INTERNO
CONSECUTIVO No 0 0 0 0 0 6 7

3 1 ENE 2024

HORA: 13:56

FIRMA:

CONCEJO DE BELLO
Una decisión para todos

RESOLUCIÓN Nº030
(Del 31 de enero de 2024)

"POR MEDIO DEL CUAL SE ADOPTA EL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD PARA LA VIGENCIA 2024 EN EL CONCEJO MUNICIPAL DE BELLO"

EL PRESIDENTE DEL CONCEJO MUNICIPAL DE BELLO en uso de sus facultades y en especial las conferidas por la Ley 136 de 1994 modificada por la Ley 1551 de 2012, la Ley 1474 de 2011, el Decreto 1078 de 2015, el Decreto 1081 de 2015, el Decreto 1499 de 2017 y,

CONSIDERANDO

Que en virtud de lo previsto en la Ley 1581 de 2012, se protegerán los datos personales de todos los ciudadanos.

Que igualmente en la Ley 1712 de 2014, se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.

Que mediante el Decreto 1078 de 2015, se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

Que en el Decreto 1083 de 2015, se expidió el Decreto Único Reglamentario del Sector de Función Pública", el cual establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran: "11. Gobierno Digital, antes Gobierno en Línea" y "12. Seguridad Digital"

Que en el Decreto 612 de 2018, se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.

Que mediante el Decreto 767 de 2022, se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

Que a través de la Resolución 00500 de 2021 del Ministerio de las TIC, se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de gobierno digital.

Que por lo anterior se hace necesario crear el Plan de Tratamiento de Riesgos de Seguridad — TIC del Concejo Municipal de Bello para la vigencia 2024.

En mérito a lo expuesto se,

RESUELVE

ARTÍCULO PRIMERO. Adoptar el Plan de Tratamiento de Riesgos de Seguridad — TIC para la vigencia 2024 del Concejo Municipal de Bello, el cual hace parte integral del presente acto administrativo.

ARTÍCULO SEGUNDO. El presente Plan será de carácter obligatorio y deberá utilizarse de manera permanente en todas las dependencias de la Corporación, con el objeto de mantener los estándares de calidad, seguridad y transparencia.

ARTÍCULO TERCERO. El seguimiento y control de las acciones contempladas en el Plan, le corresponde al Secretario General de la Corporación o quien haga sus veces.

ARTÍCULO CUARTO. La verificación de la elaboración, publicación en la página web de la entidad y evaluación de las acciones contempladas en este Plan, le corresponden al Jefe de la Oficina de Control Interno de Gestión o quien haga sus veces.

ARTÍCULO QUINTO. El Plan de Tratamiento de Riesgos de Seguridad - TIC deberá ser publicado en la página web de la Corporación.

ARTÍCULO SEXTO: La presente resolución rige a partir de la fecha de expedición.

Dado en el Municipio de Bello a los treinta y uno (31) días del mes de enero de dos mil veinticuatro (2024).

PUBLÍQUESE Y CÚMPLASE

DANIEL RODRIGO VILLA MALDONADO
Presidente Concejo Municipal de Bello

Revisó: Jose Argemiro Restrepo Restrepo, Jefe de Oficina Asesora Jurídica

Proyectó: Paola Andrea Vélez Monsalve, Profesional Universitaria Planeación y Presupuesto Paola Vélez

CONCEJO DE BELLO
Una decisión para todos

Plan de Tratamiento de Riesgo de Seguridad (TIC)

Vigencia 2024

Contenido

1 INTRODUCCION

El plan de tratamiento de riesgos de seguridad y privacidad de la información, seguridad digital y continuidad de los servicios del Concejo Municipal de Bello, se basa en una orientación estratégica que requiere el desarrollo de una cultura de carácter preventivo, de manera que, al comprender el concepto de riesgo, así como el contexto, se planean acciones que reduzcan la afectación a la entidad en caso de materialización; adicional se busca desarrollar estrategias para la identificación, análisis, tratamiento, evaluación y monitoreo de dichos riesgos con mayor objetividad, dando a conocer aquellas situaciones que pueden comprometer el cumplimiento de los objetivos trazados en el entorno de la tecnologías de la información. Dando cumplimiento a la normativa establecida por el estado colombiano y El Modelo de Seguridad y Privacidad de MINTIC.

El desarrollo de las actividades para lograr su consecución estará sujeto a la disponibilidad de recursos (humanos, técnicos, tecnológicos, financieros) que faciliten el cumplimiento de las actividades; de acuerdo con la disponibilidad presupuestal oportuna y a las orientaciones de la alta dirección que se adopten para afrontar el desarrollo y cumplimiento de las actividades planificadas.

2 PLAN TRATAMIENTOS DE RIESGOS

Mediante la definición del Plan de Tratamiento de Riesgos se busca mitigar los riesgos presentes en el análisis de riesgos (Perdida de la Confidencialidad de los activos, Perdida de Integridad de los activos y Perdida de Disponibilidad de los activos) evitando aquellas situaciones que impidan el logro de los objetivos del Concejo Municipal de Bello. El Plan de Tratamiento de Riesgo se define con el fin de evaluar las posibles acciones 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 define el nombre de la medida, objetivo, justificación, responsable de la medida y su prioridad.

3 NORMOGRAMA

Ley 909 de 2004: "Por la cual se expiden normas que regulan el empleo público, la carrera administrativa, gerencia pública y se dictan otras disposiciones".

Ley 1581 de 2012: "Por la cual se dictan disposiciones generales para la protección de datos personales".

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 y se dictan otras disposiciones".

Decreto Nacional 1078 de 2015: "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".

Decreto Presidencial 1083 de 2015: "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública", el cual establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de "11. Gobierno Digital, antes Gobierno en Línea" y "12. Seguridad Digital".

Decreto Presidencial 612 de 2018: "Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado".

Decreto Presidencial 767 de 2022: "Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".

Resolución Ministerial 00500 de 2021: "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de gobierno digital".

4 DEFINICIONES

Amenaza: es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).

Control o Medida: acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos de una entidad.

Impacto: son las consecuencias que genera un riesgo una vez se materialice.

Posibles Consecuencias: Corresponde a los posibles efectos ocasionados por el riesgo, los cuales se pueden traducir en daños de tipo económico, social, administrativo, entre otros.

Probabilidad: es la posibilidad de la amenaza aproveche la vulnerabilidad para materializar el riesgo.

Riesgo: es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos.

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: nivel de riesgo que permanece luego de tomar sus correspondientes medidas de tratamiento.

Vulnerabilidad: es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

5 OBJETIVOS

Definir y aplicar los lineamientos de seguridad de la información de conformidad con la disposición de recursos de la Corporación, para tratar de manera integral los riesgos de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios.

Proteger y preservar la integridad, confidencialidad, disponibilidad y autenticidad de la información.

Gestionar riesgos de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios, de acuerdo con los contextos establecidos y limitantes que existen en la Corporación.

Fortalecer y apropiar conocimiento referente a la gestión de riesgos seguridad y privacidad de la información y seguridad digital.

Cumplir con los requisitos legales y reglamentarios vigentes en materia de seguridad de la información.

6 ALCANCE

Realizar una eficiente gestión de riesgos de seguridad y privacidad de la información y seguridad digital que permita integrar en los procesos de la Corporación buenas prácticas que contribuyan a la toma de decisiones y prevenir incidentes que puedan afectar el logro de los objetivos.

7 CLASIFICACIÓN DE LOS RIESGOS

Riesgos de seguridad digital: Posibilidad de combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, afectar la soberanía municipal, la integridad territorial, los intereses municipales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

Riesgo estratégico: Se asocia con la forma en que se administra el Concejo Municipal de Bello, enfocándose en asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la administración municipal.

Riesgo operativo: Comprende los riegos relacionados tanto con la parte operativa como técnica, incluye riesgos provenientes de las deficiencias en los sistemas de información, en la definición de los procesos, en la estructura de la entidad, la desarticulación entre dependencias, lo cual conduce a ineficiencias, oportunidades de corrupción e incumplimiento de los compromisos institucionales.

Riesgos de tecnología: Se asocian con la capacidad de la entidad para que la tecnología disponible satisfaga las necesidades actuales y futuras de la entidad y soporten el cumplimiento de la misión.

Riesgos financieros: Se relacionan con el manejo de los recursos de la entidad que incluye, la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes de cada entidad. De la eficiencia y transparencia en el manejo de los recursos, depende en gran parte del éxito o fracaso del Concejo Municipal de Bello.

Riesgos de cumplimiento: Se asocian con la capacidad de la entidad de cumplir con los requisitos legales, contractuales, de ética y en general con su compromiso con la comunidad.

Riesgo de imagen o reputacional: Posibilidad de ocurrencia de un evento que afecte la imagen, buen nombre o reputación de una organización ante sus clientes y partes interesadas.

8 MARCO REFERENCIAL

8.1 Directrices Gestión de Riesgos

El objetivo de las directrices es establecer los parámetros necesarios para una adecuada gestión de los riesgos seguridad y privacidad de la información, seguridad digital y continuidad de los servicios del Concejo Municipal de Bello procurando que no se materialicen, atendiendo los lineamientos establecidos en el plan de tratamientos de riesgos orientando a la toma de decisiones oportunas y minimizando efectos adversos al interior de la entidad, con el fin de dar continuidad a la gestión institucional y asegurar el cumplimiento de los compromisos. Se orienta hacia una cultura de la gestión del riesgo asociados en el desarrollo de sus procesos, en aras de cumplir con su responsabilidad de diseñar, adoptar y promover las políticas, planes, programas y proyectos del sector TIC en la medida de lo posible en la Corporación.

El tratamiento de riesgos es la respuesta establecida por la primera línea de defensa, es decir, el líder o responsable del proceso junto con su equipo de trabajo para la mitigación de los diferentes riesgos.

El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:

Aceptar el riesgo: No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. (Ningún riesgo de corrupción es aceptado). La aceptación del riesgo puede ser una opción viable en la entidad, para los riesgos bajos, pero también pueden existir escenarios de riesgos a los que no se les puedan aplicar controles y, por ende, se acepta el riesgo. En ambos escenarios debe existir un seguimiento continuo del riesgo.

Reducir el riesgo: Se adoptan medidas para reducir la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles. Deben seleccionarse controles apropiados y con una adecuada segregación de funciones, de manera que el tratamiento al riesgo adoptado logre la reducción prevista sobre este.

Evitar el riesgo: Se abandonan las actividades que dan lugar al riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca.

Compartir el riesgo: Se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este. Los riesgos de corrupción se pueden compartir, pero no se puede transferir su responsabilidad. Los dos principales métodos de compartir o transferir parte del riesgo son: seguros y tercerización.

La gestión de riesgos de seguridad y privacidad de la Información, seguridad digital y continuidad de la operación de los servicios le permite al Concejo Municipal de Bello realizar una identificación, análisis y tratamiento de los riesgos que puedan generar afectación al cumplimiento de los objetivos de sus procesos, contribuyendo en la toma de decisiones, y en la prevención de la materialización de estos. La administración de riesgos de seguridad y privacidad de la información se encuentra enfocada en identificar, analizar, valorar y tratar las amenazas y vulnerabilidades de los activos de información de la entidad, teniendo presente su criticidad y protección. Las etapas presentes en la gestión de riesgos permiten alinearlas con los objetivos, estrategias y políticas corporativas, logrando un nivel de riesgo que pueda aceptar o asumir la alta dirección.

9. ANÁLISIS DE LA SITUACIÓN ACTUAL

FACTORES INTERNOS	
FORTALEZAS (F)	
• Compromiso de la Alta Dirección para la gestión de recursos para el desarrollo de proyectos de tecnológicos. • Suscripción de convenio interadministrativo con la Alcaldía Municipal de Bello para gestionar recursos y apoyo a los procesos de la Corporación	• No se cuenta con un plan de contingencia para el respaldo de la información. • No se cuenta con ningún sistema de información que permita la consolidación de la información. • La Corporación no cuenta con los recursos suficientes para adquirir la infraestructura de TI que permita una gestión eficiente en sus procesos internos y externos. • Obsolescencia del software y el hardware de la Corporación.

FACTORES EXTERNOS	
OPORTUNIDADES	**AMENAZAS**
• Disposición de donantes de orden municipal, departamental y nacional en materia de herramientas tecnológicas. • Acceso a nuevas tecnologías y herramientas web para la gestión de la información. • Disposición de recursos en el Gobierno Nacional para invertir en programas de innovación en entidades públicas.	• Riesgos de pérdida de información por agentes externos a la Corporación • No contar con instalaciones ni equipo tecnológico de propiedad de la Corporación.

9 ESTRATEGIAS DEL PLAN

Estrategia 1

Incluir en la política de gestión de riesgos las actividades a desarrollar en aras de mitigar los riesgos sobre los activos de la información, articuladas con la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información (Min TIC: 2016).

Estrategia 2

Definir las responsabilidades respecto a la administración y gestión del riesgo, esta etapa deberá ser definida por el Concejo Municipal de Bello teniendo en cuenta su estructura organizacional para la gestión de riesgos.

Estrategia 3

Gestionar los recursos necesarios para la adquisición de equipos y herramientas tecnológicas e infraestructura de TI necesarias para la operación de los procesos.

Estrategia 4

Capacitar el personal en la gestión de riesgos a nivel general con énfasis de seguridad de la información.

Estrategia 5

Actualizar la matriz de riesgos de la Corporación, incorporando los riesgos de seguridad de la información.

10 PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD

Gestión	Actividad	Tarea	Responsable	Fecha Inicio	Fecha Fin
Gestión de Riesgos	Actualización de lineamientos de riesgos	Actualizar política y metodología de gestión de riesgos.	Profesional de Planeación y Presupuesto, y líderes de proceso	01-01-2024	30-06-2024
	Sensibilización	Socialización guía y herramienta, gestión de riesgos de seguridad y privacidad de la información, seguridad digital y continuidad de la operación	Profesional de Planeación y Presupuesto, y líderes de proceso	01-01-2024	30-06-2024
	Identificación de riesgos y seguridad de la información, seguridad digital y continuidad de la operación	Identificación, análisis evaluación de riesgos y seguridad y privacidad de la información, seguridad digital y continuidad de la operación.	Profesional de Planeación y Presupuesto, Secretario General y equipo de trabajo	01-01-2024	30-06-2024
		Realimentación, revisión y verificación de los riesgos identificados.			
	Aceptación De riesgos identificados	Aceptación, aprobación de riesgos identificados y plan de tratamiento	Profesional de Planeación y Presupuesto, Secretario General y equipo de trabajo	01-01-2024	30-06-2024
	Publicación	Publicación matriz de riesgos	Profesional de Planeación y Presupuesto	01-01-2024	30-06-2024
	Seguimiento fase de tratamiento	Seguimiento estado de plan de tratamiento de riesgos identificados y verificación de evidencias.	Profesional de Planeación y Presupuesto, Secretario General y equipo de trabajo	01-07-2024	31-12-2024
	Evaluación de riesgos residuales	Evaluación de riesgos residuales	Profesional de Planeación y Presupuesto, Secretario	01-07-2024	31-12-2024

Gestión	Actividad	Tarea	Responsable	Fecha Inicio	Fecha Fin
			General y equipo de trabajo		
	Mejoramiento	Identificación de oportunidades de mejora acorde a los resultados obtenidos durante la evaluación de riesgos residuales	Profesional de Planeación y Presupuesto, Secretario General y equipo de trabajo	01-07-2024	31-10-2024
		Actualización guía de gestión de riesgos, seguridad de la información de acuerdo con los cambios identificados			
	Monitoreo y revisión	Generación, presentación y reportes de indicadores.	Profesional de Planeación y Presupuesto, Secretario General y equipo de trabajo	01-07-2024	31-11-2024

11 SEGUIMIENTO

El seguimiento y control de las acciones contempladas en el Plan, le corresponde al Secretario General de la Corporación, de la entidad o quien haga sus veces.

12 EVALUACIÓN

La verificación de la elaboración, publicación en la página web de la entidad y evaluación de las acciones contempladas en este Plan, le corresponden al Jefe de la Oficina de Control Interno de Gestión o quien haga sus veces.

DANIEL RODRIGO VILLA MALDONADO
Presidente Concejo Municipal

Revisó: Jose Argemiro Restrepo Restrepo, Jefe de Oficina Asesora Jurídica

Proyectó: Paola Andrea Vélez Monsalve, Profesional Universitaria Planeación y Presupuesto Paola Vélez