PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION DEL HONORABLE CONCEJO DISTRITAL DE BARRANQUILLA.

BARRANQUILLA

Adoptado Mediante Resolución 007 de Enero 2 de 2026

PRESENTACIÒN.

El Honorable Concejo Distrital de Barranquilla, consciente de la importancia estratégica de proteger y garantizar la seguridad y privacidad de la información institucional, y atendiendo a un entorno cada vez más dinámico y expuesto a múltiples amenazas, ha adoptado medidas orientadas a salvaguardar los datos e información que se generan, procesan y administran en el ejercicio de sus funciones misionales y administrativas.

En este contexto, la entidad ha definido un conjunto de estrategias claras y articuladas, consolidadas en el presente documento, las cuales permiten abordar de manera integral los riesgos asociados a la gestión de la información institucional. Dichas estrategias están orientadas no solo a la prevención de incidentes que puedan comprometer la confidencialidad, integridad y disponibilidad de la información, sino también a la mitigación de los impactos derivados de su eventual materialización, garantizando así la continuidad de las operaciones y la adecuada prestación del servicio público.

La Alta Dirección del Honorable Concejo Distrital de Barranquilla, en coordinación con los líderes de los procesos y los servidores que intervienen en ellos, ha incorporado en el presente Plan un diagnóstico DOFA en materia de seguridad y privacidad de la información, el cual permite contar con una visión clara y estructurada del estado actual de las operaciones institucionales donde se genera información. Este análisis identifica las fortalezas, debilidades, oportunidades y amenazas que pueden afectar a la Corporación como consecuencia de la materialización de riesgos, constituyéndose en un insumo fundamental para la toma de decisiones y la implementación de acciones de mejora orientadas a fortalecer la gestión integral de la información.

ALCANCE APLICABILIDAD

El presente Plan aplica para todos los procesos Estratégicos, Misionales, de apoyo y de evaluación Seguimiento y control y para a todos los funcionarios, contratistas, terceros y partes interesadas de la entidad que en el ejercicio de sus funciones utilicen información y servicios de nuestra entidad.

OBJETIVOS.

El presente Plan tiene como objetivo general establecer los lineamientos estratégicos, técnicos y operativos orientados a prevenir, reducir y controlar los riesgos que puedan generar la pérdida, alteración, uso indebido o indisponibilidad de los activos de información del Honorable Concejo Distrital de Barranquilla, garantizando su adecuada protección y gestión.

En concordancia con lo anterior, se definen los siguientes objetivos específicos:

- Realizar un diagnóstico institucional que permita identificar las debilidades y oportunidades asociadas a la gestión, manejo y protección de la información en los diferentes procesos de la entidad.
- Identificar y caracterizar los activos de información del Concejo Distrital de Barranquilla, así como su origen, uso y nivel de criticidad.
- Identificar las causas y fuentes de los riesgos que puedan afectar los activos de información de la entidad, y definir las acciones de prevención y mitigación necesarias para reducir la probabilidad de su materialización y el impacto asociado.
- Establecer una metodología de seguimiento, monitoreo y evaluación de los riesgos de seguridad y privacidad de la información identificados en el presente Plan.
- Designar los responsables del cumplimiento, ejecución y seguimiento de las acciones de tratamiento y mitigación de riesgos establecidas.
- Fortalecer la imagen institucional y el posicionamiento del Honorable Concejo Distrital de Barranquilla como una entidad líder en la implementación de buenas prácticas de gestión, calidad y seguridad de la información en el ámbito regional

GESTIÓN INSTITUCIONAL DE RIESGOS DE LA INFORMACIÓN

El Honorable Concejo Distrital de Barranquilla, en el marco del fortalecimiento de su Sistema Integrado de Gestión, el cual incorpora los componentes de Control Interno – MECI, el Sistema de Gestión de la Calidad certificado bajo la Norma ISO 9001:2015 y el Sistema de Gestión Ambiental conforme a la Norma ISO 14001:2015, ha otorgado un especial énfasis a la gestión integral de riesgos como elemento transversal para el cumplimiento de su misión institucional.

La gestión de riesgos de la entidad tiene alcance sobre todos los procesos institucionales, con especial atención en los procesos estratégicos y misionales, en los cuales se generan, administran y difunden la mayor cantidad de activos de información, los cuales revisten un carácter crítico para la operación institucional, la transparencia administrativa y el servicio a la ciudadanía.

En coherencia con un enfoque preventivo y prospectivo, la gestión de riesgos del Concejo Distrital de Barranquilla se encuentra armonizada con los lineamientos de la Norma ISO 31050, orientada a la identificación y gestión de riesgos emergentes, permitiendo anticipar amenazas derivadas de cambios tecnológicos, ambientales, normativos y contextuales que puedan afectar la seguridad, disponibilidad y confiabilidad de la información institucional.

En relación con la operación, administración y publicación de los activos de información, la entidad ha desarrollado un diagnóstico integral, que constituye la hoja de ruta para establecer políticas, controles y acciones claras, orientadas a una gestión eficaz del riesgo de la información, garantizando su adecuada protección y la mejora continua del Sistema Integrado de Gestión.

Comprensión del Contexto	
DEBILIDADES ● Riesgos asociados a nuestra estructura física Deficiente ● Carencia de elementos de tipo tecnológico propios, que apoyen las actividades Administrativas de esta entidad. ● Operación de actividades y procesos operados por terceros contratistas.	**OPORTUNIDADES** ● Plan de formación y capacitación, adoptado y estructurado de conformidad con las necesidades de la entidad. ● Posibilidad de entablar y realizar convenios y acuerdos de cooperación con entidades del Estado, Privadas y del exterior. ● Implementación de políticas de transparencia y acceso a la información publica.
FORTALEZAS ● Planta de personal profesionalizada, conocedora de los procesos internos y de la dinámica institucional. ● La entidad cuenta con recursos necesarios para impulsar el presente plan. ● Alto nivel de aprobación, por parte de los grupos de veeduría ciudadana y grupos de interés.	**AMENAZAS** ● Generación de Actos de Corrupción. ● Violación de la seguridad informática de los canales de comunicación de la entidad. ● Falta de autonomía institucional para la adquisición y actualización de los equipos de computo de la entidad.

En relación al anterior diagnostico podemos apreciar que contamos con un sistema que si bien es cierto, genera las protecciones mínimas de nuestro patrimonio informático y permite mantener a salvaguarda todos los datos de todas nuestras partes interesadas que intervienen en cada uno de los procesos, de igual forma podemos detectar que contamos con muchas amenazas que se potencializan gracias a consecuencia de nuestras debilidades los cuales durante la presente vigencia se implementaran las medidas encaminadas a mitigar su riesgo de generación.

CLASIFICACION DEL RIESGO:

RIESGO ESTRATEGICO:

Se asocia con la forma en que se administra el CDB, se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos.

RIESGOS OPERATIVOS:

Comprende los riesgos relacionados tanto con la parte operativa como técnica del CDB, incluye riesgos provenientes de las definiciones en los sistemas de información, en la definición de proceso, en la estructura del CDB

RIESGOS FINANCIEROS:

Se relaciona con el manejo de los recursos del CDB, que incluye, la ejecución presupuestal, la elaboración de estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes del CDB

RIESGOS DE CUMPLIMIENTOS:

Se asocia con la capacidad del CDB para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.

RIESGOS DE TECNOLOGIA:

Se asocia con la capacidad del CDB para que la tecnología disponible satisfaga las necesidades actuales y futuras del CDB y soporte el cumplimiento de la misión.

ANALISIS DEL RIESGO.

El análisis de riesgos tiene como propósito principal determinar tanto la probabilidad de que los riesgos se materialicen como las consecuencias que podrían derivarse de su ocurrencia. Este proceso permite calificar y evaluar los riesgos de manera adecuada, con el fin de obtener información valiosa para establecer el nivel de riesgo y definir las acciones que se deben implementar para mitigar sus efectos. El análisis depende en gran medida de la información recabada en el formato de identificación de riesgos, así como de la disponibilidad de datos históricos y de las aportaciones de los servidores del CDB. De esta forma, se busca construir una evaluación lo más precisa posible para tomar decisiones informadas y eficaces en la gestión de riesgos. Para estructurar este análisis, se han identificado dos aspectos fundamentales: la probabilidad y el impacto.

La probabilidad hace referencia a la posibilidad de que un riesgo se materialice, y puede ser medida a través de criterios de frecuencia o de factibilidad. Esto implica tener en cuenta diversos factores, tanto internos como externos, que podrían facilitar la ocurrencia del riesgo, aunque este aún no se haya manifestado. Por otro lado, el impacto se refiere a las posibles consecuencias que la materialización del riesgo tendría para la organización. Ambas variables, probabilidad e impacto, son fundamentales para poder valorar adecuadamente el riesgo y diseñar estrategias para su mitigación. Para llevar a cabo un análisis exhaustivo, es crucial considerar

diversos aspectos que puedan influir en la evaluación final de los riesgos y en las medidas correctivas a aplicar.

La Calificación del Riesgo: Se logra a través de la estimulación de la probabilidad de su ocurrencia y el impacto que pueda causar la materialización del riesgo. La probabilidad representa el número de veces que el riesgo se ha presentado en un determinado tiempo o puede presentarse y el impacto se refiere a la magnitud de sus efectos.

Calificación de Riesgo:

Se debe calificar cada uno de los riesgos según la matriz de acuerdo a las siguientes especificaciones:

Tabla de Probabilidad

Nivel	Probabilidad	Descripción	Frecuencia
1	Raro	El evento puede ocurrir solo en circunstancias excepcionales	No se ha presentado en los últimos 5 años.
2	Improbable	El evento puede ocurrir en algún Momento	Al menos de 1 vez en los últimos 5 años.
3	Posible	El evento podría ocurrir en algún momento	Al menos de 1 vez en los últimos 2 años.
4	Probable	El evento probablemente ocurrirá en la mayoría de las circunstancias	Al menos de 1 vez en el último año.
5	Casi seguro	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de 1 vez al año.

Tabla de Impacto

Nivel	Tipo de Impacto	Descripción
1	Insignificante	Si el hecho llegara a presentarse, tendría consecuencias o efectos mínimos sobre la entidad.
2	Menor	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad.
3	Moderado	Si el hecho llegara a presentarse, tendría medianas Consecuencias o efectos sobre la entidad.
4	Mayor	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad
5	Catastrófico	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad.

La Evaluación del Riesgo: Permite comparar los resultados de su calificación con los criterios definidos para establecer el grado de exposición del CDB al riego; de esta forma es posible distinguir entre otros riesgos aceptables, tolerables,

moderados, importantes o inaceptables y fijar las prioridades de las acciones requeridas para su tratamiento.

Con el fin de facilitar y evaluación a los riesgos, a continuación, se presenta una matriz que contempla un análisis cualitativo, que hace referencia a la utilización de formas descriptivas para presentar la magnitud de las consecuencias potenciales (impacto) y la posibilidad de ocurrencia (probabilidad) tomando las siguientes categorías: leve, moderada y catastrófica en relación con el impacto y alta media y baja respecto a la probabilidad.

Así mismo presenta un análisis cuantitativo que contempla calores numéricos que contribuyen a la calidad en la exactitud de la calificación y evaluación de los riesgos. Tanto para el impacto como para la probabilidad se han determinado valores múltiplos de 5.

MATRIZ DE CALIFICACION, EVALUACION Y RESPUESTA A LOS RIESGOS

Probabilidad	IMPACTO				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
RARO (1)	Zona de riesgo Baja	Zona de riesgo Baja	Zona de riesgo Moderada	Zona de riesgo Alta	Zona de riesgo Alta
IMPROBABLE (2)	Zona de riesgo Baja	Zona de riesgo Baja	Zona de riesgo Moderada	Zona de riesgo Alta	Zona de riesgo Extrema
POSIBLE (3)	Zona de riesgo Baja	Zona de riesgo Moderada	Zona de riesgo Alta	Zona de riesgo Extrema	Zona de riesgo Extrema
PROBABLE (4)	Zona de riesgo Moderada	Zona de riesgo Alta	Zona de riesgo Alta	Zona de riesgo Extrema	Zona de riesgo Extrema
CASI SEGURO (5)	Zona de riesgo Alta	Zona de riesgo Alta	Zona de riesgo Extrema	Zona de riesgo Extrema	Zona de riesgo Extrema

	Asumir el riesgo
	Asumir el riesgo, Reducir el riesgo
	Reducir el riesgo, Evitar, Compartir o transferir
	Reducir el riesgo, Evitar, Compartir o transferir

Evaluación del Riesgo

La evaluación del riesgo constituye una etapa fundamental del proceso de gestión del riesgo y se desarrolla a partir de los resultados obtenidos en la calificación de la probabilidad y el impacto. Este ejercicio se apoya en un instrumento técnico denominado Matriz de Calificación, Evaluación y Respuesta a los Riesgos, el cual permite establecer el nivel de exposición de la entidad y definir las acciones de tratamiento correspondientes.

Para llevar a cabo la evaluación del riesgo, se tiene en cuenta la ubicación de cada riesgo dentro de las distintas zonas definidas en la matriz, determinada por la combinación de los niveles de probabilidad e impacto, aplicando los siguientes criterios:

Cuando la probabilidad del riesgo es rara (1) y el impacto es insignificante (1) o menor (2), el riesgo se clasifica en la Zona de Riesgo Baja. En este nivel, la entidad puede aceptar el riesgo, al considerarse que se encuentra dentro de límites tolerables y que los controles existentes son suficientes, sin requerir la implementación de medidas adicionales.

Cuando la probabilidad es casi segura (5) y el impacto es catastrófico (5), el riesgo se ubica en la Zona de Riesgo Extrema. En estos casos, la matriz recomienda eliminar la actividad que origina el riesgo, siempre que ello sea posible. En caso contrario, se deberán implementar controles de prevención para reducir la probabilidad de ocurrencia y controles de protección para disminuir el impacto, así como considerar la transferencia o compartición del riesgo, mediante pólizas de seguro u otros mecanismos disponibles.

Cuando el riesgo se ubica en las zonas de riesgo moderada o alta, la entidad deberá implementar medidas orientadas a reducir el nivel de riesgo y, en lo posible, llevarlo a la Zona de Riesgo Baja. Las acciones de tratamiento dependerán de la celda específica que ocupe el riesgo en la matriz. Así, los riesgos con impacto insignificante y probabilidad casi segura deberán prevenirse; los riesgos con impacto moderado y probabilidad posible deberán reducirse o compartirse, cuando sea viable; y en los casos en que se presenten probabilidades posibles o probables con impactos mayores o catastróficos, podrá considerarse la combinación de acciones de reducción, evitación y transferencia del riesgo.

En todo caso, cuando un riesgo sea calificado con impacto catastrófico, la entidad deberá diseñar e implementar planes de contingencia que permitan mitigar los efectos de su materialización y proteger la continuidad de los procesos institucionales.

MATRIZ DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION.

En aras de poder tomar los prever aquellas situaciones que pudieran afectar la operación de la entidad, este Concejo ha diseñado la siguiente matriz de Riesgos.

MATRIZ DE RIESGOS PRIVACIDAD Y SEGURIDAD DE LA INFORMACION.						
RIESGO	**DESCRIPCION.**	**CAUSA**	**TIPOLOGIA DEL RIESGO**	**EFECTO**	**ACCION CORRECTIVA.**	**OBJETIVO.**
Afectación, sustracción y perdida de información electrónica.	Se genera cuando se pierde información importante, referente a la operación de nuestra entidad.	falla en los sistemas de seguridad informática ya sea antivirus o mecanismos de protección, que pudieran llegar a afectar los activos de información de nuestra entidad.	tecnológico.	Perdida de activos de información.	Actualización periódica de antivirus en los equipos de la entidad.	Poder generar los mecanismos de protección necesarios para salvaguardar la información de la entidad,

incapacidad de generar la salvaguarda de los activos de información de la entidad.	No poder salvaguardar en debida forma la informacion institucional.	Debido a la precaria red de datos y limitadas prestacione s de equipos de computo es imposible salvaguada en debida forma la informacion de la entidad.	Tecnologica	Perdida de activos de informacion.	Adquision y actualizacion de equipos de computo necesaria para poder guardar la informacion de la entidad	Poder contar con los elementos tecnologicos necesarios para preservar los activos de informacion de la entidad,
Operación inadecuada de las herramientas del Tics Institucionales .	se configura cuando no se realiza una correcta operación de las plataformas electrónicas de la entidad,	La operación de la pagina web, y de las actividades informaticas de la entidad son operadas por contratistas externos, por la inexistencia de un ingeniero de sistema de la planta de cargos de la entidad.	Operativo.	Imposibilidad de darle continuidad y seguimiento a los procesos de las TICs debido a la alta rotacion del personal contratista de la entidad.	Fomentar las capacitacione s y competecias en manejo y operación de las tics en un funcionario de planta de la entidad, apoyado por el personal contratista.	Poder darle continuidad a la gestion relacionada con la operación de las TICS
Perdida y manipulación intencional de la información	Se configura cuando debido a actos de corrupción se sustrae, borra o manipula de manera intencional los activos de	Actos de Corrupción.	Corrupción	Perdida de activos de información traumatismos en la operación institucional	establecer puntos de control en los equipos de computo, tal como perfiles con restriccion de operación, back ups de seguridad.	Conservar la informacion Institucional de la entidad

	informacion de la entidad.					
destrucción de información por catástrofes naturales.	Debido al alcanzado estado de deterioro el las instalaciones donde se encuentra el CDB, se aumentan las probabilidades de que se generen accidentes que puedan afectar los activos de la información de la entidad.	Debido accidentes generados por catástrofes naturales o de fuerza mayor y caso fortuito se destruye la información institucional	estratégico.	Perdida de información	Back ups de informacion en nubes o reservas fuera de la entidad.	Preservar la informacion de la entidad.

PRINCIPIOS

Los siguientes principios orientan el **Modelo de Seguridad y Privacidad de la Información** del Honorable Concejo Distrital de Barranquilla y se encuentran alineados con el **Sistema Integrado de Gestión**, en concordancia con los lineamientos de las normas **ISO 9001:2015** e **ISO 14001:2015**, promoviendo un enfoque basado en procesos, gestión del riesgo, mejora continua y cumplimiento normativo.

- Las responsabilidades frente a la seguridad y privacidad de la información serán claramente **definidas, asignadas, comunicadas y socializadas** a los funcionarios, contratistas, terceros y demás partes interesadas, garantizando su apropiación y cumplimiento en el desarrollo de los procesos institucionales.
- El Honorable Concejo Distrital de Barranquilla protegerá la información generada, recibida, procesada, almacenada y transmitida por la entidad frente a los riesgos derivados de accesos no autorizados, uso indebido, pérdida, alteración o divulgación de la información, mediante la aplicación de controles definidos en el **Mapa de Riesgos Institucional**, de acuerdo con la clasificación de la información de su propiedad o bajo su custodia.
- Los responsables de la información institucional deberán identificar, analizar y gestionar los riesgos a los que están expuestos los activos de información de sus áreas, considerando que la información puede ser copiada,

divulgada, modificada o destruida, tanto en medios físicos como digitales, por actores internos o externos.

- El Honorable Concejo Distrital de Barranquilla garantizará la protección de las instalaciones de procesamiento de información y de la infraestructura tecnológica que soporta los procesos críticos, mediante la implementación de controles físicos, lógicos y administrativos, incluyendo mecanismos de control de acceso a la información, a los sistemas y a los recursos de red.
- La entidad controlará y supervisará la operación de sus procesos, sistemas de información y redes de datos, asegurando el uso adecuado y seguro de los recursos tecnológicos, así como la continuidad de los servicios institucionales, en coherencia con el enfoque de gestión por procesos.
- El Honorable Concejo Distrital de Barranquilla asegurará que la seguridad y privacidad de la información sean un componente transversal e integral de todos los procesos institucionales, mediante la adopción y aplicación de políticas, procedimientos, análisis de riesgos y controles alineados con el Sistema Integrado de Gestión.
- La entidad promoverá la gestión oportuna y eficaz de incidentes, eventos y debilidades de seguridad y privacidad de la información, con el propósito de prevenir su recurrencia y fortalecer el **mejoramiento continuo** del modelo de seguridad de la información.
- El Honorable Concejo Distrital de Barranquilla se compromete a cumplir de manera estricta las obligaciones legales, regulatorias y contractuales aplicables en materia de seguridad y privacidad de la información, así como a adoptar las acciones necesarias para asegurar la conformidad permanente con el marco normativo vigente.

RESPONSABILIDADES

La Alta Dirección del **HONORABLE CONCEJO DISTRITAL DE BARRANQUILLA** es responsable de garantizar que la seguridad y privacidad de la información se comunique y apropie adecuadamente en la entidad. La Alta Dirección del CDB es responsable de garantizar que la seguridad y privacidad de la información sean parte de la cultura organizacional para tal efecto este establecerá las estrategias encaminadas en generar un ambiente de seguridad informática, la cual cobije a todos los procesos internos que se impulsan en esta Corporación.

Los funcionarios, contratistas, terceros y partes interesadas de la entidad tienen la responsabilidad de mantener la seguridad y privacidad de la información del CDB.

RESULTADO CLAVE

Contar con un ambiente de seguridad y privacidad de la información en **El HONORABLE CONCEJO DISTRITAL DE BARRANQUILLA** logrando el cumplimiento de los pilares de seguridad de la información que son la confidencialidad, integridad, disponibilidad y el no repudio de la misma.

CUMPLIMIENTO

Las estrategias y lineamientos establecidos en el presente Plan será de obligatorio cumplimiento para todo el recurso humano que se encuentra vinculado a los diferentes procesos de la entidad y de esta forma poder asegurar el cumplimiento de nuestro marco legal y reglamentario y minimizar la generación de riesgos de Generación de Actos de Corrupción al interior de la entidad.

MAURICIO VILLAFAÑEZ JABBA.

Presidente.