la actividad 5.2.12.

5.2.11. Informa al Jefe de la dependencia que detectó el hecho y a la Oficina de Riesgos que se tomará un tiempo de recuperación menor, siendo necesario esperar la corrección del incidente, para retomar las actividades del proceso afectado, continua con la actividad 5.2.12.

5.2.12. Diligencia el formato "[Reporte de incidente PCN](#)" (F289), y remitir a la Oficina de Riesgos, con copia al Líder del Proceso responsable del área afectada, una vez se haya solucionado el incidente.

### Incidentes Relacionados con Infraestructura Física

#### Coordinador de Grupo de Recursos Físicos

5.2.13. Con el equipo del Grupo de Recursos físicos analizan la situación presentada, determinan las causas generadoras, procesos y áreas afectadas.

5.2.14. Establecen los procedimientos de recuperación que se tienen para el incidente presentado, estimando el tiempo de ejecución de la misma.

5.2.15. Inicia ejecución del procedimiento de recuperación establecido y activa la contingencia definida para el tipo de incidente presentado.

5.2.16. Una vez se solucione la falla presentada y se recupere el servicio, solicita levantar el proceso de contingencia al personal que lo está ejecutando.

5.2.17. Informa mediante correo electrónico al Jefe de área que reportó el suceso con copia a la Oficina de Riesgos, para que retomen las actividades del proceso afectado

5.2.18. Diligencia el formato "[Reporte de incidente PCN](#)" (F289), y remitir a la Oficina de Riesgos, con copia al Líder del Proceso responsable del área afectada, una vez se haya solucionado el incidente.

### Incidentes Relacionados con Proveedores

#### Proveedor de ICETEX

5.2.19. Informa la ocurrencia del incidente al supervisor del contrato indicando los aspectos de fecha, hora de inicio del incidente, situación presentada, plan de contingencia que utilizan para dar continuidad al proceso y mecanismos de recuperación para dar solución a la falla presentada.

#### Supervisor Contrato / Procesos ICETEX

5.2.20. Informa del hecho a la Oficina de Riesgos vía correo electrónico y registra el evento en el aplicativo de gestión de riesgos.

5.2.21. Hace seguimiento al desarrollo del proceso mientras se está gestionando el incidente

#### Proveedor de ICETEX

5.2.22. Presentar a la Entidad un informe del incidente que contenga como mínimo los aspectos de fecha del incidente, duración, lugar donde se presentó, descripción, medidas contingentes adoptadas/ contramedidas, impactos sobre la operación.

5.2.23. Después de revisar una evaluación objetiva de los hechos, se procederá a informar sobre las lecciones de aprendizaje.

#### Supervisor Contrato / Procesos ICETEX

5.2.24. Diligencia el formato "[Reporte de incidente PCN](#)" (F289), y remitir a la Oficina de Riesgos, con copia al Líder del Proceso responsable del área afectada, una vez se haya solucionado el incidente.

## 6. SEGUIMIENTO Y CONTROL

ACTIVIDAD A CONTROLAR	COMO EJERCER EL CONTROL	EVIDENCIA DEL CONTROL	RESPONSABLE
Reporte incidente de contingencia o continuidad	Solicitud al líder de riesgo del área y al supervisor del contrato para los terceros de la entidad	Correos con la solicitud. formato " <a href="#">Reporte de incidente PCN</a> " (F289)	Oficina de Riesgos Líder de Riesgos y/o supervisor del contrato

## 7. DOCUMENTOS RELACIONADOS

NOMBRE DEL DOCUMENTO	CODIGO
Circular Externa 025 de 2020 de la Superintendencia Financiera de Colombia	N.A.
Circular 038/2009 – Sistema de Control Interno	N.A.
<a href="#">Formato de activación y seguimiento de contingencia en sitio</a>	<a href="#">F291</a>
<a href="#">Instructivo formato de activación y seguimiento de contingencia en sitio</a>	<a href="#">I291</a>
<a href="#">Reporte de incidentes</a>	<a href="#">F289</a>
<a href="#">Instructivo formato Reporte de incidentes</a>	<a href="#">I289</a>

[1] ISO 22301- Requisitos para el sistema de administración de continuidad de negocios – términos y definiciones.

**Historial de Versiones**

**Fecha Vigencia (Acto Adtvo) Versión Descripción de Cambios**

2021-04-22                      1                      -

COPIA CONTROLADA