FECHA: 18 de agosto de 2022

DIRIGIDO: Líder de Proceso, Carlos Alberto Restrepo Buitrago

ASUNTO: Seguimiento Matriz de Riesgos del proceso de Gestión de Tecnologías de la Información (TI)

La Oficina de Control Interno en su rol de "EVALUACIÓN A LA GESTIÓN DE RIESGOS" tiene contemplado en el Plan de Acción para la vigencia 2022 las siguientes actividades:

- Acompañar a las dependencias en la revisión de los mapas de riesgos de los procedimientos.

- Seguimiento a las dependencias en la revisión de los controles establecidos en los mapas de riesgos.

Para dar cumplimiento a lo anterior se pretende en este seguimiento:

OBJETIVO:

Hacer seguimiento a la matriz de riesgos del proceso de "Gestión de Tecnologías de la Información (TI)" al 16 de agosto de 2022, con el fin de revisar los riesgos identificados con sus causas y efectos; así como la gestión de los controles y la gestión de los riesgos materializados en el proceso.

Nota: Para el seguimiento se tomará como soporte conceptual la "Guía para la administración del riesgo y el diseño de controles en entidades públicas" –Versión 5 de 2020**.** https://www.funcionpublica.gov.co, por lo tanto, todos los conceptos que se transcriban en el presente informe son tomados de la Guía y se referenciará el número de la página facilitar al lector ampliar y afinar los conocimientos.

CRITERIOS:

- Matriz de riesgos del proceso "GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN (TI)" publicada en la intranet de la entidad. Código: IT-C01- Versión: 9 – 07/03/2022 Líder: Profesional Especializado de Sistemas

Objetivo del Proceso: Propender la cofidencialidad, la integridad y disponibilidad de la información, mediante procedimientos, lineamientos y herramientas tecnológicas que garanticen su cumplimiento y respaldo a los demás procesos de la entidad, enfocando los esfuerzos en la generación de cultura y cuidado de la seguridad informática.

Alcance: Inicia con las necesidades manifiestas por el usuario informático, así como las necesidades identificadas a nivel de infraestructura tecnológica y el análisis de resultados de indicadores e informes; y finaliza con la priorización, solución, actualización y/o implementación de proyectos de infraestructura tecnológica y seguimiento a los planes de mejoramiento para garantizar niveles óptimos de satisfacción.

ASPECTOS GENERALES

Matriz de riesgo: Se identificó en el mapa de riesgos del proceso “GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN (TI)” que se tienen identificado seis (6) riesgos a saber:

Riesgos		Descripción del Riesgo	#.Causas	#.Efectos	#.Controles
R1	Suspensión de los servicios tecnológicos ofrecidos por el área de TI	La suspensión y no disponibilidad de los servicios tecnológicos como: Impresión, internet, almacenamiento, gestión documental (Mercurio), Xenco, dominio, control de acceso, antivirus, copias de seguridad, ERP (Sicof), correo y herramientas colaborativas (Office 365), red LAN, red inalámbrica.	6	5	6
R2	Perdida de los activos de información.	La pérdida de la información valiosa de la entidad, entendiendo como activo de información toda aquella información indispensable para la cual la empresa utilizo recursos para su construcción, modificación o ajuste, es decir todo proyecto, informe o producto que se tenga en formato digital y que este almacenado en los servidores de la entidad.	6	3	6
R3	Problemas de seguridad de la información.	Las políticas de seguridad de la información cubren todos los aspectos administrativos, operativos y de control que deben ser cumplidos por los directivos, funcionarios, contratistas o terceros que laboren o tengan relación con la Empresa de Vivienda de Antioquia – VIVA, para conseguir un adecuado nivel de protección de las características de seguridad y calidad de la información relacionada.	4	7	6
R4	Exposición a agentes externos que comprometen los servicios de TI.	La falta de conocimiento sobre los servicios de TI ofrecidos por el área, sumado al mal uso de los mismos, debido al analfabetismo digital y la no aplicación del Manual de Políticas de Seguridad de la información, generan un riesgo latente en el uso de las herramientas y el manejo de la información.	6	7	5

Riesgos		Descripción del Riesgo	#.Causas	#.Efectos	#.Controles
R5	Obsolescencia de los procesos de TI	Los procesos deberán siempre permanecer actualizados bajo el ciclo del mejoramiento continuo, por lo cual deberán serán objeto de cambio según las necesidades del servicio. No reconocer el valor estratégico del área de TI y sus procesos, no homologar la necesidad de los controles implementados y no generar elementos de validación a las decisiones tomadas por el área de TI, genera una cultura de descontento y señalamiento para el proceso.	7	8	5
R6	Sanciones por productores de tecnología.	El no tener control sobre los equipos que se encuentran en la red de la Empresa de Vivienda de Antioquia y el no tener actualizado el inventario de licencias, ni renovar oportunamente las licencias que así lo requieran es un riesgo latente, que puede generar problemas legales.	3	4	7

Nivel del Riesgo Inherente

Para hallar el nivel del riesgo la entidad aplica los siguientes criterios

RIESGOS	Valoración Impacto /	
	Bajo	1
	Moderado	2
	Catastrofico	3

Valoración Probabilidad / Beneficio	
Bajo	1
Medio	2
Alto	3

Valoración Riesgo (es igual a la multiplicación de el valor de impacto por el valor de la probabilidad)	
Bajo	0-3
Medio	4-6
Alto	7-9

Tabla 1

Riesgo	Probabilidad	Impacto	Nivel de Riesgo
1	Alta	Catastrófico	Riesgo Alto
2	Alta	Catastrófico	Riesgo Alto
3	Alta	Catastrófico	Riesgo Alto
4	Media	Catastrófico	Riesgo Tolerable
5	Alta	Catastrófico	Riesgo Alto
6	Media	Moderado	Riesgo Tolerable

Fuente: Tabla adaptada del Mapa de Riesgos del proceso de Gestión de Información y Tecnología Código: CD-C01 - Versión: 09

Se observa en la tabla 1 que de los seis (6) riesgos inherentes identificados se presenta cuatro (4) riesgos con nivel alto (R1, R2, R3, R5) y dos (2) con nivel tolerable (R4, R6). Riesgo residual: *"El resultado de aplicar la efectividad de los controles al riesgo inherente".* Pag.12

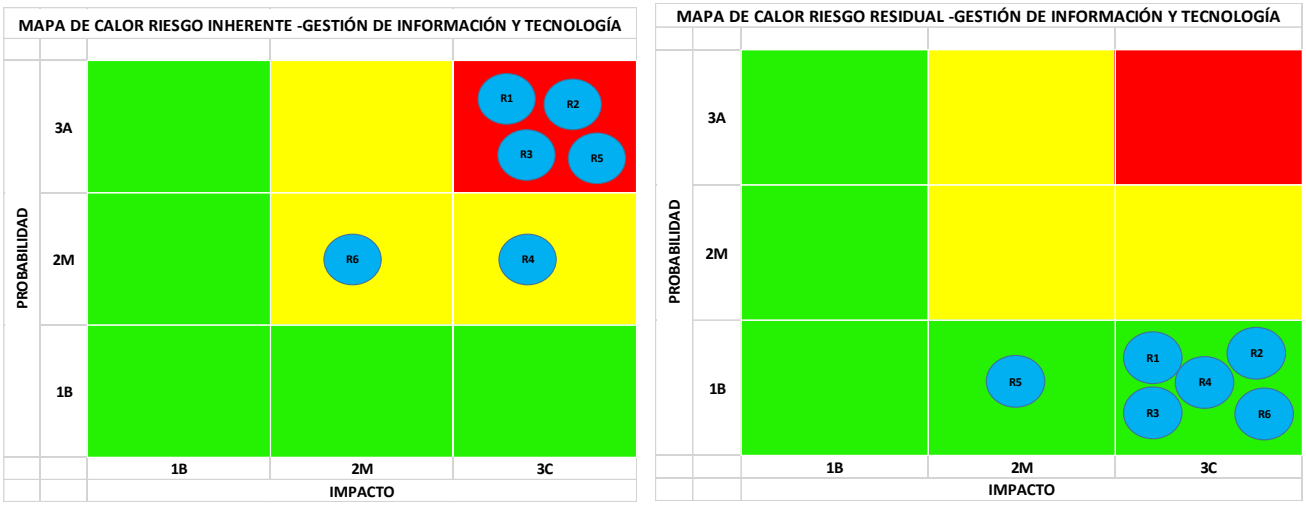
Nivel del Riesgo Residual:

Tabla 2

Riesgo Residual	Probabilidad	Impacto	Nivel de Riesgo
1	Baja	Catastrófico	Riesgo Aceptable
2	Baja	Catastrófico	Riesgo Aceptable
3	Baja	Catastrófico	Riesgo Aceptable
4	Baja	Catastrófico	Riesgo Aceptable
5	Baja	Moderado	Riesgo Aceptable
6	Baja	Catastrófico	Riesgo Aceptable

Fuente: Tabla adaptada del Mapa de Riesgos del proceso de Gestión de Información y Tecnología Código: CD-C01 - Versión: 09

En la tabla 2 se muestra el nivel del riesgo Residual una vez aplicada la efectividad de los controles donde se muestra que todos los riesgos quedaron en nivel aceptable.



Gráficos elaborados por la OCI

Fuente: Mapa de Riesgos del proceso de Gestión de Información y Tecnología Código: CD-C01 - Versión: 09

En los mapas de calor se puede observar gráficamente el comportamiento del riesgo antes y después de evaluados los controles, tal como se muestra en la siguiente tabla:

RESULTADOS DE LA EVALUACIÓN		
Riesgos	**Probabilidad**	**Impacto**
R1	Bajó	Continuó
R2	Bajó	Continuó
R3	Bajó	Continuó
R4	Bajó	Continuó
R5	Bajó	Bajó
R6	Bajó	Subió

No obstante, los resultados de la evaluación, llama la atención que el nivel de los riesgos haya variado y no se encuentre criterios de evaluación de los controles para realizar la evaluación del riesgo residual y hacer que se presente un cambio de posición en el mapa de calor, así mismo, se tienen agrupados los controles, lo cual dificulta

evaluar la efectividad de los mismos y saber si con los controles se logró un impacto en la mitigación de los riesgos.

De acuerdo con el tipo de control se dará el movimiento en el eje de probabilidad o de impacto, es decir si los controles son de tipo preventivo y detectivo mitigarán la probabilidad y si con controles de tipo correctivo mitigarán el impacto. Al aplicar la efectividad de los controles a los riesgos inherentes dará como resultado el riesgo residual.

CONCLUSIÓN (ES):

- Riesgos identificados con sus causas y efectos

Se encuentra debilidad en la redacción de los riesgos con sus causas y efectos, toda vez que los riesgos se suscriben desde el objetivo del proceso; se identifica la causa que pueda materializar el riesgo y su efecto; el control que esté dirigido a la causa y que mitigue el riesgo, lo cual no se evidenció en la identificación de causas y efectos, tales como:

Riesgo		Descripción del Riesgo	Causa	Efecto
R1.	Suspensión de los servicios tecnológicos ofrecidos por el área de TI	La suspensión y no disponibilidad de los servicios tecnológicos como: Impresión, internet, almacenamiento, gestión documental (Mercurio), Xenco, dominio, control de acceso, antivirus, copias de seguridad, ERP (Sicof), correo y herramientas colaborativas (Office 365), red LAN, red inalámbrica.	6. Apagado de la infraestructura de TI por ventana de mantenimiento de componentes y servicios tecnológicos.	3. Parálisis general en las labores de la entidad. 4. Afectación en el cumplimiento de metas. 5. Pérdida de información.
R2	Pérdida de los activos de información.	La pérdida de la información valiosa de la entidad, entendiendo como activo de información toda aquella información indispensable para la cual la empresa utilizó recursos para su construcción, modificación o ajuste, es decir todo proyecto, informe o producto que se tenga en formato digital y que este almacenado en los servidores de la entidad.	4. Desconocimiento sobre la importancia y necesidad de identificar y salvaguardar los activos de información. 5. Falta de divulgación y sensibilización frente al valor de los activos de información.	3. Disminución en la calidad y rendimiento de los procesos dependientes de la información.
R3	Problemas de seguridad de la información.	Las políticas de seguridad de la información cubren todos los aspectos administrativos, operativos y de control que deben ser cumplidos por los directivos, funcionarios, contratistas o terceros que laboren o tengan relación con la Empresa de Vivienda de Antioquia – VIVA, para conseguir un adecuado nivel de protección de las características de seguridad y calidad de la información relacionada.	3. Desconocimiento de la ley para manejo de la información personal Ley 1581 octubre 2012 y el Decreto 1377 de 2013. 4. No contar con un protocolo para la gestión de alertas, eventos e incidentes de seguridad.	4. Suplantación de personas e identidades. 6. Pérdida de información personal protegida por Ley 1581 Octubre 2012 y el Decreto 1377 de 2013. 7. Intrusiones y/o virus informáticos en la red.

Riesgo		Descripción del Riesgo	Causa	Efecto
R4	Exposición a agentes externos que comprometen los servicios de TI.	La falta de conocimiento sobre los servicios de TI ofrecidos por el área, sumado al mal uso de los mismos, debido al analfabetismo digital y la no aplicación del Manual de Políticas de Seguridad de la información, generan un riesgo latente en el uso de las herramientas y el manejo de la información.	1. Analfabetismo digital. 5. Percepción de ser quienes obstaculizan la labor por parte de la comunidad.	1. Mal uso de los recursos de TI. 3. Inconformidad con el servicio. 4. Errores en el manejo de la información y los servicios de TI. 5. Daños en los servicios de TI. 6. Suplantación de personas e identidades.
R5	Obsolescencia de los procesos de TI	Los procesos deberán siempre permanecer actualizados bajo el ciclo del mejoramiento continuo, por lo cual deberán serán objeto de cambio según las necesidades del servicio. No reconocer el valor estratégico del área de TI y sus procesos, no homologar la necesidad de los controles implementados y no generar elementos de validación a las decisiones tomadas por el área de TI, genera una cultura de descontento y señalamiento para el proceso.	1. Ambiente de inconformidad con el personal de TI. 2. Materialización de riesgos administrables. 3. Desmotivación del personal de TI.	6. Resultados no esperados. 7. Incumplimiento de la normatividad. 8. Bajo rendimiento del proceso y sus indicadores.
R6	Sanciones por productores de tecnología.	El no tener control sobre los equipos que se encuentran en la red de la Empresa de Vivienda de Antioquia y el no tener actualizado el inventario de licencias, ni renovar oportunamente las licencias que así lo requieran es un riesgo latente, que puede generar problemas legales.	1. Falta de control en la vigencia de licenciamientos. 2. Descarga e instalación no autorizada de licencias de SW.	3. Prisión.

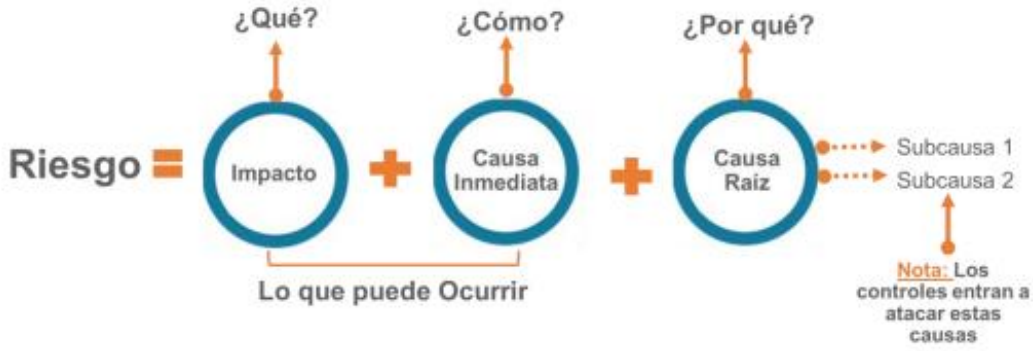
Fuente: Datos tomados del Mapa de Riesgos del proceso de Gestión de Información y Tecnología Código: CD-C01 - Versión: 09

A tener en cuenta:

Para identificar el riesgo "*se debe tener en cuenta actualizar el contexto estratégico en el que opera la entidad, la caracterización de cada proceso que contempla su objetivo y alcance y, también el análisis frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos*". Pág.27

Riesgo*: "Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales. Nota: Los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos."* Pág.12

Descripción del riesgo*: "la descripción del riesgo debe contener todos los detalles que sean necesarios y que sea fácil de entender tanto para el líder del proceso como para personas ajenas al proceso. Se propone una estructura que facilita su redacción y claridad que inicia con la frase POSIBILIDAD DE y se analizan los siguientes aspectos:"*



Fuente: "Guía para la administración del riesgo y el diseño de controles en entidades públicas" – Versión 5 de 2020. https://www.funcionpublica.gov.co. Pág.32

"La anterior estructura evita subjetividad en la redacción y permite entender la forma como se puede manifestar el riesgo, así como sus causas inmediatas y causas principales o raíz, esta es información esencial para la definición de controles en la etapa de valoración del riesgo". Pág.33

Causa: *"Todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo"* Pág.12

Causa inmediata: *"Circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo, las mismas no constituyen la causa principal o base para que se presente el riesgo."* Pág.33

Causa raíz: *es la causa principal o básica, corresponden a las razones por la cuales se puede presentar el riesgo, son la base para la definición de controles en la etapa de valoración del riesgo. Se debe tener en cuenta que para un mismo riesgo puede n existir más de una causa o subcausas que pueden ser analizadas*. Pág.33

Consecuencia*: "Los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas*. Pág.12.

Impacto: *"Las consecuencias que puede ocasionar a la organización la materialización del riesgo.* Pág. 12.

- Gestión de los controles

En la matriz se tiene agrupados los controles para cada riesgo; no se tiene criterios de construcción y ejecución, lo cual permitiría a la OCI evaluar objetivamente la pertinencia y efectividad de los mismos.

Riesgo		Descripción del Riesgo	Controles
R1.	Suspensión de los servicios tecnológicos ofrecidos por el área de TI	La suspensión y no disponibilidad de los servicios tecnológicos como: Impresión, internet, almacenamiento, gestión documental (Mercurio), Xenco, dominio, control de acceso, antivirus, copias de seguridad, ERP (Sicof), correo y herramientas colaborativas (Office 365), red LAN, red inalámbrica.	2. Control de acceso restringido por tarjeta electrónica al cuarto técnico. 3. Copias de la configuración de los equipos para recuperación ante desastres.

Riesgo		Descripción del Riesgo	Controles
R2	Perdida de los activos de información.	La pérdida de la información valiosa de la entidad, entendiendo como activo de información toda aquella información indispensable para la cual la empresa utilizo recursos para su construcción, modificación o ajuste, es decir todo proyecto, informe o producto que se tenga en formato digital y que este almacenado en los servidores de la entidad.	1. Socialización del proceso Administración de Activos de Información y el Manual de políticas de seguridad de la información.
R3	Problemas de seguridad de la información.	Las políticas de seguridad de la información cubren todos los aspectos administrativos, operativos y de control que deben ser cumplidos por los directivos, funcionarios, contratistas o terceros que laboren o tengan relación con la Empresa de Vivienda de Antioquia – VIVA, para conseguir un adecuado nivel de protección de las características de seguridad y calidad de la información relacionada.	1. Apoyo de la alta dirección sobre la implantación y aplicación de las políticas de seguridad de la información.
R4	Exposición a agentes externos que comprometen los servicios de TI.	La falta de conocimiento sobre los servicios de TI ofrecidos por el área, sumado al mal uso de los mismos, debido al analfabetismo digital y la no aplicación del Manual de Políticas de Seguridad de la información, generan un riesgo latente en el uso de las herramientas y el manejo de la información.	3. Generar cultura sobre el buen uso y apropiación de los servicios tecnológicos.
R5	Obsolescencia de los procesos de TI	Los procesos deberán siempre permanecer actualizados bajo el ciclo del mejoramiento continuo, por lo cual deberán serán objeto de cambio según las necesidades del servicio. No reconocer el valor estratégico del área de TI y sus procesos, no homologar la necesidad de los controles implementados y no generar elementos de validación a las decisiones tomadas por el área de TI, genera una cultura de descontento y señalamiento para el proceso.	2. Campañas de divulgación y sensibilización sobre la importancia y valor del proceso de TI. 4. Implementación de herramienta de Mesa de Ayuda para el registro, documentación y control de solicitudes atendidas bajo flujos de trabajo acorde a los procesos.
R6	Sanciones por productores de tecnología.	El no tener control sobre los equipos que se encuentran en la red de la Empresa de Vivienda de Antioquia y el no tener actualizado el inventario de licencias, ni renovar oportunamente las licencias que así lo requieran es un riesgo latente, que puede generar problemas legales.	7. Presentación oportuna del Informe sobre Derechos de Autor.

Fuente: Datos tomados del Mapa de Riesgos del proceso de Gestión de Información y Tecnología Código: CD-C01 - Versión: 09

Definiciones a considerar:

Control: "*Medida que permite reducir o mitigar un riesgo".* Pág.12

Valoración de controles: *"en primer lugar, conceptualmente un control se define como la medida que permite reducir o mitigar el riesgo. Para la valoración de controles se debe tener en cuenta:*

La identificación de controles se debe realizar a cada riesgo a través de las entrevistas con los líderes de procesos o servidores expertos en su quehacer. En este caso sí aplica el criterio experto.

Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo." Pág.43

Para la descripción del control, la Guía presenta la siguiente estructura:

*"**Responsable de ejecutar el control:** identifica el cargo del servidor que ejecuta el control, en caso de que sean controles automáticos se identificará el sistema que realiza la actividad.*

***Acción:** se determina mediante verbos que indican la acción que deben realizar como parte del control.*

***Complemento:** corresponde a los detalles que permiten identificar claramente el objeto del control."* Pág.43

Para definir las tipologías de los controles se debe identificar el ciclo del proceso, es decir:

Entradas: *¿Qué recursos que requiere el proceso?*	***Interrelaciones:*** *¿Cuáles actividades permiten transformar las entradas en productos y servicios?*	***Salidas:*** *¿Qué productos y/o servicios entrega el proceso?*
En esta etapa se identifican controles de tipo ***PREVENTIVOS***	*Es la etapa de ejecución, los controles a identificar son de tipo* ***DETECTIVOS***	*Los controles que se identifican son de tipo* ***CORRECTIVOS***
Preventivos, porque van a las causas del riesgo. Se acciona antes de que inicie la actividad originadora del riesgo, busca establecer las condiciones que aseguren el resultado final esperado. *Atacan la **PROBABILIDAD** de ocurrencia del riesgo.*	*Detectivos, porque permiten detectar que algo ocurre y devuelve el proceso a los controles preventivos. Se acciona durante la ejecución del proceso, detectan riesgos, pero generan reprocesos.* *Atacan la **PROBABILIDAD** de ocurrencia del riesgo.*	*Correctivos, porque es posterior a la entrega del producto o servicio y se ejecuta después de que se materializa el riesgo.* *Atacan el **IMPACTO** frente a la materialización del riesgo.*

Fuente: Tabla adaptada de la Guía para la administración del riesgo y el diseño de controles en entidades públicas" –Versión 5 de 2020. Pág.44

- Gestión de los riesgos materializados en el proceso

El proceso no realiza seguimiento ni cuenta con un instrumento para identificar y registrar los riesgos materializados.

RECOMENDACIÓN (ES):

Durante el seguimiento se evidenció que la entidad, en cabeza de la Oficina de Planeación se encuentra revisando la metodología para la Administración de los riesgos en la entidad con el fin de actualizarla e iniciar la revisión y ajuste a todos los mapas de riesgo de los procesos, por lo tanto, se considera pertinente realizar las siguientes recomendaciones:

- En coordinación con la Dirección de Planeación revisar el mapa de riesgos con el fin de identificar las debilidades encontradas en la construcción inicial.

- Revisar y ajustar la redacción del contenido en cada concepto.

- Revisar los controles y definir los criterios para obtener los nuevos resultados en la matriz de riesgo residual, para lo cual es conveniente separarlos uno a uno.

- Revisar la posibilidad de modificar denominación de la valoración del nivel de severidad del riesgo, toda vez que es igual a la valoración de la probabilidad, es decir que para ambos casos se tiene (Bajo – Medio – Alto), siendo más conveniente utilizar expresiones tales como: Probabilidad, (Alta – Media – Baja) y nivel del riesgo (Alto – Moderado – Bajo o Alto – Tolerable – Aceptable, entre otros).

Ejemplo:

Riesgo	Probabilidad	Impacto	Nivel de Riesgo
1	Alta	Moderado	Riesgo Tolerable
2	Alta	Catastrófico	Riesgo Alto
3	Alta	Moderado	Riesgo Tolerable
4	Alta	Bajo	Riesgo Aceptable

La Oficina de Control Interno, como apoyo a la gestión presenta a continuación algunos elementos que se pueden considerar para definir criterios que garanticen la implementación de controles fuertes y sirvan de análisis y gestión de los riesgos identificados en el proceso de GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN (TI):

✓ Controles de diseño – Le permite saber si el control se ejecuta correctamente (adecuado y fuerte), si presenta falencias o no se ejecuta (regular/débil)

Atributos de Eficacia	TIPO DE CONTROL	40%	Correctivo	Detectivo	Preventivo
	CAL.		10%	15%	25%
	IMPLEMENTACIÓN CÓMO SE EJECUTA?	40%	Manual	Automático	
	CAL.		15%	25%	
Atributos informativos: "*Los atributos informativos solo permiten darle formalidad al control y su fin es el de conocer el entorno del control y complementar el análisis con elementos cualitativos; sin embargo, estos no tienen una incidencia directa en su efectividad.*"	ESTÁ DOCUMENTADO?	5%	Sin documentar	Documentado	
	CAL.		0	1%	
	SE EJECUTA CON ALGUNA FRECUENCIA?	5%	No	Sí	
	CAL.		0	1%	
	TIENE EVIDENCIA?	5%	No	Sí	
	CAL.		0	1%	
	TIENE RESPONSABLE ASOCIADO?	5%	No	Sí	
	CAL.		0	1%	

Nota: Los datos anteriores no son de obligatorio cumplimiento, la entidad es la responsable de establecer e implementar la metodología y definir los criterios

- ✓ Controles de ejecución para evaluar su eficacia – puede validar si se ejecuta correctamente; no se está ejecutando correctamente; se ejecuta ocasionalmente y presenta falencias; o si requiere replantearlos.

SE HAN PRESENTADO EVENTOS?	No	Sí
CAL.	5%	0
SE REGISTRAN LOS RIESGOS MATERIALIZADOS?	No	Sí
CAL.	0%	5%
LA EVIDENCIA ES EFECTIVA?	No	Sí
CAL.	0%	5%
EL DISEÑO DEL CONTROL ES EFECTIVO	No	Sí
CAL.	0%	5%

- ✓ Registro de Eventos

Es importante que se tenga la cultura de llevar a cabo el registro de riesgos materializados porque con ello se permite identificar nuevos factores internos y externos que puedan afectar los objetivos de la entidad y tomar acciones para mitigar el impacto de dicha materialización, se puede considerar el uso de un formato o plantilla que contenga como mínimo:

Nombre del evento:	
Descripción del evento:	
Evidencia:	
Consecuencia del evento:	
Dónde ocurrió el evento:	
Fecha de ocurrencia:	

- ✓ Plan de Acción

Identificación del Riesgo:	
Tipo de Acción:	
Descripción de la acción:	
Fecha de inicio:	
Fecha de Seguimiento:	
Estado del seguimiento:	
Fecha de finalización:	
Responsable del plan de acción:	
Evidencia de la implementación de la acción:	

Para futuros seguimientos por parte de la Oficina de Control Interno es conveniente que se tengan los soportes y documentos que evidencien la gestión y administración de los mapas de riesgo con el propósito de contar con herramientas que permitan una evaluación objetiva y documentada. (Informes, comités primarios, etc.). Lo anterior teniendo en cuenta que se identificaron controles y cambios en las zonas de la matriz de riesgos, pero no se encontró información sobre la implementación y evaluación de los controles.

A nivel general es preciso que se actualice la metodología para la construcción de los mapas de riesgo de la entidad y actualizar la política de su administración, para lo cual se tiene en primera instancia tomar como referente la metodología para la Administración del Riesgo "Guía para la administración del riesgo del Departamento Administrativo de la Función Pública – DAFP", *"Las políticas identifican las opciones para tratar y manejar los riesgos basadas en la valoración de riesgos, permiten tomar decisiones adecuadas y fijar los lineamientos de la Administración del Riesgo, a su vez transmiten la posición de la dirección y establecen las guías de acción necesarias a todos los servidores de la entidad"*

La Oficina de Control Interno invita al equipo de trabajo para participar activamente en el fortalecimiento de la cultura del riesgo a nivel institucional, a través de las capacitaciones, talleres y actividades que se programen, lo cual facilita la comprensión de los conceptos básicos, la estructura de las matrices y la apropiación de la metodología que se implemente en la Entidad.

"La Administración y Gestión de los riesgos, contribuye en los resultados y el cumplimiento de los objetivos de la entidad".

JOSÉ IGNACIO CANO MARÍN
Director de Control Interno

Elaboró: Ana María González O./Profesional Universitario
Revisó: José Ignacio Cano M./Director de Control Interno