CSC
CORPORACIÓN SOCIAL
DE CUNDINAMARCA

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION
No. CONSECUTIVO 1
FECHA: 29/01/2021

REALIZÓ	**REVISÓ**	**APROBÓ**
DIANA MILENA REINA	JAVIER RICARDO CATRO DUQUE	COMITÉ DE GESTION Y DESEMPEÑO
PROFESIONAL UNIVERSITARIO	SUBGERENTE ADMINISTRATIVO Y FINANCIERO	

TABLA DE CONTENIDO

1. INTRODUCCIÓN

La información que genera constantemente la Corporación Social de Cundinamarca es crucial para su correcto desempeño y cumplimiento de los objetivos organizacionales, es por ello que la seguridad y privacidad de la información se convierte en atributos indispensables para evitar cualquier posibilidad de alteración, mal uso, perdida, entre otros eventos, que puede significar una alteración para el normal desarrollo en la prestación del servicio de la entidad.

De acuerdo a lo mencionado anteriormente, dentro de Marco de Seguridad del Modelo de Seguridad y Privacidad de la información –MSPI-, un tema decisivo, es la Gestión de riesgos la cual es utilizada para la toma de decisiones. Es por esto que Corporación Social de Cundinamarca adopta la metodología “Guía de Riesgos” del Departamento Administrativo de la Función Púbica y como herramienta metodológica la utilizada por la Unidad Nacional para la Gestión del Riesgo de Desastres de la Presidencia de la República, además ha incorporado como referente la Norma ISO 31000 con el objetivo de generar buenas prácticas de gobierno corporativo y del mejoramiento continuo en la gestión de riesgos.

El HGM acoge la gestión de riesgos como un proceso sistemático de identificación, análisis, evaluación, valoración, y tratamiento de los riesgos; aplicando los controles necesarios para evitar, reducir, compartir, transferir o asumir el riesgo con medidas preventivas o correctivas que deberá generar como resultado minimizar pérdidas, maximizar rendimientos y cuidar la seguridad del paciente.

2. MARCO NORMATIVO

- Estándares ISO 27001:2013
- El Ministerio/Fondo Único de Tecnologías de la Información y las Comunicaciones , a través de su Modelo Integrado de Gestión, se compromete a mantener una cultura de la gestión del riesgo asociados con la responsabilidad de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector TIC, regulando los riesgos de los procesos y proyectos luchando continuamente contra la corrupción, mediante mecanismos, sistemas y controles enfocados a la prevención y detección de hechos asociados a este fenómeno y fortaleciendo las medidas de control y la eficiencia a lo largo del ciclo de vida del proyecto para optimizar de manera continua y oportuna la respuesta a los riesgos además de los de seguridad y privacidad de la Información y Seguridad Digital de manera Integral. La política identifica las opciones para tratar y manejar los riesgos basados en su valoración, permiten tomar decisiones adecuadas y fijar los lineamientos para administración de los mismos; a su vez, transmiten la posición de la dirección y establecen las guías de acción necesarias a todos los colaboradores del Ministerio TIC. Se deben tener en cuenta algunas de las siguientes opciones, las cuales pueden considerarse independientemente, interrelacionadas o en conjunto:
  • Evitar: es eliminar la probabilidad de ocurrencia o disminuir totalmente el impacto, lo que requiere la eliminación de la actividad o fuente de riesgo, eliminar la exposición y su expresión máxima es dejar una actividad. Por ejemplo, para evitar perdida de documentación se prohíbe el ingreso a un área.
  • Prevenir: corresponde al área de planeación, esto es, planear estrategias conducentes a que el evento no ocurra o que disminuya su probabilidad. Un ejemplo de ello son las inspecciones el mantenimiento preventivo, las políticas de seguridad o las revisiones periódicas a los procesos
  • Reducir o mitigar: corresponde a la protección en el momento en que se presenta el riesgo se encuentra en esta categoría los planes de emergencia planes de continencia equipos de protección personal, ambiental, de acceso mantener copias de respaldo
  • Dispersar: es dividir una actividad en diferentes componentes operativos, de manera que las actividades no se concentren en un mismo sitio o bajo una sola responsabilidad. Este es el caso de los contratos de suministro de partes, la ubicación de nodos, plantas alternas, equipos paralelos, contratar obras por tramos
  • Compartir: es involucrar a un tercero para que responda en todo o en parte por el riesgo que genera una actividad. Dentro de los mecanismos de transferencia se encuentran los siguientes: contratos de seguro, transferencia explicita por medio de cláusulas contractuales, derivados financieros.Los riesgos detectados deberán ser analizados de tal forma que se pueda determinar cuál va a ser su tratamiento. Así mismo, teniendo en cuenta lo expuesto en la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información (MinTIC:2016)1 , las “(…) no se debe olvidar que dentro del análisis de los controles se debe tener en cuenta al dueño del riesgo (dueño del proceso), ya que la definición de los controles es el resultado de los análisis realizados a través del

seguimiento y aplicación de los pasos descritos anteriormente en el tratamiento del riesgo y los cuales deben tener el concurso de todos los interesados"(…)

3. OBJETIVO

Vincular la identificación y análisis de riesgos en la entidad hacia los temas de Seguridad de la Información con la metodología de riesgos del DAFP.

4. EJECUCION DEL PLAN

La gestión de riesgos de seguridad de la información y su tratamiento, podrá será aplicada sobre cualquier proceso de la Corporación Social de Cundinamarca, a cualquier sistema de información o aspecto particular de control de la Entidad, a través de los principios básicos y metodológicos para la administración de los riesgos de seguridad de la información, así como las técnicas, actividades y formularios que permitan y faciliten el desarrollo de las etapas de reconocimiento del contexto, identificación de los riesgos de seguridad de la información , análisis y evaluación, opciones de tratamiento o manejo del riesgo según la zona de riesgo; incluye además pautas y recomendaciones para su seguimiento, monitoreo y evaluación

a. ESTABLECER EL CONTEXTO PARA LA GESTIÓN DEL RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Corresponde a una visión general de los riesgos que pueden afectar el cumplimiento de los objetivos en este caso para la seguridad y privacidad de la información se analiza información de las estructuras organizacionales, del modelo de operación por procesos, del cumplimiento de planes y programas, de los recursos físicos y tecnológicos.

Para establecer el contexto para la gestión del riesgo es necesario definir los criterios de riesgos de seguridad y privacidad de la información:

b. CRITERIOS DE EVALAUCION DEL RIESGO:

Para la Evaluación de los riesgos con el fin de determinar la seguridad de la información de la organización se tienen en cuenta los siguientes aspectos:

- El valor estratégico del proceso de información para la entidad.
- La criticidad de los activos de información involucrados en el proceso.
- Los requisitos legales y reglamentarios, así como las obligaciones contractuales
- La importancia de la disponibilidad de la, confidencialidad, e integridad de la información para las operaciones y la entidad.
- Las expectativas y percepciones de las partes interesadas y las consecuencias negativas para el buen nombre y la reputación de la entidad.

c. CRITERIOS DE IMPACTO:

Los criterios de impacto del riesgo se especifican en términos del grado de daño o de los costos para la entidad, causados por un evento de seguridad de la información, y se consideran los siguientes aspectos:

1. Nivel de clasificación de los activos de la información de los procesos
2. Brechas en la seguridad de la información (ejemplo: perdida de confidencialidad, integridad y disponibilidad de la información)
3. Operaciones deterioradas
4. Perdida del negocio y del valor financiero
5. Alteración de planes y fechas limites
6. Daños para la reputación
7. Incumplimiento de los requisitos legales

d. CRITERIOS DE ACEPTACIÓN DEL RIESGO

Los criterios de aceptación del riesgo pueden definir de acuerdo con la expectativa de duración que se tenga del riesgo y se podrían considerar los siguientes elementos.

1. Criterios del negocio
2. Aspectos legales y reglamentarios
3. Operacionales
4. Tecnológicos
5. Fianzas
6. Factores sociales y humanitarios

La Corporación Social de Cundinamarca cuenta con los siguientes criterios.

- El riesgo inherente es importante porque la diferencia entre este y el riesgo residual proporciona una medida de la necesidad y la eficacia del tratamiento del riesgo actual. Si la diferencia entre el riesgo inherente y el residual es pequeña, el riesgo no necesita ser tratado o el tratamiento es ineficaz.

- Para calcular el riesgo residual es necesario primero evaluar la efectividad de los controles.

- Los responsables de los procesos, son los propietarios de sus riesgos y les corresponde rendir cuentas sobre su gestión, ellos deben realizar la medición de sus controles en términos de eficiencia, eficacia y efectividad para determinar la pertinencia, la necesidad de ajuste o modificación en caso de presentarse.

- Corresponde a todos los responsables de procesos y líderes de proyectos identificar e implementar acciones preventivas cuando el cálculo del riesgo residual los ubique en zona de riesgo inaceptable o importante.

- Cuando el cálculo del riesgo residual los ubique en zona de riesgo aceptable, tolerable o moderado, no requerirá implementar acciones preventivas, sin embargo, se debe continuar con la aplicación de los controles establecidos y el monitoreo permanente del comportamiento del riesgo.

- Cuando el impacto de la materialización del riesgo residual sea mayor o catastrófica, los responsables de los procesos y proyectos deben establecer planes de contingencia que permitan proteger la institucionalidad en caso de su ocurrencia.

CONTEXTO

EVENTO (RIESGO)		CAUSA				Consecuencia (Lo que podría ocasionar)
		CONTEXTO INTERNO		CONTEXTO EXTERNO		
N° Riesgo	Puede suceder ...	Tipo	Debido a..	Tipo	Debido a...	
R1	Interrupción de la operación del sistema de información Novasoft	Máquinas-equipos	Caída del enlace hacia el servidor Novasoft, Obsolescencia tecnológica (ej:servidores) Falta de mantenimiento a los equipos.	Tecnológicos	Caída del fluido eléctrico, falta de equipos de refrigeración y/o inconvenientes por humedad, accesos no autorizados, No disponibilidad del servicio por parte de proveedor.	No continuidad en el proceso de atención A los afiliados dse la csc y procesos de apoyo a través Del Sistema de información novasoft Pérdida de la información durante la contingencia Módulos de novasoft Pérdidas financieras . Posible ocurrencia de eventos adversos

e. VALORACION DEL RIESGO

Para la identificación y evaluación se toma como base el contexto estratégico que reconoce las situaciones de riesgo de origen interno y externo para la entidad; luego se procede a la identificación de los riesgos, reconociendo variables como agentes generadores, causas, efectos entre otros, para realizar posteriormente la calificación de los riesgos.
A partir de los factores internos y externos, se determinan los agentes generadores del riesgo de seguridad y privacidad de la información sus causas y sus consecuencias: pérdida, daño, perjuicio o detrimento.

Para los riesgos de seguridad y privacidad se debe tener en cuenta:

f. IDENTIFICACIÓN DEL RIESGO

Para la evaluación de riesgos de seguridad de la información en primer lugar se deberán identificar los activos de información por proceso en evaluación. Los **activos de información** se clasifican en dos tipos:

a) **Primarios**:

a. Procesos o subprocesos y actividades del Negocio: procesos cuya pérdida o degradación hacen imposible llevar a cabo la misión de la organización; procesos que contienen procesos secretos o que implican tecnología propietaria; procesos que, si se modifican, pueden afectar de manera muy significativa el cumplimiento de la misión de la organización; procesos que son necesarios para el cumplimiento de los requisitos contractuales, legales o reglamentarios.

b. Información: información vital para la ejecución de la misión o el negocio de la organización; información personal que se puede definir específicamente en el sentido de las leyes relacionadas con la privacidad; información estratégica que se requiere para alcanzar los objetivos determinados por las orientaciones estratégicas; información del alto costo cuya recolección, almacenamiento, procesamiento y transmisión exigen un largo periodo de tiempo y/o implican un alto costo de adquisición, etc.

c. Actividades y procesos de negocio: que tienen que ver con propiedad intelectual, los que si se degradan hacen imposible la ejecución de las tareas de la empresa, los necesarios para el cumplimiento legal o contractual, etc.

b) **De Soporte**

a. **Hardware**: Consta de todos los elementos físicos que dan soporte a los procesos (PC, portátiles, servidores, impresoras, discos, documentos en papel, etc.).
b. **Software**: Consiste en todos los programas que contribuyen al funcionamiento de un conjunto de procesamiento de datos (sistemas operativos, paquetes de software o estándar, aplicaciones, mantenimiento o administración, etc.)

c. **Redes**: Consiste en todos los dispositivos de telecomunicaciones utilizados para interconectar varios computadores remotos físicamente o los elementos de un sistema de información
(conmutadores, cableado, puntos de acceso, etc.)
d. **Personal**: Consiste en todos los grupos de personas involucradas en el sistema de información
(usuarios, desarrolladores, responsables, etc.)
e. **Sitio**: Comprende todos los lugares en los cuales se pueden aplicar los medios de seguridad de la organización (Edificios, salas, y sus servicios, etc.)
f. **Estructura organizativa**: responsables, áreas, contratistas, etc.

Después de tener una relación con todos los activos se han de conocer las **amenazas** que pueden causar daños en la información, los procesos y los soportes. La identificación de las amenazas y la valoración de los daños que pueden producir se puede obtener preguntando a los propietarios de los activos, usuarios, expertos, etc.

Posterior a la identificación del listado de activos, sus amenazas y las medidas que ya se han tomado, a continuación, se revisarán las **vulnerabilidades** que podrían aprovechar las amenazas y causar daños a los activos de información de la CSC. Existen distintos métodos para analizar amenazas, por ejemplo:

- Entrevistas con líderes de procesos y usuarios
- Inspección física
- Uso de las herramientas para el escaneo automatizado

Para cada una de las **amenazas** analizaremos las **vulnerabilidades** (debilidades) que podrían ser explotadas.

Finalmente se identificarán las **consecuencias**, es decir, cómo estas amenazas y vulnerabilidades podrían afectar la confidencialidad, integridad y disponibilidad de los activos de información.

g. IDENTIFICACIÓN DE LOS ACTIVOS

Según la norma ISO 27000:2013 un activo es todo aquello que tiene valor para la entidad y que, por lo tanto, requiere de protección. La identificación de activos se debería llevar acabo con un nivel adecuado de detalle que proporcione información suficiente para la valoración del riesgo.

h. IDENTIFICACIÓN DE LAS AMENAZAS

Una amenaza tiene el potencial de causar daños a activos tales como información, procesos y sistemas y, por lo tanto, a la entidad. Las amenazas pueden ser de origen natural o humano y podrían ser accidentales o deliberadas es recomendable identificar todos los orígenes de las amenazas accidentales como deliberadas. Las amenazas se deberían identificar genéricamente y por tipo (ej. Acciones no autorizadas, daño físico, fallas técnicas) Algunas amenazas pueden afectar a más de un activo y en tales casos pueden causar diferentes impactos dependiendo de los activos que se vean afectados.

i. IDENTIFICACIÓN DE LAS VULNERABILIDADES

Para realizar una correcta identificación de vulnerabilidades es necesario conocer la lista de amenazas comunes, la lista de inventario de activos y el listado de controles existentes. Se pueden identificar vulnerabilidades en las siguientes áreas:

- Organización.
- Procesos y procedimientos.
- Rutinas de gestión.
- Personal
- Ambiente físico
- Configuración del sistema de información.
- Hardware, software y equipos de comunicaciones.
- Dependencia de partes externas

j. IDENTIFICACIÓN DE LAS CONSECUENCIAS

Para la identificación de las consecuencias es necesario tener:
Lista de activos de información y su relación con cada proceso de la entidad.
Lista de las amenazas y vulnerabilidades con respecto a los activos y su pertinencia.

NOTA: Una consecuencia puede ser la pérdida de la eficacia, condiciones adversas de operación, pérdida del negocio, reputación, daño, entre otros.

Se deben identificar las consecuencias operativas de los escenarios de incidentes en términos de:

- Tiempo de investigación y reparación
- Pérdida de tiempo operacional
- Pérdida de oportunidad
- Salud y seguridad

- Costo financiero
- Imagen, reputación y buen nombre

5. ANALISIS DEL RIESGO

La estimación del riesgo busca establecer la *probabilidad* de ocurrencia de los riesgos y el *impacto* de sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo, su priorización y estrategia de tratamiento de estos. El objetivo de esta etapa es el de establecer una valoración y priorización de los riesgos.

Para adelantar la estimación del riesgo se deben considerar los siguientes aspectos:

- **Probabilidad**: La posibilidad de ocurrencia del riesgo, representa el número de veces que el riesgo se ha presentado en un determinado tiempo o pudiese presentarse.
- **Impacto**: Hace referencia a las consecuencias que puede ocasionar a la Agencia la materialización del riesgo; se refiere a la magnitud de sus efectos.

Se sugiere realizar este análisis con todas o las personas que más conozcan del proceso, y que por sus conocimientos o experiencia puedan determinar el impacto y la probabilidad del riesgo de acuerdo con los rangos señalados en las tablas que se muestran más adelante.

Como criterios para la estimación del riesgo desde el enfoque de impacto y consecuencias se podrán tener en cuenta: pérdidas financieras, costes de reparación o sustitución, interrupción del servicio, disminución del rendimiento, infracciones legales, pérdida de ventaja competitiva, daños personales, entre otros.

Además de medir las posibles consecuencias se deberán analizar o estimar la probabilidad de ocurrencia de situaciones que generen impactos sobre los activos de información o la operación del negocio.

PROBABILIDAD			
Concepto	**Valor**	**Descripción**	**Frecuencia**
Raro	1	El evento puede ocurrir sólo en circunstancias excepcionales.	No se ha presentado en los últimos 5 años

Improbable	2	Es muy poco factible que el evento se presente.	Al menos de 1 vez en Los últimos 5 años.
Posible	3	El evento podría ocurrir en algún momento.	Al menos de 1 vez en Los últimos 2 años.
Probable	4	El evento probablemente ocurrirá en la mayoría de las circunstancias,	Al menos de 1 vez en El último año.
Casi Certeza	5	Se espera que ocurra en la mayoría de las circunstancias	Más de 1 vez al año.

Adoptado para la CSC de la Guía de Riesgos DAFP.2013

IMPACTO		
Concepto	**Valor**	**Descripción**
Insignificante	1	La materialización del riesgo **puede ser controlado** por los participantes del proceso, y **no afecta los objetivos del proceso**.
Menor	6	La materialización del riesgo ocasiona **pequeñas demoras** en el cumplimiento de las actividades del proceso, y **no afecta significativamente el cumplimiento de los objetivos** de la Agencia. Tiene un impacto bajo en los procesos de otras áreas de la Agencia.
Moderado	7	La materialización del riesgo **demora el cumplimiento de los objetivos del proceso,** y tiene un **impacto moderado en los procesos de otras áreas** de la Agencia. Puede además causar un deterioro en el desarrollo del proceso dificultando o retrasando el cumplimiento de sus objetivos, impidiendo que éste se desarrolle en forma normal.
Mayor	11	La materialización del riesgo **retrasa el cumplimiento de los objetivos de la ANI** y tiene un **impacto significativo en la imagen pública** de la Agencia y/o de la Nación. Puede además generar impactos en: la industria; sectores económicos, el cumplimiento de acuerdos y obligaciones legales nacionales e internacionales; multas y las finanzas públicas; entre otras
Catastrófico	13	La materialización del riesgo **imposibilita el cumplimiento de los objetivos de la Agencia**, tiene un **impacto catastrófico en la imagen pública de la Agencia y/o de la Nación**. Puede además generar impactos en: sectores económicos, los mercados; la industria, el cumplimiento de acuerdos y obligaciones legales nacionales e internacionales; multas y las finanzas públicas; entre otras.

Adoptado para la CSC de la Guía de Riesgos DAFP.2013

6. EVALUACION DEL RIESGO

Una vez se valoran los impactos, la probabilidad y las consecuencias de los escenarios de incidentes sobre los activos de información, se obtendrán los niveles de riesgo, para los cuales se deberán comparar frente a los criterios básicos del contexto, para una adecuada y pertinente toma de decisiones basada en riesgos de seguridad de la información y en beneficio de reducir su impacto a la Alta Entidad.

			GRAVEDAD (IMPACTO)				
			MUY BAJO 1	BAJO 2	MEDIO 3	ALTO 4	MUY ALTO 5
PROBABILIDAD	MUY ALTA	5	5	10	15	20	25
	ALTA	4	4	8	12	16	20
	MEDIA	3	3	6	9	12	15
	BAJA	2	2	4	6	8	12
	MUY BAJA	1	1	2	3	4	5

	Riesgo extremo. Requiere medidas preventivas urgentes
	Riesgo alto. Medidas preventivas obligatorias. Se deben controlar fuertemente llas variables de riesgo .
	Riesgo moderado. Estudiar económicamente ai es posible introducir medidas preventivas para reducir el nivel de riesgo. Si no fuera posible, mantener las variables controladas.
	Riesgo bajo.Se vigilará aunque no requiere medidas preventivas de partida.

Esquema general de matriz para evaluar el riesgo institucional .

7. TRATAMIENTO DEL RIESGO

Como resultado de la etapa de evaluación del riesgo tendremos una lista ordenada de riesgos o una matriz con la identificación de los niveles de riesgo de acuerdo con la zona de ubicación, por tanto, se deberá elegir la(s) estrategia(s) de tratamiento del riesgo en virtud de su valoración y de los criterios establecidos en el contexto de gestión de riesgos.

De acuerdo con el nivel evaluación de los riesgos, se deberá seleccionar la opción de tratamiento adecuada por cada uno de los riesgos identificados; el costo/beneficio del tratamiento deberá ser un factor de decisión relevante para la decisión.

COSTO - BENEFICIO	OPCION DE TRATAMIENTO
El nivel de riesgo está muy alejado del nivel de tolerancia, su costo y tiempo del tratamiento es muy superior a los beneficios	**Evitar** el riesgo, su propósito es no proceder con la actividad o la acción que da origen al riesgo (ejemplo, dejando de realizar una actividad, tomar otra alternativa, etc.)
El costo del tratamiento por parte de terceros (internos o externos) es más beneficioso que el tratamiento directo	**Transferir o compartir** el riesgo, entregando la gestión del riesgo a un tercero (ejemplo, contratando un seguro o subcontratando el servicio).
El costo y el tiempo del tratamiento es adecuado a los beneficios	**Reducir o Mitigar** el riesgo, seleccionando e implementando los controles o medidas adecuadas que logren que se reduzca la probabilidad o el impacto
La implementación de medidas de control adicionales no generará valor agregado para reducir niveles de ocurrencia o de impacto.	**Retener o aceptar** el riesgo, no se tomará la decisión de implementar medidas de control adicionales. Monitorizarlo para confirmar que no se incrementa

El resultado de esta fase se concreta en un plan de tratamiento de riesgos, es decir, la selección y justificación de una o varias opciones para cada riesgo identificado, que permitan establecer la relación de riesgos residuales, es decir, aquellos que aún siguen existiendo a pesar de las medidas tomadas.

Nota: Será conveniente que para la selección de los controles se consideren posibles restricciones o limitantes que impidan su elección tales como: restricciones de tiempo, financieras, técnicas, operativas, culturales, éticas,

ambientales, legales, uso, de personal o las restricciones para la integración de controles nuevos y existentes.

a. DECLARACION DE APLICABILIDAD

La Declaración de Aplicabilidad, por sus siglas en ingles Statement of Applicability (SoA), es un elemento fundamental para la implementación del Modelo de Seguridad y Privacidad de la Información.
La declaración de aplicabilidad se debe realizar luego del tratamiento de riesgos, y a su vez es la actividad posterior a la evaluación de riesgos.

La declaración de aplicabilidad debe indicar si los objetivos de control y los controles se encuentran implementados y en operación, los que se hayan descartado, de igual manera se debe justificar por qué algunas medidas han sido excluidas (las innecesarias y la razón del por qué no son requerías por la Entidad).

		Objetivo de control o control seleccionado Si/No	Razón de la Selección	Objetivo de control o control Implementado Si/No	Justificación de exclusión	Referencia	Aprobado por la alta dirección Firma director de la entidad
Dominio	A.5 Políticas de seguridad de la información						
Objetivo de control	A. 5.1 Directrices establecidas por la dirección para la seguridad de la información						
Control	A. 5.1.1 Políticas para la seguridad de la información						
Control	A. 5.1.2 Revisión de las políticas para seguridad de la información						

8. COMUNICACIÓN Y CONSULTA.

La comunicación es muy importante porque permite que todas las partes interesadas emitan su propio juicio sobre los riesgos; es importante tener en cuenta que las percepciones variarán en cuanto a los valores, necesidades, suposiciones, conceptos y preocupaciones de los interesados.

9. MONITOREO DE REVISION

El monitoreo es esencial para asegurar que las acciones se están llevando a cabo y evaluar la eficiencia en su implementación:

En primera instancia el seguimiento se debe llevar a cabo por el responsable del proceso (Director, Jefe, Líder). Segundo momento de seguimiento por parte del Subgerente (Procesos asistenciales, procesos administrativos y financiero).

La Oficina de Control Interno comunicará y presentará luego del seguimiento y evaluación, los resultados y propuestas de mejoramiento y tratamiento a las situaciones detectadas

Por lo menos cada semestre, cada responsable de proceso realizará una autoevaluación a la gestión del riesgo, determinando la efectividad de sus controles para minimizar el riesgo, a su vez la Oficina de Control Interno realizará su propio informe de evaluación de riesgos y controles de segundo orden.

10. MECANISMO DE SEGUIMIENTO Y VERIFICACION

Los atributos establecidos para valorar el desempeño de la gestión de riesgos es una parte de la evaluación global de la institución y de la medición del desempeño de las áreas y de las personas.

Las valoraciones integrales de toda la institución y particulares por proceso, proyecto o estrategia correspondiente a la disminución del nivel de vulnerabilidad, por lo que se tiene el siguiente indicador:

Índice de riesgo residual por proceso: Expresado como proporción o porcentaje de la reducción de los valores estimados de probabilidad e impacto, luego de aplicar las medidas de gestión de riesgos para cada proceso o proyecto.

Formula:

RIESGO INHERENTE – **EFECTIVIDAD GESTIÓN DEL RIESGO = RIESGO RESIDUAL**

RIESGO RESIDUAL

RIESGO CONTROLADO

Meta: Índice de riesgo residual por proceso: Menor de 25

Por lo menos cada semestre, cada responsable de proceso realizará una autoevaluación a la gestión del riesgo, determinando la efectividad de sus controles para minimizar el riesgo, a su vez la Oficina de Control Interno realizará su propio informe de evaluación de riesgos y controles de segundo orden.

Se tiene dispuesto en la intranet el Mapa de los riesgos tanto clínicos como administrativos segregados por procesos y responsables para su debida consulta y gestión, este engloba la totalidad de los riesgos a gestionar en una tabla de Excel debidamente clasificados y valorados.

a. NIVEL DE MADUREZ DEL RIESGO

Herramienta utilizada para capturar y evaluar las prácticas de riesgos de la institución y proporcionar realimentación en forma de una calificación de Madurez de la Gestión de Riesgos. El índice se calcula en base a preguntas relacionadas con las actuales prácticas de gestión de riesgos, la estructura de gobierno corporativo y el proceso de toma de decisiones de la empresa.

Meta: Nivel de Madurez de la Gestión del Riesgo: Mayor de 3.0.

11. CRONOGRAMA

Actividades	2021			
	1 Trimestre	2 Trimestre	3 Trimestre	4 Trimestre
Identificar los activos de información de la entidad para gestionar los riesgos de seguridad de la información.				
Identificar las amenazas y la valoración de los daños que pueden producir.				
Revisar las vulnerabilidades que podrían aprovechar las amenazas y causar daños a los activos de información de la CSC.				
las consecuencias operativas de los escenarios de incidentes en términos de: • Tiempo de investigación y reparación •Pérdida de tiempo operacional •Pérdida de oportunidad • Salud y seguridad				
Generar la matriz integral de riesgos, con sus respectivos análisis, evaluación y tratamiento del riesgo.				
Socializar y comprometer a los funcionarios de CSC, en la formulación e implementación de controles y acciones encaminadas mitigar y administrar los riesgos.				
Establecer, mediante una adecuada administración del riesgo, una base confiable para la toma de decisiones y la planificación institucional				

12. BIBLIOGRAFIA

Guía 7 gestiones de riegos. Modelo de Seguridad y Privacidad de la Información. Ministerio de Tecnologías de la Información y las Comunicaciones, estrategia de Gobierno en Línea.

Guía 8 controles de seguridad y privacidad de la información. Modelo de Seguridad y Privacidad de la Información. Ministerio de Tecnologías de la Información y las Comunicaciones, estrategia de Gobierno en Línea.