MANUAL DE LA POLÍTICA DE SEGURIDAD PARA LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES – TICS DE LA CORPORACION AUTONOMA REGIONAL DE LA GUAJIRA – CORPOGUAJIRA

EDUARDO JOSE DAZA CUELLO
Profesional Especializado
Líder del proceso Gestión de las TICs

2020

Contenido

1. INTRODUCCIÓN

La Corporación Autónoma Regional de la Guajira – *Corpoguajira*, para el cumplimiento de la misión y del cumplimiento de su objetivo, requiere implementar reglas y medidas que permitan proteger la confidencialidad, integridad y disponibilidad en todo el ciclo de vida de la información.

El presente manual establece las políticas que integran el Sistema de Gestión de Seguridad de la Información SGSI, las cuales deben ser adoptadas por los funcionarios, contratistas, personal en comisión administrativa, visitantes y terceros que presten sus servicios o tengan algún tipo de relación con Corpoguajira. Estas se encuentran enfocadas al cumplimiento de la normatividad legal colombiana vigente y a las buenas prácticas de Seguridad de la Información, basadas en la norma ISO 27001/2013 y al modelo de seguridad y privacidad de la información de la estrategia Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia.

2. OBJETIVO

Presentar en forma clara y coherente los elementos que conforman la política de seguridad que deben conocer y cumplir todos los directivos, funcionarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con *la Corporación Autónoma Regional de La Guajira – Corpoguajira.*

3. ALCANCE

Las Políticas de Seguridad de la Información son aplicables para todos los aspectos administrativos y de control que deben ser cumplidos por los directivos, funcionarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con *la Corporación Autónoma Regional de La Guajira – Corpoguajira* 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 del presente manual. Los usuarios tienen la obligación de dar cumplimiento a las presentes políticas emitidas y aprobadas por la Dirección General.

4. APLICABILIDAD DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Las políticas del Sistema de Seguridad de la Información - SGSI aplican y son de obligatorio cumplimiento para la Alta Dirección, Directores, Subdirectores, Secretarios, Jefes de Oficina, Asesores, Coordinadores, funcionarios, contratistas, y en general a todos los usuarios que permitan el cumplimiento de los propósitos generales de Corpoguajira.

5. TÉRMINOS Y DEFINICIONES

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 o que puede tolerarse el riesgo asociado a cualquier situación bajo el supuesto de que se cuenta con un plan de acción para afrontarlo.

Activo: 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. Todo lo que contiene información, la cual posee un valor y es necesaria para realizar los procesos misionales y operativos del CORPOGUAJIRA. Se pueden clasificar de la siguiente manera:

- **Datos:** Son todos aquellos elementos básicos de la información (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en CORPOGUAJIRA. Un dato es una representación simbólica (numérica, alfabética, algorítmica, espacial, etc.) de un atributo o variable cuantitativa o cualitativa. Los datos describen hechos empíricos, sucesos y entidades.

- **Aplicaciones:** Es todo el software que se utiliza para la gestión de la información. En informática, una aplicación es un programa informático diseñado como herramienta para permitir a un usuario realizar uno o diversos tipos de tareas. Esto lo diferencia principalmente de otros tipos de programas, como los sistemas operativos (que hacen funcionar la computadora), las utilidades (que realizan tareas de mantenimiento o de uso general), y las herramientas de desarrollo de *software* (para crear programas informáticos).

- **Personal:** Se agrupa en este término a los funcionarios de Corpoguajira, a los contratistas, los clientes, los usuarios, ciudadanos y en general, todos aquellos que tengan acceso de una manera u otra a los activos de información de la Corporación.

- **Servicios:** Es un conjunto de actividades que buscan satisfacer las necesidades de un cliente. Estos servicios incluyen una diversidad de actividades que se pueden planificar desempeñadas por un gran número de personas (funcionarios, empleados, empresarios) que trabajan para el estado (servicios públicos) o para empresas particulares (servicios privados). En este término se incluyen tanto los servicios internos, como los externos.

- **Tecnología**: Es el conjunto de conocimientos técnicos, científicamente ordenados, que permiten diseñar y crear bienes, servicios que facilitan la adaptación al medio ambiente y la satisfacción de las necesidades esenciales y los deseos de la humanidad. Aunque hay muchas tecnologías muy diferentes entre sí, es frecuente usar el término tecnología en singular para referirse al conjunto de todas, o también a una de ellas. La palabra tecnología también se puede referir a la disciplina teórica que estudia los saberes comunes a todas las tecnologías, y en algunos contextos, a la educación

tecnológica, la disciplina escolar abocada a la familiarización con las tecnologías más importantes.

- **Instalaciones:** son el conjunto de redes y equipos fijos que permiten el suministro y operación de los servicios que ayudan a los edificios a cumplir las funciones para las que han sido diseñados.

- **Equipamiento auxiliar:** Son todos aquellos activos que dan soporte a los sistemas de información y que no se hallan en ninguno de los tipos anteriormente definidos. Ejemplo: Aire acondicionado, destructora de papel.

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 transferir el riesgo a otra parte, evadir el riesgo, reducir los efectos negativos del riesgo y aceptar algunas o todas las consecuencias de un riesgo particular.

Administración de incidentes de seguridad: Procedimientos, estrategias y herramientas de control, enfocados a una correcta evaluación de las amenazas existentes, en este caso hacia toda la infraestructura de TI, se basa en un análisis continuo y mejorado del desempeño de todos los activos y recursos gerenciales que tiene la entidad.

Su objetivo principal es atender y orientar las acciones inmediatas para solucionar cualquier situación que cause una interrupción de los diferentes servicios que presta la Agencia, de manera rápida y eficaz, no se limita a la solución de problemas específicos sino a buscar las causas que determinaron el incidente limitando el marco de acción de futuras ocurrencias, su enfoque se base en tres pilares fundamentales:

- Detectar cualquier alteración en los servicios TI.
- Registrar y clasificar estas alteraciones.
- Asignar el personal encargado de restaurar el servicio.

APT: (Advance Persistent Threat) Amenaza Avanzada Persistente, especie de ciberataque que es responsable del lanzamiento de ataques de precisión y tienen como objetivo comprometer una máquina en donde haya algún tipo de información valiosa.

Alcance: Ámbito de la organización que queda sometido al SGSI (Sistema de Gestión de la Seguridad de la Información). 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): Base de datos que contiene toda la información pertinente acerca de los componentes de cualquier sistema de información utilizado en la Agencia 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.

BS 7799: Estándar británico de seguridad de la información, publicado por primera vez en 1995. En 1998, fue publicada la segunda parte. La parte primera es un conjunto de buenas prácticas para la gestión de la seguridad de la información –no es certificable- y la parte segunda especifica el sistema de gestión de seguridad de la información -es certificable-o La parte primera es el origen de ISO 17799 e ISO 27002 Y la parte segunda de ISO 27001. Como tal el estándar, ha sido derogado ya, por la aparición de estos últimos.

Características de la Información:

- **Actualizada:** implica que ésta es capturada cuando se genera y no un tiempo después mediante procesos adicionales.
- **Disponible:** la que se presente para tomas de decisiones debe ser relevante, es decir, ni más ni menos que la necesaria. Se debe proveer el mecanismo más ágil disponible

para el acceso a esta información y garantizar que haya conectividad entre las diferentes bases de información.

- **Oportuna:** lo que implica tener una alta velocidad de acceso a la información la cual se puede proveer con conexiones permanentes en "línea" a las bases de datos. Adicionalmente, la oportunidad exige disponibilidad de alto nivel, lo que ocasiona el establecimiento de planes de continuidad que garanticen el acceso a la misma. La información debe generarse y notificarse a la par con los acontecimientos de tal manera que permita la toma de decisiones y la actuación inmediata.
- **De calidad:** debe tener altos niveles de confiabilidad. Es decir, qué tanto se puede creer en la información que se está recibiendo. Las bases de datos actualmente proveen herramientas como la integridad referencial, sin embargo si no hay conciencia en la necesidad de la calidad sobre la velocidad o facilidad de uso para el usuario, es probable que el sistema de información quede produciendo a altas velocidades cifras irrelevantes que ocasionen errores en las decisiones.
- **Explicable**: Es decir, se debe poder ver a todos los niveles de detalle el origen de toda información. Para cada total, se tienen también los valores de los componentes de estos totales. Además se deberá poder analizar la información en el tiempo por lo que se requiere acceso a la información tanto presente como histórica.
- **Exacta**: En este sentido la información debe reflejar el evento al cual se refiere y su sistema de medición expresado con poca variabilidad.
- **Objetiva**: La información debe ser el producto de criterios establecidos que permitan la interpretación en forma estandarizada por diferentes personas en circunstancias diversas de tiempo y lugar.
- **Válida**: Se refiere a que la información ha de permitir medir en forma precisa el concepto que se estudia, con criterios uniformes.
- **Con continuidad**: La información ha de ser generada en forma permanente de tal manera que exista la disponibilidad de los datos a través del proceso de vigilancia.
- **Completa**: Debe contener todos los datos y variables previamente establecidas para cumplir con su finalidad en cada evento epidemiológico.
- **Comparable**: que permita ser confrontada con datos similares.

Checklist (Lista de Chequeo): Lista de apoyo para el auditor con los puntos a auditar, que ayuda a mantener claros los objetivos de la auditoría, sirve de evidencia del plan de auditoría, asegura su continuidad y profundidad y reduce los prejuicios del auditor y su carga de trabajo, Este tipo de listas también se pueden utilizar durante la implantación del SGSI para facilitar su desarrollo.

CobiT (Control Objectives for Information and related Technology): Controles 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.

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 (Worn): 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: Es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje. 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.

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: Garantía de que alguien no puede negar algo. Normalmente, el no repudio se refiere a la capacidad de garantizar que una parte de un contrato o una comunicación no pueda negar la autenticidad de su firma en un documento o el envío de un mensaje que se originó. 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 de escritorio despejado: La política de la empresa que indica a los funcionarios, contratista y demás colaboradores de Corpoguajira, que 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.

Ransomware: Código malicioso para secuestrar datos, una forma de explotación en la cual el atacante encripta los datos de la víctima y exige un pago por la clave de descifrado.

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.

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 las acciones 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 directivos, funcionarios, contratistas, terceros y otros colaboradores Corpoguajira, debidamente autorizados para usar equipos, sistemas o aplicativos informáticos disponibles en la red de Corpoguajira 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.

VPN (Virtual Private Network): es una tecnología de red que permite una extensión segura de la red privada de área local (LAN) sobre una red pública o no controlada como Internet.

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.

6. COMPROMISO DE LA DIRECCIÓN

La Alta Dirección de la Corporación Autónoma Regional de La Guajira - CORPOGUAJIRA aprueba el *Manual de Políticas de Seguridad de la Información*, como muestra de su compromiso y apoyo hacia la gestión de seguridad de la información que se lleva a cabo en la Institución, mediante el SGSI y el Modelo de Seguridad y Privacidad de la Información (MSPI) de Gobierno Digital, antes llamado Gobierno en Línea.

La Alta Dirección de CORPOGUAJIRA demuestra su compromiso de apoyo a la política de seguridad de la información y las comunicaciones destinando los recursos suficientes y adecuados para implementar y mantener las políticas contenidas en este manual y a realizar, entre otras acciones:

- La revisión y aprobación del Manual de Políticas de Seguridad de la Información para la Institución.
- La promoción activa de una cultura de seguridad de la información en los servidores públicos, contratistas, proveedores y ciudadanía en general, que tengan acceso a los sistemas de información, repositorios e instalaciones físicas de la corporación.
- La divulgación de este manual.
- La verificación del cumplimiento de las políticas aquí mencionadas.

7. POLITICA GENERAL DE SEGURIDAD DE INFORMACION

La dirección de la Corporación Autónoma Regional de La Guajira – CORPOGUAJIRA, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la Implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el

ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la corporación.

Para CORPOGUAJIRA, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

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

- Minimizar el riesgo en las funciones más importantes de la corporación.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de CORPOGUAJIRA
- Garantizar la continuidad del negocio frente a incidentes.
- CORPOGUAJIRA ha decidido definir, implementar, operar y mejorar de forma continua un **Sistema de Gestión de Seguridad de la Información**, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

8. POLÍTICAS, PROCEDIMIENTOS Y CONTROLES

8.1. Políticas de seguridad de la información

Las *Políticas de Seguridad de la Información*, surge como una herramienta institucional para sensibilizar a cada uno de los directivos, funcionarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con CORPOGUAJIRA sobre la importancia y sensibilidad de la información y servicios críticos, de tal forma que le permitan desarrollar adecuadamente sus labores y cumplir con su propósito misional.

Objetivo General: Definir las pautas de propósito general para asegurar una adecuada protección de la información de CORPOGUAJIRA.

Objetivo Específico: Brindar apoyo y orientación a la dirección con respecto a la seguridad de la información, de acuerdo con los requisitos de la corporación y la reglamentación y las leyes pertinentes.

Aplicabilidad: Estas son políticas que aplican a la Alta Dirección, Directores, Subdirectores, Secretarios, Asesores, Jefes de Oficina, funcionarios, contratistas, y en general a todos los usuarios de la información que cumplan con los propósitos generales de CORPOGUAJIRA.

Directrices:

1. Se debe verificar que se definan, implementen, revisen y actualicen las políticas de seguridad de la información.
2. Diseñar, programar y realizar los programas de auditoría del sistema de gestión de seguridad de la información, los cuales estarán a cargo de la Oficina de Control Interno.
3. Todo aplicativo informático o software que se adquiera e instale debe ser licenciado y debe ser aprobado por el Líder del proceso de Gestión de las TICS en concordancia con la política de adquisición de bienes de la corporación de acuerdo con lo definido en el proceso respectivo.
4. CORPOGUAJIRA debe contar con un *firewall* o dispositivo de seguridad perimetral para la conexión a Internet o para la conexión a otras redes en *outsourcing* o de terceros.
5. La conexión remota a la red de área local de CORPOGUAJIRA debe realizarse a través de una conexión VPN segura suministrada por la corporación, la cual debe ser aprobada, registrada y auditada, a excepción de los casos que autorice el proceso de Gestión de las TICS.
6. Los jefes de área o dependencia (Directores, Subdirectores, Secretarios, Jefes de Oficina, Asesores, Coordinadores) deben asegurarse que todos los procedimientos de seguridad de la información dentro de su área de responsabilidad, se realizan correctamente para lograr el cumplimiento de las políticas y estándares de seguridad de la información de CORPOGUAJIRA.

7. CORPOGUAJIRA en caso de tener un servicio de transferencia de archivos, deberá realizarlo empleando protocolos seguros. Cuando el origen sea de CORPOGUAJIRA hacia entidades externas, la Corporación establecerá los controles necesarios para preservar la seguridad de la información. Cuando el origen de la transferencia sea una entidad externa, se acordarán las políticas y controles de seguridad de la información con esa entidad. En todo caso se deben revisar y proponer controles en concordancia con las políticas de seguridad de la información de la corporación. 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 CORPOGUAJIRA.
8. Se establecerá un ***Comité de Seguridad Informática y de Sistemas*** de la Corporación el cual definirá de acuerdo a la clasificación de la información, que datos deben ser cifrados y dará las directrices necesarias para la implementación de los respectivos controles (dispositivos a emplear, mecanismos de administración de claves, políticas de uso de sistemas de cifrado de datos).

8.1.1. Política de clasificación de la información.

Objetivo: Asegurar que la información recibe el nivel de protección apropiado de acuerdo al tipo de clasificación establecido por la ley y CORPOGUAJIRA.

Aplicabilidad: Estas políticas se aplican a la Alta Dirección, Directores, Subdirectores, Secretarios, Asesores, Jefes de Oficina.

Directrices:

1. Se considera información toda forma de comunicación o representación de conocimiento o datos digitales, escritos en cualquier medio, ya sea magnético, papel, visual u otro que genere CORPOGUAJIRA como por ejemplo:
   - Formularios / comprobantes propios o de terceros.
   - Información en los sistemas, equipos informáticos, medios magnéticos/electrónicos o medios físicos como papel.
   - Otros soportes magnéticos/electrónicos removibles, móviles o fijos.
   - Información transmitida vía oral o por cualquier otro medio de comunicación.
2. Los usuarios responsables de la información de CORPOGUAJIRA, deben identificar los riesgos a los que está expuesta la información de sus áreas, teniendo en cuenta que la información pueda ser copiada, divulgada, modificada o destruida física o digitalmente por personal interno o externo.
3. 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 CORPOGUAJIRA.

Independiente del tipo de activo, se deben considerar las siguientes características:

a) El activo de información es reconocido como valioso para la Corporación.
b) No es fácilmente reemplazable sin incurrir en costos, habilidades especiales, tiempo, recursos o la combinación de los anteriores.
c) Forma parte de la identidad de la organización y sin el cual la Corporación puede estar en algún nivel de riesgo. (La determinación del nivel y tipo de riesgo se estima sobre la base del modelo MECI de CORPOGUAJIRA).
d) Los niveles de clasificación de la información que se ha establecido son: INFORMACIÓN PÚBLICA RESERVADA, INFORMACIÓN PÚBLICA CLASIFICADA (PRIVADA Y SEMI-PRIVADA) e INFORMACIÓN PÚBLICA.

Los aspectos detallados de la política de clasificación de la información se deberán establecerse en un documento que sirva de **GUÍA PARA LA CLASIFICACIÓN DE LA INFORMACIÓN DE ACUERDO CON SUS NIVELES DE SEGURIDAD.**

8.1.2. Políticas de seguridad para los recursos humanos.

Objetivo: Asegurar que los funcionarios, contratistas y demás colaboradores de CORPOGUAJIRA, entiendan sus responsabilidades y las funciones de sus roles y usuarios, con el fin de reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información y de las instalaciones.

Aplicabilidad: Estas son políticas que aplican a la Alta Dirección, Directores, Subdirectores, Secretarios, Jefes de Oficina, Asesores, funcionarios, contratistas, y en general a todos los usuarios de la información que cumplan con los propósitos generales de CORPOGUAJIRA.

Directrices:

1. Se debe asegurar que los funcionarios, contratistas y demás colaboradores de CORPOGUAJIRA, entiendan sus responsabilidades en relación con las políticas de seguridad de la información de la Corporación 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 empleados para el tratamiento de la información.

8.1.3. Políticas específicas para usuarios de CORPOGUAJIRA.

Objetivo: Definir las pautas generales para asegurar una adecuada protección de la información de la Corporación por parte de los usuarios de la entidad.

Aplicabilidad: Estas son políticas que aplican a la Alta Dirección, Directores, Subdirectores, Secretarios, Jefes de Oficina, Asesores, funcionarios, contratistas, y en general a todos los usuarios de la información que cumplan con los propósitos generales de CORPOGUAJIRA.

Directrices:

1. CORPOGUAJIRA suministrará una **cuota de almacenamiento** de la información en un servidor de archivos para que cada usuario que lo requiera, guarde la información que considere importante y sobre ella se garantizará la disponibilidad en caso de un daño en el equipo asignado. Esta información será guardada durante un máximo de 2 años. El funcionario deberá copiar la información necesaria en una carpeta de su computador destinada para este fin e informar al funcionario Líder del proceso Gestión de las Tics para que copie la información en el servidor de archivos. La cuota de almacenamiento asignada será concertada entre el Funcionario, el Jefe Inmediato y el Líder del proceso de Gestión de las TICs.
2. CORPOGUAJIRA instalará copia de los programas que han sido adquiridos legalmente en los equipos asignados en las cantidades requeridas para suplir las necesidades. El uso de programas sin su respectiva licencia y autorización de la Corporación (imágenes, vídeos, software o música), obtenidos a partir de otras fuentes (internet, dispositivos de almacenamiento externo), puede implicar amenazas legales y de seguridad de la información para la corporación, por lo que ésta práctica no está autorizada.
3. Todo el software usado en la plataforma tecnológica de CORPOGUAJIRA debe tener su respectiva licencia y acorde con los derechos de autor.
4. CORPOGUAJIRA no se hace responsable por las copias no autorizadas de programas instalados o ejecutados en los equipos asignados a sus funcionarios o contratistas.
5. El uso de dispositivos de almacenamiento externo (dispositivos móviles, DVD, CD, memorias USB, agendas electrónicas, celulares, etc.) pueden ocasionalmente generar riesgos para la corporación 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. Para utilizar dispositivos de almacenamiento externo se debe obtener la aprobación formal e individual del Profesional Especializado de Gestión de las TICs, previa solicitud escrita por parte del jefe inmediato.
6. Los programas instalados en los equipos y la información que contienen, son de propiedad de CORPOGUAJIRA, por lo tanto, la copia no autorizada de programas o de su documentación, implica una violación a la política general de la Corporación. Aquellos funcionarios, contratistas o demás colaboradores que utilicen copias no autorizadas de programas o su respectiva documentación, quedarán sujetos a las acciones disciplinarias establecidas por CORPOGUAJIRA o las sanciones que especifique la ley.
7. CORPOGUAJIRA se reserva el derecho de proteger su buen nombre y sus inversiones en hardware y software, fomentando controles internos para prevenir el uso o la realización de copias no autorizadas de los programas de propiedad de la corporación. Estos controles pueden incluir valoraciones periódicas del uso de los programas, auditorías anunciadas y no anunciadas.
8. Los recursos tecnológicos y de software asignados a los funcionarios de CORPOGUAJIRA son responsabilidad de cada funcionario.

9. Los usuarios son los responsables de la información que administran en sus equipos personales y deben abstenerse de almacenar en ellos información no institucional, de acuerdo con la guía de clasificación de la información.
10. Los usuarios solo tendrán acceso a los datos y recursos autorizados por CORPOGUAJIRA, y serán responsables disciplinaria y legalmente de la divulgación no autorizada de esta información.
11. Es responsabilidad de cada usuario proteger la información que está contenida en documentos, formatos, listados, etc., los cuales son el resultado de los procesos informáticos; adicionalmente se deben proteger los datos de entrada de estos procesos.
13. Los dispositivos electrónicos (computadores, impresoras, fotocopiadoras, escáner, etc.) solo deben utilizarse para los fines autorizados por la corporación.
14. Cualquier evento o posible incidente que afecte la seguridad de la información, debe ser reportado inmediatamente al Líder del proceso Gestión de las TICS.
15. Los jefes de las diferentes áreas de la Corporación (Directores, Subdirectores, Secretarios, Jefes de Oficina, Asesores), en conjunto con el ***Comité de Seguridad Informática y de Sistemas*** propiciarán actividades para concienciar al personal sobre las precauciones necesarias que deben realizar los usuarios finales, para evitar revelar información confidencial cuando se hace una llamada telefónica, que pueda ser interceptada mediante acceso físico a la línea o al auricular o ser escuchada por personas que se encuentren cerca. Lo anterior debe aplicar también cuando el funcionario, contratista o colaborador se encuentre en sitios públicos como restaurantes, transporte público, ascensores, etc.

8.1.4. Políticas específicas para el proceso de Gestión de las TICS.

Objetivo: Definir las pautas generales para asegurar una adecuada protección de la información de CORPOGUAJIRA por parte de los funcionarios y contratistas del proceso de Gestión de las TICS de la corporación.

Aplicabilidad: Estas políticas aplican a los funcionarios, contratistas, colaboradores de CORPOGUAJIRA actuales o por ingresar y a terceros que estén encargados de cualquier sistema de información y hacen parte del proceso de Gestión de las TICS de la corporación.

Directrices:

1. El personal Corpoguajira con acceso a equipos y sistemas de información no debe dar a conocer sus claves y/o usuarios a terceros sin previa autorización del Jefe de Oficina de Planeación o del Profesional Especializado Líder del proceso de Gestión de las TICS.
2. Los usuarios y claves de los administradores de sistemas y del personal de Gestión de las TICS son de uso personal e intransferible.

3. Los funcionarios y contratistas de Gestión de las TICS deben emplear obligatoriamente las claves o contraseñas con un alto nivel de complejidad y utilizar los servicios de autenticación que posea la corporación de acuerdo al rol asignado.
4. Los administradores de los sistemas de información deben seguir las políticas de cambio de clave y utilizar procedimiento de salvaguarda o custodia de las claves o contraseñas en un sitio seguro. A este lugar solo debe tener acceso el Jefe de Oficina Asesora de Planeación y el Profesional Especializado Líder del proceso Gestión de las TICS.
5. Los documentos y en general la información de procedimientos, seriales, software etc. deben mantenerse custodiados en todo momento para evitar el acceso a personas no autorizadas.
6. Para el cambio o retiro de equipos de funcionarios, se deben seguir políticas de saneamiento, es decir llevar a cabo mejores prácticas para la eliminación de la información de acuerdo al software disponible en la corporación. Ej.: Formateo seguro, destrucción total de documentos o borrado seguro de equipos electrónicos.
7. Los funcionarios encargados de realizar la instalación o distribución de software, sólo instalarán productos con licencia y software autorizado.
8. Los funcionarios del proceso de Gestión de las TICS no deben otorgar privilegios especiales a los usuarios sobre las estaciones de trabajo, sin la autorización correspondiente del Jefe de la Oficina Asesora de Planeación o del Profesional Especializado de Gestión de las TICS y el registro en el formato correspondiente.
9. Los funcionarios del proceso de Gestión de las TICS no utilizarán la información para fines comerciales o diferentes al ejercicio de sus funciones.
10. Toda licencia de software o aplicativo informático y sus medios, se deben guardar y relacionar de tal forma que asegure su protección y disposición en un futuro.
11. Las copias licenciadas y registradas del software adquirido, deben ser únicamente instaladas en los equipos y servidores de la corporación. Se deben hacer copias de seguridad en concordancia con las políticas del proveedor y de la corporación.
12. El acceso a cualquier servicio, servidor o sistema de información debe ser autenticado y autorizado.
13. Todos los servidores deben ser configurados con el mínimo de servicios necesarios y obligatorios para desarrollar las funciones designadas.

8.1.5. Políticas específicas para Webmaster.

Objetivo: Proteger la integridad de las páginas Web institucionales, el software y la información contenida.

Aplicabilidad: Estas políticas aplican a los funcionarios, contratistas, colaboradores de CORPOGUAJIRA actuales o por ingresar y a terceros que se encuentren desempeñando el rol de Webmaster.

Directrices:

1. Los responsables de los contenidos de las páginas Web (*webmasters*), deben preparar y depurar la información de la página web y aplicar los requerimientos de actualización de la versión del software. Se deberá seguir la Política Editorial y Actualización de Contenidos Web, que permita auditar la publicación o modificación de información oficial en las páginas web. Las claves de acceso de los responsables de los contenidos de las páginas Web (*web masters*), son estrictamente confidenciales, personales e intransferibles.

8.1.6. Política de Tercerización u Outsourcing.

Objetivo: Mantener la seguridad de la información y los servicios de procesamiento de información, a los cuales tienen acceso terceras partes, entidades externas o que son procesados, comunicados o dirigidos por estas.

Aplicabilidad: Estas son políticas que aplican a contratistas, proveedores de outsourcing, consultores y contratistas externos, personal temporal y en general a todos los usuarios de la información que realicen estas tareas en CORPOGUAJIRA.

Directrices:

1. ***Selección de outsourcing :*** Se deben establecer criterios de selección que contemplen la historia y reputación de terceras partes, certificaciones y recomendaciones de otros clientes, estabilidad financiera de la compañía, seguimiento de estándares de gestión de calidad y de seguridad y otros criterios que resulten de un análisis de riesgos de la selección y los criterios establecidos por la corporación.
2. ***Análisis de riesgos:*** Se deben identificar los riesgos para la información y los servicios de procesamiento de información que involucren partes externas a la Corporación. El resultado del análisis de riesgos será la base para el establecimiento de los controles y debe ser presentado al Comité de Seguridad Informática y de Sistemas antes de firmar el contrato de *outsourcing*.
3. ***Acuerdos con terceras partes:*** Con el fin de proteger la información de ambas partes, se debe formalizar un acuerdo de confidencialidad. El acuerdo deberá definir claramente el tipo de información que intercambiarán las partes, los medios, la frecuencia y los procedimientos a seguir.

8.1.7. Política de retención y archivo de datos.

Objetivo: Mantener la integridad y disponibilidad de la información y de los servicios de procesamiento de información.

Aplicabilidad: Estas son políticas que aplican a la Alta Dirección, Directores, Subdirectores, Secretarios, Jefes de Oficina, Asesores, funcionarios, contratistas, y en general a todos los usuarios de la información que cumplan con los propósitos generales de CORPOGUAJIRA.

Directrices:

1. La política de retención de archivos debe establecer cuánto tiempo se deben mantener almacenados los archivos en CORPOGUAJIRA de acuerdo a las tablas de retención documental – TRD.
2. Las reglas y los principios generales que regulan la función archivística del Estado, se encuentran definidos por la Ley, la cual es aplicable a la administración pública en sus diferentes niveles producidos en función de su misión y naturaleza.
3. La ley prevé el uso de las tecnologías de la información y las comunicaciones en la administración, conservación de archivos y en la elaboración e implantación de programas de gestión de documentos.

8.1.8. Política de disposición de información, medios y equipos.

Objetivo: Contrarrestar las interrupciones en las actividades de la Corporación y proteger sus procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres y propender por su recuperación oportuna.

Aplicabilidad: Estas son políticas que aplican a la Alta Dirección, Directores, Subdirectores, Secretarios, Jefes de Oficina, Asesores, funcionarios, contratistas, y en general a todos los usuarios de la información que cumplan con los propósitos generales de CORPOGUAJIRA.

Directrices:

1. Los medios y equipos donde se almacena, procesa o comunica la información, deben mantenerse con las medidas de protección físicas y lógicas, que permitan su monitoreo y correcto estado de funcionamiento; para ello se debe realizar los mantenimientos preventivos y correctivos que se requieran.

8.1.9. Política de respaldo y restauración de información.

Objetivo: Proporcionar medios de respaldo adecuados para asegurar que toda la información esencial y el software, se pueda recuperar después de una falla.

Aplicabilidad: Esta política será aplicada por los administradores de tecnología, encargados de sistemas de información y jefaturas de área que decidan sobre la disponibilidad en integridad de los datos.

Directrices:

1. La información de cada sistema debe ser respaldada regularmente sobre un medio de almacenamiento como discos duros externos, almacenamiento en la nube, cinta, cartucho, CD, DVD, etc.

2. Los administradores de los servidores, los sistemas de información o los equipos de comunicaciones, son los responsables de definir la frecuencia de respaldo y los requerimientos de seguridad de la información (codificación) y el administrador del sistema de respaldo, es el responsable de realizar los respaldos periódicos.
3. Todas las copias de información crítica deben ser almacenadas en un área adecuada y con control de acceso.
4. Las copias de respaldo se guardarán únicamente con el objetivo de restaurar el sistema luego de un virus informático, defectos en los discos de almacenamiento, problemas de los servidores o computadores, materialización de amenazas, catástrofes y por requerimiento legal.
5. Un plan de emergencia debe ser desarrollado para todas las aplicaciones que manejen información crítica; el dueño de la información debe asegurar que el plan es adecuado, frecuentemente actualizado y periódicamente probado y revisado.
6. Ningún *tipo de información institucional* puede ser almacenada en forma exclusiva en los discos duros de las estaciones de trabajo; por lo tanto, es obligación de los usuarios finales realizar las copias en las carpetas destinadas para este fin.
7. Deben existir al menos una copia de la información de los discos de red, la cual deberá permanecer fuera de las instalaciones de la sede principal de CORPOGUAJIRA.
8. La restauración de copias de respaldo en ambientes de producción debe estar debidamente aprobada por el propietario de la información.
9. Semanalmente los administradores de infraestructura de CORPOGUAJIRA, verificarán la correcta ejecución de los procesos de backup utilizado.
10. El Profesional Especializado Líder del proceso de Gestión de las TICS debe mantener un inventario actualizado de las copias de respaldo de la información, de los aplicativos y los sistemas de información de CORPOGUAJIRA.
11. Los medios que vayan a ser eliminados deben surtir un proceso de borrado seguro y posteriormente serán eliminados o destruidos de forma adecuada. El borrado seguro se ejecuta cuando al borrar un archivo o formatear un dispositivo de almacenamiento, alguna utilidad de borrado escribe ceros (o) sobre el archivo, no permitiendo que éste se pueda recuperar posteriormente.
12. Es responsabilidad de cada dependencia mantener depurada la información de las carpetas de almacenamiento virtuales para la optimización del uso de los recursos de almacenamiento que entrega el CORPOGUAJIRA a los usuarios.

8.1.10. Política de gestión de activos de información.

Objetivo: Establecer la forma en que se logra y mantiene la protección adecuada de los activos de información.

Aplicabilidad: Estas son políticas que aplican a la Alta Dirección, Directores, Subdirectores, Secretarios, Jefes de Oficina, Asesores, funcionarios, contratistas, y en general a todos los usuarios de la información que cumplan con los propósitos generales de CORPOGUAJIRA.

Directrices:

1. ***Inventario de activos de información:*** CORPOGUAJIRA mantendrá un inventario o registro actualizado de sus activos de información, bajo la responsabilidad de cada propietario de información y centralizado por el proceso de Gestión de las TICS. El Registro de Activos de Información deberá ser publicado en la página web de la Corporación, acorde con lo establecido en el literal j del Artículo 11 de la Ley 1712 de 2014.
2. ***Propietarios de los activos de información:*** CORPOGUAJIRA es propietario de los activos de información y los administradores de estos activos son los funcionarios, contratistas o demás colaboradores de la Corporación (denominados "usuarios") que estén autorizados y sean responsables por la información de los procesos a su cargo, de los sistemas de información o aplicaciones informáticas, hardware o infraestructura de tecnología de información y comunicaciones (TIC).

8.1.11. Política de uso de los activos de información.

Objetivo: Lograr y mantener la protección adecuada de los activos de información mediante la asignación de estos a los usuarios finales que deban administrarlos de acuerdo a sus roles y funciones.

Aplicabilidad: Estas son políticas que aplican a la Alta Dirección, Directores, Subdirectores, Secretarios, Jefes de Oficina, Asesores, funcionarios, contratistas, y en general a todos los usuarios de la información que cumplan con los propósitos generales de CORPOGUAJIRA.

Directrices:

1. Los activos de información pertenecen a CORPOGUAJIRA y el uso de los mismos debe emplearse exclusivamente con propósitos laborales.
2. Los usuarios deberán utilizar únicamente los programas y equipos autorizados por el Líder del proceso de Gestión de las TICS.
3. CORPOGUAJIRA proporcionará a los usuarios los equipos informáticos y los programas instalados en ellos. Los datos/información creados, almacenados y recibidos, serán propiedad de la Corporación. Los funcionarios solo podrán realizar backup de sus archivos personales o de información pública. Para copiar cualquier tipo de información clasificada o reservada debe pedir autorización a su jefe inmediato, de acuerdo a las normas sobre clasificación de la información de acuerdo a los niveles de seguridad establecidos por CORPOGUAJIRA. Su copia, sustracción, daño intencional o utilización para fines distintos a las labores

propias de la Institución, serán sancionadas de acuerdo con las normas y legislación vigentes.

4. Periódicamente, Gestión de las TICS efectuará la revisión de los programas utilizados en cada dependencia. La descarga, instalación o uso de aplicativos o programas informáticos no autorizados será considera como una violación a las Políticas de Seguridad de la Información de CORPOGUAJIRA.
5. Todos los requerimientos de aplicativos, sistemas y equipos informáticos deben ser solicitados al Profesional Especializado Líder del proceso de Gestión de las TICS, previa autorización del Jefe inmediato, con su correspondiente justificación para su respectiva viabilidad.
6. Estarán bajo custodia del Profesional Especializado Líder del proceso Gestión de las TICS los medios magnéticos/óptico/electrónicos (discos, memorias USB, DVD, CD u otros) que vengan originalmente con el software y sus respectivos manuales y licencias de uso. Adicionalmente las claves para descargar el software de fabricantes de sus páginas web o sitios en internet y las contraseñas de administración de los equipos informáticos, sistemas de información o aplicativos.
7. En caso de ser necesario y previa autorización del **Comité de Seguridad Informática y de Sistemas** de CORPOGUAJIRA, los funcionarios podrán acceder a revisar cualquier tipo de **activo de información** y material que los usuarios creen, almacenen, envíen o reciban, a través de Internet o de cualquier otra red o medio, en los equipos informáticos a su cargo.
8. Los recursos informáticos de CORPOGUAJIRA no podrán ser utilizados, sin previa autorización escrita, para divulgar, propagar o almacenar contenido personal o comercial de publicidad, promociones, ofertas, programas destructivos (virus), propaganda política, material religioso o cualquier otro uso que no esté autorizado.
9. Los usuarios no deben realizar intencionalmente actos que impliquen un mal uso de los recursos tecnológicos. Estos actos incluyen, pero no se limitan a: envió de correo electrónico masivo con fines no institucionales y práctica de juegos en línea.
10. Los usuarios no podrán efectuar ninguna de las siguientes labores sin previa autorización del Profesional Especializado Líder del proceso Gestión de las TICS:
    a) Instalar software en cualquier equipo de la Corporación.
    b) Bajar o descargar software de Internet u otro servicio en línea en cualquier equipo de CORPOGUAJIRA.
    c) Modificar, revisar, transformar o adaptar cualquier software propiedad del CORPOGUAJIRA;
    d) Descompilar o realizar ingeniería inversa en cualquier software de propiedad del CORPOGUAJIRA.
    e) Copiar o distribuir cualquier software de propiedad del CORPOGUAJIRA.
11. El usuario deberá informar al Jefe Inmediato de cualquier violación de las políticas de seguridad o uso indebido que tenga conocimiento y este a su vez al Líder del Proceso de Gestión de las TICS.
12. El usuario será responsable de todas las transacciones o acciones efectuadas con su “cuenta de usuario”.

13. Ningún usuario deberá acceder a la red o a los servicios TIC del CORPOGUAJIRA, utilizando una cuenta de usuario o clave de otro usuario. En casos excepcionales deberá mediar una autorización expresa y limitada en el tiempo que permita identificar quien estaba utilizando el usuario y clave.
14. Cada usuario es responsable de asegurar que el uso de redes externas, tal como Internet, no comprometa la seguridad de los recursos informáticos del CORPOGUAJIRA. Los funcionarios del proceso de Gestión de las TICS de CORPOGUAJIRA, son responsables de realizar el aseguramiento de los accesos a internet, acceso a redes de terceros y a las redes de la corporación. Esta responsabilidad incluye, pero no se limita a prevenir que intrusos tengan acceso a los recursos informáticos y a prevenir la introducción y propagación de virus.
15. Todo archivo o material recibido a través de medio magnético/electrónico o descarga de Internet o de cualquier red externa, deberá ser revisado para detección de virus y otros programas destructivos antes de ser instalados en cualquier equipo que haga parte de la infraestructura tecnológica de CORPOGUAJIRA.
16. Todos los archivos provenientes de equipos externos al CORPOGUAJIRA, deben ser revisados para detección de virus antes de su utilización dentro de la red de la Corporación.

8.1.12. Política de uso de estaciones cliente.

Objetivo: Garantizar que la seguridad es parte integral de los activos de información y que son bien utilizados por los usuarios finales.

Aplicabilidad: Estas son políticas que aplican a la Alta Dirección, Directores, Subdirectores, Secretarios, Jefes de Oficina, Asesores, funcionarios, contratistas, y en general a todos los usuarios de la información que cumplan con los propósitos generales de CORPOGUAJIRA.

Directrices:

1. La instalación de software en los computadores suministrados por CORPOGUAJIRA, es una función exclusiva del proceso de Gestión de las TICS.
2. Se definirán en los computadores dos (2) perfiles de Administradores locales:
    a) Usuario Sistemas con permisos de administrador.
    b) Usuarios que necesitan utilizar software específico, que por su naturaleza requieren permisos de administrador local para su ejecución.
3. Los usuarios no deben mantener almacenados en los discos duros de los computadores asignados, estaciones cliente o discos virtuales de red: archivos de vídeo, música y fotos que no sean de carácter institucional.
4. En el Disco C:\ de las estaciones cliente y computadores se tiene configurado el sistema operativo, aplicaciones y perfil de usuario. El usuario deberá abstenerse de realizar modificaciones a éstos archivos.

5. Los usuarios deberán ubicar copias y documentos finales en las carpetas que se establezca para cumplir con las tablas de retención documental TRD de la Corporación.
6. El préstamo de equipos de cómputo, computadores portátiles y vídeo proyectores se debe tramitar con la oficina que tenga asignado los elementos, lo cual debe hacerse con anticipación y se proveerá de acuerdo a la disponibilidad.
7. Los equipos que ingresan temporalmente a CORPOGUAJIRA que son de propiedad de terceros: deben ser registrados en las porterías de la corporación para poder realizar su retiro sin autorización. La corporación no se hará responsable en caso de pérdida o daño de algún equipo informático de uso personal o que haya sido ingresado a sus instalaciones. De igual manera no es responsable del contenido y legalidad de la información almacenada en dicho equipo.
8. El proceso de Gestión de las TICS prestará servicio de soporte técnico (revisión, configuración, manejo de información, copias de seguridad e instalación de programas) de forma directa o través de terceros a equipos que sean de propiedad de CORPOGUAJIRA o que estén amparados bajo un contrato de alquiler. Los servicios de mantenimiento y reparación se harán de acuerdo a lo establecido en Plan de Mantenimiento de la Corporación.

8.1.13. Política de uso de Internet.

Objetivo: Establecer unos lineamientos que garanticen la navegación segura y el uso adecuado de la red por parte de los usuarios finales, evitando errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones WEB.

Aplicabilidad: Estas son políticas que aplican a la Alta Dirección, Directores, Subdirectores, Secretarios, Jefes de Oficina, Asesores, funcionarios, contratistas, y en general a todos los usuarios de la información que cumplan con los propósitos generales de CORPOGUAJIRA.

Directrices:
1. La navegación en Internet debe realizarse de forma razonable y con propósitos laborales.
2. No se permite la navegación a sitios con contenidos contrarios a la ley o a las políticas de CORPOGUAJIRA o que representen peligro para la corporación como: pornografía, terrorismo, hacktivismo, segregación racial u otras fuentes definidas por la corporación.
3. El acceso a contenidos no permitidos con propósitos de estudio de seguridad o de investigación, debe contar con la autorización expresa del Comité de Seguridad Informática y de Sistemas de la CORPORACION.
4. La descarga de archivos de Internet debe ser con propósitos laborales y de forma razonable para no afectar el servicio de Internet/Intranet, en forma

específica el usuario debe cumplir los requerimientos de la política de uso de internet descrita en este manual.

8.1.14. Política de uso de mensajería instantánea y redes sociales.

Objetivo: Definir las pautas generales para asegurar una adecuada protección de la información de CORPOGUAJIRA, en el uso del servicio de mensajería instantánea y de las redes sociales, por parte de los usuarios autorizados.

Aplicabilidad: Estas son políticas que aplican a la Alta Dirección, Directores, Subdirectores, Secretarios, Jefes de Oficina, Asesores, funcionarios, contratistas, y en general a todos los usuarios de la información que cumplan con los propósitos generales de CORPOGUAJIRA.

Directrices:

1. El uso y administración de los servicios de mensajería instantánea y redes sociales como canales oficiales estarán autorizados solo para un grupo reducido de usuarios, teniendo en cuenta sus funciones y para facilitar canales de comunicación con la ciudadanía.
2. No se permite el envío de mensajes con contenido que atente contra la integridad de las personas o instituciones o cualquier contenido que represente riesgo de código malicioso.
3. La información que se publique o divulgue por redes sociales o cualquier medio de Internet, de cualquier funcionario, contratista o colaborador de CORPOGUAJIRA, que sea creado a nombre personal, como redes sociales, *twitter*®, *facebook*®, *youtube*® likedink® o *blogs,* se considera fuera del alcance del SGSI y por lo tanto su confiabilidad, integridad y disponibilidad y los daños y perjuicios que pueda llegar a causar serán de completa responsabilidad de la persona que las haya generado.

8.1.15. Política de uso de discos de red o carpetas virtuales.

Objetivo: Asegurar la operación correcta y segura de los discos de red o carpetas virtuales.

Aplicabilidad: Estas son políticas que aplican a la Alta Dirección, Directores, Subdirectores, Secretarios, Jefes de Oficina, Asesores, funcionarios, contratistas, y en general a todos los usuarios de la información que cumplan con los propósitos generales de CORPOGUAJIRA.

Directrices:

1. Para que los usuarios tengan acceso a la información ubicada en los discos de red, se debe registrar la solicitud a través de servicios compartidos especificando el acceso y permisos, correspondientes al rol y funciones a desempeñar, al Líder del proceso Gestión de las TICS de CORPOGUAJIRA. Los usuarios tendrán

permisos de escritura, lectura o modificación de información en los discos de red, dependiendo de sus funciones y su rol.
2. La información institucional que se trabaje en las estaciones cliente de cada usuario debe ser trasladada periódicamente a los discos de red por ser información institucional.
3. La información almacenada en cualquiera de los discos de red debe ser de carácter institucional.
4. Está prohibido almacenar archivos con contenido que atente contra la moral y las buenas costumbres de la corporación o las personas, como pornografía, propaganda racista, terrorista o cualquier software ilegal o malicioso, ya sea en medios de almacenamiento de estaciones de trabajo, computadores de escritorio o portátiles, tablets, celulares inteligentes, etc. o en los discos de red.
5. Se prohíbe extraer, divulgar o publicar información de cualquiera de los discos de red o estaciones de trabajo, sin expresa autorización de su jefe inmediato.
6. Se prohíbe el uso de la información de los discos de red con fines publicitarios, de imagen negativa, lucrativa o comercial.
7. La responsabilidad de generar las copias de respaldo de la información de los discos de red, está a cargo del Líder del proceso Gestión de las TICS de CORPOGUAJIRA.
8. La responsabilidad de custodiar la información en copias de respaldo controladas, fuera de la sede principal de la Corporación, estará a cargo del Líder del proceso Gestión de las TICS de CORPOGUAJIRA.

8.1.16. Política de uso de impresoras y del servicio de Impresión.

Objetivo: Asegurar la operación correcta y segura de las impresoras y del servicio de impresión.

Aplicabilidad: Estas son políticas que aplican a la Alta Dirección, Directores, Subdirectores, Secretarios, Jefes de Oficina, Asesores, funcionarios, contratistas, y en general a todos los usuarios de la información que cumplan con los propósitos generales de CORPOGUAJIRA.

Directrices:
1. Los documentos que se impriman en las impresoras de CORPOGUAJIRA deben ser de carácter institucional.
2. Es responsabilidad del usuario conocer el adecuado manejo de los equipos de impresión (escáner y fotocopiado) para que no se afecte su correcto funcionamiento.
3. Ningún usuario debe realizar labores de reparación o mantenimiento de las impresoras. En caso de presentarse alguna falla, esta se debe reportar al Líder del proceso de Gestión de las TICS de CORPOGUAJIRA quien revisará y evaluará el estado de la impresora. En caso de requerir reparación se trasladará al encargado de Logística para que de acuerdo al Plan de Mantenimiento haga lo respectivo.

8.1.17. Política de uso de puntos de red de datos (red de área local – LAN).

Objetivo: Asegurar la operación correcta y segura de los puntos de red.

Aplicabilidad: Estas son políticas que aplican a la Alta Dirección, Directores, Subdirectores, Secretarios, Jefes de Oficina, Asesores, funcionarios, contratistas, y en general a todos los usuarios de la información que cumplan con los propósitos generales de CORPOGUAJIRA.

Directrices:

1. Los usuarios deberán emplear los puntos de red, para la conexión de equipos informáticos estándar. Los equipos de uso personal, que no son de propiedad de CORPOGUAJIRA, solo tendrán acceso a servicios limitados destinados a invitados o visitantes, estos equipos deben ser conectados a los puntos de acceso autorizados y definidos por el Líder del proceso Gestión de las TICS.
2. La instalación, activación y gestión de los puntos de red es responsabilidad del proceso de Gestión de las TICS.

8.1.18. Políticas de seguridad del centro de datos y centros de cableado.

Objetivo: Asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.

Aplicabilidad: Estas políticas aplican a los funcionarios, contratistas, colaboradores de CORPOGUAJIRA actuales o por ingresar y a terceros que estén encargados de cualquier parte o sistema de la plataforma informática.

Directrices:

1. No se permite el ingreso al centro de datos, al personal que no esté expresamente autorizado.
2. El Líder del proceso de Gestión de las TICS debe garantizar que el control de acceso al centro de datos de CORPOGUAJIRA y contar con dispositivos electrónicos de autenticación o sistema de control biométrico.
3. El proceso de Gestión de las TICS deberá garantizar que todos los equipos de los centros de datos cuenten con un sistema alterno de respaldo de energía
4. La limpieza y aseo del centro de datos estará a cargo de Secretaría General y debe efectuarse en presencia de un funcionario o contratista del proceso de Gestión de las TICS de CORPOGUAJIRA. El personal de limpieza debe ser ilustrado con respecto a las precauciones mínimas a seguir durante el proceso de limpieza. Debe prohibirse el ingreso de personal de limpieza con maletas o elementos que no sean estrictamente necesarios para su labor de limpieza y aseo.
5. En las instalaciones del centro de datos o centros de cableado, no se debe fumar, comer o beber; de igual forma se debe eliminar la permanencia de papelería y materiales que representen riesgo de propagación de fuego, así

como mantener el orden y limpieza en todos los equipos y elementos que se encuentren en este espacio.

6. **El centro de datos debe estar provisto de:**
   a) 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 ocupacional.
   b) Pisos elaborados con materiales no combustibles.
   c) Sistema de refrigeración por aire acondicionado de precisión. Este equipo debe ser redundante para que en caso de falla se pueda continuar con la refrigeración.
   d) 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.
   e) Alarmas de detección de humo y sistemas automáticos de extinción de fuego, conectada a un sistema central. Los detectores deberán ser probados de acuerdo a las recomendaciones del fabricante o al menos una vez cada 6 meses y estas pruebas deberán estar previstas en los procedimientos de mantenimiento y de control.
   f) 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.

7. El cableado de la red debe ser protegido de interferencias por ejemplo usando canaletas que lo protejan.
8. Los cables de potencia deben estar separados de los de comunicaciones, siguiendo las normas técnicas.
9. La grabación de vídeo en las instalaciones del centro de datos debe estar expresamente autorizada por el ***Comité de Seguridad Informática y de Sistemas*** y exclusivamente con fines institucionales.
10. Las actividades de soporte y mantenimiento dentro del centro de datos siempre deben ser supervisadas por un funcionario o contratista autorizado de CORPOGUAJIRA.
11. Las puertas del centro de datos deben permanecer cerradas. Si por alguna circunstancia se requiere ingresar y salir del centro de datos, el funcionario responsable de la actividad se ubicará dentro del centro de datos.
12. Cuando se requiera realizar alguna actividad sobre algún armario (*rack*), este debe quedar ordenado, cerrado y con llave, cuando se finalice la actividad.
13. Mientras no se encuentre personal dentro de las instalaciones del centro de datos, las luces deben permanecer apagadas.
14. Los equipos del centro de datos que lo requieran, deben estar monitoreados para poder detectar las fallas que se puedan presentar.

8.1.19. Políticas de seguridad de los Equipos

Objetivo: Asegurar la protección de la información en los equipos.

Aplicabilidad: Estas son políticas que aplican a la Alta Dirección, Directores, Subdirectores, Secretarios, Jefes de Oficina, Asesores, funcionarios, contratistas, y en general a todos los usuarios de la información que cumplan con los propósitos generales de CORPOGUAJIRA.

Directrices:

1. ***Protecciones en el suministro de energía:*** A la red de energía regulada de los puestos de trabajo solo se pueden conectar equipos como computadores, pantallas; los otros elementos deberán conectarse a la red no regulada. Esta labor debe ser revisada por el encargado de Logística de secretaría General.
2. ***Seguridad del cableado:*** Los cables deben estar claramente marcados para identificar fácilmente los elementos conectados y evitar desconexiones erróneas. Deben existir planos que describan las conexiones del cableado. El acceso a los centros de cableado (Racks), debe estar protegido.
3. ***Mantenimiento de los Equipos:*** *CORPOGUAJIRA debe mantener contratos de soporte y mantenimiento de los equipos críticos.* Las actividades de mantenimiento tanto preventivo como correctivo deben registrarse para cada elemento. Las actividades de mantenimiento de los servidores, elementos de comunicaciones, energía o cualquiera que pueda ocasionar una suspensión en el servicio, deben ser realizadas y programadas.
    a) Los equipos que requieran salir de las instalaciones CORPOGUAJIRA para reparación o mantenimiento, deben estar debidamente autorizados y se debe garantizar que en dichos elementos no se encuentra información establecida como crítica en la clasificación de la información de acuerdo a los niveles de clasificación de la información. Para que los equipos puedan salir fuera de las instalaciones, se debe suministrar un nivel mínimo de seguridad, que al menos cumpla con los requerimientos internos, teniendo en cuenta los diferentes riesgos de trabajar en un ambiente que no cuenta con las protecciones ofrecidas en el interior de CORPOGUAJIRA.

    b) Cuando un dispositivo vaya a ser reasignado o retirado de servicio, debe garantizarse la eliminación de toda información residente en los elementos utilizados para el almacenamiento, procesamiento y transporte de la información, utilizando herramientas para realizar sobre-escrituras sobre la información existente o la presencia de campos magnéticos de alta intensidad. Este proceso puede además incluir, una vez realizado el proceso anterior, la destrucción física del medio, utilizando impacto, fuerzas o condiciones extremas.
4. ***Ingreso y retiro de activos de información de terceros:*** El retiro e ingreso de todo **activo de información** de propiedad de los usuarios de CORPOGUAJIRA, utilizados para fines personales, se realizará mediante los procedimientos establecidos por la Administración. CORPOGUAJIRA no se hace responsable de los bienes o los problemas que se presenten al conectarse a la red eléctrica pública.

5. El retiro e ingreso de todo **activo de información** de los visitantes que presten servicios a CORPOGUAJIRA (consultores, pasantes, visitantes, etc.) será registrado y controlado en las porterías del edificio. El personal de vigilancia de recepción verificará y registrará las características de identificación del activo de información. El traslado entre dependencias de CORPOGUAJIRA de todo activo de información, está a cargo del área Administrativa, para el control de inventarios.

8.1.20. Política de escritorio y pantalla limpia.

Objetivo: Definir las pautas generales para reducir el riesgo de acceso no autorizado, pérdida y daño de la información durante y fuera del horario de trabajo normal de los usuarios.

Aplicabilidad: Estas son políticas que aplican a la Alta Dirección, Directores, Subdirectores, Secretarios, Jefes de Oficina, Asesores, funcionarios, contratistas, y en general a todos los usuarios de la información que cumplan con los propósitos generales de CORPOGUAJIRA.

Directrices:

1. El personal de CORPOGUAJIRA debe conservar su escritorio libre de información, propia de la corporación, que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.
2. El personal de CORPOGUAJIRA debe bloquear la pantalla de su computador con el protector de pantalla, en los momentos que no esté utilizando el equipo o cuando por cualquier motivo deba dejar su puesto de trabajo.
3. Al imprimir documentos de carácter confidencial, estos deben ser retirados de la impresora inmediatamente y no se deben dejar en el escritorio sin custodia.
4. No se debe utilizar fotocopiadoras, escáneres, equipos de fax, cámaras digitales y en general equipos tecnológicos que se encuentren desatendidos.

8.1.21. Política de uso de correo electrónico.

Objetivo: Definir las pautas generales para asegurar una adecuada protección de la información de CORPOGUAJIRA, en el uso del servicio de correo electrónico por parte de los usuarios autorizados.

Aplicabilidad: Estas son políticas que aplican a la Alta Dirección, Directores, Subdirectores, Secretarios, Jefes de Oficina, Asesores, funcionarios, contratistas, y en general a todos los usuarios de la información que cumplan con los propósitos generales de CORPOGUAJIRA.

Directrices:

1. Esta política define y distingue el uso de correo electrónico aceptable/apropiado e inaceptable/inapropiado y establece las directrices para el uso seguro del servicio.

2. **Servicio de correo electrónico:** Permite a los usuarios de CORPOGUAJIRA, el intercambio de mensajes, a través de una cuenta de correo electrónico institucional, que facilita el desarrollo de sus funciones.

3. **Principios guía**
   a) Los usuarios del correo electrónico corporativo son responsables de evitar prácticas o usos del correo que puedan comprometer la seguridad de la información.
   b) Los servicios de correo electrónico corporativo se emplean para servir a una finalidad operativa y administrativa en relación con la corporación. Todos los correos electrónicos procesados por los sistemas, redes y demás infraestructura TIC de CORPOGUAJIRA se consideran bajo el control de la corporación.
   c) Este servicio debe utilizarse exclusivamente para las tareas propias de la función desarrollada en CORPOGUAJIRA y no debe utilizarse para ningún otro fin.
   d) El envío de cadenas de correo, envío de correos masivos con archivos adjuntos de gran tamaño que puedan congestionar la red, no está autorizado.
   e) No está autorizado, el envío de correos con contenido que atenten contra la integridad y dignidad de las personas y el buen nombre de la corporación.
4. Cuando un funcionario, contratista o colaborador al que le haya sido autorizado el uso de una cuenta de correo electrónico y se retire de CORPOGUAJIRA, su cuenta de correo será desactivada. Los correos electrónicos deben contener la siguiente nota respecto al manejo del contenido:

   "El contenido de este mensaje y sus anexos son propiedad de la Corporación Autónoma Regional de La Guajira – Corpoguajira, es únicamente para el uso del destinatario ya que puede contener información pública reservada o información pública clasificada (privada o semiprivada), las cuales no son de carácter público. Si usted no es el destinatario, se informa que cualquier uso, difusión, distribución o copiado de esta comunicación está prohibido. Cualquier revisión, retransmisión, diseminación o uso del mismo, así como cualquier acción que se tome respecto a la información contenida, por personas o entidades diferentes al propósito original de la misma, es ilegal. Si usted es el destinatario, le solicitamos dar un manejo adecuado a la información; de presentarse cualquier suceso anómalo, por favor informarlo al correo servicioalcliente@Corpoguajira.gov.co."

5. El tamaño del buzón de correo electrónico estará determinado por las capacidades del servicio contratado y por el rol desempeñado por el usuario en CORPOGUAJIRA. En todo caso no podrá ser superior al definido como "tamaño máximo" por el Líder del proceso Gestión de las TICS de CORPOGUAJIRA.
6. Cada área deberá solicitar la creación, modificación o cancelación de las cuentas electrónicas de los funcionarios y contratistas. Igualmente la Coordinación de

Talento Humanos podrá solicitar la creación, modificación o cancelación de las cuentas electrónicas al proceso de Gestión de las TICS de CORPOGUAJIRA.

7. Las cuentas de correo electrónico son propiedad de CORPOGUAJIRA, las cuales son asignadas a personas que tengan algún tipo de vinculación laboral con la corporación, ya sea como personal de planta, contratistas, consultores o personal temporal, quienes deben utilizar este servicio única y exclusivamente para las tareas propias de la función desarrollada en la Corporación y no debe utilizarse para ningún otro fin.
8. Cada usuario es responsable del contenido del mensaje enviado y de cualquier otra información adjunta al mismo, de acuerdo a la clasificación de la información establecida por CORPOGUAJIRA.
9. Todos los mensajes pueden ser sujetos a análisis y conservación permanente por parte de la Corporación.
10. Todo usuario es responsable por la destrucción de los mensajes cuyo origen sea desconocido y por lo tanto asumirá la responsabilidad y las consecuencias que puede ocasionar la ejecución de cualquier archivo adjunto. En estos casos no se debe contestar dichos mensajes, ni abrir los archivos adjuntos y se debe reenviar el correo a la cuenta sistemas@Corpoguajira.gov.co con la frase "correo sospechoso" en el asunto.
11. El único servicio de correo electrónico autorizado en la corporación es el correo corporativo con dominio **@Corpoguajira.gov.co** asignado por Gestión de las TICS de CORPOGUAJIRA.

8.1.22. Política de control de acceso.

Objetivo: Definir las pautas generales para asegurar un acceso controlado, físico o lógico, a la información de la plataforma informática de CORPOGUAJIRA, así como el uso de medios de computación móvil.

Aplicabilidad: Estas son políticas que aplican a la Alta Dirección, Directores, Subdirectores, Secretarios, Jefes de Oficina, Asesores, funcionarios, contratistas, y en general a todos los usuarios de la información que cumplan con los propósitos generales de CORPOGUAJIRA.

Directrices:

1. CORPOGUAJIRA proporcionará a los funcionarios y contratistas (personas naturales) todos los recursos tecnológicos necesarios para que puedan desempeñar las funciones para las cuales fueron contratados, por tal motivo no se permite conectar a la red o instalar dispositivos fijos o móviles personales, tales como: computadores portátiles, *tablets*, enrutadores, agendas electrónicas, celulares inteligentes, *access point*, que no sean autorizados por el líder del proceso Gestión de las TICS de CORPOGUAJIRA. En los casos en que se requiera, el jefe inmediato o el supervisor del contratista, solicitará el acceso a la red de datos y/o a los servicios de internet de la corporación.
2. CORPOGUAJIRA suministrará a los usuarios las claves respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido

autorizados, las claves son de uso personal e intransferible. Es responsabilidad del usuario el manejo que se les dé a las claves asignadas.

3. Solo usuarios designados por el Líder del proceso Gestión de las TICS de CORPOGUAJIRA estarán autorizados para instalar software o hardware en los equipos, servidores e infraestructura de telecomunicaciones de la corporación.
4. Todo trabajo que utilice los servidores CORPOGUAJIRA con información de la corporación, debe ser autorizado por el Líder del proceso Gestión de las TICS de CORPOGUAJIRA. No se podrá realizar ninguna actividad de tipo remoto sin la debida aprobación de CORPOGUAJIRA.
5. La conexión remota a la red de área local de CORPOGUAJIRA debe ser hecha a través de una conexión VPN segura suministrada por la corporación, la cual debe ser aprobada, registrada y auditada. En todo, caso, otro tipo de conexión deberá ser aprobada y auditada por el Líder del proceso Gestión de las TICS de CORPOGUAJIRA.

8.1.23. Política de establecimiento, uso y protección de claves de acceso.

Objetivo: Controlar el acceso a la información.

Aplicabilidad: Estas son políticas que aplican a la Alta Dirección, Directores, Subdirectores, Secretarios, Jefes de Oficina, Asesores, funcionarios, contratistas, y en general a todos los usuarios de la información que cumplan con los propósitos generales de CORPOGUAJIRA.

Directrices:

1. Se debe concienciar y controlar que los usuarios sigan buenas prácticas de seguridad en la selección, uso y protección de claves o contraseñas, las cuales constituyen un medio de validación de la identidad de un usuario y consecuentemente un medio para establecer derechos de acceso a las instalaciones, equipos o servicios informáticos.
2. Los usuarios 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 Corporación.
3. Los usuarios deben tener en cuenta los siguientes aspectos:
    a) No incluir contraseñas en ningún proceso de registro automatizado, por ejemplo almacenadas en un macro o en una clave de función.
    b) El cambio de contraseña solo podrá ser solicitado por el titular de la cuenta o su jefe inmediato.
    c) Terminar las sesiones activas cuando finalice, o asegurarlas con el mecanismo de bloqueo cuando no estén en uso.
    d) Se bloqueará el acceso a todo usuario que haya intentado el ingreso, sin éxito, a un equipo o sistema informático, en forma consecutiva por cinco veces.
    e) La clave de acceso será desbloqueada sólo por funcionarios del proceso Gestión de las TICS de CORPOGUAJIRA, luego de la solicitud formal por parte del responsable de la cuenta. Para todas las **cuentas especiales**,

la reactivación debe ser documentada y comunicada al Jefe de la Oficina Asesora de Planeación y al Profesional Especializado Líder del proceso Gestión de las TICS.

4. Las claves o contraseñas deben:
    a) 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.
    b) Tener mínimo diez caracteres alfanuméricos.
    c) Cambiarse obligatoriamente la primera vez que el usuario ingrese al sistema.
    d) Cambiarse obligatoriamente cada 60 días, o cuando lo establezca el proceso Gestión de las TICS de CORPOGUAJIRA.
    e) Cada vez que se cambien estas deben ser distintas por lo menos de las últimas tres anteriores.
    f) Cambiar la contraseña si ha estado bajo riesgo o se ha detectado anomalía en la cuenta de usuario.
    g) No se deben usar caracteres idénticos consecutivos, ni que sean todos numéricos, ni todos alfabéticos.
    h) No debe ser visible en la pantalla, al momento de ser ingresada o mostrarse o compartirse.
    i) No ser reveladas a ninguna persona, incluyendo al personal del proceso Gestión de las TICS de CORPOGUAJIRA.
    j) No regístralas en papel, archivos digitales o dispositivos manuales, a menos que se puedan almacenar de forma segura y el método de almacenamiento este aprobado.

8.1.24. Política de adquisición, desarrollo y mantenimiento de sistemas de información.

Objetivo: Garantizar que la seguridad es parte integral de los sistemas de información.

Aplicabilidad: Estas son políticas que aplican a la Alta Dirección, Directores, Subdirectores, Secretarios, Jefes de Oficina, Asesores, funcionarios, contratistas y en general a todos los usuarios de la información que cumplan con los propósitos generales de CORPOGUAJIRA.

Directrices:

1. Asegurar que los sistemas de información o aplicativos informáticos incluyen controles de seguridad y cumplen con las políticas de seguridad de la información.
2. En caso de desarrollos propios de la corporación se debe verificar que están completamente documentados, que las diferentes versiones se preservan adecuadamente en varios medios y se guarda copia de respaldo externa a la

corporación y que sean registrados ante la Dirección General de Derechos de Autor del Ministerio del Interior y de Justicia.

3. Desarrollar estrategias para analizar la seguridad en los sistemas de información.
4. Todo nuevo hardware y software que se vaya a adquirir y conectar a la plataforma tecnológica de CORPOGUAJIRA, por cualquier dependencia o proyecto de la CORPORACION, deberá ser gestionado por el Profesional Especializado Líder del proceso Gestión de las TICS de CORPOGUAJIRA.
5. Al comprar la licencia de un programa, se permitirá a CORPOGUAJIRA realizar una copia de seguridad (a no ser que esté estipulado de manera distinta), para ser utilizada en caso de que el medio se averíe.
6. Cualquier otra copia del programa original será considerada como una copia no autorizada y su utilización conlleva a las sanciones administrativas y legales pertinentes.
7. Los funcionarios del proceso Gestión de las TICS de CORPOGUAJIRA serán los únicos autorizados para realizar copia de seguridad del software original.
8. La instalación del software en las máquinas y/o equipos de CORPOGUAJIRA, se realizará únicamente a través de los funcionarios y/o contratistas autorizados por el Profesional Especializado de Gestión de las TICS de CORPOGUAJIRA.
9. El software proporcionado por CORPOGUAJIRA no puede ser copiado o suministrado a terceros.
10. En los equipos de CORPOGUAJIRA solo se podrá utilizar el software licenciado por CORPOGUAJIRA y el adquirido o licenciado por los proyectos o programas que se encuentran en CORPOGUAJIRA.
11. Para la adquisición y actualización de software, es necesario efectuar la solicitud al Profesional Especializado Líder del proceso Gestión de las TICS con su justificación, quien analizará las propuestas presentadas para su evaluación y aprobación.
12. El software que se adquiera a través de los proyectos o programas, debe quedar a nombre de la Corporación Autónoma Regional de La Guajira - CORPOGUAJIRA.
13. Se encuentra prohibido el uso e instalación de juegos y programas de ocio en los computadores de CORPOGUAJIRA.
14. Cuando un software no se utilice y no sea requerido, se presentará al para ser dado de baja, de acuerdo con los lineamientos dados por la Corporación.

8.1.25. Política de uso de dispositivos móviles

Objetivo: Establecer las directrices de uso y manejo de dispositivos móviles (teléfonos móviles, teléfonos inteligentes (Smart phones) tabletas, entre otros) de la corporación.

Aplicabilidad: Estas son políticas que aplican a la Alta Dirección, Directores, Subdirectores, Secretarios, Jefes de Oficina, Asesores, funcionarios, contratistas, y en general a todos los usuarios de la información que cumplan con los propósitos generales de CORPOGUAJIRA.

Directrices:

1. Los dispositivos móviles (teléfonos móviles, teléfonos inteligentes (Smart phones) tabletas, entre otros) de la corporación, son una herramienta de trabajo que se deben utilizar únicamente para facilitar las comunicaciones de los usuarios de la corporación.
2. Los dispositivos móviles de la corporación podrán estar integrados a las plataformas de administración controlada por el proceso Gestión de las TICS de CORPOGUAJIRA.
3. Los usuarios podrán tener instaladas las aplicaciones distribuidas y autorizadas por el administrador de la plataforma.
4. Los dispositivos móviles de propiedad de la corporación deben tener configurado la cuenta de correo electrónico de la corporación.
5. Los usuarios que hagan uso de dispositivos móviles corporativos que requieran configuración, deben hacerlo asociándolos a la cuenta de correo corporativo del usuario.
6. Ante la pérdida del equipo, ya sea por sustracción o extravío, deberá dar cuenta en forma inmediata al funcionario de Almacén y al Profesional Especializado de Líder del proceso Gestión de las TICS.
7. Los teléfonos móviles y/o teléfonos inteligentes de propiedad de la corporación, deben permanecer encendidos y cargados durante las horas laborales o de acuerdo a la responsabilidad y a los requerimientos propios del cargo.
8. Es responsabilidad del usuario hacer buen uso del dispositivo suministrado por CORPOGUAJIRA con el fin de realizar actividades propias de su cargo o funciones asignadas en la corporación.
9. En caso de requerir instalación de aplicaciones adicionales en el dispositivo móvil se debe solicitar al Profesional Especializado Líder del proceso de Gestión de las Tics para su aprobación.

8.1.26. Política para realización de copias en estaciones de trabajo de usuario final.

Objetivo: Asegurar la operación de realización de copias de información en estaciones de trabajo de usuario final.

Aplicabilidad: Estas son políticas que aplican a la Alta Dirección, Directores, Subdirectores, Secretarios, Jefes de Oficina, Asesores, funcionarios, contratistas, y en general a todos los usuarios de la información que cumplan con los propósitos generales de CORPOGUAJIRA.

Directrices:

1. De acuerdo a lo previsto por el artículo 91 de la Ley 23 de 1982, los derechos de autor sobre las obras creadas por los empleados y funcionarios en virtud de su vinculación a la Entidad pública correspondiente, en este caso a la Corporación

Autónoma Regional de La Guajira - CORPOGUAJIRA, son de propiedad de esta con las excepciones que la misma ley han señalado.

2. En el evento de retiro de un funcionario o traslado de dependencia, previa notificación del Área de Talento Humano, el Líder del proceso Gestión de las TICS de CORPOGUAJIRA generará una copia de la información contenida en el equipo asignado al perfil del usuario a una unidad de almacenamiento. Si el jefe de la dependencia de la cual se retira el usuario requiere copia de esta información, debe realizar solicitud a Gestión de las TICS.
3. Se debe seguir un procedimiento de **Borrado Seguro** para equipos Final, a fin garantizar la copia de la información para la entidad y la eliminación de la información almacenada en el disco local.
4. En caso de presentarse alguna falla en los equipos de cómputo, se debe reportar a Gestión de las TICS. En caso de requerirse copia de la información, esta se realizará de manera temporal durante las diferentes labores de reparación o mantenimiento.

8.1.27. Política de uso de Token (RSA)

Objetivo: Establecer las directrices de uso del mecanismo de doble autenticación (Token), para los diferentes servicios prestados por CORPOGUAJIRA o entidades externas (Bancos, Ministerios u otros).

Aplicabilidad: Estas son políticas que aplican a la Alta Dirección, Directores, Subdirectores, Secretarios, Jefes de Oficina, Asesores, funcionarios, contratistas, y en general a todos los usuarios de la información que cumplan con los propósitos generales de CORPOGUAJIRA.

Directrices:

1. Gestión de las TICS verificará la asignación de los Token a funcionarios de CORPOGUAJIRA por parte de las diferentes entidades, de acuerdo a los accesos a las plataformas que lo requieran.
2. La asignación de Token VPN a los funcionarios dependerá del desarrollo de sus funciones, y deberá estar autorizado por el ***Comité de Seguridad Informática y de Sistemas***.
3. La asignación de Token a los funcionarios para la autenticación del equipo con otras entidades dependerá del tipo de información que maneje y se establezca como información pública reservada o información pública clasificada.
4. Es responsabilidad del usuario hacer buen uso del dispositivo entregado, con el fin de realizar actividades propias de su cargo o funciones asignadas.
5. La pérdida del Token entregado debe ser reportado de inmediato a Gestión de las TICS y solicitar su debida desactivación y bloqueo.
6. En caso de no requerir más el uso del Token o retiro definitivo de CORPOGUAJIRA, el funcionario debe realizar la devolución del mismo en las condiciones que le fue entregado.

8.2. Procedimientos que apoyan la Política de Seguridad

Los procedimientos son uno de los elementos dentro de la documentación del ***Manual de la Política de Seguridad para las Tecnologías de la Información y las comunicaciones***. Un procedimiento describe de forma más detallada lo que se hace en las actividades de un proceso, en él se especifica cómo se deben desarrollar las actividades, cuáles son los recursos, el método y el objetivo que se pretende lograr o el valor agregado que genera y caracteriza el proceso.

También es recomendable el uso de instructivos para detallar aún más las tareas y acciones puntuales que se deben desarrollar dentro de un procedimiento, como son los instructivos de trabajo y de operación; los primeros para la ejecución de la tarea por la persona y los segundos para la manipulación o la operación de un equipo.

8.2.1. Procedimiento de control de documentos

Garantiza que la organización cuente con los documentos estrictamente necesarios a partir de su perfil de actuación en cada momento y maneja la dinámica del mejoramiento, mostrando la realidad que atraviesa la corporación en cada momento, porque incorpora la eficacia de las diferentes acciones, a través de la revisión documental y del cumplimiento de los requisitos idénticos en los diferentes modelos de gestión, sobre el control de documentos. Así mismo, busca garantizar que los documentos en uso son confiables y también se pretende mantenerlos actualizados, una vez se evidencia la eficacia de las acciones correctivas, preventivas y de mejora que hacen que los procesos se ajusten y evolucionen y que los documentos existentes en el momento de la evaluación y comprobación del cambio que se implementó como solución a un problema, riesgo o a una oportunidad se conserven.

De acuerdo a la correspondencia y vínculos técnicos entre las normas NTCGP1000 y NTC-IS09001 y las normas NTC-IS09001 y NTC-IS027001 se tienen en cuenta los lineamientos establecidos en la documentación del Sistema Integrado de Gestión de la Corporación, se utiliza el Procedimiento de control de documentos del Proceso Gestión Documental.

8.2.2. Procedimiento de control de registros

Está definido para evidenciar las acciones realizadas y los resultados obtenidos en la ejecución de las actividades, con el fin de analizar los datos, y lo que es más importante, para la toma de decisiones, de tal forma que registro que no aporta valor o no lleva a una decisión de mejora o de acción, no se debe tener en el sistema, ya que lo único que haría es desgastar a la organización y generar residuos sólidos como papel mal utilizado.

De acuerdo a la correspondencia y vínculos técnicos entre las normas NTCGP1000 y NTC-IS09001 y las normas NTC-IS09001 y NTC-IS027001 se utiliza el Procedimiento de control de registros del Proceso Gestión Documental.

8.2.3. Procedimiento de auditoría interna

La auditoría interna es una herramienta para la alta dirección, en el momento de determinar la eficacia y la eficiencia del sistema de gestión, a través de la identificación de las fortalezas y debilidades. Esta es la razón por la cual se recomienda siempre realizar auditorías internas antes de llevar a cabo la revisión gerencial, ya que para esta última se requiere información sobre el sistema y los procesos, de tal manera que se pueda evaluar la adecuación, la conveniencia y la eficacia del sistema de gestión.

Se hacen auditorias para evaluar la conformidad con las políticas de la organización, para evaluar el nivel de implementación del sistema de gestión, para evaluar el estado de mantenimiento y la capacidad de mejoramiento del sistema de gestión.
De acuerdo a la correspondencia y vínculos técnicos entre las normas NTCGP1000 y NTC-IS09001 y las normas NTC-IS09001 y NTC-IS027001 se utiliza el documento administración de auditorías internas.

8.2.4. Procedimiento de acción correctiva

El objetivo de este procedimiento es definir los lineamientos para eliminar la causa de no conformidades asociadas con los requisitos de la política de seguridad de CORPOGUAJIRA, así como: definir los lineamientos para identificar, registrar, controlar, desarrollar, implantar y dar seguimiento a las acciones correctivas necesarias para evitar que se repita la no conformidad.

De acuerdo a la correspondencia y vínculos técnicos entre las normas NTCGP1000 y NTC-IS09001 y las normas NTC-IS09001 y NTC-IS027001 se utiliza el procedimiento de elaboración y seguimiento de planes de mejoramiento del Proceso Evaluación, Control y Mejoramiento.

8.2.5. Procedimiento de acción preventiva

El objetivo de este procedimiento es definir los lineamientos para identificar, registrar, controlar, desarrollar, implantar y dar seguimiento a las acciones preventivas generadas por la detección de una no conformidad real o potencial en el sistema de gestión de seguridad de la información y eliminar sus causas.

De acuerdo a la correspondencia y vínculos técnicos entre las normas NTCGP1000 y NTC-IS09001 y las normas NTC-IS09001 y NTC-IS027001 se utiliza el procedimiento de elaboración y seguimiento de planes de mejoramiento del Proceso Evaluación, Control y Mejoramiento.

8.2.6. Procedimiento de revisión del Manual de la Política de Seguridad

El objetivo de este procedimiento es el de revisar, por parte de la dirección o su representante, el Manual de la Política para la Tecnología de Información y Comunicaciones - Tics de la Corporación Autónoma Regional de La Guajira - CORPOGUAJIRA en intervalos planificados, para asegurar su conveniencia, eficiencia y eficacia continua.

De acuerdo a la correspondencia y vínculos técnicos entre las normas NTCGP1000 y NTC-IS09001 y las normas NTC-IS09001 y NTC-IS027001 se utilizan los requisitos: 5.6. Responsabilidad y Autoridad- se debe realizar e implementar este procedimiento.

8.3. Gestión de los Incidentes de la Seguridad de la Información

Asegurar que los eventos e incidentes de seguridad que se presenten con los activos de información, sean comunicados y atendidos oportunamente, empleando los procedimientos definidos, con el fin de que se tomen oportunamente las acciones correctivas.

8.4. Proceso Disciplinario

Dentro de la estrategia de seguridad de la información de CORPOGUAJIRA, está establecido un proceso disciplinario formal para los funcionarios que hayan cometido alguna violación de la Política de Seguridad de la Información. El proceso disciplinario también se debería utilizar como disuasión para evitar que los funcionarios, contratistas y otros colaboradores de CORPOGUAJIRA violen las políticas y los procedimientos de seguridad de la información, así como para cualquier otra violación de la seguridad. Las investigaciones disciplinarias corresponden a actividades pertenecientes al Proceso de Talento Humano.

8.4.1 Violación de la seguridad de la información

Las siguientes actuaciones conllevan a la violación de la seguridad de la información establecidas por CORPOGUAJIRA.

- No firmar los acuerdos de confidencialidad o de entrega de información o de activos de información.
- Ingresar a equipos y carpetas de otros procesos, unidades, grupos o áreas, sin autorización, vulnerando contraseñas y no reportarlo a Gestión de las TICS.
- No reportar a Gestión de las TICS los incidentes de seguridad o las violaciones a las políticas de seguridad, cuando se tenga conocimiento de ello.

- Dejar información pública reservada, en carpetas compartidas o en lugares distintos al computador asignado, obviando las medidas de seguridad.
- Dejar los computadores encendidos en horas no laborables sin que se este realizando un proceso que así lo amerite.
- Almacenar en los discos duros de los computadores personales de los usuarios, la información reservada de la corporación.
- Solicitar cambio de contraseña de otro usuario, sin la debida autorización del titular o su jefe inmediato.
- Hacer uso de la red de datos de la institución, para obtener, mantener o difundir en los equipos de sistemas, material pornográfico u ofensivo, cadenas de correos y correos masivos no autorizados.
- Utilización de software no relacionados con la actividad laboral y que pueda degradar el desempeño de la plataforma tecnológica institucional.
- Enviar información pública reservada o información pública clasificada (privada o semiprivada) por correo, copia impresa o electrónica sin la debida autorización y sin la utilización de los protocolos establecidos para la divulgación.
- Negligencia en el cuidado de los equipos, dispositivos portátiles o móviles entregados para actividades propias de CORPOGUAJIRA.
- No cumplir con las actividades designadas para la protección de los activos de información del CORPOGUAJIRA.
- Descuidar documentación con información pública reservada o clasificada de la institución, sin las medidas apropiadas de seguridad que garanticen su protección.
- Archivar información pública reservada o clasificada, sin claves de seguridad o cifrado de datos.
- El que sin autorización, acceda en todo o parte del sistema informático de la corporación o se mantenga dentro del mismo en contra de la voluntad del CORPOGUAJIRA.
- El que impida u obstaculice el funcionamiento o el acceso normal al sistema informático de la corporación, a los datos informáticos o las redes de telecomunicaciones de CORPOGUAJIRA, sin estar autorizado.
- El que destruya, dañe, borre, deteriore o suprima datos informáticos o un sistema de tratamiento de información de CORPOGUAJIRA.
- El que de manera consciente, distribuya, envíe, introduzca software malicioso u otros programas de computación de efectos dañinos en la plataforma tecnológica de CORPOGUAJIRA.
- El que viole datos personales de las bases de datos de CORPOGUAJIRA.
- El que superando las medidas de seguridad informática, suplante un usuario ante los sistemas de autenticación y autorización establecidos por CORPOGUAJIRA.
- No mantener la confidencialidad de las contraseñas de acceso a la red de datos, los recursos tecnológicos o los sistemas de información de CORPOGUAJIRA o permitir que otras personas accedan con el usuario y clave del titular a éstos.

- Llevar a cabo actividades fraudulentas o ilegales, o intentar acceso no autorizado a cualquier computador de CORPOGUAJIRA o de terceros.
- Ejecutar acciones tendientes a eludir o variar los controles establecidos por CORPOGUAJIRA.
- Retirar de las instalaciones de la institución, estaciones de trabajo o computadores portátiles que contengan información institucional sin la autorización pertinente.
- Sustraer de las instalaciones de CORPOGUAJIRA, documentos con información institucional calificada como información pública reservada o clasificada, o abandonarlos en lugares públicos o de fácil acceso.
- Entregar, enseñar y divulgar información institucional, calificada como información pública reservada y clasificada a personas o entidades no autorizadas.
- Ejecución de cualquier acción que pretenda difamar, abusar, afectar la reputación o presentar una mala imagen de CORPOGUAJIRA o de alguno de sus funcionarios.
- Acceder, almacenar o distribuir pornografía infantil.
- Instalar programas o software no autorizados en las estaciones de trabajo o equipos portátiles institucionales, cuyo uso no esté autorizado por el proceso Gestión de las TICS de la Corporación.
- Copiar sin autorización los programas de CORPOGUAJIRA o violar los derechos de autor o acuerdos de licenciamiento.

8.5. Gestión de la Continuidad del Negocio

Es el conjunto de procedimientos y estrategias definidos para contrarrestar las interrupciones en las actividades misionales de la corporación, 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.

1. Buscan prevenir interrupciones en las actividades de la plataforma informática de CORPOGUAJIRA que van en detrimento de los procesos críticos de TI afectados por situaciones no previstas o desastres.
2. Se debe desarrollar e implantar un Plan de Contingencia para los Sistemas de Información para asegurar que los procesos misionales de CORPOGUAJIRA puedan ser restaurados dentro de escalas de tiempo razonables.
3. La corporación deberá tener definido un plan de acción que permita mantener la continuidad del negocio teniendo en cuenta los siguientes aspectos:
    - Identificación y asignación de prioridades a los procesos críticos de TI de CORPOGUAJIRA de acuerdo con su impacto en el cumplimiento de la misión de la corporación.
    - Documentación de la estrategia de continuidad del negocio.

- Documentación del plan de recuperación de las operaciones de acuerdo con la estrategia definida anteriormente.
- Plan de pruebas de la estrategia de continuidad del negocio.

4. La continuidad del negocio deberá ser gestionada por la Secretaria General de CORPOGUAJIRA.
5. La alta dirección de CORPOGUAJIRA será la responsable de velar por la implantación de las medidas relativas a ésta. Igualmente, es responsable de desarrollar las tareas necesarias para el mantenimiento de estas medidas.
6. La alta dirección de la Corporación, se encargará de la definición y actualización de las normas, políticas, procedimientos y estándares relacionados con la continuidad del negocio, igualmente velará por la implantación y cumplimiento de las mismas.

8.6. Cumplimiento

1. Los diferentes aspectos contemplados en este Manual son de obligatorio cumplimiento para todos los funcionarios, contratistas y otros colaboradores de CORPOGUAJIRA. En caso de que se violen las políticas de seguridad ya sea de forma intencional o por negligencia, la Corporación tomará las acciones disciplinarias y legales correspondientes.
2. El Manual de la Política de Seguridad para las Tecnologías de la Información y las Comunicaciones - TICs debe prevenir el incumplimiento de las leyes, estatutos, regulaciones u obligaciones contractuales que se relacionen con los controles de seguridad.

8.7. Controles

El Manual de la Política de Seguridad para las Tecnologías de la Información y las Comunicaciones de CORPOGUAJIRA esta soportado en un conjunto de procedimientos que se encuentran documentados en archivos complementarios a este manual. Los usuarios de los servicios y recursos de tecnología de la Corporación pueden consultar los procedimientos del Sistema de Gestión de Calidad de la corporación.

8.8. Declaración de aplicabilidad

La Declaración de Aplicabilidad (Statement of Applicability - SOA) referenciado en la cláusula 4.2.1j del estándar ISO 27001 es un documento que lista los objetivos y controles que se van a implementar en la Corporación, así como las justificaciones de aquellos controles que no van a ser implementados.

Para el caso específico de CORPOGUAJIRA, este tipo de análisis se hace evaluando el cumplimiento de la norma ISO 27002, para cada uno de los controles establecidos en los 11 dominios o temas relacionados con la gestión de la seguridad

de la información que este estándar específica, y una vez se complete este análisis ya se puede realizar la Declaración de aplicabilidad.

7. MARCO LEGAL

• Constitución Política de Colombia 1991.
• Código Penal Colombiano - Decreto 599 de 2000
• Ley 906 de 2004, Código de Procedimiento Penal.
• Ley 87 de 1993, por la cual se dictan Normas para el ejercicio de control interno en las entidades y organismos del Estado, y demás normas que la modifiquen.
• Decreto 1599 de 2005, por el cual se adopta el Modelo Estándar de Control Interno MECI para el Estado Colombiano.
• Ley 734 de 2002, del Congreso de la República de Colombia, Código Disciplinario Único.
• Ley 23 de 1982 de Propiedad Intelectual - Derechos de Autor.
• Ley 594 de 2000 - Ley General de Archivos.
• Ley 80 de 1993, Ley 1150 de 2007 y decretos reglamentarios.
• Ley 527 de 1999, por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.
• Directiva presidencial 02 del año 2000, Presidencia de la República de Colombia, Gobierno en línea.
• Ley 1032 de 2006, por el cual se dictan disposiciones generales del Habeas
• Data y se regula el manejo de la información contenida en base de datos personales.
• Ley 1266 de 2007, por la cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.
• Ley 1273 de 2009, "Delitos Informáticos" protección de la información y los datos.
• Ley 1437 de 2011, "Código de procedimiento administrativo y de lo contencioso administrativo".
• Ley 1581 de 2012, "Protección de Datos personales".
• Decreto 2609 de 2012, por la cual se reglamenta la ley 594 de 200 y ley 1437 de 2011
• Decreto 1377 de 2013, por la cual se reglamenta la ley 1581 de 2012
• Ley 1712 de 2014, “De transparencia y del derecho de acceso a la información pública nacional”

8. REQUISITOS TÉCNICOS

- Norma Técnica Colombiana NTCIISO 27001 Sistemas de gestión de la seguridad de la información
- Norma Técnica Colombiana NTC/ISO 17799 Código de práctica para la gestión de la seguridad de la información.

- ISO/IEC 27005 Information technology Systems- Security techniques- information security risk management.
- Modelo Estándar de Control Interno MECI 1000 2da versión "Subsistema: Control de Gestión; Componente: Actividades de Control; Elemento: Monitoreo y Revisión e Información".
- Norma Técnica Colombiana NTC - ISO 19011 "Directrices para la Auditoria de los Sistemas de Gestión de la Calidad y/o Ambiental"

9. RESPONSABLE DEL DOCUMENTO

Profesional Especializado 2028 Grado 13 de la Oficina Asesora de planeación responsable del Proceso Gestión de las TICS