Contenido

1. OBJETIVO

Establecer las estrategias de continuidad ante los escenarios de posibles fallas que se presenten en el ICETEX con fin de regresar a la operación en el menor tiempo posible, garantizando el servicio a sus diferentes grupos de interés.

2. ALCANCE

Este procedimiento aplica para determinar cuál es la selección de las estrategias de continuidad que se deben seguir ante una interrupción para mantener o reanudar las actividades de la Entidad y sus dependencias.

3. DEFINICIONES

Análisis de Impacto del Negocio – BIA (Business Impact Analysis): Se identifica como BIA por sus siglas en Ingles), es una etapa que permite identificar la urgencia de recuperación de cada procedimiento, los recursos y sistemas críticos para estimar el tiempo que ICETEX puede tolerar en caso de un incidente o desastre.

- **Ausencias de personal:** Se presenta cuando el colaborador no puede asistir a trabajar para desarrollar las actividades propias de su cargo.
- **CEP:** Sigla para referenciar a los Centro de experiencia personal de atención al usuario.
- **Colaborador:** Termino utilizado para referenciar a un funcionario y contratista de la Entidad.
- Estrategias de continuidad: Corresponden a las acciones que se deben tomar con el objetivo de restablecer las operaciones del negocio, en el plazo determinado, una vez que ocurra alguna interrupción o falla en los procesos o funciones críticas.
- **Indisponibilidad del proveedor**: Se presenta cuando el proveedor contratado para la prestación del servicio o bien de Icetex no esté disponible por la ocurrencia de algún evento que afecta la continuidad de la operación.
- **Indisponibilidad de tecnología:** se presenta cuando el hardware y/o software presenta fallas, o cuando haya interrupción prolongada de las comunicaciones.
- **Indisponibilidad de la Infraestructura física:** Se presenta cuando la infraestructura física, de los CEP de la entidad y sede principal que se requiere para prestar los servicios requeridos están imposibilitados para su acceso sea total o parcialmente.
- No acceso al sitio normal de trabajo: Se presenta cuando el personal no puede acceder a su lugar de trabajo para desarrollar las actividades propias de su cargo para salvaguardar su integridad en la declaración de Emergencia Sanitaria u otros eventos que se puedan presentar, los cuales se describen en el presente procedimiento.
- **Pandemia**: Se llama pandemia a la propagación mundial de una nueva enfermedad.[1]
- **Plan de Contingencia:** Conjunto de acciones y recursos para responder a las fallas e interrupciones específicas de un sistema o proceso.
- **Posible contaminación o contagio del sitio de trabajo:** Evento que puede conducir a una contaminación o contagio en el lugar de trabajo por la presencia de un virus o enfermedad declarada por la Organización mundial de la Salud - OMS
- **Proceso crítico:** Proceso que afecta de forma directa la satisfacción del cliente, el cumplimiento regulatorio, la reputación y la eficiencia económica de la organización.
- **Sitio alterno**: Sitio de operación definido por Icetex para operar en contingencia.
- **Trabajo remoto:** Es una modalidad de empleo organizada, colaborativa y planificada, que permite trabajar desde el hogar, oficinas compartidas (Coworking) o cualquier lugar diferente a una oficina y en la mayoría de casos no obedece a horarios definidos sino a tareas u objetivos a cumplir.
- **Tiempo de recuperación objetivo (RTO- Recovery Time Objetive):** Hace referencia al tiempo máximo, durante el cual debe ser recuperado el procedimiento y sus recursos, posterior a la ocurrencia de un incidente.[2]
- **Punto de recuperación objetivo (RPO- Recovery Point Objetive):** 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".

- **VPN- Virtual Private network)[3],** también llamada red privada virtual, es una tecnología de red de ordenadores que permite una extensión segura de la red de área local sobre una red pública o no controlada como Internet.

4. CONDICIONES GENERALES

- Los escenarios de falla para los cuales se definen estrategias de continuidad son: Ausencia o indisponibilidad de personal, fallas tecnológicas, indisponibilidad de la infraestructura física, indisponibilidad del proveedor que presta el servicio o bien contratado por Icetex, a continuación, se establecen las posibles causas en cada caso:
  - o Ausencia o indisponibilidad del personal: Afectaciones masivas al personal por pandemias, intoxicaciones, enfermedades, contaminaciones o contagios u otra tipología declarada por la Organización Mundial de la salud OMS, por vandalismos, asonadas y desastres naturales.
  - o Indisponibilidad de la infraestructura física: Afectaciones a la infraestructura física por contaminación del sitio por epidemias, pandemias, virus, u otros que catalogue Organización Mundial de la Salud, fallos internos como inundación, incendios, falencias con el sistema eléctrico, desastres naturales, manifestaciones, asonadas u otros.
  - o Indisponibilidad tecnológica (Hardware y Software): cuando el hardware y/o software presenta fallas, o cuando haya interrupción prolongada de las comunicaciones que supere los tiempos de recuperación establecidos para cada procedimiento o proceso según aplique los cuales son de 4 horas, 8 horas, 24 horas y 48 horas resultantes del análisis de impacto de negocio.
  - o Indisponibilidad del proveedor: cuando el proveedor contratado para la prestación del servicio del Grupo de Gestión Documental no esté disponible por la ocurrencia de algún evento que afecta la continuidad de la operación.

-

- Las estrategias de continuidad en cada escenario de falla presentando en ICETEX se especifican en los siguientes anexos:.
  - Anexo 1 Directorio de contingencia
  - Anexo 2 Relación entre procesos críticos y escenarios de falla
  - Anexo 3 Escenarios de falla y estrategias de continuidad
  - Anexo 4 Relación de personal de backup líderes de riesgo
- Igualmente, la relación entre procesos críticos y escenarios de falla se encuentran en el anexo del mismo nombre.
- Para definir las estrategias de continuidad posibles o viables, de manera efectiva y eficiente, se debe contar con un entendimiento sobre los siguientes aspectos,
  - o Resultados del Análisis de Impacto al Negocio (BIA- Business Impact Analysis).
  - o Tiempos y puntos objetivo de recuperación (RTO y RPO) requeridos para los procesos críticos.
  - o Procesos críticos a soportar
  - o Resultados del análisis de riesgos y las alternativas de tratamiento de riesgo a implementar sobre los activos asociados a los procesos.
  - o Amenazas posibles a los activos de los procesos.
  - o Vulnerabilidades existentes en los activos de los procesos
- Los factores a tener en cuenta para la actualización del procedimiento son: nuevos requerimientos legales aplicables, nuevos protocolos de bioseguridad, cambios en los procesos o sistemas de gestión del instituto, cambios de sitio alterno, cambios en las estrategias de continuidad, incorporación de nuevos escenarios disruptivos.
- Las estrategias de continuidad definidas para los proceso catalogados como críticos, resultantes del análisis de impacto de negocio, se establecen en los planes de contingencia operativos, los cuales estarán a cargo de cada área según aplique al proceso, relacionados en el presente procedimiento y en el "Manual de Administración de la continuidad de Negocio" (M14).
- Con las estrategias de continuidad se busca garantizar que los colaboradores:
  - ✓ Estén protegidos
  - ✓ Comprenden su papel
  - ✓ Saben a dónde ir
  - ✓ Saben qué hacer
  - ✓ Saben qué recursos necesitan
  - ✓ Entienden la secuencia de las tareas críticas

5. DESCRIPCIÓN

5.1 DIAGRAMA

(No plica)

5.2. ACTIVIDADES

¿Cuál es la falla?

- Ausencia o indisponibilidad del personal, continúa 5.2.1
- Fallas en la infra estructura física, continúa 5.2.2
- Indisponibilidad tecnológica, continúa 5.2.3
- Indisponibilidad del proveedor, continúa 5.2.4
- ausencia definitiva o parcial del líder de riesgos, continúa 5.2.5
- Indisponibilidad del sitio de operación, continúa 5.2.6

Colaboradores / Icetex

5.2.1 Si el escenario de falla es la ausencia o indisponibilidad del personal se deberá desarrollar las estrategias de Backup del personal clave (designación colabores suplentes), transferencia del conocimiento clave para la prestación de los servicios del ICETEX y trabajo remoto con uso de VPN. (Consultar Anexo Escenarios de falla y estrategias de continuidad)

5.2.2 Si el escenario de falla es la indisponibilidad de la infraestructura física se deberá desarrollar las estrategias procesos críticos del BackOffice: Traslado al sitio alterno de Icetex y trabajo remoto con uso de VPN. (Consultar Anexo Escenarios de falla y estrategias de continuidad).

Dirección de Tecnología/ Icetex

5.2.3 Si el escenario de falla es la Indisponibilidad Tecnológica se deberá desarrollar las estrategias de Contingencia manual, el Datacenter alterno establecido por el proveedor del servicio de la Dirección de Tecnología, ejecución del Plan establecido por el proveedor del servicio contratado por Icetex. (Consultar Anexo Escenarios de falla y estrategias de continuidad).

5.2.4 Si el escenario de falla es la indisponibilidad del proveedor catalogado como crítico se deberá desarrollar las estrategias de inclusión de la cláusula de continuidad de negocio establecidas en la suscripción del contrato, establecer acuerdos de nivel de servicio – ANS, tener el plan de contingencia (consultar anexo escenarios de falla y estrategias de continuidad).

Líderes de riesgo/ Icetex

5.2.5 En caso de ausencia definitiva o parcial del líder de riesgos se tiene como estrategia, la designación de un suplente, que desarrollará las funciones del principal. (consultar el anexo relación de personal de backup de los líderes de riesgos).

Dirección de Tecnología/ Icetex

5.2.6 En caso de presentarse los escenarios de falla de: Indisponibilidad del sitio de operación, indisponibilidad de la tecnología, ciberataques, desastre natural se deberá notificar a las áreas relacionadas en el Directorio de Contingencia, para lo cual podrá consultar el anexo del mismo nombre.

6. SEGUIMIENTO Y CONTROL

ACTIVIDAD ACONTROLAR	CÓMO EJERCE CONTROL	EVIDENCIA DEL CONTROL	RESPONSABLE
Escenario de falla presentado	Aplicación de la estrategia de continuidad	Estrategia implementada	• Comité SARO-SARLAFT • Responsables de la continuidad de negocio. • Coordinadores de recuperación

7. DOCUMENTOS RELACIONADOS

NOMBRE DEL DOCUMENTO	CODIGO
Manual de Administración del Plan de Continudad del Negocio	**M14**
Anexo 1 Directorio de contingencia	N.A.
Anexo 2 Relación entre procesos críticos y escenarios de falla	N.A.
Anexo 3 Escenarios de falla y estrategias de continuidad	N.A.
Anexo 4 Relación de personal de backup líderes de riesgo	N.A.

[1] https://www.who.int/csr/disease/swineflu/frequently_asked_questions/pandemic/es/
[2] ISO 22301- Requisitos para el sistema de administración de continuidad de negocios – términos y definiciones.
[3] https://es.wikipedia.org/wiki/Red_privada_virtual

Anexos:

Anexo1 Directorio en Contingencia.pdf
Editado por Elda Yolanda Castellanos Monroy, mar 18 2021 15:38 p.m.

Anexo 2 Relación entre procesos críticos y escenarios de falla.pdf
Editado por Elda Yolanda Castellanos Monroy, mar 18 2021 15:38 p.m.

Anexo 3 Escenarios de falla y estrategias de continuidad.pdf
Editado por Elda Yolanda Castellanos Monroy, mar 18 2021 15:38 p.m.

Anexo 4 Relación de personal de backup de los líderes de riesgos.pdf
Editado por Elda Yolanda Castellanos Monroy, mar 18 2021 15:38 p.m.

Historial de Versiones

Fecha Vigencia (Acto Adtvo)	Versión	Descripción de Cambios
2021-03-23	1	-