PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

CORPORACION PARA EL DESARROLLO SOSTENIBLE DELNORTE Y EL ORIENTE AMAZÓNICO -CDA-

Inírida – Guainía
2024

- Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
- Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
- Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
- Website: w w w . c d a . g o v . c o e - m a i l : c d a @ c d a . g o v . c o

TABLA DE CONTENIDO

Contenido

- Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
- Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
- Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
- Website: w w w . c d a . g o v . c o e - m a i l : c d a @ c d a . g o v . c o

INTRODUCCION

Teniendo en cuenta el Plan Nacional de Desarrollo 2022 – 2026 "Colombia potencia mundial de la vida" (Ley 2294 de 2023), el cual con respecto a las tecnologías de la información busca promover el uso y aprovechamiento de las TIC para mejorar la calidad de vida de los ciudadanos y el desarrollo del país, estableciendo como objetivo que Colombia sea un líder en transformación digital, y por tanto requiere que las entidades del orden nacional trabajen en la implementación de acciones y proyectos que permitan que el Estado colombiano sea más eficiente, transparente y cercano a los ciudadanos.

El plan de tratamiento de riesgo de seguridad y privacidad de la información seguridad digital de la CORPORACION PARA DESARROLLO SOSTENIBLE DEL NORTE Y EL ORIENTE AMAZONICO CDA. Se basa en la 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 reduzca la afectación a la CORPORACION CDA.

Si bien la información durante mucho tiempo ha sido considerada como un activo valioso e importante, el aumento de la economía del conocimiento ha llevado a las organizaciones a depender cada vez más en la información, procesamiento de la información y sobre todo de TI. Varios eventos o incidentes pueden comprometer de alguna manera, por lo tanto, pueden causar impactos adversos en los procesos de la organización o de su misión, que van desde intrascendente a catastrófica.

Lo anterior dando cumplimiento a la normativa establecida por el estado colombiano, CONPES 3995 de 2020, Modelo de Seguridad y Privacidad de MINTIC y lo establecido en el decreto 1008 de 14 de junio 2018, a la Resolución 500 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 adoptando las buenas prácticas y los lineamientos de los

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

estándares ISO 27001, ISO 31000:2018 y la guía para la administración del riesgo y el diseño de controles en entidades públicas – Riesgos de gestión, corrupción y seguridad digital, establecidos en el Modelo Integrado de Planeación y Gestión-MIPG.

Por este motivo se ha visto la necesidad de desarrollar un análisis de riesgo tecnológico de la Corporación CDA; para considerar y tratar de evitar las posibles causas que conlleven a una NO DESEADA perdida de información.

DEFINICIONES

- **Riesgo:** Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.

- **Riesgo de Seguridad de la Información**: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

- **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).

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

- **Probabilidad:** se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando.

- **Impacto:** consecuencias que puede ocasionar a la organización la materialización del riesgo.

- **Control o Medida:** Medida que permite reducir o mitigar un riesgo.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

OBJETIVOS

- Desarrollar una propuesta de gestión de seguridad y privacidad que permita minimizar los riesgos de pérdida de activos de la información en la Corporación CDA.
- Incentivar al personal de la Corporación CDA a seguir normas y procedimientos referentes a la seguridad de la información y recursos.
- Cumplir con los requisitos legales, reglamentarios, regulatorios y de las normas técnicas colombianas.
- Gestionar los riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios (riesgos de interrupción), de acuerdo con los contextos establecidos en la Entidad.
- Fortalecer y apropiar conocimiento referente a la gestión de riesgos de Seguridad y Privacidad de la información, Seguridad Digital y Continuidad de la Operación de los servicios (riesgos de interrupción) de la CORPORACION –CDA-.

ALCANCE

- El Plan de Tratamiento de Riesgo tendrá en cuenta todos los riesgos en especial los que se encuentren en los niveles Moderado, Alto y Extremo acorde con los lineamientos definidos por el Ministerio de TIC, teniendo en cuenta que los riesgos que se encuentren en niveles inferiores serán aceptados por la Entidad.
- Este documento contiene las recomendaciones para tratar los riesgos que superan el nivel de riesgo aceptable en la Corporación CDA, es decir, que tienen un nivel moderado o alto de acuerdo a lo

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

evidenciado en el estado actual de la Corporación.

IDENTIFICACIÓN DEL RIESGO.

El análisis de riesgos informáticos es un proceso que comprende la identificación de activos informáticos, sus vulnerabilidades y amenazas a los que se encuentran expuestos así como su probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo. Dentro de estos parámetros, como lo propone la Guía de gestión de riesgos, Seguridad y privacidad de la información de *comparación en la cual se presenta el análisis de la probabilidad de ocurrencia del riesgo versus el impacto del mismo, obteniendo al final la matriz denominada "Matriz de Calificación, Evaluación y respuesta a los Riesgos", con la cual la guía presenta la forma de calificar los riesgos con los niveles de impacto y probabilidad establecidos anteriormente, así como las zonas de riesgo presentando la posibles formas de tratamiento que se le puede dar a ese riesgo*".

Donde se podrán identificar los siguientes riesgos tres (3) riesgos inherentes de seguridad de la información:

- Perdida de la confidencialidad.
- Perdida de la integridad.
- Perdida de la disponibilidad

VALORACION DEL RIESGO.

La valoración de los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios (riesgos de interrupción) DE LA CORPORACION PARA EL DESARROLLO SOSTENIBLE PARA EL NORTE Y ORIENTE AMAZONICO-CDA-.se realizará acorde a la metodología para la administración de riesgos mencionada en la Guía (GUIA PARA LA ADMINISTRACION DEL RIESGO Y EL DISEÑO DE CONTROLES EN ENTIDADES PUBLICAS-V5 DEL 2020 emitida por el Departamento Administrativo de la Función Pública.

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

se analiza el contexto, se identifican los riesgos y se realiza el análisis de la probabilidad e impacto como valoración preliminar para identificar el nivel del riesgo inherente, asociando sus vulnerabilidades e identificando los controles para mitigarlas. A estos controles se le identifican las variables a evaluar para el adecuado diseño de controles como son: responsable, periodicidad, propósito, cómo se realiza la actividad de control, observaciones o desviaciones y la evidencia de la ejecución del control. Adicionalmente se evalúa que cada control se ejecute de manera consistente, de tal forma que pueda mitigar el riesgo. Esta valoración se realiza de acuerdo con las tablas y metodología establecida y mencionada en la Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP.

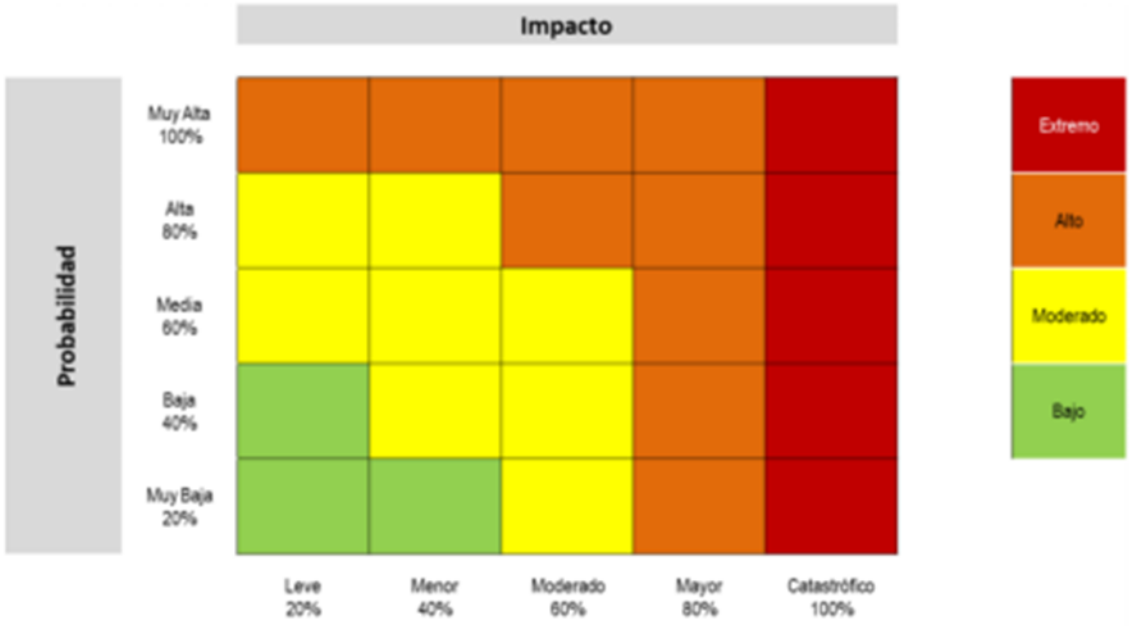
El proceso donde se identifica el riesgo aporta los niveles de probabilidad, impacto y riesgo inherente que genera la posible indisponibilidad del activo.

Para la evaluación de riesgos se cuenta con una matriz de calificación tal cual como se muestra con la siguiente imagen:

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

	Afectación Económica	Reputacional
Leve 20%	Afectación menor a 10 SMLMV .	El riesgo afecta la imagen de algún área de la organización.
Menor-40%	Entre 10 y 50 SMLMV	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores.
Moderado 60%	Entre 50 y 100 SMLMV	El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos.
Mayor 80%	Entre 100 y 500 SMLMV	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal.
Catastrófico 100%	Mayor a 500 SMLMV	El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país



- Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
- Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
- Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
- Website: w w w . c d a . g o v . c o e - m a i l : c d a @ c d a . g o v . c o

METODOLOGIA.

El Plan de Tratamiento de Riesgos contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos identificados en la entidad, estas actividades se estructuraron de la siguiente manera, siguiendo las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información.

Nro.	Actividad	Responsable de la tarea	Fecha de inicio	Fecha final
1	Actualizar el instrumento de Registro Activos de Información con el insumo del inventario de activos de Información.	Oficina de sistemas	Febrero	Marzo
2	Publicación del Registro Activos de Información en la sección de transparencia y en el portal de datos abiertos de la entidad.	Oficina asesora de planeación	Marzo	Marzo
3	Creación de la política, metodología y lineamientos de la gestión de riesgos	Oficina de sistemas	Abril	Mayo
4	Socialización de lineamientos y Herramienta - Gestión de Riesgos de Seguridad y privacidad de la Información y Seguridad Digital	Oficina de sistemas	Enero	Febrero
5	Identificación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y continuidad de la Operación	Oficina de sistemas	Abril	Mayo
	Seguimiento y			

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

6	monitoreo a la implementación de las diferentes políticas y planes propuestos por la oficina de sistemas y aprobados por la alta dirección.	Oficina de control interno	Octubre	Noviembre
7	Realizar seguimiento a los informes de eventos y vulnerabilidades asociados a SGSI	Oficina de control interno	Cada 4 meses	Cada 4 meses
8	Creación de manuales de los diferentes programas implementados dentro de la entidad	Oficina de Sistemas	Enero	Febrero
9	Creación de las diferentes políticas y planes para ciberseguridad, Ciberdefensa alineados bajo la Norma iso 27001	Oficina de sistemas	Enero	Abril
10	Creación del documento plan de continuidad de la operación.	Oficina de sistemas	Marzo	Abril
11	Reuniones de Socialización de los avances de la implementación del plan de Seguridad Digital y la Estrategia del Modelo de Seguridad y Privacidad de la información	Oficina de sistemas	Cada 6 mese	Cada 6 meses
12	Formular, Implementar y actualizar los indicadores del SGSI	Oficina de sistemas	Enero	Cada 4 mese
13	Reportar indicadores	Oficina de sistemas	Enero	Cada 6 meses
14	Definir los lineamientos y el alcance para la realización de	Oficina de sistemas	Marzo	Abril

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

	pruebas de vulnerabilidades			
15	Concientización y sensibilización en Seguridad y Privacidad de la información	Oficina de sistemas	Enero	Diciembre
16	Realizar ejercicios y simulaciones para fortalecer el reporte y gestión de incidentes de seguridad y privacidad de la información	Oficina de sistemas	Junio	Diciembre
	Aumento de cuentas de correo electrónico	Oficina asesora de planeación	Enero	Diciembre
	Adquisición e instalación de software de Antivirus en los PC y en los Sistemas de Información	Oficina de sistemas	Enero	Junio
	Generación e implementación de la política de respaldo de la información	Oficina de sistema	Enero	Abril
	Migración de protocolo de comunicaciones de IPV4 a IPV6	Oficina de sistemas	Enero	Diciembre
	Virtualización de servidores	Oficina de sistemas	Enero	Marzo
	Implementación del cableado estructurado dentro de las instalación es de la Corporación CDA	Oficina de sistemas	Enero	Diciembre

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: w w w . c d a . g o v . c o e - m a i l : c d a @ c d a . g o v . c o

DESARROLLO METODOLOGICO.

ESTABLECIMIENTO DEL CONTEXTO.

El contexto en términos generales relaciona los aspectos externos, internos y del proceso que se deben tener en cuenta para gestionar los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital de LA CORPORACION PARA DESARROLLO SOSTENIBLE DEL NORTE Y ORIENTE AMAZONICO-CDA. A partir del contexto es posible establecer las posibles causas de los riesgos a identificar. De esta forma para la definición del contexto se seguirán las metodologías dispuestas en la entidad para lograr establecer las posibles causas y determinar la identificación de los riesgos.

IDENTIFICACION DEL RIESGO.

Para la identificación de riesgos de Seguridad y Privacidad de la Información y Continuidad de la Operación de los Servicios (riesgos de interrupción) de la Corporación Para el Desarrollo Sostenible Del Norte y Oriente Amazónico CDA se debe tener en cuenta diferentes aspectos como infraestructura física, áreas de trabajo, entorno y ambiente en general,

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

para lo cual se hace indispensable que cada uno de los procesos tenga identificado los activos de información, y reconocer las situaciones potenciales que causarían daño a la entidad poniendo en riesgo el logro de los objetivos establecidos.
La falta de apropiación en temas referentes a la seguridad de la información o la ausencia de controles (vulnerabilidades) puede ser aprovechadas por una amenaza causando la materialización de un riesgo (Incidente), por lo que es preciso identificar: El atributo de la triada de la información afectado (Confidencialidad, Integridad, Disponibilidad), el proceso dueño del riesgo, activo de información afectado, amenazas, vulnerabilidades y consecuencias.
Para la identificación se pueden abarcar datos históricos, análisis teóricos, opiniones informadas y expertas, y las necesidades de las partes involucradas.

MATERIALIZACION.

En el caso de materializarse un riesgo, este debe ser reportado de acuerdo con el procedimiento de gestión de incidentes de seguridad y privacidad de la información. Así mismo se deberá analizar el riesgo y validar en qué nivel queda posterior a la materialización, registrando los cambios respectivos en el mapa de riesgos. En caso de que se materialice un riesgo que no esté identificado, deberá ser reportado para que se inicie su correspondiente identificación en el mapa de riesgos

OPORTUNIDAD DE MEJORA.

LA CORPORACION PARA EL DESARROLLO SOSTENIBLE DEL NORTE Y ORIENTE AMAZONICO-CDA-.no sólo deberá centrarse en los riesgos identificados, sino que este análisis o apreciación del riesgo debe ser la base para identificar oportunidades. Por lo anterior la oportunidad deberá entenderse como la consecuencia positiva frente al resultado del tratamiento del Riesgo.

INDICADORES.

En el plan de acción de la vigencia 2024 se incluye el indicador Porcentaje de implementación del PTRSI, a través de cual se realizará la medición mensual del avance de la ejecución del proyecto, líneas de acción y

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co

actividades incluidas en el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información (PTRSI). El reporte de este indicador será llevado a cabo por parte de la Oficina de Tecnologías de la Información.

SEGUIMIENTO, ANALISIS Y EVALUACION.

Como mecanismos de análisis y evaluación desde la Oficina de Tecnologías se realizará el seguimiento mensual a la información reportada por el responsable en los instrumentos dispuestos por la Oficina Asesora de Planeación donde se reporta el resultado del avance de los indicadores, con el fin de gestionar las actividades que garanticen el cumplimiento razonable de los objetivos y mantener el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2024, los objetivos estratégicos y ejes transformacionales para el cumplimiento de la misión de la Unidad.

Adicionalmente, se cuenta con los Informes de Seguimiento y Recomendaciones mensuales resultado del análisis de los indicadores por parte de la Oficina Asesora de Planeación como segunda línea de defensa y también se cuenta con las auditorías que se programan de acuerdo con el Plan de Auditoría por la Oficina de Control Interno como tercera línea de defensa, donde se emiten informes con hallazgos, observaciones y/o recomendaciones, así como el permanente monitoreo de los riesgos.

BIBLIOGRAFÍA.

Ministerio de tecnologías de la información y las comunicaciones
https://www.mintic.gov.co/portal/inicio/

Función publica (2020) Guía para la Administración del riesgo y el diseño de controles y entidades Públicas- Versión 5.
https://www.funcionpublica.gov.co/documents/418537/506911/1592.pdf/73e5a159-2d8f-41aa-8182-eb99e8c4f3ba

Sede Principal: Inírida – Guainía, Calle 26 No 11 -131. Tel: (608) 3143717167 –3115138768-3102051477
Seccional Guaviare: San José del Guaviare, Transv. 20 No 12-135 Cel: 311 513 88 04
Seccional Vaupés: Mitú, Av. 15 No. 8-144, Cel.: 310 7869166
Website: www.cda.gov.co e-mail: cda@cda.gov.co