Contraloría
General Departamento del Chocó
Nit. 818000365-0

POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Dimensión MIPG: Gestión con valores para el resultado**.**

2018 - 2019

El artículo 15 de la Constitución Política A, consagra el derecho fundamental de las personas a conservar su intimidad personal y familiar, al buen nombre y a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellos en bancos de datos y en archivos de las entidades públicas y privadas.

La Contraloría General del Departamento del Chocó, se compromete a adoptar las medidas técnicas, jurídicas y administrativas necesarias a través de la estrategia de la administración de riesgo, dando un tratamiento transparente y correcto a la información pública del Municipio, fomentando una cultura de mejora de la seguridad de la información, preservando los activos de información y tecnológicos de la entidad, para asegurar la confidencialidad, integridad y disponibilidad de la información; con el fin de apoyar el cumplimiento de la gestión de la entidad y promover la confianza en la ciudadanía.

En la actualidad, el gobierno colombiano reconoce la información como un activo valioso y a medida que los sistemas de información apoyan cada vez más los procesos de misión, se requiere contar con estrategias de alto nivel que permitan el control y administración efectiva de los datos. Por esto, el Ministerio de Tecnologías de la Información y las Telecomunicaciones por medio del Decreto 1078 de 2015, da la directriz para que, entre otros ejes, se implemente el eje de seguridad y privacidad de la información basada en la norma técnica colombiana 27001 “Tecnología de la Información Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información”. Considerando también, el Modelo integrado de Planificación y gestión MIPG y su actualización mediante el decreto 1499 de 2017, en su articulado 2.2.22.1.5 Articulación y complementariedad con otros sistemas de gestión. Establece que: “El Sistema de Gestión se complementa y articula, entre otros, con los sistemas nacional de servicio al ciudadano, de gestión de la seguridad y salud en el trabajo, de gestión ambiental y de Seguridad de la Información”.

Calle 27 № 6 – 40- **Teléfono** (094)6711334 – Fax (094)6712474
www.contraloria-choco.gov.co –Email: contactenos@contraloria-choco.gov.co

En ese orden de ideas, la Contraloris, implementa la norma técnica colombiana NTC ISO/IEC 27001 dentro del Sistema de Gestión y Control Integrados y reconoce que los sistemas, los activos de información y la red de información enfrentan amenazas de seguridad que incluyen, entre muchas otras: el fraude por computadora, espionaje, sabotaje, vandalismo, desastres naturales. Las posibilidades de daño y pérdida de información por causa de código malicioso, mal uso de la información, poca protección de la información, la no definición de procedimientos o ataques informáticos, son cada vez más comunes y ponen cada vez más en riesgo los activos de información. Por esta razón se deben definir las políticas que permitan proteger los Sistemas de Información y establecer un sistema de gestión de seguridad de la información.

La política de alto nivel o política general, aborda la necesidad de la implementación de un **sistema de gestión de seguridad de la información (SGSI)** planteado desde la descripción del quién, qué, por qué, cuándo y cómo, en torno al desarrollo de la implementación del SGSI.

El Modelo de Seguridad y Privacidad de la Información – MSPI, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos. A través del decreto único reglamentario 1078 de 2015, del sector de Tecnologías de Información y las Comunicaciones, se define el componente de seguridad y privacidad de la información, como parte integral de la estrategia GEL.

Propósitos

- Establecer los lineamientos bajo los cuales se debe desarrollar la protección de los sistemas de información de acuerdo a lo establecido en ISO 27001, propendiendo por reducir el robo, daño y/o abuso de los mismos, así como indicar los parámetros por los usuarios dentro del marco de la seguridad de la información.

- Controlar las vulnerabilidades y amenazas que enfrentan los activos de información y tecnológicos mediante la elaboración de los mapas de riesgos, para asegurar la confidencialidad, integridad y disponibilidad de la información de todos los Organismos de la Entidad

- Fortalecer la cultura de seguridad de la información mediante difusión, sensibilización y capacitación de funcionarios, con el fin de dar tratamiento transparente y correcto de la información de todos los procesos de la Contraloría General del Departamento del Chocó.

- Gestionar el inventario de los activos informáticos y de información que garantice la Identificación, clasificación y el mantenimiento de la información, para lograr su uso apropiado durante todo su ciclo de vida en todos los procesos de la entidad.

Alcance

Aplica en toda la Entidad y sus correspondientes dependencias, así como incluye a cada uno de los usuarios internos y externos proveedores y terceros, de los sistemas de información como parte del Modelo de Seguridad y Privacidad de la Información de la estrategia de Gobierno en Línea, según lo establecido en el Decreto 1078 de 2015.

Glosario

- **Acceso a la Información Pública**: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)

- **Activo** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

- **Activo de Información**: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

- **Archivo:** Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)

- **Amenazas** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000). • Análisis de Riesgo Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

- **Auditoría** Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000).

- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3) • Bases de Datos Personales: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)

- **Ciberseguridad** Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

- **Ciberespacio** Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

- **Control** Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

- **Datos Abiertos:** Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6)

- **Datos Personales**: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

- **Datos Personales Públicos:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y

sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3).

- **Datos Personales Privados**: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)

- **Datos Personales Mixtos:** Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles. • Datos Personales Sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)

- **Declaración de aplicabilidad** Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000). • Derecho a la Intimidad: Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

- **Encargado del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. (Ley 1581 de 2012, art 3)

- **Gestión de incidentes de seguridad de la información** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

- **Información Pública Clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su

acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

- **Información Pública Reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

- **Ley de Habeas Data:** Se refiere a la Ley Estatutaria 1266 de 2008.

- **Ley de Transparencia y Acceso a la Información Pública:** Se refiere a la Ley Estatutaria 1712 de 2014.

- **Mecanismos de protección de datos personales:** Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.

- **Plan de continuidad del negocio** Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

- **Plan de tratamiento de riesgos** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

- **Privacidad:** En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

- **Registro Nacional de Bases de Datos:** Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)

- **Responsabilidad Demostrada:** Conducta desplegada por los Responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

- **Responsable del Tratamiento de Datos:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).

- **Riesgo** 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).

- **Seguridad de la información** Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

- **Sistema de Gestión de Seguridad de la Información SGSI** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

- **Titulares de la información:** Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)

- **Tratamiento de Datos Personales**: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

- **Trazabilidad** Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

- **Vulnerabilidad** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000). •

- **Partes interesadas (Stakeholder)** Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

- **Política:** Declaración de alto nivel que describe la posición de la entidad sobre un tema específico.

- **Estándar:** Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares son diseñados para promover la implementación de las políticas de alto nivel de la entidad antes de crear nuevas políticas.

- **Mejor Práctica:** Una regla de seguridad específica o una plataforma que es aceptada, a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de los sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la entidad.

- **Guía:** Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares buenos prácticas. Las guías son esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo.

- **Procedimiento:** Los procedimientos, definen específicamente como las políticas, estándares, mejores prácticas y guías que serán implementadas en una situación dada. Los procedimientos son independientes de la tecnología o de los procesos y se refieren a las plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para

implementar la seguridad relacionada con dicho proceso o sistema específico. Generalmente los procedimientos son desarrollados, implementados y supervisados por el dueño del proceso o del sistema, los procedimientos seguirán las políticas de la entidad, los estándares, las mejores prácticas y las guías tan cerca como les sea posible, y a la vez se ajustarán a los requerimientos procedimentales o técnicos establecidos dentro del a dependencia donde ellos se aplican.

A continuación, se establecen 12 principios de seguridad que soportan el SGSI de la Contraloría General del Departamento del Chocó: -

1. La Contraloría General del Departamento protegerá su información de las amenazas originadas por parte del personal.

2. La Contraloría General del Departamento del Chocó protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

3. La Entidad controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos. •
4. La Entidad implementará control de acceso a la información, sistemas y recursos de red.
5. La Entidad garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
6. La Entidad garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
7. La Entidad garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
8. La Contraloría garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.
9. Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, socios de negocio o terceros.
10. La Contraloría General protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.

11. La La Contraloría General del Departamento del Chocó protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
12. La Contraloría General del Departamento del Chocó protegerá su información de las amenazas originadas por parte del personal.

Lineamientos

1. La Alta Dirección, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.
2. Para la Contraloria, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- ✓ Minimizar el riesgo en las funciones más importantes de la entidad. ¬
- ✓ Cumplir con los principios de seguridad de la información. ¬
- ✓ Cumplir con los principios de la función administrativa. ¬
- ✓ Mantener la confianza de sus clientes, socios y empleados. ¬

- ✓ Apoyar la innovación tecnológica. ¬
- ✓ Proteger los activos tecnológicos. ¬
- ✓ Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- ✓ Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de la Alcaldía Municipal de Quibdó
- ✓ Garantizar la continuidad del negocio frente a incidentes. ¬
- ✓ La alcaldía Contraloría ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

3. La información de la entidad debe ser clasificada de acuerdo con la estimación de confidencialidad, integridad, disponibilidad y requerimientos legales que la misma pueda tener (Ver Anexo 1 Clasificación de la Información).

4. Cada 6 meses se deberá elegir los miembros del Comité de Seguridad de la Información, el cual estará compuesto por el Secretario general, Jefe de la Oficina de la oficina de Sistemas, así como elegir al Oficial y/o líder en seguridad de la información para la entidad.

5. Es responsabilidad del jefe en cada una de las áreas realizar la correspondiente clasificación de la información, de acuerdo con lo establecido en la norma ISO 27001.

6. Es responsabilidad de la oficina de sistemas gestionar los controles de acceso de los usuarios, propendiendo por reducir el fraude, robo de información, uso mal intencionado de la misma y el error humano.

7. Los accesos otorgados a los colaboradores deben partir tanto de la clasificación de la información, como de la gestión que deben realizar desde el cargo y rol desempeñado en la Entidad.

8. Es responsabilidad de todos los funcionarios según su cargo y responsabilidades, administrar y gestionar la información a la cual tiene acceso para el desarrollo de su trabajo.

9. Es responsabilidad de la Oficina de Sistemas diseñar los controles orientados a prevenir los accesos físicos no autorizados, la seguridad ambiental y el acceso a dispositivos móviles.

10. Cada 6 meses se realizarán pruebas de acceso para la información con mayor nivel de criticidad, validando los controles implementados, por expertos externos.

11. Es deber de nuestra entidad cumplir con todas las normas externas de la geografía en la cual operamos y las cuales regulan la administración y seguridad de la información, para lo cual es responsabilidad de la Oficina de Sistemas actualizar el documento del anexo con los cambios y/o nuevas regulaciones-

12. Es responsabilidad de la Secretaria General realizar la divulgación de la presente política a nivel interno, dado que cualquier violación frente a la seguridad de la información por parte de los usuarios puede causar una sanción externa por parte de los entes de control y/o de los dueños de la misma.

13. Los terceros que accedan a la RED de la Entidad, deben suscribir un acuerdo de aceptación tanto de la presenten política como de los procedimientos que regulan la seguridad de la información, así como cualquier incumplimiento de los mismos puede tener efectos legales en el desarrollo de contratos y/o convenios.

14. Todos los funcionarios deben acceder a la página Web para conocer regularmente las actualizaciones y/o los cambios que se han presentado en las políticas, y así desarrollar su trabajo y manejar dicha información.

15. Anualmente, se debe considerar un entrenamiento a los funcionarios sobre la seguridad de la información, que incluya tanto las políticas y procedimientos, así como la regulación externa, entre otros.

16. Cualquier cambio en los sistemas de información, debe considerar el riesgo de seguridad que los mismos pueden presentar y por tanto siempre deberá desarrollarse un plan para gestionar tanto el riesgo de seguridad, como de cumplimiento legal.

17. El plan de continuidad de la organización debe incluir dentro de su plan la gestión y seguridad de la información.

18. El retiro temporal o permanente de un usuario son causal de la suspensión temporal y/o permanente según corresponda de los accesos otorgados a los usuarios.

19. Los equipos de uso para los funcionarios tanto fijos como móviles que contengan información, deberán contar con un procedimiento para retirar su información, una vez el funcionario es retirado y/o trasladado del área.

20. El incumplimiento de la presente política por parte de los funcionarios, es causal para iniciar un proceso disciplinario, que puede inclusive terminar en el despido con justa causa.

21. Cualquier incidente con el manejo de la información que un usuario identifique y/o observe en el desarrollo de su trabajo debe reportarlo a la Secretaria General

22. Cualquier duda de interpretación de la presente política debe ser resuelta por la Oficina de Sistemas.

SEGUIMIENTO Y MONITOREO

La Oficina Sistemas mediante el procedimiento de Revisión por la Dirección realizarán el monitoreo de la Política de Seguridad de la Información por lo menos una vez al año. Los líderes de los procesos harán la revisión de los controles establecidos según la periodicidad definida en el procedimiento de administración de riesgos definido por la entidad. La Oficina de Control Interno realizará la evaluación independiente según los lineamientos establecidos en el procedimiento de auditorías aprobado por la entidad.

RECURSOS

El Comité Institucional de Gestión y Desempeño es responsable por asegurar los recursos para la implementación de esta política del Sistema de Gestión de Seguridad de la

Información, la cual hace parte de las políticas del Modelo Integrado de Planificación y Gestión – MIPG y la estrategia de Gobierno en línea.

Anexo 1 **Clasificación de la Información**

Clasificación	Definición	Tipo de Información
Clasificada	Acceso solo a miembros específicos según su rol	Información personal de funcionarios, información financiera y PQRD
Reservada	Acceso solo a miembros específicos según su rol	Procesos jurídicos coactivos, sancionatorios y de responsabilidad fiscal
Uso Interno	Acceso a todos los miembros de un área y/o proceso	Correspondencia interna, documentos de los Comité.
Publica	Acceso a todo el publico	Reglamentos, normas, página web

La presente Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de la administración de la Contraloría General del Departamento del Chocó con respecto a la protección de los activos de información (los funcionarios, contratistas, terceros. la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la

asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

Dada en Quibdó, el 31 de agosto de 2018.

PAZLEYDA MURILLO MENA
Contralora General del Departamento del Chocó