VISITA DE: SEGUIMIENTO_X___ AUDITORIA____ ASESORIA __ SOLICITUD INFORMACION____
Asunto: **Seguimiento a las acciones del Mapa de Riesgos de gestion TICS, con corte diciembre de 2022.**
Dependencia, Fecha y Hora**:** **Todas las dependencias – Bucaramanga, Diciembre 15 al 21, 2:00 pm**
Funcionarios que atienden la visita: **Javier Orlando Nuñez Latorre – Asesor de TICS**
Funcionario(s) de Control Interno: **Oscar Leandro Flórez Herrera – Contratista Oficina de Control Interno** **Jorge Vargas Arciniegas – Jefe Oficina de Control Interno**

OBSERVACIONES DEL TEMA DE VISITA

SEGUIMIENTO MAPA DE RIESGOS DE GESTION
PROCESO TICS

INTRODUCCION:

La administración del riesgo es un mecanismo de control de la función pública, que al interactuar con sus diferentes elementos le permite a la Entidad auto controlar aquellos eventos que pueden afectar el cumplimiento de sus objetivos y tiene como fin hacer énfasis en la necesidad imperiosa de que las entidades públicas tengan inmersos en sus procesos los controles necesarios para el logro de los objetivos y metas institucionales. En consecuencia, la práctica administrativa se enmarca dentro del conjunto de actividades de gestión desarrolladas para el cumplimiento de las funciones del Modelo Estándar de Control Interno MECI, para lo cual, se siguen las directrices definidas por el Departamento Administrativo de la Función Pública – DAFP.

El propósito del seguimiento fue la revisión y análisis de riesgos, causas, diseño y efectividad de controles y cumplimiento de acciones en respuesta a los riesgos de corrupción resultado de los doce (12) procesos de la Entidad. Se analizaron los riesgos de corrupción, con corte a 31 de diciembre de 2022. Se tomó como guía la Metodología para la Administración y Control de Riesgos del INVISBU, Versión 1 2019 y lo estipulado en la Guía para la Administra del Riesgo y diseño de Controles en Entidades Públicas Versión 4 Octubre 2018 – DAFP, donde se indica que para la identificación de riesgos de gestión se debe: Identificar el contexto (evaluación de factores internos MEFI – evaluación de factores externos MEFE) y determinar los factores generadores de riesgos, identificar el proceso, el objetivo, establecer las causas, identificar los eventos de riesgo, consecuencias, determinar y adoptar los controles o medidas conducentes a controlar el riesgo inherente, establecer la manera como se realiza el control, el responsable y la periodicidad de su ejecución, monitoreo y revisión.

OBJETIVO: Realizar el seguimiento y control a los mapas de riesgos del proceso TCIS del Instituto de vivienda de interés social y reforma urbana del municipio de Bucaramanga – INVISBU, para asegurar que las acciones en la implementación de los controles se estén llevando a cabo y evaluar la eficiencia en su implementación, para asegurar un efectivo manejo del riesgo.

ALCANCE: La observancia se basó no solo en examinar los avances de las acciones, sino también los soportes que avalan lo consignado en cada uno de los diferentes mapas de riesgos en el proceso de TICS. Seguimiento y control, corte diciembre 2022 y ponderando y calificando los riesgos determinando la nueva matriz de calificación, evaluación y respuesta a los riesgos para esta vigencia.

METODOLOGIA: Esta Oficina realizó una verificación del cumplimiento de las actividades por parte de cada proceso mediante la observación de registros, evidencia objetiva, revisando en forma detallada cada riesgo propuesto, al igual que sus controles y las acciones planteado para su manejo y control.

FUENTES DE INFORMACION: La oficina de Control Interno verifico la matriz del proceso TICS, en forma detallada cada riesgo propuesto, al igual que los controles, acciones encaminadas, probabilidad de ocurrencia, manejo, cronograma, entre otros. Se evaluaron bajo los criterios establecidos por el DAFP, para determinar la valoración de los

riesgos y la nueva matriz a trabajar en la presente vigencia.

MARCO LEGAL:

- Ley 87 de 1993: Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones.
- Ley 489 de 1998: Estatuto Básico de Organización y Funcionamiento de la Administración Pública. Capítulo VI. Sistema Nacional de Control Interno.
- Ley 1437 de 2011: Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo.
- Ley 1474 del 2011: Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
- Ley 1712 de 2014: Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.
- NTC- ISO 31000 Gestión del riesgo. Principios y directrices,
- Guía para la Administración del Riesgo y Diseño de Controles Versión 4, octubre 2018 – Departamento Administrativo de la Función Pública – DAFP.
- Marco internacional para la Práctica Profesional de la Auditoría Interna IIA Norma 2120 Gestión de Riesgos.
- Metodología para la Administración y Control de Riesgos del INVISBU, Versión 1,2019.

DEFINICIONES: Para facilitar la comprensión del presente documento, se definen los siguientes términos:

Administración del riesgo: La capacidad que tiene la Entidad para emprender las acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales, y protegerla por los eventos ocasionados por su ocurrencia.

Amenazas: Son obstáculos externos, situaciones que provienen del entorno y que pueden llegar a afectar negativamente los objetivos de la Entidad.

Causas (factores internos o externos): Son los medios, las circunstancias y agentes generadores de riesgo. Los agentes generadores que se entienden como todos los sujetos u objetos que tienen la capacidad de originar un riesgo.

Explotar el riesgo: Se selecciona esta estrategia cuando la organización desea asegurarse que la oportunidad se haga realidad. Esta estrategia busca eliminar la incertidumbre asociada con un riesgo del lado positivo en particular haciendo que la oportunidad efectivamente se concrete.

Fortalezas: Aspectos positivos y capacidades que le permitirán soportar las adversidades y problemas.

Gestión continúa del riesgo: Aumentar o maximizar la probabilidad y el impacto de los eventos positivos para mejorar los objetivos del proyecto, y disminuir o minimizar la probabilidad y el impacto de los eventos adversos que puedan afectar los objetivos del proyecto.

Impacto: Consecuencias que puede ocasionar a la organización la materialización del riesgo.

Mapa de riesgos: Es la representación final de la probabilidad e impacto de uno o más riesgos frente a un proceso, proyecto o programa.

Oportunidades: Situaciones coyunturales de índole externo que pueden capitalizarse en beneficio propio.

Probabilidad: 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 este no se haya materializado.

Riesgo: Es la posibilidad de que suceda algún evento que tendrá un impacto (positivo o negativo) sobre los objetivos institucionales o del proceso. Se expresa en términos de probabilidad y consecuencias.

Riesgo inherente: Es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.

Riesgo residual: Se define como aquel que permanece después que la dirección desarrolle sus respuestas a los riesgos.

Riesgo como una oportunidad: Implica que su gestión está dirigida a maximizar los resultados que este genera.

DESARROLLO DEL INFORME:

Se identifica la política de Administración de riesgos, compilada en la Guía para la Administración de riesgos del INVISBU, en la cual contiene los lineamientos de la Alta Dirección en la administración de los riesgos de gestión, los objetivos a alcanzar y las estrategias para alcanzar los objetivos, el tratamiento a los riesgos según su evaluación y valoración.

Dichas políticas de administración del riesgo son socializadas en los procesos de inducción y reinducción, garantizando el conocimiento sobre el tratamiento a los riesgos y las medidas que se deben tomar para evitar la materialización de los mismos.

La Entidad revisa una vez al año sus políticas de administración del riesgo y se van actualizando las actividades de mitigación de acuerdo a las situaciones o el contexto estratégico que se presentan al interior y en el entorno de la Entidad.

Para cada uno de los procesos se realizó la identificación de los riesgos, identificando las causas que los generan, teniendo en cuenta las situaciones o factores de riesgo internos y externos, detectando aquellos eventos que generan oportunidades o que afectan negativamente el cumplimiento de la misión y los objetivos del proceso y de la Institución.

La Entidad cuenta con un mapa de riesgos elaborado bajo la metodología del DAFP, el cual contó con la participación de los líderes de procesos y equipos de trabajo. En él se identifican el proceso, el objetivo del proceso, los riesgos relacionados con el objetivo del proceso, o los programas y proyectos institucionales, las causas, consecuencias o efectos, los controles y las acciones para su mitigación.

MAPA DE RIESGOS DE GESTION DEL PROCESO TICS

Una vez confrontados los resultados de la evaluación del riesgo con los controles identificados, se establecieron los siguientes niveles de riesgo, a saber:

La identificación de los riesgos de gestion del proceso TICS.

Identificación del riesgo						
Referencia	Impacto	Causa Inmediata	Causa Raíz	Descripción del Riesgo	Clasificación del Riesgo	Frecuencia con la cual se realiza la actividad
1	Económico y Reputacional	Pérdida de la información	Cumplimiento en la realización de las copias de seguridad	Posibilidad reputacional y económica por pérdida de la información por incumplimiento en la realización de las copias de seguridad	Ejecucion y Administracion de procesos	24
2	Reputacional	Desactualización de la infraestructura técnologia	Falta de recursos financieros. Técnicos y humanos	Posibilidad de pérdida reputacional por la desactualización de la infraestructura técnologia por falta de recursos financieros, técnicos y humanos	Ejecucion y Administracion de procesos	365
3	Económico y Reputacional	Investigaciones, sanciones disciplinarias por organos de control	Incumplimiento de la normatividad relacionadas con TIC	Posibilidad de pérdida reputacional y económica por inventigaciones y sanciones disciplinarias por organos de control por incumplimiento de la normatividad relacionadas con TIC.	Ejecucion y Administracion de procesos	2
4	Reputacional	Desactualización del plan de contingencia	Escases de recursos , financieros, técnicos y humanos	Posibilidad de pérdida reputacional por la desactualización del plan de contingencia por escases de recursos , financieros, técnicos y humanos	Ejecucion y Administracion de procesos	365
5	Económico y Reputacional	Desactualización de licencias de software	Falta de recursos financieros e ineficiente control.	Posibilidad de pérdida reputacional y económica por la desactualización de licenscias de softwafre por recursos financieros e ineficiente control.	Ejecucion y Administracion de procesos	2

A continuación, se relación el análisis del riesgo inherente del proceso TICS.

Análisis del riesgo inherente					
Probabilidad Inherente	%	Criterios de impacto	Impacto Inherente	%	Zona de Riesgo Inherente
Baja	40%	El riesgo afecta la imagen de la entidad internamente, de conocimiento general, nivel interno, de junta dircetiva y accionistas y/o de provedores	**Menor**	40%	**Moderado**
Media	60%	El riesgo afecta la imagen de la entidad internamente, de conocimiento general, nivel interno, de junta dircetiva y accionistas y/o de provedores	**Menor**	40%	**Moderado**

Muy Baja	20%	El riesgo afecta la imagen de la entidad internamente, de conocimiento general, nivel interno, de junta dircetiva y accionistas y/o de provedores	**Menor**	40%	**Bajo**
Media	60%	El riesgo afecta la imagen de la entidad internamente, de conocimiento general, nivel interno, de junta dircetiva y accionistas y/o de provedores	**Menor**	40%	**Moderado**
Muy Baja	20%	El riesgo afecta la imagen de la entidad internamente, de conocimiento general, nivel interno, de junta dircetiva y accionistas y/o de provedores	**Menor**	40%	**Bajo**

Se puede evidenciar que el proceso tiene una valoración del riesgo y valoración de controles:

Evaluación del riesgo - Valoración de los controles									
No. Control	**Descripción del Control**	**Afectación**	**Atributos**						
			Tipo	**Implementación**	**Calificación**	**Documentación**	**Frecuencia**	**Evidencia**
1	Aumentar el número de copias de acuerdo a las necesidades de los sistemas de información, garantizando la seguridad de la información de la entidad y dar uso al sistema de la nube para garantizar la conservación de la información.	Probabilidad	Preventivo	Automático	50%	Documentado	Continua	Con Registro
1	Adoptar una política que permita identificar y mitigar la desactualización técnologica de la entidad, haciendo un análisis dónde se identifique la desactualziación de los equipos técnologicos	Probabilidad	Preventivo	Manual	40%	Documentado	Continua	Con Registro
1	El líder del proceso realiza permanentemente actualización normativa, elabora cronogramas de capacitación para su personal de apoyo e impartida a las démas áreas de la entidad	Probabilidad	Preventivo	Manual	40%	Documentado	Continua	Con Registro
1	El líder del proceso periodicamenre efectua seguimiento al plan de contingencia efectuando las diferentes socializaciones.	Probabilidad	Preventivo	Manual	40%	Documentado	Continua	Con Registro
1	El líder del proceso efectua revisión y seguimiento e informa a las partes interesadas	Probabilidad	Preventivo	Manual	40%	Documentado	Continua	Con Registro

La oficina pudo constatar el plan de acción para este proceso:

Plan de Acción	Responsable
Asignación de recursos presupuestales, y elaboración del plan de actividades de copias de seguridad	Asesor Oficina TIC´s
Hacer un análisis técnologico, determinando necesidades de presupuesto	Asesor Oficina TIC´s
Actualización de normograma y actualización del PETIC, SPI, el de Riesgos y Gobierno Dígital	Asesor Oficina TIC´s
Realziar dos (2) socializaciones y capacitaciones sobre el plan de contingencia	Asesor Oficina TIC´s
Verificación de inventario de licencias y asignación de rescursos financieros	Asesor Oficina TIC´s

CONTROL INTERNO RECOMIENDA:

- Se hace necesario fortalecer los mecanismos que se soportan en las políticas institucionales, para que cada responsable de las correspondientes áreas intensifique e involucren a todos los funcionarios en la participación de un ambiente de compromiso y auténtica conciencia en la búsqueda de acciones encaminadas a la prevención y administración de los Riesgos.

- Los resultados de las acciones mitigadas en el manejo de riesgos se tengan en cuenta dentro de los procesos y procedimientos.

- Fortalecer el aprendizaje en temas de riesgos y crear cultura de autocontrol consciente de la gestión del riesgo y sus controles.

CONCLUSIONES:

Las recomendaciones generales que desde el proceso de Control y Mejoramiento Continuo pueden considerarse para establecer acciones que propicien el mejoramiento continuo de la gestión del riesgo en la entidad, son las siguientes:

- Reforzar los controles previstos en la Matriz de Riesgos de del proceso TICS, en especial los relacionados con el hardware y software, con el fin de evitar la ocurrencia de las consecuencias relacionadas con cada riesgo identificado.

- Es importante poder intensificar los controles establecidos en la matriz con el fin de fortalecerlos y no lograr su materialización.

- Es importante determinar si el proceso requiere incluir o actualizar los riesgos de la matriz con el fin de poder lograr un mayor control sobre el proceso.

NOMBRES	FIRMAS
Elaborado por: **Oscar Leandro Flórez Herrera** **Contratista OCI**	
Revisado por: **VºBº. Jorge Vargas Arciniegas** **Jefe Oficina de Control Interno**	