1. OBJETIVO

Establece la metodología que permita la identificación y gestión de los riesgos y las oportunidades en la ejecución de los procesos, la prestación de los servicios y la seguridad de la información en el marco del Sistema Integrado de Gestión facilitando definir acciones para minimizar los niveles de riesgo, la vulnerabilidad y la atención de las oportunidades que se consideren.

2. ALCANCE

El presente documento contempla las actividades de identificación, clasificación, análisis, evaluación, valoración y monitoreo de riesgos, así como la identificación y evaluación de las oportunidades, y es aplicado por todos los procesos de SysCafé.

El procedimiento abarca los riesgos de los procesos, gestión de servicios y seguridad de la información asociados a los procesos institucionales y es el mecanismo por el cual se hace operativa la declaración de las intenciones generales de la organización respecto a su gestión.

3. RESPONSABLES

- Líderes de Proceso y Área de SysCafé

4. TÉRMINOS Y DEFINICIONES

Activo: Se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo.

Amenaza: Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización.

Análisis del riesgo: Proceso sistemático para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

Ciberseguridad: Es el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el ciberespacio.

Consecuencia: Resultado o impacto de un evento que afecta a los objetivos.

Contexto externo: Ambiente externo en el cual la organización busca alcanzar sus objetivos.

Contexto interno: Ambiente interno en el cual la organización busca alcanzar sus objetivos.

Control: Medida que modifica al riesgo, medios para gestionar el riesgo e incluye políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal.

Criterios del riesgo: Términos de referencia frente a los cuales se evalúa la importancia de un riesgo.

Evaluación del riesgo: Proceso de comparación de los resultados del análisis del riesgo, con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

Evitar el riesgo: Decisión de no involucrarse o de retirarse de una situación de riesgo.

Evento: Presencia o cambio de un conjunto particular de circunstancias.

Fuente de riesgo: Elemento que solo o en combinación tiene el potencial intrínseco de originar un riesgo.

Frecuencia: Medición del número de ocurrencias por unidad de tiempo.

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

Identificación del riesgo: Proceso para encontrar, reconocer y describir el riesgo.

Incidente de seguridad de la información: Uno o múltiples eventos de seguridad de la información relacionados e identificados que pueden dañar los activos de información de la organización o comprometer sus operaciones.

Inventario de activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten, por tanto, ser protegidos de potenciales riesgos.

Monitoreo: Verificación, supervisión, observación crítica o determinación continúa del Estado con el fin de identificar cambios con respecto al nivel de desempeño exigido o esperado.

Nivel de riesgo: Magnitud de un riesgo o de una combinación de riesgos expresada en términos de la combinación de las consecuencias y su probabilidad.

Organización: Grupo de personas e instalaciones con distribución de responsabilidades, autoridades y relaciones.

Oportunidades: Posibilidad de que un riesgo tenga un efecto positivo. En otras palabras, es un riesgo considerado que puede verse como una oportunidad y generar beneficios o recompensas.

Parte involucrada: Persona u organización que puede afectar, verse afectada o percibirse a sí misma como afectada, por una decisión o una actividad.

Peligro: Una fuente de daño potencial.

Pérdida: Cualquier consecuencia negativa o efecto adverso, financiero u otro.

Perfil del riesgo: Descripción de cualquier conjunto de riesgos.

Política: Intenciones y dirección de una organización como las expresa formalmente su alta dirección.

Política para la gestión del riesgo: Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo.

Posibilidad: Se utiliza como descripción general de la probabilidad o la frecuencia.

Plan para la gestión del riesgo: Esquema dentro del marco de referencia para la gestión del riesgo que especifica el enfoque, los componentes y los recursos de la gestión que se van a aplicar a la gestión del riesgo.

Probabilidad: Oportunidad de que algo suceda.

Proceso para la gestión del riesgo: Aplicación sistemática de las políticas, los procedimientos y las prácticas de gestión a las actividades de comunicación, consulta, establecimiento del contexto, y de identificación, análisis, evaluación, tratamiento, monitoreo y revisión del riesgo.

Propietario del riesgo: Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.

Revisión: Acción que se emprende para determinar la idoneidad, conveniencia y eficacia de la materia en cuestión para lograr los objetivos establecidos.

Reducción del riesgo: Acciones que se toman para disminuir la posibilidad, las consecuencias negativas o ambas, asociadas con un riesgo.

Retención del riesgo: Aceptación del peso de la pérdida o del beneficio de la ganancia proveniente de un riesgo particular.

Riesgo: Efecto de la incertidumbre sobre los objetivos.

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no repudio y confiabilidad pueden estar involucradas.

Tratamiento del riesgo: Proceso para modificar el riesgo.

Valoración del riesgo: Proceso global de identificación del riesgo, análisis del riesgo y evaluación del riesgo.

Vulnerabilidad: Es una debilidad, atributo o falta de control que permitiría o facilitaría la actuación de una amenaza contra información clasificada, los servicios y recursos que la soportan.

5. POLÍTICAS

- Es responsabilidad de los líderes de los procesos la gestión de los riesgos e identificación de oportunidades directamente relacionados con sus procesos.
- Todos los colaboradores que realicen actividades en el marco de los procesos establecidos son responsables de la aplicación de los controles sugeridos con el objeto de minimizar los riesgos.
- Todos los activos de la organización deben ser identificados en relación con los procesos evaluados.
- Para cada uno de los activos identificados debe realizarse la evaluación de riesgos.
- Para cada uno de los riesgos identificados se establecerán los controles existentes o que se deben implementar y deberán ser usados por los directos usuarios de los activos.
- Para cada uno de los riesgos identificados, los responsables de éstos, deben considerar si el riesgo puede verse como una oportunidad y generaría un beneficio para la organización, para esto se deberá consignar su análisis en la matriz de riesgos en el espacio establecido.
- El Monitoreo de los riesgos y los controles establecidos debe hacerse con una frecuencia anual, después de la revisión del Sistema Integrado de Gestión o cuando se presente un cambio significativo en el sistema o los procesos que lo componen.
- Los riesgos identificados y el riesgo residual deben ser aprobados por el Equipo Directivo.
- Es responsabilidad de los líderes de los procesos la gestión de los riesgos directamente relacionados con sus procesos y la aplicación de los controles que se adopten.

6. DESCRIPCIÓN GENERAL

El procedimiento de gestión de riesgo y oportunidades consta de la definición del enfoque organizacional para la valoración del riesgo y su posterior tratamiento y se basa en las directrices sugeridas por la norma ISO 31000.

.

6.1 Identificación de los riesgos por Proceso

De acuerdo con el inventario de activos realizado y su relación con cada uno de los procesos identificados, el responsable del proceso con la colaboración de su área, identifica las vulnerabilidades y amenazas para su proceso, las cuales pueden ser internas o externas, según lo que haya identificado y de acuerdo con el ejemplo de amenazas que se indican en el formato de Matriz de identificación, análisis, evaluación y respuesta a los riesgos (GSI-FRT-006) identificadas en relación con la disponibilidad, confidencialidad e Integridad del Inventario de Activos.

El propósito de la identificación de los riesgos es determinar qué podría suceder que cause una pérdida potencial, y llegar a comprender el cómo, dónde, y por qué podría ocurrir está perdida, las siguientes etapas deberían recolectar datos de entrada para esta actividad.

6.2 Identificación de los riesgos

6.2.1 Identificación de Vulnerabilidades

La vulnerabilidad de un activo es la potencialidad o la posibilidad de que se materialice una amenaza sobre el activo de información.

La vulnerabilidad es una propiedad de la relación entre un activo y una amenaza, aunque se suele vincular más al activo como una no calidad de éste. La vulnerabilidad es un concepto que tiene dos aspectos básicos:

- Forma parte del estado de seguridad del activo en su función-propiedad de mediación entre el activo y la amenaza como acción.

- En su aspecto dinámico, es el mecanismo obligado de conversión de la amenaza en una agresión que se ha materializado sobre el activo de información.

Para realizar una correcta identificación de vulnerabilidades es necesario conocer la lista de amenazas comunes que se indican en el formato de Matriz de identificación, análisis, evaluación y respuesta a los riesgos (GSI-FRT-006). 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.

6.2.2 Identificación de Amenazas

Tomando como base las amenazas que se indican en el formato de Matriz de identificación, análisis, evaluación y respuesta a los riesgos (GSI-FRT-006) se identifican aquellas que están directamente relacionadas con el proceso revisado.

Una amenaza tiene el potencial de causar daños a activos tales como información, procesos y sistemas y, por lo tanto, a la organización. 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.

6.2.3 Identificación de Consecuencias

Se debe para cada vulnerabilidad y amenaza identificada, siendo la consecuencia identificada como:

- Incumplimiento de los Acuerdos de nivel de servicio
- Incumplimiento de los objetivos del proceso
- Pérdidas económicas o del negocio
- Afectación a la reputación
- Demandas civiles o penales

En esta actividad se deben identificar los daños o las consecuencias para la entidad que podrían ser causadas por un escenario de vulnerabilidad o amenaza. Un escenario de vulnerabilidad o amenaza es la descripción de una amenaza que explota una vulnerabilidad determinada o un conjunto de vulnerabilidades relacionadas al activo del proceso evaluado.

6.3 Análisis y Evaluación del Riesgo

Para continuar con el análisis y la evaluación del riesgo depende de la información obtenida en las fases de identificación anteriormente descritas para la Identificación de los riesgos, es por ello por lo que se han establecido los criterios de riesgo definiendo los niveles de riesgo aceptado por la Organización.

De esta forma se deben tener en cuenta los pasos claves en el análisis de riesgos, probabilidad e impacto, definiendo como sigue cada uno de ellos:

Por Probabilidad se entiende la posibilidad de ocurrencia del riesgo; esta puede ser medida con criterios de Frecuencia, si se ha materializado (por ejemplo: número de veces en un tiempo determinado), o de Factibilidad teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque éste no se haya materializado.

Por Impacto se entienden las consecuencias que puede ocasionar a la organización la materialización del riesgo.

De esta forma se procede a hacer la "calificación del riesgo" y se genera en forma automática en la Matriz de identificación, análisis, evaluación y respuesta a los riesgos (GSI-FRT-006) columna N el nivel de **Prioridad** del riesgo. Esta se hace de manera cualitativa generando una comparación

en la cual se presenta el análisis de la probabilidad de ocurrencia del riesgo versus el impacto de este.

Los niveles de Probabilidad e Impacto por medio de los cuales se genera la Prioridad de los riesgos se muestran a continuación:

Figura 2. Evaluación y Clasificación de Riesgos

EVALUACIÓN Y CLASIFICACIÓN DE RIESGOS

Probabilidad		
	Muy Alta	10
	Alta	8
	Moderada	5
	Baja	3
	Muy Baja	1

10	30	50	70	100
8	24	40	64	80
5	15	25	40	50
3	9	15	24	30
1	3	5	8	10

1	3	5	8	10
Muy Bajo	Bajo	Moderado	Alto	Muy Alto
Impacto				

Tabla de Prioridad

Zona de riesgo baja: Asumir el Riesgo	**1 a 7**
Zona de Riesgo moderado: Asumir el riesgo, reducir el riesgo	**8 a 23**
Zona de Riesgo alto: Reducir el riesgo, evitar, compartir o transferir	**24 a 40**
Zona de Riesgo Crítico: Reducir el riesgo, evitar, compartir o transferir	**41 a 100**

De acuerdo con la prioridad identificada, se establece en forma automática en la Matriz de identificación, análisis, evaluación y respuesta a los riesgos (GSI-FRT-006) columna O la **Clasificación de Riesgo**, que está determinada por:

Baja:	**Asumir el Riesgo**
Moderado:	**Asumir el riesgo, reducir el riesgo**
Crítico:	**Reducir el riesgo, evitar, compartir o transferir**
Alto:	**Reducir el riesgo, evitar, compartir o transferir**

6.3.1 Identificación de los Controles existentes

Se debe realizar la identificación de los controles existentes para evitar trabajo o costos innecesarios, por ejemplo, la duplicidad de controles, además de esto mientras se identifican los controles se recomienda hacer una verificación para garantizar que los existentes funcionan correctamente.

Los controles que se planifican para implementar de acuerdo con los planes de implementación de tratamiento de riesgo se deberían considerar en la misma forma que aquellos que ya están implementados.

Se identifica si se tiene o no un control o controles que permitan minimizar el riesgo identificado. Si se tienen controles o no se debe diligenciar la columna P de la Matriz de identificación, análisis, evaluación y respuesta a los riesgos (GSI-FRT-006).

Se debe realizar la descripción del control que se tiene en la actualidad y se está aplicando, por medio del diligenciamiento de la columna Q de la Matriz de identificación, análisis, evaluación y respuesta a los riesgos (GSI-FRT-006).

Se debe indicar el responsable del Control, por medio del diligenciamiento de la columna R de la Matriz de identificación, análisis, evaluación y respuesta a los riesgos (GSI-FRT-006).

6.4 Riesgo Residual

Luego de la evaluación de la clasificación del riesgo (columna O) y de la existencia de controles (columna P) en forma automática se describe la Clasificación del Riesgo Residual (columna S) de la Matriz de identificación, análisis, evaluación y respuesta a los riesgos (GSI-FRT-006).

Para aquellos riesgos que luego del análisis de la clasificación del riesgo y el análisis de controles se encuentren en Clasificación del riesgo Crítico y Alto, es necesario realizar un plan de tratamiento de los riesgos, como se indica a continuación.

6.5 Tratamiento de los Riesgos

Mediante la definición del Plan de Tratamiento de Riesgos se busca mitigar los riesgos presentes en el análisis de riesgos evitando aquellas situaciones que impidan el logro de los objetivos de la organización, esto se logra por medio de la definición e implementación de un control o controles que se adecuen a las necesidades de los procesos, servicios y seguridad de la información.

El Plan de Tratamiento de Riesgo se define con el fin de evaluar las posibles acciones (controles) que se deben tomar para mitigar los riesgos existentes, estas acciones son organizadas en forma de medias de seguridad, y para cada una de ellas se debe definir en un documento que incluya como mínimo el nombre de la medida, objetivo, justificación, responsable de la medida y su prioridad.

Con los resultados de la evaluación se determinan las acciones de tratamiento de riesgo que pueden incluir:

- Cambiar la probabilidad de ocurrencia mediante controles siguiendo los lineamientos de la Norma ISO27001, ISO 9000 e ISO 20000-1
- Cambiar las posibles consecuencias mediante planes de contingencia que mitiguen los impactos y aseguren la continuidad.
- Compartir el riesgo para mitigar impactos con alianzas estratégicas, pólizas u otras acciones

Se debe ingresar el avance del plan(es) de tratamiento de riesgos en la Matriz de Identificación, Análisis, Evaluación y respuesta a los Riesgos.

6.6 Análisis y tratamiento de Oportunidades

6.6.1 Análisis de oportunidades

Una vez realizado el análisis de riesgos por parte de los directos responsables de cada proceso o líderes de proceso, se debe analizar cada uno de los riesgos en procura de generar oportunidades que representen un posible beneficio para la organización, desde el punto de vista del logro de los objetivos del proceso, estratégicos o del sistema de gestión.

En la matriz de riesgos se debe registrar en el campo de proceso el nombre del proceso que está realizando el análisis y se registra en el campo de descripción de la oportunidad una descripción o título que permita identificar la oportunidad. Se debe incluir en el campo de objetivos de la oportunidad, al menos dos objetivos que se busca alcanzar con esta oportunidad.

Los líderes de proceso son los responsables de proponer las iniciativas estratégicas que permitan maximizar las oportunidades identificadas, para esto deben determinar a qué categoría del factor del contexto se encuentra la oportunidad identificada de acuerdo con:

-Factor económico
-Factor social y cultural
-Factor tecnológico
-Factor ecológico y ambiental

Una vez identificado el factor del contexto, se procederá a calificar los criterios de viabilidad y conveniencia que son los que determinará si la oportunidad se puede llevar a cabo o no.

Viabilidad: Es la probabilidad de que se pueda llevar a cabo la oportunidad con éxito. Se relacionará la viabilidad de acuerdo con los siguientes criterios:

CRITERIOS DE VIABILIDAD	
Operativo	Capacidad operativa y de procesos para el desarrollo de la oportunidad
Financiero	Recursos o capacidad financiera para el desarrollo de la oportunidad
Humano	Recursos humanos y conocimientos requeridos para el desarrollo de la

	oportunidad

Conveniencia: Se refiere a la magnitud del impacto interno o externo que se logrará por el aprovechamiento de la oportunidad. Se relacionará la conveniencia de acuerdo con los siguientes criterios:

CRITERIOS DE CONVENIENCIA	
Económico	Impacto positivo en términos económicos para la organización
Reputacional	Impacto positivo en la imagen o reputación de la organización
Procesos	Impacto positivo en la eficiencia y productividad del proceso

6.6.2 Tratamiento de oportunidades

La identificación de las oportunidades que se consoliden en la matriz de riesgos definitiva se presentará a la Alta dirección para su análisis. Luego de la revisión y análisis que efectué la alta dirección se debe registrar su decisión de viabilidad o no de la oportunidad en el campo de Resultado Análisis Alta Dirección.

Si el resultado del análisis de la alta dirección es negativo, se registra y termina el proceso. Si es positivo se debe registrar el proyecto que llevará a cabo la materialización de la oportunidad en el campo de Proyecto Relacionado, y su gestión y seguimiento formará parte del desarrollo normal de dicho proyecto.

6.7 Monitoreo y revisión

Verificar el cumplimiento de las acciones de tratamiento de riesgo según los compromisos establecidos y evaluar el riesgo residual

El Riesgo residual se evalúa teniendo en cuenta la efectividad de los controles establecidos y evaluar si es necesario nuevos activos, nuevas amenazas para los activos existentes y reevaluar los controles

7. CONTROL DE CAMBIOS

CONTROL DE CAMBIOS						
N° Versión	Fecha de cambio			Descripción de cambios	Numeral(es)	Responsable
	Mes	Dia	Año			
1	06	30	2020	Versión inicial del procedimiento	Todo el documento	José Omar Mayorga Pabón, Gerente General
2	02	03	2023	Ajuste del procedimiento de tratamiento del riesgo residual	6.4	Jorge Armando Varela Rendón, Asesor en Gestión Documental
3	01	04	2025	Ajuste del procedimiento	Numeral 5, 6 inciso 6.6, Objetivo y alcance	Diana Karime Cruz Celis Coordinador(a) Infraestructura