Contenido

1. OBJETIVO

Identificar, evaluar y gestionar eficientemente el riesgo de continuidad con el fin de proteger a la Entidad ante la indisponibilidad de recursos que soportan la operación.

2. ALCANCE

El procedimiento comienza con la elaboración del cronograma de Monitoreo de Riesgos de PCN y finaliza con el seguimiento a los tratamientos o acciones.

3. DEFINICIONES

- **Riesgo:** Es la probabilidad de materialización de una amenaza por la existencia de una o varias vulnerabilidades con impactos adversos resultantes para la Entidad.
- **Frecuencia:** Estimación de ocurrencia de un evento en un período de tiempo determinado.
- **Impacto:** Es el efecto que causa la ocurrencia de un incidente o siniestro. La implicación del riesgo se mide en aspectos económicos, imagen reputacional, disminución de capacidad de respuesta y competitividad, interrupción de las operaciones, consecuencias legales y afectación física a personas.
- **Control:** Es el proceso, política, dispositivo, práctica u otra acción existente que actúa para minimizar el riesgo o potenciar oportunidades positivas.
- **Disponibilidad:** La información debe estar en el momento y en el formato que se requiera ahora y en el futuro, igual que los recursos necesarios para su uso[1].
- **Riesgo de continuidad del negocio**: Posibilidad de incurrir faltas o fallas en la disponibilidad de las personas, proveedores, información, sistemas o infraestructura física.
- **Líder de Riesgo PCN:** Son los funcionarios asignados por proceso para apoyar la gestión de riesgos de continuidad del negocio.

4. CONDICIONES GENERALES

- El manejo de continuidad del negocio es responsabilidad de todo el personal del Instituto, contratado directa o indirectamente, independientemente de su nivel y funciones a cargo.
- Se asigna un Líder de Riesgo de PCN en cada área, el cual gestiona la continuidad de la operación del área que representa incluido este tipo de riesgo, dentro del marco de la metodología establecida para el mismo. Esta actividad es adicional a sus responsabilidades de línea normales.
- La gestión de riesgos de continuidad de negocio se lleva a cabo de acuerdo con la Metodología descrita en el Manual de Administración de Plan de Continuidad del Negocio.
- La gestión de riesgos de continuidad del negocio, realizada por las áreas de la Entidad con apoyo de la Oficina de Riesgos se compone de las fases de identificación de riesgos y causas, su evaluación, medición, identificación de controles y establecimiento de planes de tratamiento para causas que no cuentan con controles o cuya evaluación de riesgo residual está en estado grave o crítico.
- El procedimiento de gestión de riesgos debe ejecutarse en forma permanente. Las áreas deben realizar este procedimiento al menos semestralmente, o cuando cambios externos o internos afecten considerablemente el perfil de riesgo de la función de negocio/apoyo. La Oficina de Riesgos efectúa el seguimiento de la gestión realizada por las diferentes áreas.
- La Entidad definió la aplicación de riesgos no financieros como la herramienta de registro y administración para el riesgo de continuidad, en el cual se lleva la relación de todos los riesgos, causas, controles y planes de tratamiento, así como sus responsables, calificaciones y planes de mitigación.
- Todo riesgo identificado debe tener asignado un responsable.
- Los siguientes riesgos de continuidad son transversales a la operación, siendo identificados y administrados en el área origen de este:

Riesgo	Área responsable

Asociados con fallos y/o caídas del sistema de información	Dirección de Tecnología
Asociados con personal	Secretaria General – Grupo de Talento Humano
Asociados con infraestructura física	Secretaria General – Grupo de Recursos Físicos

- A este procedimiento le es aplicable la siguiente normatividad:

  - Capítulo XXIII "Reglas Relativas a la Administración del Riesgo Operativo" de la Superintendencia Financiera de Colombia: Las entidades debe 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.
  - Circular 042/2012: Exigir que los terceros contratados dispongan de planes de contingencia y continuidad debidamente documentados. Las entidades deberán verificar que los planes, en lo que corresponde a los servicios convenidos, funcionen en las condiciones pactadas.

5. DESCRIPCIÓN

5.1. DIAGRAMA DE FLUJO

(Ver Anexo1 Diagrama de Flujo)

5.2. ACTIVIDADES

Analista de Riesgo PCN / Oficina de Riesgos

5.2.1. Elabora cronograma de Monitoreo de Riesgos de PCN, el cual se realiza en Excel, donde se agende al Líder de PCN.

Líder de Riesgo PCN / Procesos ICETEX

5.2.2. Establece los riesgos de continuidad que se pueden presentar en las diferentes actividades que conforman el proceso.

5.2.3. Identifica las causas que dan origen a los riesgos definidos, teniendo como criterio básico el aporte de los funcionarios, especialmente los involucrados en los respectivos procesos, así como:

- Bajo el enfoque de juicio de expertos se procede a identificar los riesgos mediante reuniones con los líderes de proceso o líderes de riesgo y con base en su conocimiento de la operación, se describir los posibles riesgos que lleven a una interrupción en la operación. Adicional, se puede tomar como guía el anexo "Tipos de Amenazas" que se encuentra en el Manual de Administración de Plan de Continuidad de Negocio, donde se detallan posibles fuentes de peligro, las cuales se deben evaluar si tales situaciones pueden darse en el proceso analizado. Es de aclarar, que esta tabla es solamente una guía pudiendo incluirse muchas otras amenazas.

- Determinar las causas o debilidades internas que tiene el proceso para cada riesgo identificado. Para identificarla es necesario responder esta pregunta: ¿Cómo puede ocurrir el riesgo? Al responderla, se evalúa si dentro del Instituto puede darse esa circunstancia.

  Se recomienda utilizar como guía con el anexo "Tabla de Vulnerabilidades", que se encuentra en el Manual de Administración de Plan de Continuidad de Negocio, donde se encuentra una relación de debilidades que podrían llegar a generar la interrupción del proceso. Es de aclarar, que esta tabla es solamente una guía pudiendo incluirse muchas otras situaciones de debilidades.

- Además, para la identificación de riesgos y causas se debe tener en cuentas las siguientes consideraciones de hallazgos de las auditorías internas y/o externas realizadas a los procesos y procedimientos de la entidad y la base de datos del registro de eventos e incidentes. Este mecanismo permite asociar al proceso de identificación de los riesgos, un componente objetivo y preciso.

- Describir el riesgo y la causa contemplando las variables de amenaza y vulnerabilidad.

- Contemplar los factores de la continuidad:
  - Personas
  - Infraestructura física
  - Infraestructura de tecnología de información
  - Procesos

5.2.4. Identifica los controles existentes por cada una de las causas que prevengan y detecten la ocurrencia de un riesgo o que mitiguen el impacto en caso de materialización del riesgo evaluado.

5.2.5. Registra la información de los riesgos identificados, causas y controles en el aplicativo de gestión de riesgo, junto con el acompañamiento de la Oficina de Riesgos (en caso de requerirse).

5.2.6. Evalúa la probabilidad y el impacto de las causas identificadas, midiendo las posibles consecuencias que tendría para ICETEX la materialización de los

riesgos previamente identificados. Esta evaluación se realiza bajo los criterios de medición de probabilidad e impacto definidos en el sistema los cuales están alineados con la Metodología de Riesgos de Continuidad del Negocio.

5.2.7. Realiza la calificación de los controles asociados al proceso, esta actividad se realiza en el aplicativo de gestión de riesgo.

Analista de Riesgos PCN / Oficina de Riesgos

5.2.8. Valida los resultados arrojados por el aplicativo de gestión de riesgos, el riesgo residual y elabora mapa térmico, basado en las calificaciones dadas por el Líder de Riesgo PCN.

Líder de Proceso / Procesos ICETEX

5.2.9. Analiza el resultado del mapa y verifica la descripción del riesgo, causas, descripción del impacto y medición del riesgo inherente.

- En caso de existir inconsistencias, continúe con la actividad 5.2.10.
- En caso de que no existan inconsistencias, continúe con la actividad 5.2.12.

5.2.10. Solicita los ajustes pertinentes.

Líder de Riesgo PCN / Procesos ICETEX

5.2.11. Incorpora las observaciones realizadas y/o realiza los ajustes pertinentes.

Analista de Riesgos PCN / Oficina de Riesgos

5.2.12. Consolida y evalúa los riesgos, causas y controles identificados para los procesos.

5.2.13. Informa a los Líderes de proceso y Líderes de riesgo CN sobre el resultado de la evaluación de las causas de riesgos:

- Si determina que las causas de acuerdo con la calificación otorgada requieren planes de tratamiento, entonces continúe con la actividad 5.2.14.
- Si determina que las causas de acuerdo con la calificación otorgada no requieren planes de tratamiento, entonces se da por finalizado el procedimiento.

Líder de Proceso - Líder de Riesgo PCN / Procesos ICETEX

5.2.14. Define en el aplicativo de gestión de riesgos el plan de tratamiento para las causas que requieran de éste, documentando las actividades a realizar, los tiempos programados y las personas responsables de su implementación.

Analista de Riesgos PCN / Oficina de Riesgos

5.2.15. Realiza seguimiento a los tratamientos o acciones de forma periódica.

6. SEGUIMIENTO Y CONTROL

ACTIVIDAD A CONTROLAR	COMO EJERCER EL CONTROL	EVIDENCIA DEL CONTROL	RESPONSABLE
Identifica los riesgos relacionados en cada proceso, detallando sus causas y controles	Verificación de la información ingresada al sistema por el Líder de Riesgo PCN	Registro en el aplicativo de gestión de riesgos.	Líder de Riesgo PCN del área
Mide cada uno de los riesgos, causas y controles identificados.	Seguimiento a la calificación de los riesgos	Registro en el aplicativo de gestión de riesgo	Líder de Riesgo PCN del área

7. DOCUMENTOS RELACIONADOS

NOMBRE DEL DOCUMENTO	CÓDIGO
Manual de Administración del Plan de continuidad del Negocio	M14

[1] Concepto tomado del Capítulo XII – Requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios- Título I de la Circular Básica Jurídica de la Superfinanciera.

Anexos:
E2-1-15 Identificación de Riesgos de Continuidad de Negocio V1.pdf

Historial de Versiones

Fecha Vigencia (Acto Adtvo)	Versión	Descripción de Cambios
2018-7-9	1	-