Contenido

1 OBJETIVO

Establecer lineamiento procedimental para la gestión de riesgos de seguridad de la información y los controles para analizar situaciones adversas que pueden desencadenar en impactos, con el fin de tomar decisiones y reducir el riesgo a nivel aceptable para el instituto.

2 ALCANCE

Este documento considera las etapas para identificar, analizar, evaluar y tratar de manera adecuada la gestión de Riesgos de Seguridad de la Información involucrando todos los procesos de negocio y sus dependencias de servicios con terceras partes, cuya sinergia incorpora la participación activa en el monitoreo periódico, en la Gestión de Incidentes de Seguridad de la Información y Gestión de Cambios; aspectos relevantes en la modificación del mapa de riesgo de seguridad de la información.

3 DEFINICIONES

- **Amenaza:** Situación proveniente de actores externos e internos no controlada, que puede constituirse como causa de riesgo que perjudicar negativamente uno o más activos, éstas pueden ser intencionales o accidentales.
- **Aceptación del riesgo:** Es el nivel aceptable de variación que la dirección del instituto está dispuesta a permitir para cada riesgo durante la búsqueda de los objetivos institucionales.
- **Comunicación del riesgo:** Intercambiar o compartir información acerca del riesgo entre las personas que toman las decisiones y otras partes interesadas.
- **Estimación del riesgo:** Proceso sistemático para asignar valores de probabilidad y a las consecuencias de un riesgo de seguridad de la información.
- **Gestión de riesgo:** Actividades coordinadas para dirigir y controlar una organización, con respecto al riesgo.
- **Identificación del riesgo:** Es la forma para encontrar, enumerar y caracterizar los elementos de riesgos de seguridad de la información.
- **Impacto:** Es el efecto que causa la ocurrencia de un incidente o siniestro. La implicación del riesgo se mide en aspectos económicos, imagen reputacional, afectación en los procesos Mide el nivel de degradación de uno de los siguientes elementos de seguridad de la información: Confiabilidad, disponibilidad e integridad.
- **Probabilidad:** Grado de amplitud de que un suceso pueda ocurrir.
- **Riesgo Aceptable:** Es el nivel de riesgo que el Instituto está dispuesto a aceptar.
- **Riesgo Inherente:** Es el cálculo del daño probable a un activo de encontrarse desprotegido de controles de seguridad.
- **Riesgo Residual:** Es el riesgo remanente tras la aplicación de controles.
- **Riesgo de seguridad de la información:** Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de éstos causando daño al instituto.
- **Reducción del riesgo:** Acciones tomadas para reducir la probabilidad o las consecuencias negativas o ambas asociadas con un riesgo.
- **Retención del riesgo:** Aceptación de la pérdida o ganancia proveniente de un riesgo particular.
- **Riesgo Tolerable:** Es el nivel aceptable de variación del riesgo en el logro de los objetivos.
- **Transferencia de riesgo:** Compartir con otras partes la pérdida o ganancia de un riesgo.
- **Tratamiento del riesgo:** Proceso de selección y de implementación de medidas para modificar el riesgo.
- **Vulnerabilidades:** Son debilidades, brechas de seguridad o situaciones inherentes a los activos de información que pueden ser explotadas por las amenazas.
- **Zona de riesgo**: Ubicación del riesgo dentro del mapa térmico en la herramienta de administración de riesgos no financieros.

4 CONDICIONES GENERALES

- El manejo de riesgo de seguridad de la información es responsabilidad de todo el personal de la Entidad, contratado directa o indirectamente, independientemente de su nivel y funciones a cargo.
- Los funcionarios que ingresen al ICETEX deben recibir una inducción de seguridad de la información y los funcionarios antiguos deben recibir capacitación y actualización en el mismo tema por lo menos una vez al año.
- La Oficina de Riesgos debe administrar la información la base de datos de riesgos de seguridad de la información.
- La Oficina de Riesgos debe apoya a los Líderes de Proceso y Líderes de Riesgo en la identificación de los hechos que puedan representar la materialización de un riesgo, para la generación de alertas, así como apoyar en la gestión de incidentes para que sean diligenciados completamente y planteado un plan de acción.
- La gestión de riesgos de seguridad de la información debe realizarse permanentemente por parte de los Líderes de Riesgos de procesos.
- Como mínimo anualmente se debe monitorear y evaluar los riesgos de seguridad de la información, así como los tratamientos con sus respectivos avances.
- A este procedimiento le es aplicable la siguiente normatividad:
    - Circular 042 de la Superintendencia Financiera.
    - Modelo de Seguridad y Privacidad de la Información.

5 DESCRIPCIÓN

Las actividades que a continuación se describen son ejecutadas mediante la revisión de la documentación existente del proceso y actividades realizadas por los Líderes de Riesgos por cada proceso con el apoyo de la Oficina de Riesgos.

5.1 DIAGRAMA DE FLUJO

N/A

5.2 ACTIVIDADES

Analista de Oficina de Riesgos

5.2.0 Elaborar cronograma de Monitoreo de Riesgos de Seguridad de la información, anualmente, donde se agende al Líder de Riesgos.

Líder de Riesgos de Proceso

5.2.1 Identificar en la matriz de riesgos de seguridad de la conformación las actuales causas, riesgos e incidentes de seguridad que intervienen en el proceso.

En el caso que exista nuevos riesgos y causas como las que se mencionan a continuación, el área se debe comunicar con el Líder de Riesgos para solicitar la creación de parámetros como se identifica en la actividad 5.2.3

- Riesgos y causas encontradas en auditorías internas y externas realizadas al proceso.
- Reporte de incidentes de seguridad de la información.
- Apertura o modificación a nuevos productos o servicios en el proceso.
- Apoyo en el proceso por terceras partes.
- Generación o modificación de nuevos controles.
- Suspensión de controles.

De no existir riesgos o causas nuevas, o modificación de controles, se continua con la actividad 5.2.4.

Analista de Oficina de Riesgos

5.2.2 Registrar y parametrizar la información de los nuevos riesgos, causas y controles, en el aplicativo de Gestión de Riesgos No Financieros y así comunicar al Líder de Riesgos del proceso para continuar con el proceso de evaluación.

Líder de Riesgos de Proceso

5.2.3 Realizar la evaluación de las causas definidas bajo los criterios de medición de probabilidad e impacto definidos en el sistema.

5.2.4 Realizar la evaluación de los controles asociados al proceso que permiten prevenir y/o detectar cada una de las causas asociadas a los riesgos y los controles que al implementarse logren disminuir el impacto o la frecuencia de las causas identificadas y asociadas a cada riesgo, esta actividad se realiza en el aplicativo de Riesgos No Financieros.

Analista de Oficina de Riesgos

5.2.5 Validar y analizar los resultados arrojados por el Aplicativo de Riesgos No Financieros.

5.2.6 Elaborar reporte de mapa térmico, calificación de causas y controles con los resultados del riesgo por proceso.

Líder de Oficina de Riesgos

5.2.7 Verificar el resultado del mapa y la descripción del riesgo, causas y controles. En caso de existir inconsistencias solicitar su ajuste al Líder de Riesgo de Proceso, caso en el que pasa a la actividad 5.2.10.

5.2.8 De encontrarse acorde, pasar a la actividad 5.2.11.

Líder de Riesgos de Proceso

5.2.9 Incorporar las observaciones realizadas y/o realiza los ajustes pertinentes juntamente con el líder de Riesgos y nuevamente volver a la actividad 5.2.9.

Líder de Proceso

5.2.10 Revisar el mapa de riesgo de seguridad de la información, si considera que se debe ajustar, proceder a indicar al Líder de Riesgo su corrección (actividad 5.2.2).

5.2.11 De estar de acuerdo con el mapa de riesgo de seguridad de la información, aprobar en el aplicativo de Riesgos No Financieros.

Analista de Oficina Riesgos

5.2.12 Consolidar y evaluar los riesgos, causas y controles identificados para el proceso.

En caso de existir causas graves y críticas que requieran planes de tratamiento para la mitigación del riesgo, informar a los líderes de proceso y líderes de riesgo las causas de acuerdo con la calificación otorgada. Continuar con la actividad 5.2.14. En caso contrario el proceso finaliza.

Líder de Riesgo de Proceso

5.2.13 Definir en el Aplicativo de Riesgos No Financiero 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.

Realizar seguimiento a los tratamientos o acciones de forma periódica.

Líder de Riesgos

5.2.14 Diligenciar el F462 Formato de seguimiento al sistema de seguridad digital, con frecuencia trimestral.

Líder de Proceso

5.2.15 Revisa el diligenciamiento del F462 Formato de seguimiento al sistema de seguridad digital, procediendo así:

- De estar de acuerdo con el diligenciamiento del F462 Formato de seguimiento al sistema de seguridad digital, firma el instrumento.
- De no estar de acuerdo o tener dudas con alguna de las respuestas del instrumento, solicitar aclaración al Líder de Riesgos, vuelve a la actividad 5.2.14.

Líder de Riesgos

5.2.16 Envía F462 Formato de seguimiento al sistema de seguridad digital a la Oficina de Riesgos, vía correo electrónico.

Analista de Riesgos – Oficina de Riesgos

5.2.17 Revisa las respuestas del F462 Formato de seguimiento al sistema de seguridad digital, donde:

- Identifica puntos favorables
- Identifica puntos de mejora para hacer seguimiento y apoyar a cada área

5.2.18 Archiva F462 Formato de seguimiento al sistema de seguridad digital en carpera compartida de la Oficina de Riesgos.

6. SEGUIMIENTO Y CONTROL

ACTIVIDAD A CONTROLAR	COMO EJERCER EL CONTROL	EVIDENCIA DEL CONTROL	RESPONSABLE
Identificación y validación de los riesgos y /o causas en el proceso	Verificación periódica de la matriz de riesgos de seguridad de la información	Registro en el Aplicativo de Riesgos No Financieros.	Líder de Riesgos de Proceso
Medición de los riesgos del proceso	Validación y análisis de la calificación del riesgo	Registro en el Aplicativo de Riesgos No Financieros.	Analista / Oficina de Riesgos
Generación y aprobación del mapa de riesgo	Revisión y análisis de los resultados arrojados en el mapa	Estado de “aprobado” del mapa de riesgos en el Aplicativo de Riesgos No Financieros.	Líder Riesgos de Procesos
Elaboración y ejecución del Plan de Tratamiento	Hacer seguimiento al Plan de Tratamiento de forma periódica	Plan de tratamiento en el Aplicativo de Riesgos No Financieros.	Líder Riesgos de Procesos

7. DOCUMENTOS RELACIONADOS

NOMBRE DEL DOCUMENTO	CÓDIGO
Manual de políticas de seguridad digital	M11
Modelo de seguridad y privacidad de la información	M16
Formato de seguimiento al sistema de seguridad digital	F462

Modificaciones

Descripción de cambios

1. En objetivo se adiciona los lineamientos procedimentales para la gestión de riesgo de seguridad de la información y los controles.
2. En condiciones generales se modifican los debe de la oficina de riesgos y los lideres de riesgo, dejando en la redacción los componentes generales.
3. En descripción se incluye el siguiente párrafo descriptivo “Las actividades que a continuación se describen son ejecutadas mediante la revisión de la documentación existente del proceso y actividades realizadas por los Líderes de Riesgos por cada proceso con el apoyo de la Oficina de Riesgos.”
4. En 5.2. Actividades se incluye el primer ejecutor por Analista de oficina de riesgos con la actividad 5.2.0. junto con la actividad de elaborar cronograma de monitoreo de riesgo.
5. Se modifica la numeración y la descripción en general de las actividades.
6. En documentos relacionados se incluye el F462 Formato de seguimiento al sistema de seguridad digital.

Historial de Versiones

Fecha Vigencia (Acto Adtvo)	Versión	Descripción de Cambios
2021-11-25	2	1. En objetivo se adiciona los lineamientos procedimentales para la gestión de riesgo de seguridad de la información y los controles. 2. En condiciones generales se modifican los debe de la oficina de riesgos y los lideres de riesgo, dejando en la redacción los componentes generales. 3. En descripción se incluye el siguiente párrafo descriptivo “Las actividades que a continuación se describen son ejecutadas mediante la revisión de la documentación existente del proceso y actividades realizadas por los Líderes de Riesgos por cada proceso con el apoyo de la Oficina de Riesgos.” 4. En 5.2. Actividades se incluye el primer ejecutor por Analista de oficina de riesgos con la actividad 5.2.0. junto con la actividad de elaborar cronograma de monitoreo de riesgo. 5. Se modifica la numeración y la descripción en general de las actividades. 6. En documentos relacionados se incluye el F462 Formato de seguimiento al sistema de seguridad digital.
2017-09-20	1	-