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 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 y mantener actualizada los datos de riesgos de seguridad de la información.
- Lo Lideres de Riesgos del proceso deben diligenciar trimestralmente el formato F462 Formato de seguimiento al sistema de seguridad digital y este debe ser firmado por el Vicepresidente/ Jefe de oficina/ Director o Coordinador del proceso, con el fin de identificar falencias u oportunidades de mejora en la gestión de la seguridad de la información, enviado por correo electrónico al líder de la oficina de riesgos.
- 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

Ver anexo

5.2 ACTIVIDADES

Analista - Oficina de Riesgos

5.2.1. Elabora el cronograma de Monitoreo de Riesgos de Seguridad de la información, anualmente, donde se agende al Líder de Riesgos, se realizan sesiones de socialización y el envío del cronograma.

Líder de Riesgos de Proceso

5.2.2. Revisa los riesgos de seguridad de la información establecidos para el proceso, los actualiza e identifica nuevos riesgos si es necesario. Para esta revisión se deben tener en cuenta estos parámetros.

- 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.
- Tratamiento de activos de información por terceras partes.
- Generación o modificación de nuevos controles.
- Suspensión de controles.
- Nuevas amenazas y/o vulnerabilidades.

5.2.3. Realiza la evaluación de los riesgos identificados bajo los criterios de medición de probabilidad e impacto definidos en la herramienta para establecer la zona de riesgo inherente.

5.2.4. Realiza la evaluación de los controles asociados al proceso que permiten prevenir y/o detectar o corregir, cada una de las amenazas y vulnerabilidades asociadas a los riesgos y los controles que al implementarse logren disminuir el impacto o la probabilidad de la materialización de los riesgos, esta actividad se realiza en la herramienta de Riesgos No Financieros, para establecer la zona de riesgo residual.

Analista - Oficina de Riesgos

5.2.5. Valida y/o ajusta el mapa térmico del riesgo inherente y del riesgo residual, calificación de amenazas, vulnerabilidades, controles y planes de tratamiento si aplica, con los resultados del riesgo junto con el Líder de Riesgos del proceso.

¿Se presentan riesgos en zona de riesgo residual alto o externo?

- Si, se requieren planes de tratamiento para la mitigación del riesgo, continúa con la actividad 5.2.6.
- No, Se informa mediante correo electrónico al Líder de la Oficina de Riesgos para su verificación, continua con la actividad 5.2.7.

Líder de Riesgos de Proceso

5.2.6. Define en la herramienta de Riesgos No Financiero el plan de tratamiento para los riesgos residual alto o extremo, documentando las actividades a realizar, los tiempos programados y las personas responsables de su implementación, continua con la actividad 5.2.5.

Líder - Oficina de Riesgos

5.2.7. Verifica el resultado del mapa y la descripción del riesgo, amenazas, vulnerabilidades, controles y plan de tratamiento si se requiere.

- En caso de existir inconsistencias solicitar su ajuste, continua con la actividad 5.2.5.
- De encontrarse acorde, pasar a la actividad 5.2.8.

Analista - Oficina de Riesgos

5.2.8. Realiza o ajusta el acta de aceptación de los resultados de la evaluación de riesgos de seguridad de la información, para remitir al Líder de riesgos del proceso junto con el mapa de riesgos por correo electrónico.

Vicepresidente/ Jefe de oficina/ Directores/ Coordinadores – del Proceso

5.2.9. Revisa el acta y el mapa de riesgos de seguridad de la información,

- Si considera que se debe ajustar, continua con la actividad 5.2.8.
- De estar de acuerdo con el acta y mapa de riesgo de seguridad de la información, continua con la actividad 5.2.10.

5.2.10. Firma el acta y la remite por correo electrónico al Líder 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 la herramienta 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 herramienta 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 la herramienta 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 la herramienta 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

Anexos:
E2-1-12 Gestionar riesgos de seguridad de la información V3_ Diagrama de flujo.pdf
Editado por Lina Marcela Carmona Parra, jul 12 2024 11:24 a.m.

Modificaciones

Descripción de cambios

1. Se realiza ajuste de la matriz de mapa de riesgos, por la herramienta de riesgos no financieros.
2. Se realizan ajustes generales en el procedimiento.

Historial de Versiones

Fecha Vigencia (Acto Adtvo)	Versión	Descripción de Cambios
2024-07-12	3	1. Se realiza ajuste de la matriz de mapa de riesgos, por la herramienta de riesgos no financieros. 2. Se realizan ajustes generales en el procedimiento.
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	-

¿Ha revisado el documento en su totalidad?
SI