Corporación Autónoma Regional del Tolima
¡Siembra Tu Futuro!

# Manual De La Política Del Sistema De Gestión De Seguridad De La Información Sgsi

# 2023

Oficina Asesora de Direccionamiento Estratégico TIC

SIEMBRA TU FUTURO

www.cortolima.gov.co @Cortolima

@cortolima.tol @Cortolima

# TABLA DE CONTENIDO

*1. ALCANCE ..... 6*

**1.1 Objetivo ..... 6**

**1.2 Estado y Aplicabilidad ..... 6**

**1.3 A Quien Está Dirigido ..... 7**

*2. TÉRMINOS Y DEFINICIONES ..... 8*

*3. DOCUMENTACIÓN DE SEGURIDAD DE LA INFORMACIÓN ..... 19*

**Fundamento de Documentación ..... 19**

**3.1 Objetivo: ..... 19**

3.1.1 Políticas de Seguridad de la Información: ..... 19

3.1.2 Plan de Gestión de Riesgos de Seguridad de la Información: ..... 19

3.1.3 Plan de Seguridad de la Información: ..... 20

3.1.4 Estándares de Seguridad de la Información: ..... 20

3.1.5 Procedimientos de Seguridad de la Información: ..... 20

3.1.6 Guías de Seguridad de la Información: ..... 20

**3.2 Revisión y Mantenimiento de la Documentación ..... 21**

*4. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN ..... 22*

**4.1 Revisiones de Seguridad de la Información ..... 22**

**4.2 Gestión de Conflicto de Intereses ..... 22**

*5. POLÍTICA ESTRATÉGICA DEL SGSI ..... 23*

**5.1 Objetivos de Seguridad de la Información ..... 23**

**5.2 Indicadores de Gestión de SGSI ..... 24**

*6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN ..... 25*

**6.1 Organización Interna. ..... 25**

6.1.1 Roles y Responsabilidades Para SI. ..... 25

6.1.1.1 Funciones y responsabilidades del Comité: ..... 26

6.1.2 Oficial de seguridad de la información: ..... 26

6.1.2.1 Funciones y responsabilidades del oficial de seguridad de la información: ..... 26

6.1.3 Propietario de activos de información ..... 27

6.1.3.1 Funciones y responsabilidades del propietario del activo de información: ..... 27
6.1.4 Custodio de la información ..... 28
6.1.4.1 Funciones y responsabilidades del custodio de la información: ..... 28
6.1.5 Usuario final ..... 28
6.1.5.1 Funciones y responsabilidades del usuario final: ..... 29
6.1.6 Directrices específicas CORTOLIMA ..... 29

**6.2 Contacto con Autoridades ..... 29**

**6.3 Contacto con Grupos de Interés ..... 29**

**6.4 Dispositivos Móviles ..... 30**

**6.5 Seguridad de la información Gestión de Proyectos ..... 30**

***7. SEGURIDAD DE LOS RECURSOS HUMANOS ..... 31***

**7.1 Selección de Empleados ..... 31**

**7.2 Términos y Condiciones de Empleo ..... 31**

**7.3 Proceso Disciplinario ..... 32**

**7.4 Terminación del Contrato o Traslado ..... 32**

**7.5 política de reporte de novedades de personal ..... 33**

**7.6 Toma de Conciencia ..... 33**

***8. GESTIÓN DE ACTIVOS ..... 34***

**8.1 Clasificación de la Información. ..... 34**

**8.2 Inventario de Activos de Información. ..... 34**

**8.3 Disposición de Información en Medios Removibles. ..... 34**

**8.4 Uso de los Activos de Información de Propiedad de la Corporación ..... 35**

**8.5 Uso de Internet ..... 36**

**8.6 Uso de mensajería instantánea y redes sociales. ..... 36**

**8.7 Uso de discos de red o carpetas virtuales. ..... 37**

**8.8 Uso de impresoras y del servicio de Impresión. ..... 37**

**8.9 Uso de servicio de correo electrónico. ..... 38**

**8.10 Uso de Telefonía ..... 38**

**8.11 Uso de servicio de digitalización ..... 39**

**8.12 Devolución de Activos. ..... 39**

**8.13 Disposición Final de Activos de Información ..... 39**

***9. CONTROL DE ACCESO ..... 41***

**9.1 Sistemas Operativos. ..... 41**

**9.2 Aplicaciones ..... 41**

**9.3 Internet. ..... 42**

**9.4 Equipos de Cómputo. ..... 42**

**9.5 Servidores. ..... 43**

**9.6 Correo Electrónico. ..... 44**

**9.7 Bases De Datos. ..... 44**

**9.8 Administración de Accesos de Usuarios. ..... 45**

**9.9 Acceso a Redes. ..... 45**

**9.10 Revisión y Retiro de los Derechos de Acceso. ..... 46**

**9.11 Accesos Privilegiados. ..... 47**

**9.12 Contraseñas. ..... 47**

9.12.1 Los usuarios deben tener en cuenta los siguientes aspectos: ..... 48

9.12.1.1 Las contraseñas deben: ..... 48

***10. SEGURIDAD FÍSICA Y DEL ENTORNO ..... 50***

**10.1 Seguridad del Cableado y Puntos de Red. ..... 50**

**10.2 Mantenimiento de Equipos Tecnológicos. ..... 50**

**10.3 Seguridad Centro de Procesamiento de Datos. ..... 51**

10.3.1 El centro de procesamiento datos debe estar provisto de: ..... 52

**10.4 Suministro de Equipos de Soporte Energético. ..... 53**

**10.5 Perímetro de Seguridad de áreas seguras. ..... 53**

**10.6 Retiro de las instalaciones de Equipos de propiedad de la Entidad. ..... 53**

**10.7 Trabajo en Áreas Seguras y Oficinas. ..... 53**

**10.8 Escritorio y Pantalla Limpia. ..... 54**

***11. SEGURIDAD DE LAS OPERACIONES ..... 55***

**11.1 Procedimientos de Operación Documentados. ..... 55**

**11.2 Gestión de Cambios. ..... 55**

**11.3 Gestión de Capacidad..... 55**

**11.4 Segregación de Ambientes de Desarrollo, Pruebas y Producción. ..... 56**

**11.5 Protección Contra Código Malicioso. ..... 56**

**11.6 Respaldo de Información. ..... 57**

**11.7 Sincronización de Relojes ..... 58**

**11.8 Vulnerabilidades Técnicas. ..... 58**

***12. SEGURIDAD DE LAS COMUNICACIONES..... 59***

**12.1 Gestión De Redes..... 59**

**12.2 Transferencia De Información. ..... 59**

***13. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS ..... 60***

**13.1 Principios de Desarrollo de Software. ..... 60**

**13.2 Desarrollo Seguro, Realización de Pruebas y Soporte ..... 61**

**13.3 Estrategia de Pruebas de Software. ..... 61**

***14. RELACIONES CON PROVEEDORES..... 62***

**14.1 Servicios Tercerizados. ..... 62**

***15. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN..... 63***

***16. SEGURIDAD DE INFORMACIÓN Y LA CONTINUIDAD DE SERVICIO ..... 64***

***17. CUMPLIMIENTO ..... 65***

**17.1 Legislación Aplicable. ..... 66**

**17.2 Protección de Datos y Privacidad de Información Personal..... 66**

**17.3 Derechos de Propiedad Intelectual. ..... 66**

**17.4 Protección de Registros..... 66**

**17.5 Cumplimiento de Políticas..... 66**

***18. PROCESO DE CONTROL INTERNO A LA GESTIÓN Y/O CONTROL INTERNO DISCIPLINARIO..... 68***

***19. CONTROL DE CAMBIOS..... 68***

# 1. ALCANCE

## 1.1 Objetivo

Comunicar las directrices, políticas y estándares de seguridad de la información que permitan asegurar la protección constante y adecuada de los activos de información de la Corporación Autónoma regional del Tolima – CORTOLIMA, a través de la comprensión de los objetivos de seguridad de la información y el soporte a las políticas presentadas en el presente documento, por parte de todos los funcionarios, contratistas, SENAS, pasantes, judicantes o partes interesadas que presten sus servicios o tengan algún tipo de relación con la Corporación.

## 1.2 Estado y Aplicabilidad

El presente manual aprobado por el Comité Institucional de Desempeño fue elaborado y revisado por los funcionarios que hacen parte de la Mesa Temática de Gestión Tecnológica y Seguridad de la Información en los cuales se encuentran los principios, políticas, estándares y demás lineamientos concernientes a las políticas de seguridad, este documento se convierte en un acto mandatorio y de estricto cumplimiento como directriz para la Corporación Autónoma Regional del Tolima - CORTOLIMA.

El manual de seguridad de la información es aplicable para:

- Toda la Corporación Autónoma Regional del Tolima - CORTOLIMA.

- Todos los aspectos administrativos y de control que deben ser cumplidos por los funcionarios, o partes interesadas que presten sus servicios o tengan algún tipo de relación con Corporación Autónoma regional del Tolima – CORTOLIMA, para el adecuado cumplimiento de sus funciones y para conseguir un adecuado nivel de protección de las características de calidad y seguridad de la información, aportando con su participación en la toma de medidas preventivas y correctivas, siendo un punto clave para el logro del objetivo y la finalidad de dicho manual.

- Todos los activos de información de propiedad de la Corporación Autónoma Regional del Tolima.

Las declaraciones de políticas y lineamientos de seguridad de la información serán compatibles con una serie de controles de seguridad documentados en procedimientos de

operación, controles técnicos incorporados y sistemas de información, y otros controles de aplicación por parte de los funcionarios y/o terceros a través de su desempeño de sus labores dentro de la Entidad.

### 1.3 A Quien Está Dirigido

- Mesa Temática de Gestión Tecnológica y Seguridad de la Información, como el marco de referencia para el sistema de gestión de seguridad de la información.

- Direccionamiento Estratégico TIC, Incluyendo los funcionarios quienes laboran en la oficina Asesora y el personal de apoyo.

- Gestión de Soporte TIC, Incluyendo los funcionarios quienes laboran en la oficina y el personal de apoyo.

- Otros procesos tales como: Relacionamiento Institucional, Planeación Institucional y Direccionamiento Estratégica, Direccionamiento estratégico TIC, Desarrollo Ambiental Sostenible, Autorizaciones, permisos y licencias Ambientales, Control, Seguimiento, Vigilancia y Sancionatorios, Planificación Ambiental Sostenible, Gestión Financiera, Gestión de Talento Humano, Gestión de Ingresos, Gestión de Contratación, Defensa Jurídica, Gestión de Soporte TIC, Gestión Documental, Gestión Administrativa, Servicio al Ciudadano y Evaluación Institucional

- Funcionarios y Terceras partes, tales como proveedores, contratistas, SENAS, pasantes auditores externos, entidades de orden nacional, departamental y municipal, ONG´s y organismos de control, quienes:

    1. Deben ser informados de las responsabilidades de seguridad a través de los términos y condiciones o contratos laborales, procedimientos de seguridad y guías, capacitación y sensibilización.

    2. Requieren de su consulta para la comprensión de la estructura y conformación de la seguridad de la información, en beneficio del cumplimiento de las obligaciones legales, contractuales y demás aplicables.

# 2. TÉRMINOS Y DEFINICIONES

A continuación de identifica una serie de términos y definiciones que soportan, guían y sensibilizan los propósitos del manual de seguridad de la información, y que apoyarán su uso, aplicabilidad y/o consulta.

- **Acción correctiva:** Medida de tipo reactivo orientada a eliminar la causa de una no conformidad asociada a la implementación y operación del SGSI con el fin de prevenir su repetición.

- **Acción preventiva:** Medida de tipo pro-activo orientada a prevenir potenciales no conformidades asociadas a la implementación y operación del SGSI.

- **Aceptación del Riesgo:** Decisión de aceptar un riesgo.

- **Activo de Información:** Según [ISO/IEC 13335-12004]: Cualquier cosa que tiene valor para la organización. También se entiende por cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización.

Un activo de información es un elemento definible e identificable que almacena registros, datos o información en cualquier tipo de medio y que es reconocida como “Valiosa” para la Corporación Autónoma regional del Tolima – CORTOLIMA.; Independiente del tipo de activo, se deben considerar las siguientes características:

No es fácilmente reemplazable sin incurrir en costos, habilidades especiales, tiempo, recursos o la combinación de los anteriores.

Forma parte de la identidad de la organización y sin el cual la Corporación Autónoma regional del Tolima – CORTOLIMA puede estar en algún nivel de riesgo. (La determinación del nivel y tipo de riesgo se estima sobre la base del modelo de MIPG de la Corporación Autónoma regional del Tolima – CORTOLIMA). Se pueden clasificar de la siguiente manera:

- **Información:** Son todos aquellos elementos básicos de la información (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en Corporación Autónoma regional del Tolima – CORTOLIMA.

- **Aplicaciones:** Es todo el software que se utiliza para la gestión de la información. Ejemplo: Actuaciones Ambientales.

- **Personal:** Es todo persona (partes interesadas), que tengan acceso de una manera u otra a los activos de información de la Corporación Autónoma regional del Tolima – CORTOLIMA.

- **Servicios:** Son tanto los servicios internos, aquellos que una parte de la organización suministra a otra, como los externos, aquellos que la organización suministra a los clientes internos y externos.

- **Tecnología:** Son todos los equipos utilizados para gestionar la información y las comunicaciones.

- **Instalaciones:** Son todos los lugares en los que se alojan los sistemas de información.

- **Documentos:** Son todos aquellos recursos en los cuales se encuentra impresa información de la Entidad.

- **Administración de riesgos:** Gestión de riesgos, es un enfoque estructurado para manejar la incertidumbre relativa a una amenaza, a través de una secuencia de actividades humanas que incluyen evaluación de riesgo, estrategias de desarrollo para manejarlo y mitigación del riesgo utilizando recursos gerenciales. Las estrategias incluyen (1) transferir el riesgo a otra parte o tercero, (2) evitar el riesgo, (3) reducir o mitigar los efectos negativos y probabilidades del riesgo y (4) aceptar algunas o todas las consecuencias de un riesgo particular.

- **Administración de incidentes de seguridad:** Un sistema de seguimiento de incidentes (denominado en inglés como issue tracking system, trouble ticket system o incident ticket system) es un paquete de software que administra y mantiene listas de incidentes, conforme son requeridos por una institución. Los sistemas de este tipo son comúnmente usados en la central de llamadas de servicio al cliente de una organización para crear, actualizar y resolver incidentes reportados por usuarios, o inclusive incidentes reportados por otros funcionarios, contratistas, colaboradores de la entidad o de terceras partes. Un sistema de seguimiento de incidencias también contiene una base de conocimiento que contiene información de cada cliente, soluciones a problemas comunes y otros datos relacionados. Un sistema de reportes de incidencias es similar a un Sistema de seguimiento de errores (bugtracker) y, en algunas ocasiones, una entidad de software puede tener ambos, y algunos bugtrackers pueden ser usados como un sistema de seguimiento de incidentes, y viceversa.

- **Alcance de SGSI:** Ámbito de la organización que queda sometido al Sistema de Gestión de seguridad de la información, en el cual se debe incluir la identificación clara de las

dependencias, interfaces y límites con el entorno, sobre todo si sólo incluye una parte de la organización.

- **Alerta:** Una notificación formal de que se ha producido un incidente relacionado con la seguridad de la información que puede evolucionar hasta convertirse en desastre.

- **Amenaza:** Según [ISO/IEC 13335-1:2004): causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

- **Análisis de riesgos:** Según [ISO/IEC Guía 73:2002): Uso sistemático de la información para identificar fuentes y estimar el riesgo.

- **Auditabilidad:** Los activos de información deben tener controles que permitan su revisión. Permitir la reconstrucción, revisión y análisis de la secuencia de eventos.

- **Auditor:** Persona encargada de verificar, de manera independiente, la calidad e integridad del trabajo que se ha realizado en un área particular.

- **Auditoria:** Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del SGSI de una organización.

- **Autenticación:** Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.

- **Autenticidad:** Los activos de información solo pueden estar disponibles verificando la identidad de un sujeto o recurso, Propiedad que garantiza que la identidad de un sujeto o recurso es la que declara, Se aplica a entidades tales como usuarios, procesos, sistemas de información.

- **Base de datos de gestión de configuraciones (CMDB, Configuration Management Database):** Es una base de datos que contiene toda la información pertinente acerca de los componentes del sistema de información utilizado en una organización de servicios de TI y las relaciones entre esos componentes. Una CMDB ofrece una vista organizada de los datos y una forma de examinar los datos desde cualquier perspectiva que desee. En este contexto, los componentes de un sistema de información se conocen como elementos de configuración (CI). Un CI puede ser cualquier elemento imaginable de TI, incluyendo software, hardware, documentación y personal, así como cualquier combinación de ellos. Los procesos de gestión de la configuración tratan de especificar, controlar y realizar seguimiento de elementos de configuración y los cambios introducidos en ellos de manera integral y sistemática.

- **Características de la Información:** las principales características son la confidencialidad, la disponibilidad y la integridad.

- **CobiT - Control Objectives for Information and related Technology:** Publicados y mantenidos por ISACA. Su misión es investigar, desarrollar, publicar y promover un conjunto de objetivos de control de Tecnología de Información rectores, actualizados, internacionales y generalmente aceptados para ser empleados por gerentes de empresas y auditores.

- **Compromiso de la Dirección:** Alineamiento firme de la Dirección de la organización con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI.

- **Computo forense:** El cómputo forense, también llamado informática forense, computación forense, análisis forense digital o exanimación forense digital es la aplicación de técnicas científicas y analíticas especializadas a infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.

- **Confiabilidad:** Se puede definir como la capacidad de un producto de realizar su función de la manera prevista, de otra forma, la confiabilidad se puede definir también como la probabilidad en que un producto realizará su función prevista sin incidentes por un período de tiempo especificado y bajo condiciones indicadas.

- **Confidencialidad:** Acceso a la información por parte únicamente de quienes estén autorizados, Según [ISO/IEC 13335-1:2004]:" característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.

- **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, (Nota: Control es también utilizado como sinónimo de salvaguarda).

- **Control correctivo:** Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas. Supone que la amenaza ya se ha materializado pero que se corrige.

- **Control detectivo:** Control que detecta la aparición de un riesgo, error, omisión o acto deliberado. Supone que la amenaza ya se ha materializado, pero por sí mismo no la corrige.

- **Control disuasorio:** Control que reduce la posibilidad de materialización de una amenaza, p.ej., por medio de avisos disuasorios.

- **Control preventivo:** Control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.

- **Declaración de aplicabilidad:** Documento que enumera los controles aplicados por el SGSI de la organización - tras el resultado de los procesos de evaluación y tratamiento de riesgos- además de la justificación tanto de su selección como de la exclusión de controles incluidos en el anexo A de la norma.

- **Denegación de servicios:** Acción iniciada por una persona u otra causa que incapacite el hardware o el software, o ambos y después niegue el servicio.

- **Desastre:** Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse la misma afectada de manera significativa.

- **Directiva:** Según [ISO/IEC 13335-1: 2004): una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.

- **Disponibilidad:** Según [ISO/IEC 13335-1: 2004): característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.

- **Evaluación de riesgos:** Según [ISO/IEC Guía 73:2002]: proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.

- **Evento:** Según [ISO/IEC TR 18044:2004]: Suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardas, o una situación anterior desconocida que podría ser relevante para la seguridad.

- **Evidencia objetiva:** Información, registro o declaración de hechos, cualitativa o cuantitativa, verificable y basada en observación, medida o test, sobre aspectos relacionados con la confidencialidad, integridad o disponibilidad de un proceso o servicio o con la existencia e implementación de un elemento del sistema de seguridad de la información.

- **Gestión de claves:** Controles referidos a la gestión de claves criptográficas.

- **Gestión de riesgos:** Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos.

Según [ISO/IEC Guía 73:2002]: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

- **Gusanos:** Es un programa de computador que tiene la capacidad de duplicarse a sí mismo. A diferencia del virus, no precisa alterar los archivos de programas, sino que reside en la memoria y se duplica a sí mismo. Siempre dañan la red (aunque sea simplemente consumiendo ancho de banda).

- **Impacto:** Resultado de un incidente de seguridad de la información.

- **Incidente:** Según [ISO/IEC TR 18044:2004]: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

- **Información:** La información constituye un importante activo, esencial para las actividades de una organización y, en consecuencia, necesita una protección adecuada. La información puede existir de muchas maneras. Puede estar impresa o escrita en papel, puede estar almacenada electrónicamente, ser transmitida por correo o por medios electrónicos, se la puede mostrar en videos, o exponer oralmente en conversaciones.

- **Ingeniería Social:** En el campo de la seguridad informática, es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos ganando su confianza muchas veces. Es una técnica que pueden utilizar investigadores privados, criminales, delincuentes computacionales (conocidos como cracker) para obtener información, acceso o privilegios en sistemas de información que les permiten realizar algún acto que perjudique o exponga a la persona o entidad a riesgos o abusos.

- **Integridad:** Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Según [ISOIIEC 13335-1: 2004]: propiedad/característica de salvaguardar la exactitud y completitud de los activos.

- **Inventario de activos:** Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.) dentro

del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

- **IPS:** Sistema de prevención de intrusos. Es un dispositivo que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos.

- **ISO:** Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de organizaciones nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares.

- **ISO 17799:** Código de buenas prácticas en gestión de la seguridad de la información adoptado por ISO transcribiendo la primera parte de BS7799. A su vez, da lugar a ISO 27002 por cambio de nomenclatura el 1 de julio de 2007. No es certificable.

- **ISO 19011:** "Guidelines for quality and/or environmental management systems auditing". Guía de utilidad para el desarrollo de las funciones de auditor interno para un SGSI.

- **ISO 27001:** Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO transcribiendo la segunda parte de BS 7799. Es certificable. Primera publicación en 20005.

- **ISO 27002:** Código de buenas prácticas en gestión de la seguridad de la información (transcripción de ISO 17799). No es certificable. Cambio oficial de nomenclatura de ISO 17799:20005 a ISO 27002:20005 el 1 de Julio de 2007.

- **ISO 9000:** Normas de gestión y garantía de calidad definidas por la ISO.

- **ISO/IEC TR 13335-3:** "Information technology. Guidelines for the management of IT Security .Techniques for the management of IT Security." Guía de utilidad en la aplicación de metodologías de evaluación del riesgo.

- **ISO/IEC TR 18044:** "Information technology. Security techniques. Information security incident management". Guía de utilidad para la gestión de incidentes de seguridad de la información.

- **ITIL - IT Infrastructure Library:** Un marco de gestión de los servicios de tecnologías de la información.

- **Keyloggers:** Aplicaciones que registran el teclado efectuado por un usuario.

- **Legalidad:** El principio de legalidad o Primacía de la ley es un principio fundamental del Derecho público conforme al cual todo ejercicio del poder público debería estar sometido a la voluntad de la ley de su jurisdicción y no a la voluntad de las personas (ej. el Estado sometido a la constitución o al Imperio de la ley). Por esta razón se dice que el principio de legalidad establece la seguridad jurídica, Seguridad de Información, Seguridad informática y garantía de la información.

- **No conformidad:** Situación aislada que, basada en evidencias objetivas, demuestra el incumplimiento de algún aspecto de un requerimiento de control que permita dudar de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo menor.

- **No conformidad grave:** Ausencia o fallo de uno o varios requerimientos de la ISO 27001 que, basada en evidencias objetivas, permita dudar seriamente de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo inaceptable.

- **No repudio:** Los activos de información deben tener la capacidad para probar que una acción o un evento han tenido lugar, de modo que tal evento o acción no pueda ser negado posteriormente.

- **PDCA - Plan-Do-Check-Act:** Modelo de proceso basado en un ciclo continuo de las actividades de planificar (establecer el SGSI), realizar (implementar y operar el SGSI), verificar (monitorizar y revisar el SGSI) y actuar (mantener y mejorar el SGSI).

- **Phishing:** Tipo de delito encuadrado dentro del ámbito de las estafas, que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria).

- **Plan de continuidad del negocio (Bussines Continuity Plan):** Plan orientado a permitir la continuación de las principales funciones de la Entidad en el caso de un evento imprevisto que las ponga en peligro.

- **Plan de tratamiento de riesgos (Risk treatment plan):** Documento de gestión que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

- **Política de seguridad:** Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información. Según

[ISO/IEC 27002:20005): intención y dirección general expresada formalmente por la Dirección.

- **Política dé escritorio despejado:** La política de la empresa que indica a los funcionarios, contratista y demás colaboradores la Corporación Autónoma regional del Tolima – CORTOLIMA deben dejar su escritorio libre de cualquier tipo de informaciones susceptibles de mal uso al finalizar el día.

- **Protección a la duplicidad:** La protección de copia, también conocida como prevención de copia, es una medida técnica diseñada para prevenir la duplicación de información. La protección de copia es a menudo tema de discusión y se piensa que en ocasiones puede violar los derechos de copia de los usuarios, por ejemplo, el derecho a hacer copias de seguridad de una videocinta que el usuario ha comprado de manera legal, el instalar un software de computadora en varias computadoras, o el subir la música a reproductores de audio digital para facilitar el acceso y escucharla.

- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Según [ISO Guía 73:2002]: combinación de la probabilidad de un evento y sus consecuencias.

- **Riesgo Residual:** Según [ISOIIEC Guía 73:2002] El riesgo que permanece tras el tratamiento del riesgo.

- **Salvaguarda:** Véase: Control.

- **Segregación de tareas:** Separar tareas sensibles entre distintos funcionarios o contratistas para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.

- **Seguridad de la información:** Según [ISO/IEC 27002:20005]: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio, trazabilidad y fiabilidad pueden ser también consideradas.

- **Selección de controles:** Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.

- **SGSI Sistema de Gestión de la Seguridad de la Información:** Según [ISO/IEC 27001: 20005]: la parle de un sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. (Nota: el sistema de gestión incluye una estructura de organización,

políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos).

- **Servicios de tratamiento de información:** Según [ISO/IEC 27002:20005]: cualquier sistema, servicio o infraestructura de tratamiento de información o ubicaciones físicas utilizados para su alojamiento.

- **Spamming:** Se llama spam, correo basura o sms basura a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina spamming. La vía más usada es el correo electrónico.

- **Sniffers:** Programa de captura de las tramas de red. Generalmente se usa para gestionar la red con una finalidad docente o de control, aunque también puede ser utilizado con fines maliciosos.

- **Spoofing:** Falsificación de la identidad origen en una sesión: la identidad es por una dirección IP o Mac Address.

- **Tercero o Tercera Parte:** Toda persona natural o jurídica que tenga algún tipo de relación contractual o laboral con la Corporación, y que no sean parte de la planta global de personal de la Entidad.

- **Tratamiento de riesgos:** Según [ISO/IEC Guía 73:2002]: Proceso de selección e implementación de medidas para modificar el riesgo.

- **Trazabilidad:** Propiedad que garantiza que la acción de una entidad se puede rastrear únicamente hasta dicha entidad.

- **Troyano:** Aplicación que aparenta tener un uso legítimo pero que tiene funciones ocultas diseñadas para sobrepasar los sistemas de seguridad.

- **Usuario:** En el presente documento se emplea para referirse a funcionarios y partes interesadas de la Corporación Autónoma regional del Tolima – CORTOLIMA, debidamente autorizados para usar equipos, sistemas o aplicativos informáticos disponibles en la red de la Corporación Autónoma regional del Tolima – CORTOLIMA y a quienes se les otorga un nombre de usuario y una clave de acceso.

- **Valoración de riesgos:** Según [ISO/IEC Guía 73:2002]: Proceso completo de análisis y evaluación de riesgos.

- **Virus:** tiene por objeto alterar el normal funcionamiento de la computadora, sin el permiso o conocimiento del usuario.

- **Vulnerabilidad:** Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISOIIEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

# 3. DOCUMENTACIÓN DE SEGURIDAD DE LA INFORMACIÓN

**Fundamento de Documentación**

**3.1 Objetivo:**

La documentación de seguridad de la información se deberá producir para describir propósitos estratégicos de seguridad de la información para demostrar el buen gobierno, entre otros como:

### 3.1.1 Políticas de Seguridad de la Información:

Documento de alto nivel que denota compromiso de la alta dirección con respecto a seguridad de la información, definición de reglas de comportamiento asociado a protección de activos de información.

Para proveer consistencia en la documentación se deberá tener en cuenta:

- Objetivos de la política
- Cómo los objetivos serán alcanzados
- Marco legal y guías de operación
- Partes interesadas
- Comunicación y sensibilización
- Recursos necesarios para soporte de la implementación
- Medición de desempeño
- Monitoreo y revisión
- Mantenimiento

### 3.1.2 Plan de Gestión de Riesgos de Seguridad de la Información:

Buena práctica para identificar y reducir riesgos de seguridad potenciales (marco de referencia)

Identificar la base de información que permita gestionar toda situación o amenaza potencial que pudiese impactar a la Entidad. Un marco de referencia donde se establezca el procedimiento para determinar los riesgos y su tratamiento, hasta su aceptación por parte de la alta dirección.

### 3.1.3 Plan de Seguridad de la Información:

Describe cómo implementar y operar controles dentro del SGSI, todos los sistemas deberán estar dentro de alcance de la documentación.

Se deberá identificar las actividades necesarias para el cumplimiento de los propósitos de seguridad de la información, al igual que los responsables de la ejecución de las mismas.

La definición de términos de tiempos de evaluación o seguimiento permitirán identificar desviaciones en el cumplimiento de las actividades y su necesidad de toma de decisiones.

Se deberá establecer sistemas de medición de desempeño del plan de seguridad de la información.

### 3.1.4 Estándares de Seguridad de la Información:

Son requerimientos particulares mandatorios que soportan políticas individuales.

### 3.1.5 Procedimientos de Seguridad de la Información:

Son mandatorios y describen el paso a paso y detalles de las acciones requeridas para completar una actividad o tarea.

Con el propósito de asegurar que el personal comprenda sus actividades de manera apropiada, sin oportunidad de confusión, es importante se defina roles y responsabilidades asociadas.

### 3.1.6 Guías de Seguridad de la Información:

Las guías contienen la descripción general diseñadas para lograr alcanzar los objetivos de una política, pero presentando el marco de referencia (recomendaciones).

### 3.2 Revisión y Mantenimiento de la Documentación

Toda la documentación asociada al sistema de gestión de seguridad de la información deberá ser revisada y/o actualizada (si aplica) con periodicidad por lo menos una vez al año, teniendo en cuenta la dinámica de la Entidad, sus procesos y demás.

# 4. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

La Corporación Autónoma regional del Tolima – CORTOLIMA., mediante el uso de sus facultades legales conferidas integró el grupo operativo denominado "MESA TEMÁTICA DE SEGURIDAD DE LA INFORMACIÓN Y LAS COMUNICACIONES", designando funciones y responsabilidades a sus integrantes y a su líder como Oficial de seguridad de la Información.

## 4.1 Revisiones de Seguridad de la Información

La postura de revisión de seguridad de la información de la Corporación Autónoma Regional del Tolima es anual, para responder a la identificación de las amenazas del momento, asociadas a cambios de la Entidad, ambientales, de plataforma tecnológica y/o documentación en general.

El enfoque de revisión de seguridad de la información se fundamenta en incidentes, cambios significativos y/o, pequeños cambios que pueden requerir revisiones de seguridad, orientados además en el mejoramiento continuo del sistema.

Se deberá programar y ejecutar la(s) auditoría(s) Internas del sistema de gestión de seguridad de la información, las cuales estarán a cargo de la Oficina de Control Interno a la Gestión en coordinación con el Sistema de Gestión Integrado.

## 4.2 Gestión de Conflicto de Intereses

Las revisiones deberán ser realizadas por personal independiente al objetivo de la evaluación o por una tercera parte independiente para garantizar que no hay conflicto de intereses, como postura de revisión de seguridad de la información de la Corporación Autónoma Regional del Tolima.

# 5. POLÍTICA ESTRATÉGICA DEL SGSI

La Política de Seguridad de la Información es la declaración general que representa la posición de la administración de la Corporación Autónoma Regional del Tolima – CORTOLIMA, con respecto a la protección de sus activos de información de la Entidad y para la cual identifica y publica la siguiente política:

*"CORTOLIMA reconociendo el valor de su información como uno de sus activos más valiosos y consciente de la importancia de su protección, desarrolla actividades dentro un sistema de gestión de seguridad de la información orientado a la conservación de su confidencialidad, disponibilidad e integridad, así como de los diferentes activos de información, sistemas tecnológicos e informáticos que la soportan, bajo una adecuada gestión de los riesgos asociados y el cumplimiento de todos los requisitos propios de su actividad, legales, reglamentarios y contractuales que le son de aplicabilidad; de esta manera, la Entidad busca mantener e incrementar la confianza de los usuarios y demás partes interesadas".*

## 5.1 Objetivos de Seguridad de la Información

Los objetivos de seguridad de la información permitirán apoyar el cumplimiento de los propósitos del sistema de gestión de seguridad de la información, a continuación, se identifican los objetivos, los cuales deberán ser revisados periódicamente y actualizados en su necesidad.

- Proteger los activos de información de la Corporación frente a amenazas tanto internas como externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de su confidencialidad, integridad y disponibilidad.

- Asegurar la implementación de las medidas de control necesarias para apoyar la política del sistema de gestión de seguridad de la información de la Corporación.

- Garantizar que los riesgos de seguridad de la información se mantengan en un nivel aceptable.

- Generar un ambiente de trabajo enfocado a la seguridad de la información por parte de los colaboradores y partes interesadas, en donde se identifique, se reconozca y valore su apoyo para el SGSI.

- Minimizar todo tipo de impacto negativo que por incidentes de seguridad de la información pudiese afectar a la Corporación.

- Mantener un ambiente de cumplimiento de requisitos de seguridad de la información de tipo legal o contractual aplicables a la Corporación.

### 5.2 Indicadores de Gestión de SGSI

Con el propósito de establecer el cumplimiento de los objetivos de seguridad de la información, se deberán definir puntos de referencia (indicadores de gestión) que permitan establecer el desempeño y posibles desviaciones para una toma de decisiones oportuna y eficaz;

Ejemplos de enfoques pueden ser.

- Cumplimiento de planes de seguridad de la información.

- Estados de efectividad de los controles de seguridad de la información implementados.

- Estados de efectividad en los procesos de seguridad de la información.

# 6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

**6.1 Organización Interna.**

Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de un marco de la Corporación, a través de:

## 6.1.1 Roles y Responsabilidades Para SI.

Mesa Temática de Gestión Tecnológica y Seguridad de la Información, integrado por los siguientes funcionarios:

- Oficina Asesora Territoriales o su delegado
- Oficina de Control Interno a la Gestión o su delegado
- Oficina Asesora de Control Interno disciplinario o su delegado
- Oficina Asesora de Planeación Institucional y Direccionamiento estratégico o su delegado.
- Subdirección Jurídica o su delegado.
- Subdirección de planeación Ambiental y Desarrollo Sostenible o su delegado.
- Subdirección de Desarrollo Ambiental Sostenible o su delegado.
- Subdirección de Administración de Recursos Naturales o su delegado.
- Subdirección Administrativa y Financiera o su delegado.
- Oficina Asesora de Direccionamiento Estratégico TIC o su delegado.
- Profesional Especializado Oficina Asesora de Direccionamiento Estratégico TIC.
- Profesionales Universitarios Oficina Asesora de Direccionamiento Estratégico TIC

#### 6.1.1.1 Funciones y responsabilidades del Comité:

- Establecer la alineación estratégica de la seguridad de la información con los objetivos estratégicos de la Corporación.

- Identificar y aprobar el alcance, la política del sistema de seguridad de la información y sus objetivos como sistema de gestión.

- Aprobar el manual de políticas de seguridad de la información y sus diferentes actualizaciones.

- Aprobar políticas y lineamientos de gestión de seguridad de la información y de seguridad informática.

- Revisar y aprobar las actualizaciones del sistema de gestión de seguridad de la información por lo menos una vez al año, con el propósito de asegurar su continua conveniencia, idoneidad y efectividad.

- Evaluar y aprobar el plan de desarrollo tecnológico.

- Evaluar y aprobar lineamientos asociados a continuidad de negocio.

### 6.1.2 Oficial de seguridad de la información:

Se designa por parte del comité el oficial de seguridad del sistema el cual debe ser al Líder del Sistema de Gestión Integrado como oficial de seguridad de la información, quien, con independencia de otras responsabilidades, tiene la responsabilidad de:

#### 6.1.2.1 Funciones y responsabilidades del oficial de seguridad de la información:

- Apoyar en el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejoramiento continuo del sistema de gestión de seguridad de la información.

- Crear planes de seguridad de la información para soportar los objetivos estratégicos y tácticos del SGSI.

- Identificar mecanismos de control y medición del cumplimiento de las metas de los planes de seguridad de la información.

- Participar en las actividades de revisión, actualización y divulgación de la política de seguridad de la información, sus directrices y procedimientos que la soportan.

- Establecer procesos que permitan determinar tendencias futuras de seguridad de la información.

- Monitorear la gestión de los riesgos de seguridad de la información de la Corporación.

- Establecer mecanismos que permitan monitorear vulnerabilidad en la red, aplicaciones de negocio y demás activos de información críticos de la Corporación.

- Participar en la definición de la estrategia de sensibilización, entrenamiento y educación en seguridad de la información.

- Apoyar al equipo auditor en los ejercicios de auditoría tanto internas como externas y en el suministro de la documentación sobre los controles de seguridad de la información implementados.

- Difundir entre los miembros de la Corporación, la cultura de la seguridad de la información y asegurar el buen funcionamiento del proceso.

### 6.1.3 Propietario de activos de información

Se designa al funcionario quien es responsable máximo de su protección, se puede nombrar también como dueño del activo de información, tiene la responsabilidad de:

#### 6.1.3.1 Funciones y responsabilidades del propietario del activo de información:

- Propender por el cumplimiento de la política de seguridad de la información para establecer y mantener la confidencialidad, la integridad y la disponibilidad de los activos de información a su cargo.

- Determinar el nivel de clasificación de cada uno de los activos de información de los cuales es responsable, de acuerdo con su sensibilidad y criticidad para el negocio y sus objetivos estratégicos.

- Gestionar los riesgos a los cuáles se encuentran expuestos los activos de información a su cargo.

- Definir los controles necesarios de seguridad para los activos de información de acuerdo a las situaciones de riesgos asociadas.

- Mantener control sobre la operación y eficacia de los controles implementados.

- Evaluar y autorizar el acceso y uso de los activos de información tanto a colaboradores, como otras partes interesadas, que por sus responsabilidades y/o necesidad lo requieran.

- Monitorear los niveles de acceso de colaboradores y partes interesadas a los activos de información para asegurar la confidencialidad e integridad de la información almacenada, resguardada o procesada en los mismos.

- Asegurar la devolución de los activos de información en situaciones de novedad de personal, tales como retiro definitivo o cambio de área.

### 6.1.4 Custodio de la información

Los cargos que desempeñan este rol son, todos aquellos colaboradores y/o partes interesadas, con designación formal por el propietario del activo de información, para la protección del activo de información.

#### 6.1.4.1 Funciones y responsabilidades del custodio de la información:

- Proveer operativamente el aseguramiento de la Confidencialidad, Integridad y Disponibilidad de la información.

- Proporcionar asistencia al Propietario del activo de Información en la selección de soluciones técnicas para mantener los niveles de seguridad apropiados.

- Apoyar en la identificación de controles que satisfagan los requerimientos de seguridad de la información especificados por el propietario del activo de información.

### 6.1.5 Usuario final

Los cargos que desempeñan este rol son: Todos los colaboradores o terceras partes a quienes por autorización expresa se le asigna acceso y/o uso del activo de información.

#### 6.1.5.1 Funciones y responsabilidades del usuario final:

- Mantener la confidencialidad e integridad de los activos de información provistos por la Entidad para llevar a cabo sus labores.

- Reportar las violaciones a las políticas de seguridad de la información identificadas al Oficial de Seguridad de la información.

- Aplicar las políticas y buenas prácticas de seguridad de la información de la Entidad incluidas en el Manual de Políticas de Seguridad de la Información.

### 6.1.6 Directrices específicas CORTOLIMA

Los Subdirectores, Jefes de oficina o asesores deben asegurarse que todos los procedimientos de seguridad de la Información dentro de sus áreas de responsabilidad, se realizan correctamente para lograr el cumplimiento de las políticas y estándares de seguridad de la información de la Corporación Autónoma regional del Tolima – CORTOLIMA.

Los líderes de las diferentes áreas de La Corporación Autónoma regional del Tolima – CORTOLIMA., en conjunto con el Comité de SGSI propiciarán actividades para concientizar al personal sobre las precauciones necesarias que deben realizar y/o tener en cuenta los usuarios finales, para evitar revelar información confidencial, interna o privada de la Entidad por cualquier medio posible.

## 6.2 Contacto con Autoridades

La Corporación deberá identificar los contactos con aquellas autoridades con las cuales requiera de apoyo ante alguna situación de seguridad de la información que se identifique dentro de la Entidad; para aquellas situaciones de algún incidente de seguridad de la información, tal como, pérdida, robo, fuga u otra similar, y para la cual se requiera de la colaboración de una entidad (autoridad) para el reporte y seguimiento, se debe dar aviso a las autoridades competentes, luego que sea revisado y determinado por el Oficial de Seguridad de la Información (ver documento política).

## 6.3 Contacto con Grupos de Interés

Se deberán establecer los grupos de interés asociados, con los cuales se pueda tener contacto para el intercambio de información a modo de retroalimentación en temas de seguridad de la información (ver documento política).

### 6.4 Dispositivos Móviles

CORTOLIMA reconoce el alto grado de exposición que representa la información y los datos almacenados en dispositivos móviles (computadores portátiles, PDA´s, teléfonos inteligentes, Tabletas, etc.), institucionales y personales debido a sus riesgos asociados; por tanto, declara que:

Todo dispositivo móvil de propiedad de la Corporación deberá estar incluido dentro de un inventario de equipos tecnológicos, con la instalación del software autorizado y legal, configurado con los controles de seguridad de la información para la protección de su información.

- Todo dispositivo móvil (portátiles) que ingresa a la Corporación, deberá ser registrado tanto en su ingreso como en su retiro de las oficinas de la Entidad, incluidos aquellos que no son de propiedad de la Corporación.

- Los equipos móviles deberán contar con la protección de acceso a la información mediante la instauración de validación de usuario y contraseña o cifrado de disco.

- Se deberá disponer de la estrategia de solución de copias de seguridad de la información contenida en los dispositivos móviles de la corporación.

- Los equipos móviles deberán contar con el control de restricción de instalación de software y con el control de protección contra software malicioso.

### 6.5 Seguridad de la información Gestión de Proyectos

- Toda creación de proyectos que se requieran en la Corporación, deberá considerar las necesidades de seguridad y protección de la confidencialidad, disponibilidad e integridad información, a través del cumplimiento de todos los lineamientos y políticas identificadas en el manual de seguridad de la información.

# 7. SEGURIDAD DE LOS RECURSOS HUMANOS

Se debe asegurar que los funcionarios, contratistas y demás colaboradores de la Corporación Autónoma regional del Tolima – CORTOLIMA., entiendan sus responsabilidades en relación con las políticas de seguridad de la información, y actúen de manera consistente frente a las mismas, con el fin de reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información o los equipos utilizados para el tratamiento de la información.

La responsabilidad de seguridad de la información es parte de los términos y condiciones del contrato. La violación o no cumplimiento de cualquiera de las directrices documentadas en las políticas de seguridad de la información establecidas por la Corporación, serán argumentos para la aplicación de acciones disciplinarias y/o administrativas, sin perjuicio de acciones de otra índole que se deriven.

## 7.1 Selección de Empleados

El área de Gestión Humana deberá establecer los procedimientos para realizar una verificación de los requisitos de seguridad de personas, conocimiento, experiencia y referencias a todo candidato potencial que pueda llegar a ser empleado de la Entidad.

## 7.2 Términos y Condiciones de Empleo

Los funcionarios, contratistas, pasantes, judicantes, practicantes, terceros o cualquier persona que tenga una relación contractual o laboral con la Entidad, o que tenga acceso a los activos de información de la Corporación, deben mantener la confidencialidad de la información dentro o fuera de las instalaciones de la Entidad.

Los funcionarios, contratistas, pasantes, judicantes, practicantes, terceros o cualquier persona que tenga una relación contractual o laboral con la Entidad, deben ser sujeto a socialización de los propósitos del presente manual, y entender las políticas, los procedimientos y/o instructivos de seguridad definidos por la Corporación.

Los funcionarios, contratistas, pasantes, judicantes, practicantes, terceros o cualquier persona que tenga una relación contractual o laboral con la Entidad, aceptarán y cumplirán con las políticas, procedimientos y/o lineamientos presentados en el manual de seguridad de la información, mediante la firma de un compromiso de confidencialidad.

- Los funcionarios, contratistas, pasantes, judicantes, practicantes, terceros o cualquier persona que tenga una relación contractual o laboral con la Entidad, deben firmar el

Compromiso de confidencialidad en el momento de su vinculación. Los contenidos de los compromisos de confidencialidad deben ser revisados y/o actualizados (si aplica) por lo menos una vez al año.

- Previo a recibir su cuenta de acceso a los sistemas de aplicaciones de la Corporación, todos los empleados deberán firmar y aceptar una declaración de responsabilidad sobre las acciones realizadas con dichas cuentas, y que serán susceptibles a supervisión por parte de la Entidad.

### 7.3 Proceso Disciplinario

La corporación deberá asegurar la existencia de un proceso disciplinario para los empleados y su relación para con aquellas situaciones en que se cometan incumplimientos de las políticas por el manual de seguridad de la información exigidas.

- El proceso disciplinario no debe iniciarse sin una verificación previa de la ocurrencia del incumplimiento a los lineamientos de la seguridad de la información.

- El proceso disciplinario formal debe asegurar el tratamiento correcto y justo para los empleados que incumplan con las políticas de SI.

- El proceso disciplinario debe proporcionar una respuesta equilibrada que tome en consideración factores como la naturaleza y gravedad del incumplimiento y su impacto en el negocio.

- En caso de incurrir en conducta irregular por parte de un funcionario o contratista, el proceso dará la facultad de remover sus derechos de acceso y privilegios; y si fuere necesario, dar aviso a Control interno disciplinario y/o a las autoridades pertinentes según corresponda.

### 7.4 Terminación del Contrato o Traslado

- Se deberá establecer un procedimiento o instructivo a seguir para aquellas situaciones en que se presentan traslados de personal a cargos y responsabilidades diferentes y para terminación del contrato.

- Se debe asegurar que el compromiso de confidencialidad identifique las responsabilidades de confidencialidad de la información posterior a la desvinculación y terminación del contrato.

- Cualquier activo de información asignado por la Corporación a los funcionarios y/o contratistas, deberán ser regresados o devueltos a la misma, siguiendo los procedimientos establecidos.

### 7.5 política de reporte de novedades de personal

Talento Humanos deberá reportar oportunamente en el sistema de Información las novedades de personal (licencias No remuneradas, vacaciones, etc.) para la inactivación de usuarios durante el tiempo de su novedad.

### 7.6 Toma de Conciencia

La Corporación deberá definir la estrategia de sensibilización, entrenamiento y educación en seguridad de la información dirigida a los funcionarios, contratistas y demás, con el propósito de asegurar la responsabilidad sobre la protección de los activos de información en la Entidad.

# 8. GESTIÓN DE ACTIVOS

### 8.1 Clasificación de la Información.

La información de la Corporación deberá recibir el nivel de clasificación acorde a su sensibilidad y criticidad, para establecer y aplicar los controles de etiquetado y seguridad de información necesarios, que aseguren su confidencialidad, integridad y disponibilidad.

Toda información que es recibida, procesada y/o almacenada en medio físico y/o magnético en la Corporación es responsabilidad de su protección por parte de la Entidad y sus funcionarios y terceros.

La responsabilidad de realizar la clasificación de la información de la Corporación Autónoma regional del Tolima – CORTOLIMA, es de los propietarios de la misma; para ello y a manera de guía, se deberán conciderar las amenazas y los riesgos a los que se está expuesta, como pueden ser; copia, divulgación, modificación, eliminación o destrucción física o electrónica no autorizadas.

### 8.2 Inventario de Activos de Información.

Se deberá elaborar y mantener una lista de todos los activos de información dentro del alcance del SGSI, en la cual se especifique los activos de información de la Corporación, el nombre del activo de información, su ubicación física, el propietario del activo (responsable) y el custodio (responsable de su protección). Esta lista se debe actualizar por lo menos una vez al año.

Responsables de áreas de la Corporación deberán identificar y mantener el inventario de activos de información bajo su responsabilidad.

### 8.3 Disposición de Información en Medios Removibles.

Se deberán establecer los lineamientos para el uso de los medios removibles dentro de la Corporación.

El uso de dispositivos de almacenamiento externo (dispositivos móviles, DVD, memorias USB, agendas electrónicas, celulares, discos duros, etc.), podrían ocasionalmente generar riesgos para la entidad al ser conectados a los computadores, ya que son susceptibles de transmisión de virus informáticos o pueden ser utilizados para la extracción de información no autorizada, por lo tanto:

- Para el uso dispositivos de almacenamiento externo a través de los puertos USB de los equipos y/o unidades de lectura de disco de los componentes tecnológicos de propiedad de la Corporación, se deberá solicitar y obtener aprobación formal e individual por parte del Oficial de Seguridad de la Información. (definir el formato para solicitud y Autorización).

- Los medios removibles no deberán ser utilizados para realizar el intercambio de información sensible de los sistemas de información y aplicaciones.

### 8.4 Uso de los Activos de Información de Propiedad de la Corporación

El uso de los activos de información (equipos de cómputo, internet, correo electrónico, impresoras) de la Corporación debe ser exclusivamente con propósitos laborales.

- Los usuarios deberán utilizar únicamente los programas y equipos autorizados por la Corporación.

- Los datos/información creados, almacenados y recibidos desde y en los equipos tecnológicos asignados, serán propiedad de la Corporación; su copia, sustracción, daño intencional o utilización para fines distintos a las labores propias de la Entidad, determinará la actuación acorde con el proceso de control interno a la gestión y/o de control interno disciplinario.

- En caso de ser necesario y previa autorización del funcionario o contratista, la Corporación podrá realizar monitoreo o seguimiento al uso de activos de información asignados.

- Los activos de información de la Corporación no podrán ser utilizados para actividades de divulgación, propagación o almacenamiento de contenido personal o comercial de publicidad, promociones, ofertas, programas destructivos (virus), propaganda política, material religioso, o cualquier otro uso que no esté autorizado.

- Los funcionarios no podrán efectuar ninguna de las siguientes labores sin previa autorización de Soporte TIC:

    1. Instalar software en cualquier equipo de cómputo de propiedad de la Corporación.

    2. Bajar o descargar en los equipos de cómputo de propiedad de la Corporación a través de Internet u otro servicio en línea, software o material que pudiese vulnerar los derechos de autor.

3. Modificar, revisar, transformar o adaptar cualquier parámetro de configuración lógica del equipo o del software de propiedad de la Corporación.

4. Descompilar o realizar ingeniería inversa en cualquier software de propiedad de la Corporación.

5. Copiar o distribuir cualquier software de propiedad de la Corporación.

- Todo archivo o material electrónico recibido a través de medio removible, descarga a través de Internet o de cualquier red externa, previo a ser accedido o ejecutado en la infraestructura TIC de la Corporación, deberá ser analizado o revisado por antivirus en beneficio de la detección y prevención de virus u otros programas maliciosos.

**8.5 Uso de Internet**

Su propósito es establecer lineamientos que garanticen la navegación segura y el uso adecuado del (los) canales de red por parte de los usuarios finales, los cuales son:

- La Corporación tendrá el derecho a realizar monitoreo o seguimiento de los accesos a través de Internet realizados por los funcionarios; dicha actividad está basada en la previa puesta en conocimiento y aprobación por parte de los funcionarios a través del compromiso de Confidencialidad; de esta manera, la Oficina Asesora de Direccionamiento Estratégico TIC tendrá la potestad de restringir los accesos a aquellos sitios que pudiesen generar sobrecarga o vulnerabilidad técnica sobre la plataforma tecnológica de la Corporación.

- La navegación en Internet debe realizarse de forma razonable y con propósitos laborales.

- No se permite la navegación a sitios con contenidos orientados en contra de la ley o a las políticas que representen impacto para la entidad tales como, pornografía, terrorismo, contenidos obscenos, segregación racial o similares.

- Ningún funcionario o contratista podrá realizar ejercicios con propósitos de estudio o análisis de seguridad informática, sin autorización expresa del Asesor de Direccionamiento estratégico TIC.

**8.6 Uso de mensajería instantánea y redes sociales.**

- La Corporación tendrá el derecho a realizar monitoreo o seguimiento al uso de la mensajería instantánea y redes sociales utilizadas a través de Internet, teniendo en cuenta que su uso deberá ser con propósitos laborales; de esta manera, la Oficina Asesora de Direccionamiento Estratégico TIC tendrá la potestad de restringir su uso en aquellas situaciones que pudiesen generar sobrecarga o vulnerabilidad técnica sobre la plataforma tecnológica de la Corporación.

- En caso de uso de mensajería instantánea o redes sociales no se permitirá el envío de mensajes con contenido que atente contra la integridad de las personas o instituciones.

- La información que se publique o divulgue por cualquier medio (mensajería instantánea o redes sociales) por parte de un funcionario, contratista o colaborador de la Entidad, se considera fuera del alcance del SGSI y por lo tanto, los daños y perjuicios que pueda llegar a causar, serán de completa responsabilidad de la persona que la haya generado.

**8.7 Uso de discos de red o carpetas virtuales.**

- Disponibles exclusivamente para el almacenamiento de información institucional y serán suministradas y administradas por la Oficina Asesora de Direccionamiento Estratégico TIC. Es responsabilidad de cada funcionario mantener depurada la información de las carpetas virtuales, en beneficio de la optimización del uso de los recursos de almacenamiento que entrega la Entidad a los usuarios.

- El acceso a la información ubicada en discos en la red o el uso de tecnología de almacenamiento en la nube, deberá estar acompañado de una autorización por parte su jefe inmediato y Oficial de Seguridad de la información, indicando el tipo de permiso asignado (escritura, lectura o modificación de información).

- El almacenamiento de contenidos tales como pornografía, propaganda racista, terrorista o cualquier software ilegal o malicioso, fines publicitarios de imagen negativa, lucrativa o comercial en los discos de red o carpetas virtuales es estrictamente prohibido.

**8.8 Uso de impresoras y del servicio de Impresión.**

- Los documentos que se impriman en las impresoras de la Corporación, deberán ser de carácter institucional.

- Es responsabilidad del usuario conocer el adecuado manejo de los equipos de impresión (escáner y copiado) para que no se afecte su correcto funcionamiento.

- Labores de reparación o mantenimiento de las impresoras es exclusivo de ejecución por parte de Soporte TIC y ningún funcionario o persona podrá realizar dicha actividad.

**8.9 Uso de servicio de correo electrónico.**

- La Corporación tendrá el derecho a realizar monitoreo o seguimiento del uso del correo electrónico por parte de los funcionarios; dicha actividad está basada en la previa puesta en conocimiento y aprobación por parte de los funcionarios a través del Compromiso de Confidencialidad; de esta manera, la Oficina Asesora de Direccionamiento Estratégico TIC tendrá la potestad de restringir los accesos o realizar los bloqueos necesarios que pudieran generar vulnerabilidad técnica o fallas de seguridad.

- Los usuarios no deberán participar en correo electrónico que incite o incentive el envío de cadenas o publicidad que no sean interés o estén relacionados con la Corporación.

- Los usuarios no deberán realizar el envío o distribución de información catalogada como confidencial, interna o privada dentro o fuera de la de la Corporación, sin la autorización correspondiente del propietario de la misma.

- Los usuarios de correo electrónico no deberán usar lenguaje ofensivo, inapropiado o con declaraciones de blasfemia, obscenidad, ilegales, incitadores a infringir la ley, hostigamiento basado en sexo, raza, nacionalidad, contenido despectivo o difamatorio en cualquier mensaje electrónico para con sus compañeros, clientes, proveedores u otros.

- Se prohíbe el envío de correos masivos al interior de la organización; sólo los usuarios autorizados por el Jefe de la Oficina Asesora de Direccionamiento Estratégico TIC podrán enviar dichos correos.

- Está prohibido utilizar el correo electrónico para el intercambio de información o de software que violen las leyes de derechos de autor.

- Se prohíbe la difusión de información oficial de la Corporación a través de correos electrónicos no oficiales.

**8.10 Uso de Telefonía**

- Usuarios deberán tener cuidado al transmitir información por teléfono, ya que este medio no es seguro y puede ser interceptada por personas no autorizadas.

- Conversaciones o mensajes con información confidencial no deberán ser dejados con otras personas o en buzones de voz.

- El uso de la telefonía de la Corporación es exclusiva para propósitos institucionales; contraseñas asignadas para su uso serán de exclusividad por parte del funcionario a quien se le haya asignado.

### 8.11 Uso de servicio de digitalización

- El funcionario que haga uso de los recursos de digitalización, debe asegurar que el contenido del material digitalizado sea almacenado sólo con propósitos de la entidad.

- El material confidencial o privado que sea digitalizado deberá ser almacenado de manera segura y no compartido en carpetas de red controladas.

### 8.12 Devolución de Activos.

Se deberá asegurar que los funcionarios, contratistas, colaboradores y en general a todos aquellos a quienes se les haya asignado activos de información de la Corporación, realicen la devolución de los mismos a la terminación de su empleo o contrato.

Ante la devolución de equipos de cómputo, se deberán seguir procedimientos adecuados para asegurar que toda la información relevante, sea transferida, respaldada y/o eliminada de manera segura.

### 8.13 Disposición Final de Activos de Información

- Para todo equipo de cómputo que vaya a ser reasignado o retirado de servicio se deberá garantizar el respaldo y/o la eliminación de toda su información residente y mediante prácticas seguras disponibles.

- Para el retiro de equipos de cómputo por obsolescencia y/o daño, se deberá garantizar la aplicación del instructivo borrado de final de datos, es decir llevar a cabo buenas prácticas para la eliminación y/o destrucción de la información con herramientas automáticas que aseguren que la misma no pueda en ningún caso ser recuperada.

- En caso de la necesidad de destrucción física de discos duros se deberá asegurar buenas prácticas de destrucción adecuada o la entrega a personas o entidades con la competencia para tal actividad.

- Otros activos de información tales como documentos con información confidencial pero obsoleta o fuera de la necesidad de retención del mismo, deberán ser eliminados mediante destrucción física.

# 9. CONTROL DE ACCESO

## 9.1 Sistemas Operativos.

Inicio de sesión seguro

- Después de tres (3) intentos fallidos de autenticación consecutivos, las cuentas deben ser bloqueadas automáticamente

- El ingreso a sistemas operativos con usuarios por primera vez deberá exigir el cambio obligatorio de la contraseña.

- Usuarios temporales están permitida previa autorización, dichos permisos deberán ser deshabilitados tan pronto se finalice su propósito de uso.

- Equipo Desatendido e inactividad de la sesión

- El tiempo de bloqueo de las sesiones en los sistemas operativos por inactividad, deberá ser de 10 minutos.

- Uso de las utilidades del sistema solo está autorizado para Soporte TIC.

- Los servicios de configuración del sistema y los controles de aplicación utilizados para llevar a cabo el mantenimiento del sistema deberán:

    1. Ser documentados mediante procedimientos o instructivos de mantenimiento.

    2. Definir el procedimiento para la autorización de acceso y uso.

    3. Estar limitado a usuarios autorizados.

## 9.2 Aplicaciones

El acceso a las aplicaciones cualquiera sea su arquitectura, deberá cumplir los siguientes requerimientos de control de acceso:

- Autenticarse a través de usuario y contraseña

- La autorización de accesos deberá estar orientada al modelo basado en roles y bajo un modelo del menor privilegio.

- Todos los módulos de la aplicación deberán verificar la autenticidad del usuario y niveles de permisos asignados.

- Los accesos a las aplicaciones se deben restringir a nivel de usuario.

- Se deberá definir el alcance de la información de transacciones y las tablas de bases de datos sobre las cuales se mantendrá una bitácora de actividades, ejemplo:

  1. Nombre de usuario.

  2. Objeto al que accede.

  3. Fecha y Hora de Acceso.

  4. Tipo de Operación (ejemplo, Modificación, Borrado o Eliminación, Inserción).

**9.3 Internet.**

El acceso a internet es proveído por la Corporación como un apoyo al cumplimiento de objetivos de los procesos.

- Los accesos a Internet deberán ser concedidos y validados a través del Firewall corporativo, mediante el uso de listas de control de acceso (ACL).

- Los accesos deberán ser autenticados, autorizados y auditados.

- Los accesos deberán ser concedidos acorde a los roles definidos por la Corporación.

- Los accesos a través de Internet podrán ser monitoreados por la Entidad sin incurrir en violación de la privacidad, dado que el servicio de internet está destinado a actividades laborales.

- Los accesos a servicios P2P (por siglas en Inglés Peer to Peer – ejemplo, ARES, BIT TORRENT). No están permitidos.

**9.4 Equipos de Cómputo.**

- La solicitud para asignación de equipos de cómputo deberá ser formalmente presentada por los jefes inmediatos.

- El control de accesos a los equipos de cómputo se deberá realizar a través de un servicio de directorio activo, que permita su autenticación, autorización y auditoría.

- Ningún funcionario podrá tener privilegios de administrador local en su equipo de cómputo asignado solo el personal del Soporte TIC y los funcionarios autorizados de la Oficina Asesora de Direccionamiento Estratégico TIC.

- Los usuarios de equipos de cómputo no deberán modificar las configuraciones del mismo a través de herramientas administrativas del sistema.

- Instalaciones y tareas administrativas sobre los equipos de cómputo deberán ser realizadas por usuarios con privilegios autorizados por la Oficina Asesora de Direccionamiento Estratégico TIC.

- Se deberá crear una cuenta de administrador local con la asignación de una contraseña segura, para uso exclusivo del personal de Soporte TIC.

- Equipos de cómputo portátiles deberán ser protegidos físicamente cuando se encuentren fuera de las instalaciones de la Corporación en las actividades de alto riesgo o de campo.

- Los equipos portátiles deberán exigir la validación de usuario y contraseña para el inicio de la sesión en el sistema operativo.

- Discos duros de equipos portátiles de propiedad de la Corporación deberán contar con el control de cifrado de disco.

**9.5 Servidores.**

- Accesos a los servidores con sistema operativo Windows deberán ser controlados a través de un servicio de directorio activo; excepciones serán administradas por el proceso de Soporte TIC.

- El acceso debe estar autenticado, autorizado y auditado.

- No es permitida la conexión de dispositivos de almacenamiento externos sobre los servidores, salvo autorización de la Oficina Asesora de Direccionamiento Estratégico TIC y con propósitos justificados.

- Las contraseñas de acceso a servidores deberán cumplir con las condiciones mínimas de complejidad y seguridad.

- Contraseñas de acceso a equipos servidores deberán ser almacenadas en medio seguro y cifrado.

- El acceso administrativo a servidores se debe asignar por medio de usuarios personalizados identificables por funcionario, con la determinación de permisos mínimos necesarios para sus tareas administrativas.

- Cuentas de acceso de administración local deberán ser inactivadas.

- El acceso a tareas administrativas se deberá realizar por medio de protocolos seguros y cifrados, o por consola directa en el equipo.

- Los eventos generados por el servidor deberán ser registrados en la bitácora del sistema (registro de eventos).

- Se deberán realizar actividades de revisión y monitoreo a la bitácora del sistema (registro de eventos).

### 9.6 Correo Electrónico.

- El acceso a correo electrónico debe estar autenticado, autorizado y auditado.

- El acceso debe realizarse a través de protocolos seguros.

- la Oficina Asesora de Direccionamiento Estratégico TIC definirá los niveles de capacidad de envío y recepción de correos electrónicos.

- Todo correo electrónico podrá ser objeto de monitoreo por parte de la Corporación previa autorización del funcionario, sin incurrir en violación de la privacidad, dado que este servicio está destinado a actividades institucionales.

- El acceso a correo electrónico personal (Gmail, Hotmail y otros) no se utilizará para actividades corporativas.

### 9.7 Bases De Datos.

Para prevenir accesos no autorizados a las bases de datos:

- La autenticación a las bases de datos se debe realizar a través de un servicio de directorio activo.

- La autorización de acceso debe ser orientada a un modelo basado en roles y bajo un modelo del menor privilegio.

- El acceso debe estar autenticado, autorizado y auditado.

- Se debe renombrar la cuenta de DBA, aquellas por defecto, y establecer contraseñas seguras.

- Contraseñas de acceso a usuarios administradores de bases de datos deberán ser almacenadas en medio seguro y cifrado.

- El acceso administrativo se debe realizar por usuarios identificables e intransferibles y se deben determinar los permisos mínimos necesarios para sus tareas administrativas.

- Se deben activar los mecanismos de auditoría para aquellas operaciones sobre la base de datos que la Oficina Asesora de Direccionamiento Estratégico TIC considere pertinentes.

- No se permite la ejecución de consultas por parte de usuarios no administrativos.

- No se permitirá realizar modificaciones a la información directamente sobre la base de datos. Solo se podrá realizar bajo la aprobación del propietario de la información y en situación excepcionales con apoyo y control de la Oficina Asesora de Direccionamiento Estratégico TIC.

- Bases de datos deberán ser sujetas a revisiones regulares de integridad.

- Toda base de datos deberá tener asociado un diccionario de datos y la asignación de su responsabilidad.

### 9.8 Administración de Accesos de Usuarios.

Se deberán implementa procedimientos formales para controlar la asignación de derechos de acceso a los sistemas, datos y servicios de información (solicitud, modificación y/o eliminación de usuarios).

### 9.9 Acceso a Redes.

- Los accesos a la red deberán ser concedidos por un servidor DHCP y controlados a través del directorio activo del domino.

- El servicio de red deberá prestarse a los servidores, equipos de trabajo y dispositivos que sean propiedad de la Corporación, incluidos de terceros con previa autorización por parte de la Oficina Asesora de Direccionamiento Estratégico TIC

- Un procedimiento formal deberá ser documentado para indicar cómo realizar el requerimiento, la autorización y el acceso a recursos de la plataforma de TI.

- Tráfico de la red podrá ser monitoreado sin incurrir en violación de la privacidad, dado que el servicio de red está destinado a actividades laborales.

- El acceso tanto local como remoto deberá ser autenticado, autorizado y auditado.

- Se deben definir segmentos de red que permitan la separación de los servicios críticos e información sensible de la Entidad.

- Los accesos a los recursos de red deberán asegurar los controles para los siguientes servicios:

    1. Sistemas de mensajería

    2. Transferencias de archivos

    3. Acceso interactivo a los sistemas y aplicaciones.

- Los funcionarios de la Corporación solo tendrán acceso a los servicios de red para cuyo acceso y uso estén autorizados.

- la Oficina Asesora de Direccionamiento Estratégico TIC implementará los controles de seguridad lógica necesarios para proteger el acceso a las conexiones y servicios de red.

### 9.10 Revisión y Retiro de los Derechos de Acceso.

La revisión y retiro de derechos de acceso incluyen, acceso físico, acceso lógico, asignación de llaves, tarjetas de identificación, acceso biométrico y medios de procesamiento de información.

- Revisiones periódicas deberán ser realizadas con respecto a los derechos de acceso de usuarios y de manera individual, por parte de los propietarios de los sistemas de información.

- Los derechos de acceso de todos los funcionarios, contratistas y terceros a la información deben ser retirados de manera inmediata a la terminación de su empleo, contrato o acuerdo, firmando la lista de verificación al terminar la vinculación con la Corporación.
- Los cambios de un cargo deberán asegurar y evidenciar el retiro de todos los derechos de acceso asignados; los nuevos accesos por asignar deberán ser aprobados y acordes a su rol funcional.

### 9.11 Accesos Privilegiados.

Se limitará y controlará la asignación y uso de accesos con privilegios, debido a que su uso inadecuado podría resultar frecuentemente en el factor más importante que contribuye a los ataques a los sistemas.

Los sistemas multiusuario que requieren protección contra accesos no autorizados, deben prever una asignación de privilegios controlada mediante un proceso de autorización formal. Se deben tener en cuenta los siguientes pasos:

- Identificar los privilegios asociados a cada producto del sistema, por ejemplo, sistema operativo, sistema de administración de bases de datos y aplicaciones, y las categorías de personal a las cuales deben asignarse los productos.

- Asignar los privilegios sobre la base de la necesidad de uso y por nivel de requerimiento mínimo para su rol funcional.

- Los privilegios no deben ser otorgados hasta tanto se haya completado el procedimiento formal de autorización.

- Promover el desarrollo y uso de rutinas del sistema para evitar la necesidad de otorgar privilegios a los usuarios.

- El comité de seguridad de la Información, mediante la aprobación de procedimientos, estará encargado de la asignación de privilegios a los diferentes roles que se determinen.

- El área de Gestión Tecnológica se encargará de asignar los privilegios a los usuarios, dependiendo al rol respectivo para cada uno.

### 9.12 Contraseñas.

- Se deberán realizar sesiones de capacitación y concientización dirigida a los funcionarios y/o contratistas a quienes se les otorga acceso mediante usuario y contraseña.

- Se deberá cumplir con un mínimo de complejidad y seguridad en la creación y cambio de contraseña.
- Los funcionarios y/o contratistas son responsables del uso de las claves o contraseñas de acceso que se le asignen para la utilización de los equipos o servicios informáticos de la Entidad.

### 9.12.1 Los usuarios deben tener en cuenta los siguientes aspectos:

- No registrar las contraseñas en ningún medio físico o lógico.

- El cambio de contraseña solo podrá ser solicitado por el titular de la cuenta.

- Las sesiones inactivas deberán ser terminadas o bloqueadas cuando no estén en uso o en su ausencia del lugar de trabajo.

- Se bloqueará el acceso a todo usuario que haya intentado el ingreso sin éxito (3 intentos fallidos de manera consecutiva).

- La clave de acceso será desbloqueada sólo por la Oficina Asesora de Direccionamiento Estratégico TIC y basada con la solicitud formal por parte del responsable de la cuenta.

#### 9.12.1.1 Las contraseñas deben:

- Poseer algún grado de complejidad y no deben ser palabras comunes que se puedan encontrar en diccionarios, ni tener información personal, por ejemplo: fechas de cumpleaños, nombre de los hijos, placas de automóvil, etc.

- Tener mínimo ocho (8) caracteres alfanuméricos.

- La entrega del usuario por parte de la Oficina Asesora de Direccionamiento Estratégico TIC estará acompañada de una contraseña temporal, la cual deberá ser modificada por solicitud automática y como requisito para su uso.

- La contraseña de acceso a la Red deberá tener una expiración automática para su cambio obligatorio cada 60 días.

- Cada vez que se cambien las contraseñas, deberá existir la validación automática del histórico (2 últimas anteriores).

- Cambiar la contraseña si ha estado bajo riesgo o se ha detectado anomalía en la cuenta de usuario.

- No se deben usar caracteres idénticos, consecutivos, ni que sean todos numéricos, ni todos alfabéticos.

- No debe ser visible en la pantalla, deben estar protegidas.

- No ser reveladas a ninguna persona.

- No ser registradas en papel, archivos digitales o dispositivos manuales, a menos que se puedan almacenar de forma segura y el método de almacenamiento este aprobado.

# 10. SEGURIDAD FÍSICA Y DEL ENTORNO

## 10.1 Seguridad del Cableado y Puntos de Red.

- Se deberán realizar monitoreos periódicos, por lo menos una vez al año, sobre seguridad física de las redes de cableado y los gabinetes de cableado.

- Se deberá mantener la identificación de la configuración de la infraestructura de la red y de cada centro de cableado.

- Instalaciones de ductos para cableado de voz, datos y eléctrico deberán asegurar segregación de los mismos, con el ánimo de evitar y/o reducir interferencia o interceptación.

- Los centros de cableado (áreas seguras) deberán tener una evaluación de amenazas y riesgos de tipo ambientales y seguridad física, con la cual se detetrermine el plan de tratamiento y los controles a implementar.

NOTA: Una evaluación de riesgos ambientales deberá estar orientada a la identificación de amenazas tales como, fuego, humo, agua, polvo, vibraciones, agentes químicos o radiaciones electromagnéticas, y de acceso físico no autorizado; y un plan de tratamiento de riesgos orientados a la definición de controles ambientales tales como, sistemas de extinción de incendio, generadores de temperatura controlada (aire acondicionado), detectores de humo y alarma, aspersores de químico de sofocación de oxígeno (si aplica), etc. al igual que de controles de seguridad de acceso físico mediante uso de llave o biométrico (si aplica).

- Los Funcionarios y terceros solo podrán conectar a la red aquellos equipos y/o dispositivos que hayan sido previamente autorizados por el proceso de Gestión de Soporte TIC.

## 10.2 Mantenimiento de Equipos Tecnológicos.

- Se deberán definir planes de mantenimiento, cronogramas y procedimientos para garantizar la actividad sobre la infraestructura tecnológica, con el objetivo de reducir la frecuencia y/o el impacto de posibles fallas que afecten su desempeño. (procedimientos de mantenimiento de equipos).

- Solo personal calificado y autorizado podrá realizar las actividades de mantenimiento y/o reparación de equipos tecnológicos.

- Las actividades de mantenimiento deberán ser documentadas bajo procedimientos y evidenciados mediante registros.

- En situaciones en que el equipo de cómputo en mantenimiento deba ser retirado de las instalaciones, deberá contar con autorización por parte de propietario de activo y/o de Gestión Tecnológica. (se cumple mediante el uso de un formato de Almacen).

- Se deberán programar y realizar pruebas de funcionamiento de manera periódica a todos los sistemas de: control de acceso, control ambiental y de seguridad física, para verificar que se mantienen operando correctamente.

### 10.3 Seguridad Centro de Procesamiento de Datos.

- Las instalaciones de procesamiento de datos (centro de datos) deberá ser supervisada las 24 horas al día.

- Los cuartos utilizados como instalaciones de procesamiento de información no se deben utilizar para imprimir, almacenaje de computadoras, piezas de computadoras o papelería.

- Se deberá contar con registros de acceso de personal (bitácora) a las instalaciones de procesamiento de información.

- Los cuartos que contienen el cableado de red o los equipos de comunicaciones, deben ser accedidos únicamente por personal autorizado.

- Equipos de protección tanto física (puertas de seguridad) como ambiental contra fuego deben ser implementados dentro del área de procesamiento de datos.

- Se deberá identificar el procedimiento para realizar la evacuación de las instalaciones ante situaciones de emergencia; visitantes deben ser puestos en conocimiento.

- Periódicamente se deberá realizar la revisión de registros (logs) con la identificación de los accesos de personal tanto interno, como de visitantes al centro de procesamiento de datos.

### 10.3.1 El centro de procesamiento datos debe estar provisto de:

- Señalización adecuada de todos y cada uno de los diferentes equipos y elementos, así como luces de emergencia y de evacuación, cumpliendo las normas de seguridad industrial y de salud en el trabajo.

- Sistema de refrigeración por aire acondicionado acorde a la necesidad. Este equipo debe tener redundancia para que en caso de falla se pueda continuar con la refrigeración.

- Unidades de potencia ininterrumpida UPS, que proporcionen respaldo al mismo, con el fin de garantizar el servicio de energía eléctrica durante una falla momentánea del fluido eléctrico de la red pública.

- Alarmas de detección de humo y sistemas de extinción de fuego deberán ser instalados. Los controles deberán ser sujetos a pruebas de manera regular.

- Extintores de incendios o un sistema contra incendios debidamente probados y con la capacidad de detener el fuego generado por equipo eléctrico, papel o químicos especiales.

- Los equipos tecnológicos, base de la plataforma tecnológica de la Corporación, deberán ser ubicados o localizados de tal forma que se protejan ante amenazas de ataques físicos, hurto o daño de los equipos.

- El cuarto adyacente al centro de cómputo no se debe utilizar para almacenaje de cualquier elemento inflamable, para cuarto de electricidad, o para instalaciones con tubería con fluido de agua.

- El personal que desempeña labores en las instalaciones de procesamiento de información y personal que realiza labores de seguridad para las mismas, deberán ser entrenados en el uso de cualquier sistema automático de control o extinción de incendio, el uso de los extintores portables, acciones en respuesta apropiada a la presencia de humo y con las alarmas de incendio.

- Fumar, ingerir y/o ingresar bebidas y/o alimentos en instalaciones de procesamiento de datos está terminantemente prohibido; personales visitantes deberán ser puestos en conocimiento de dicho lineamiento.

### 10.4 Suministro de Equipos de Soporte Energético.

- Fuentes de alimentación continuas (UPS) y plantas eléctricas deberán ser suministradas para la protección y continuidad de equipos que apoyan las operaciones claves del negocio; dichos dispositivos deben ser sujetos a revisión de funcionalidad periódicamente.

- Los interruptores de emergencia deben ubicarse cerca de las salidas de emergencia de las instalaciones del centro de procesamiento de información, deben ser sujetos a pruebas de verificación periódica.

- Se deben implementar sistemas de protección contra rayos en la edificación, para protección de los enlaces de telecomunicaciones externos y demás.

### 10.5 Perímetro de Seguridad de áreas seguras.

- •Toda área segura deberá contar con el registro de acceso a personal interno autorizado y registro de visitantes.

- Los visitantes a áreas seguras deberán ser identificados (registro de visitante) y ser acompañados por un Funcionario durante su tiempo de visita.

- Las áreas seguras deben equiparse con sistemas de control de acceso seguros, en la medida de lo posible con dispositivos de autenticación electrónicos y/ con puertas que impidan el ingreso no autorizado.

- Todos los funcionarios, contratistas, judicantes y/o practicantes, que pierdan su carne de identificación de ingreso a la Corporación, deben reportar inmediatamente la pérdida del mismo a soporte TIC, soportado con la constancia de perdida de documentos y/o elementos, expedida por la Policía Nacional.

### 10.6 Retiro de las instalaciones de Equipos de propiedad de la Entidad.

Todo retiro de equipo tecnológico deberá ser autorizado previamente por el área encargada en la Corporación (Almacén).

### 10.7 Trabajo en Áreas Seguras y Oficinas.

- Toda la información sobre pizarrones o salas de juntas debe ser eliminada, una vez finalice la reunión.

- Las impresoras y/o fotocopiadores deberán estar en todo momento libre de documentos.

- Durante cualquier reubicación del espacio de trabajo de un empleado, éste debe propender para que los activos de información a su cargo estén protegidos durante dicho proceso.

- Todo trabajo realizado en áreas seguras debe ser supervisado por el responsable de ésta.

- No se permite dentro de un área segura, el ingreso de equipos de video, imágenes, audio o almacenamiento de datos que no hayan sido autorizados por el responsable del área.

### 10.8 Escritorio y Pantalla Limpia.

- Los escritorios (mesas) deberán estar en la medida de lo posible organizados y libres de la exposición de información documental que sea clasificada como confidencial.

- Las pantallas de equipos de usuarios deberán ser bloqueadas para aquellos momentos en que no esté utilizando el equipo o ante la ausencia del funcionario de su puesto de trabajo.

- El almacenamiento de los archivos electrónicos deberá ser realizado en las carpetas lógicas definidas por gestión tecnológica para tal propósito, y no en el escritorio virtual de los equipos.

# 11. SEGURIDAD DE LAS OPERACIONES

## 11.1 Procedimientos de Operación Documentados.

Las actividades operacionales del área de gestión tecnológica deberán ser documentadas mediante procedimientos operativos, en los cuales se describa el detalle de las mismas y las responsabilidades para cada una de ellas (ejemplo, inicio/apagado de equipos servidores, revisión/depuración de información, copias de respaldo de información, entre otros).

## 11.2 Gestión de Cambios.

- Los cambios relevantes en la infraestructura tecnológica (software / Hardware) deberán estar definidos bajo un procedimiento documentado, el cual describa los lineamientos específicos para la atención de cada uno de ellos de manera adecuada y controlada.

- Los cambios relevantes en la infraestructura tecnológica a nivel de software o hardware deberán ser formalmente solicitados y ejecutados bajo los lineamientos del procedimiento de gestión de cambios y en concordancia con la protección de los activos de información, como propósito del sistema de gestión de seguridad de la información.

- Todo cambio en la plataforma de TI deberá basarse en la necesidad y justificación del mismo; deberán ser sujetos a evaluación de análisis de impacto, identificación de beneficios, para su correspondiente aprobación por parte de los responsables y/o encargados.

- Los cambios relevantes en la plataforma de TI se deberán identificar y/o registrar de manera que se asegure la trazabilidad del mismo, a nivel de su evaluación, tratamiento, ejecución pruebas y su puesta en producción.

- Todo cambio deberá ser ejecutado, probado y recibido a conformidad por los responsables o solicitantes, antes y/o después de su puesta en ambiente de producción.

## 11.3 Gestión de Capacidad.

- Estrategias de evaluación y monitoreo de la capacidad tanto de la plataforma de hardware como de los sistemas de información deberán ser aplicadas, con el propósito proactivo de atender a situaciones especiales que puedan conllevar a un impacto operativo en la Corporación.

- La evaluación y el monitoreo deberán ser realizados de manera automática (en la medida de lo posible), definiendo para cada uno de los activos de información especialmente críticos, los niveles (umbrales) para los cuales se debe reportar y atender de manera oportuna.

### 11.4 Segregación de Ambientes de Desarrollo, Pruebas y Producción.

- la Oficina Asesora de Direccionamiento Estratégico TIC deberá asegurar la separación de los ambientes de desarrollo, pruebas y producción.

- Las herramientas de desarrollo de software no deberán estar instaladas en el ambiente de producción.

- El ambiente de pruebas debe emular el ambiente de producción.

### 11.5 Protección Contra Código Malicioso.

- Se deberán establecer los procedimientos, instructivos y controles para prevenir y/o tratar el(los) código(s) malicioso(s).

- Archivos descargados a través de Internet, en medios de almacenamiento y/o archivos adjuntos de los correos electrónicos, deberán ser analizados por el sistema contra código malicioso.

- Sistemas contra códigos malicioso deberán ser configurados para que su ejecución se realice al inicio de los equipos, en tiempo real, y en otros intervalos requeridos en caso de sospecha de software malicioso; la totalidad de equipos de cómputo que cuente con el acceso a la red deberán contar con la implementación de dicho software debidamente licenciado; su ejecución de actualización deberá ser en la medida de los posible con periodicidad diaria.

- Se deberán realizar actividades de verificación de la eficacia del sistema contra código malicioso implementado.

- Situaciones de infección de código malicioso deberán ser registradas, analizadas y atendidas como un incidente de seguridad.

- Usuarios deberán ser sensibilizados con respecto al tratamiento de situaciones de incidentes de seguridad de la información asociados a código malicioso.

### 11.6 Respaldo de Información.

- Información tanto crítica como sensible de la Corporación deberá ser respaldada y custodiada de manera segura, siguiendo el procedimiento establecido.

- Procedimientos e instructivos para la toma de respaldo y recuperación de información deberán ser documentados; de igual manera, se deberá identificar los tiempos de retención de los medios donde se almacena la información de respaldo.

- Cronograma de respaldos deberá ser definido y de acuerdo a la criticidad para el(los) procesos; la rotación y retención de los medios de almacenamiento deberá ser establecida de acuerdo a las necesidades.

- Los medios de almacenamiento de los respaldos deberán ser almacenados en un área segura, con control de acceso, y una copia adicional fuera de las instalaciones de la Corporación, de acuerdo a la clasificación de la información y a la rotación definida en el procedimiento.

- Los medios de almacenamiento para la toma de respaldos deben asegurar la capacidad requerida y la vida útil necesaria.

- Los medios de almacenamiento con la información de respaldo deberán ser sujetos a pruebas de restauración y de confiabilidad de la información de manera periódica (por lo menos una vez cada tres meses).

- Se realizarán copias de seguridad cada vez que se requiera o que se realice un cambio en la estructura TI (Hardware o Software).

- La restauración de copias de respaldo en ambientes de producción debe estar debidamente aprobada por el propietario de la información.

- la Oficina Asesora de Direccionamiento Estratégico TIC debe mantener un inventario actualizado con la identificación de las copias de respaldo de la información.

- Los medios de respaldo que vayan a ser eliminados deben surtir un proceso de borrado seguro (cuando sea posible) y posteriormente destruidos de forma adecuada y controlada.

### 11.7 Sincronización de Relojes

- Los equipos de la plataforma tecnológica deberán estar sincronizados con respecto a la hora oficial colombiana, permitiendo de esta manera asegurar las tareas de trazabilidad de eventos o situaciones especiales a través del registro de los tiempos exactos de ocurrencia de eventos.

- La Corporación deberá documentar el instructivo técnico para realizar la actividad de sincronización y verificación del reloj para todos los dispositivos tecnológicos que soporten esta configuración.

### 11.8 Vulnerabilidades Técnicas.

- El procedimiento para la ejecución de aplicaciones de identificación de vulnerabilidades técnicas en la plataforma tecnológica deberá ser documentado; en caso de ser una actividad contratada, se deberán implementar las prácticas de seguridad de accesos de terceros a la información de la Corporación.

- La Mesa Temática de Seguridad de la Información es responsable de autorizar las excepciones relacionadas con la solución de vulnerabilidades.

- Las vulnerabilidades técnicas deberán ser clasificadas de acuerdo a su impacto para la Corporación.

# 12. SEGURIDAD DE LAS COMUNICACIONES

## 12.1 Gestión De Redes.

- Procedimientos, instructivos y controles operacionales para proteger las redes de la Corporación deberá ser establecidos, documentado y aplicados.

- Administradores de redes deberán mantener la segregación de sus funciones con respecto al administrador de los sistemas operativos, bases de datos y aplicaciones (en la medida de lo posible).

- La información confidencial o privada que se transmita a través de las redes debe ser protegida de manera segura mediante cifrado.

## 12.2 Transferencia De Información.

La Corporación Autónoma regional del Tolima – CORTOLIMA, en caso de tener un servicio de transferencia de archivos deberá realizarlo empleando protocolos seguros; cuando el origen sea desde la Corporación hacia entidades externas, deberá establecer los controles necesarios para preservar la seguridad de la información ejemplo (cifrado); cuando el origen de la transferencia sea una entidad externa, se acordarán las políticas y controles de seguridad de la información con dicha entidad; paro los dos casos, se deberán revisar y proponer controles en concordancia con las políticas de seguridad de la información de CORTOLIMA.; los resultados de la revisión de requerimientos de seguridad se documentarán y preservarán para futuras referencias o para demostrar el cumplimiento con las políticas y con los controles de seguridad de la información de la Entidad.

# 13. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

## 13.1 Principios de Desarrollo de Software.

la Oficina Asesora de Direccionamiento Estratégico TIC será el área responsable de dirigir el sistema del ciclo de vida de desarrollo de software (SDLC) para los proyectos de la Corporación, al igual que establecer la metodología de desarrollo, que incluya la definición de requerimientos de seguridad y las buenas prácticas de desarrollo seguro, con el fin de proporcionar a los desarrolladores la visión clara de lo que se espera de ellos.

- Todo software desarrollado al interior de la Entidad deberá ser desarrollado de acuerdo al SDLC, a partir de un análisis o estudio de viabilidad, análisis de impactos y oportunidades, especificación de diseño y desarrollo, control de calidad, pruebas de aceptación, implementación, las actividades de revisión y mantenimiento post-implementación.

- Los desarrolladores deberán certificar que todo desarrollo utilice las herramientas licenciadas y autorizadas.

- Actividades de soporte de desarrollo deberán estar soportadas por una iniciativa, solicitud o requerimiento en formato establecido.

- Todos los sistemas de información o aplicativos informáticos, especialmente aquellos asociados a la misión crítica de la Corporación deberán asegurar la inclusión de controles de seguridad de acceso y autenticación de usuarios.

- Todos los requerimientos o solicitudes de cambio en sistemas de información y aplicaciones deberán tener diligenciado el campo “Requerimientos de Seguridad de la Información”.

- Desarrollos propios de la entidad deberán ser debidamente documentados mediante manuales técnicos y de usuario.

- Todo nuevo software, herramienta automática o sistema de información a ser adquirido e implementado en la Corporación, deberá ser evaluado, verificado y aprobado por la Oficina Asesora de Direccionamiento Estratégico TIC, en beneficio de asegurar su compatibilidad, licenciamiento e integración con la plataforma tecnológica.

- Toda adquisición o compra de software o sistema de información deberá ser realizada bajo los lineamientos establecidos en el procedimiento de adquisición de bienes y servicios.

### 13.2 Desarrollo Seguro, Realización de Pruebas y Soporte

- la Oficina Asesora de Direccionamiento Estratégico TIC deberá velar porque el desarrollo interno y/o externo de los sistemas de información que cumplan con los requerimientos de seguridad esperados, con las buenas prácticas para el desarrollo seguro de aplicativos.

- Todo uso de nuevos lenguajes de programación o tecnologías de desarrollo deberá estar acompañado de un documento con la identificación de los principios de desarrollo seguro.

- la Oficina Asesora de Direccionamiento Estratégico TIC deberá asegurar que todo software desarrollado o adquirido, interna o externamente, cuente con el nivel de soporte requerido por la Corporación.

- Se deberá asegurar la implementación de las migraciones entre los ambientes (pruebas – producción) basado con un procedimiento controlado y bajo previa aprobación.

### 13.3 Estrategia de Pruebas de Software.

- la Oficina Asesora de Direccionamiento Estratégico TIC deberá establecer la metodología para la realización de pruebas de aceptación y seguridad al software desarrollado.

- Los propietarios de los sistemas de información serán los responsables de realizar las pruebas para asegurar que cumplen con los requerimientos de funcionalidad y de seguridad antes de su paso a producción, y mediante el uso de metodología para tal fin.

- Los propietarios de los sistemas de información serán los encargados de realizar y documentar las pruebas de nuevas entregas de funcionalidades y/o ajustes a funcionalidades.

# 14. RELACIONES CON PROVEEDORES

## 14.1 Servicios Tercerizados.

- CORTOLIMA establecerá los criterios de selección de proveedores en beneficio del apoyo a la gestión de la seguridad de la información, contemplando, reputación, certificaciones, calificaciones y recomendaciones de otros clientes, estabilidad financiera de la compañía, seguimiento de estándares de gestión de calidad y de seguridad, entre otros criterios que resulten de un análisis de riesgos de la selección y aquellos que por ley sean exigidos.

- Con el fin de proteger la información entre las dos partes, se deberá formalizar compromiso de confidencialidad, que defina claramente las responsabilidades de las mismas.

- En caso de intercambio de información, aspectos de control y niveles de seguridad de información deberán basarse de acuerdo a su nivel de clasificación; el compromiso de confidencialidad entre la entidad y el proveedor deberá ser específico, de acuerdo al objetivo y al alcance del contrato (firmado por las dos partes).

# 15. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

- Un procedimiento de gestión de incidentes de seguridad de la información deberá ser documentado como guía de atención eficiente para cada uno de ellos.

- Se deben implementar instructivos y controles para identificar, comunicar y tratar los eventos y debilidades de seguridad de la información de forma oportuna.

- Los incidentes de seguridad de información deberán ser identificados, registrados en un sistema definido y atendidos de manera eficaz, permitiendo reducir los posibles impactos para la Entidad.

- Incidentes de seguridad de la información que, por necesidad de instauración de acciones judiciales o disciplinarias, deberán estar soportados con evidencia adecuadamente recopilada, y con adopción de las mejores prácticas de cadena de custodia.

- Incidentes de seguridad de la información deberán ser documentados con respecto a su solución y lecciones aprendidas.

- Registros de incidentes de seguridad de la información deberán ser cerrados hasta el momento en que se haya solucionado la situación y/o por revisión de solución y aceptación por parte de usuarios.

# 16. SEGURIDAD DE INFORMACIÓN Y LA CONTINUIDAD DE SERVICIO

Será el conjunto de procedimientos y estrategias que la Corporación deberá definir para contrarrestar las posibles interrupciones en sus actividades misionales, para proteger sus procesos críticos contra fallas mayores en los sistemas de información o contra desastres y asegurar que las operaciones se recuperen oportuna y ordenadamente, generando un impacto mínimo o nulo ante una contingencia.

La definición y actualización de las normas, políticas, procedimientos y estándares relacionados con la continuidad del negocio, estará bajo la responsabilidad de la alta dirección de la Corporación; de igual manera, estará encargada de velar por su implementación y cumplimiento.

La Corporación deberá incorporar en el plan de continuidad del negocio, aspectos de seguridad de la información relevantes para asegurar que los procesos misionales soportados por la infraestructura tecnológica sean restaurados dentro de escalas de tiempo razonables, protegiendo la información en su confidencialidad e integridad, para reducir impactos de alto nivel sobre la Entidad.

Dentro de los aspectos a tener en cuenta, serán:

- Identificación y asignación de prioridades a los procesos críticos de negocio y de TI de la Corporación de acuerdo con su impacto en el cumplimiento de la misión de la entidad.

- Identificación de la documentación de la estrategia de continuidad del negocio.

- Identificación del plan de recuperación del negocio de acuerdo con la estrategia definida anteriormente.

- Definir el plan de pruebas de la estrategia de continuidad del negocio.

- Se deberán implementar medidas de control necesarias para el aseguramiento de la continuidad de negocio.

- Sesiones de revisión y mantenimiento del plan de continuidad de negocio se deberán realizar por lo menos una vez al año para asegurar su vigencia y aplicabilidad.

- Una copia de los planes de continuidad de negocio deberá ser almacenada y resguardada en sitio externo.

- Los planes de continuidad del negocio deberán asegurar la restauración o mantenimiento de las operaciones de negocio en el tiempo requerido después de cualquier interrupción del servicio o desastre.

- Copias de los planes de continuidad del negocio deberán ser distribuidos y de conocimiento de la totalidad de funcionarios de la Entidad, al igual que distribuido apropiadamente cuando los planes sean actualizados.

# 17. CUMPLIMIENTO

### 17.1 Legislación Aplicable.

- La Corporación deberá identificar toda aquella normatividad legal y jurídica aplicable asociada a seguridad de la información que debe cumplir.

- Las responsabilidades específicas para el cumplimiento de la legislación aplicable, es de responsabilidad de toda la organización.

### 17.2 Protección de Datos y Privacidad de Información Personal.

- Los requisitos legales definidos para proteger la información personal deberán ser de estricto cumplimiento por la Corporación.

- Controles de acceso a la información sensible (datos personales) deberá ser implementados en beneficio del cumplimiento con la legislación.

### 17.3 Derechos de Propiedad Intelectual.

- Todo software comercial que requiera derechos de autor o propiedad intelectual debe ser licenciado.

- Todo el software instalado debe ser previamente aprobado por la Oficina Asesora de Direccionamiento Estratégico TIC

- Todos los contratos que contemplen el desarrollo de software deben establecer claramente la propiedad del software y del código fuente.

- El Oficial de Seguridad de la Información deberá realizar revisiones periódicas del uso del software instalado en los equipos de cómputo y servidores de la Entidad.

- Todo software que viole los acuerdos de licenciamiento y/o no aprobación deberá ser desinstalado.

### 17.4 Protección de Registros.

Los instructivos para la recolección, resguardo, manejo y destrucción de registros deben ser documentados y aplicados por los propietarios de la información.

### 17.5 Cumplimiento de Políticas.

- Funcionarios deberán ejecutar los procedimientos e instructivos definidos para la protección y seguridad de la información.

- Los propietarios de la información deben informar las excepciones a las políticas de seguridad de la Entidad.

- Se deberán realizar revisiones regulares de los procesos y procedimientos de seguridad de la información con enfoque de cumplimiento de las políticas de seguridad de la información.

- El Oficial de Seguridad de la Información y el Jefe de la Oficina de Control Interno deberán definir las actividades de revisión para mantener el cumplimiento con las políticas de seguridad de la información de la Entidad.

# 18. PROCESO DE CONTROL INTERNO A LA GESTIÓN Y/O CONTROL INTERNO DISCIPLINARIO

Dentro de la estrategia de seguridad de la información de La Corporación Autónoma regional del Tolima – CORTOLIMA, está establecido un proceso disciplinario formal de carácter legal, tanto para los funcionarios como para contratistas y otros colaboradores que desempeñen funciones públicas (interventores o supervisores externos) que cometan alguna violación o incumplimiento de la Política del SGSI con carácter para iniciar investigación interna o disciplinaria.

# 19. CONTROL DE CAMBIOS

| FECHA | VERSIÓN | DESCRIPCIÓN |
|---|---|---|
| 1/12/2023 | 00 | Creación de la política de Seguridad |

| ELABORO | REVISO | APROBO |
|---|---|---|
| Katherine Silva Garibello | Comité Institucional de Gestión y Desempeño | Comité Institucional de Gestión y Desempeño<br>01 de Diciembre de 2023 |