TABLA DE CONTENIDO

INTRODUCCIÓN

Conscientes de que la seguridad informática se fundamenta en la existencia y aplicación de un conjunto de lineamientos que brindan orientaciones claras relativas a la seguridad y privacidad de la información, el Consejo Profesional Nacional de Ingeniería (COPNIA) presenta el manual de seguridad de la información, como parte del compromiso de la entidad con los pilares fundamentales de confidencialidad, integridad y disponibilidad de la información.

El presente manual de seguridad de la información desarrolla las políticas y lineamientos que integran el Sistema de Gestión de Seguridad de la Información (SGSI), orientando el cumplimiento de la normatividad legal Colombiana vigente y a las buenas prácticas de seguridad de la información, basadas en el modelo de seguridad y privacidad de la información de la estrategia Gobierno en Línea (GEL) del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, las cuales deben ser adoptadas por los funcionarios, contratistas, visitantes y terceros que presten sus servicios o tengan algún tipo de relación con el COPNIA.

Cada uno de los numerales presentes en el documento son aplicables a todos los procesos de la entidad, a la implementación de proyectos, intercambio de información con terceros, gestión de la información y a la operación diaria de las actividades propias del COPNIA.

1. OBJETO Y ALCANCE

1.1 OBJETO

Establecer los lineamientos que regulan la seguridad de la información en el Consejo Profesional Nacional de Ingeniería – Copnia, con el fin de que sean conocidos y acatados por los funcionarios, contratistas, proveedores y demás terceros, que desarrollen actividades, presten algún servicio o tengan algún tipo de relación con la entidad, con el propósito de mitigar el riesgo de pérdida, acceso, uso, divulgación, interrupción o destrucción no autorizada de información.

Nota: Para el desarrollo del Manual de Seguridad de la Información, se utilizó como referencia la Guía no.2 "Elaboración de la política general de seguridad de la información y privacidad de la información", Versión inicial 1.0.0 de 11 de mayo de 2016.

1.2 ALCANCE

El Manual de Seguridad de la Información contiene los lineamientos generales para la implementación de un modelo de gestión de seguridad y privacidad de la información, a través de la identificación de responsabilidades y disposiciones generales en torno a la gestión de activos, el control de accesos, el no repudio, la privacidad y confidencialidad, la integridad, la disponibilidad del servicio y la información, el registro y la auditoría, la gestión de incidentes y las acciones de capacitación y sensibilización.
El Manual de Seguridad de la Información es aplicable a todos los procesos, así como a todos los aspectos administrativos, contractuales y de control que deben ser cumplidos por los funcionarios, supernumerarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con el Consejo Profesional Nacional de Ingeniería – Copnia.
La inobservancia de las disposiciones de este documento podrá dar lugar según corresponda, a la iniciación de las investigaciones y aplicación de las sanciones, de conformidad con las disposiciones legales vigentes.

2. MARCO INSTITUCIONAL

2.1 NATURALEZA DEL COPNIA

El Consejo Profesional Nacional de Ingeniería – COPNIA, creado mediante la Ley 94 de 1937, es la **entidad pública que tiene la función de inspeccionar y vigilar el ejercicio de la ingeniería, de sus profesiones afines y de sus profesiones auxiliares en general, en el territorio nacional**; de acuerdo con lo dispuesto en el Artículo 26 de la Constitución Política y en la Ley 842 de 2003 y demás normas complementarias y suplementarias, autorizando a nombre del Estado el ejercicio de una profesión que implica riesgo social, o suspendiendo el ejercicio profesional, previo la aplicación del debido proceso, a quienes se les compruebe la violación del Código de Ética o del correcto ejercicio de la profesión autorizada; esto último en su calidad de Tribunal de Ética de las profesiones tuteladas, por quejas interpuestas por la ciudadanía.

En razón de lo anterior, el COPNIA desarrolla su función mediante la expedición de cuatro herramientas legales a saber: **Matrícula Profesional**, para los ingenieros; **Certificado de Inscripción Profesional**, para profesionales afines y profesionales auxiliares; **Certificado de Matrícula,** para maestros de obra y **Permisos Temporales,** para profesionales graduados y domiciliados en el exterior que pretendan ejercer temporalmente en Colombia, de acuerdo con lo dispuesto en el artículo 23 de la Ley 842 de 2003.

Cuenta con una sede central de carácter nacional en la ciudad de Bogotá, D.C. y con 17 Consejos Seccionales que actúan como primera instancia en sendos Departamentos, en los que existen Facultades de Ingeniería o Instituciones de Educación Superior que otorgan títulos de ingeniero, de profesional afín o de profesional auxiliar, respectivamente, de las profesiones controladas por el COPNIA en virtud de lo dispuesto en la Ley 842 de 2003.

Al COPNIA lo conforman actualmente: la Junta Nacional de Consejeros (Art.26 de la Ley 435 de 1998 y Art.3 de la Ley 1325 de 2009), y 17 Juntas de Consejos Seccionales en cada uno de los Departamentos del país en los que existen Facultadas de Ingeniería, integradas según lo dispuesto en el artículo 28 de la Ley 842 de 2003.

La expedición de la Ley 1325 de 2009, le otorgó nuevamente al COPNIA, la competencia para controlar e inspeccionar el ejercicio de las ingenierías: Agrícola, Forestal, Agronómica y Pesquera, así como de la Agronomía y de la Agrología, de sus profesiones Afines y de sus profesiones Auxiliares, ampliando a la vez la conformación de la Junta Nacional de Consejeros, con el Ministro de Agricultura o su delegado y el Presidente de uno de los gremios involucrados, elegido en Junta convocada por el COPNIA, para tal fin.

2.2 MISIÓN

Somos la autoridad pública encargada de proteger a la sociedad del inadecuado ejercicio profesional de los ingenieros, profesionales afines y auxiliares, mediante la autorización, inspección, control y vigilancia que se concreta, de acuerdo con las competencias otorgadas por la ley, con la inscripción del Registro Profesional y con la función de Tribunal de Ética Profesional.

1. TÉRMINOS Y DEFINICIONES

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

- **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.

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

- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC27000).

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

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

- **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 2005, segunda publicación en 2013.

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

- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)

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

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

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

- **Seguridad de la información:** Son todos los controles técnicos y metodológicos que permiten mitigar los riesgos a los que se expone la información en general.

- **SGSI:** Sistema de Gestión de Seguridad de la Información. Es el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.

- **TIC:** El término tecnologías de información y comunicación (TIC).

2. NORMATIVIDAD

- Constitución Política de Colombia 1991. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data.

- Constitución Política de Colombia 1991. Artículo 20. Libertad de Información.

- Código Penal Colombiano - Decreto 599 de 2000

- Ley 679 de 2001- Por medio de la cual se expide un estatuto para prevenir y contrarrestar la explotación, la pornografía y el turismo sexual con menores, en desarrollo del artículo 44 de la Constitución

- 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.

- 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 la 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".

- Ley 962 de 2005. "Simplificación y Racionalización de Trámite. Atributos de seguridad en la Información electrónica de entidades públicas;"

- Ley 1150 de 2007. "Seguridad de la información electrónica en contratación en línea"

- Ley 1341 de 2009. "Tecnologías de la Información y aplicación de seguridad".

- Decreto 2952 de 2010. "Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008".

- Decreto 886 de 2014. "Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012".

- Decreto 1083 de 2015. "Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012".

- CONPES 3701 de 2011 Lineamientos de Política para Ciberseguridad y Ciberdefensa.

- CONPES 3854 de 2016 Política Nacional de Seguridad digital.

3. LINEAMIENTO PARA LA IMPLEMENTACIÓN DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

3.1 Organización para la seguridad de la información[1]

Los lineamientos relativos a la organización de la seguridad de la información, tales como conformación y objetivos de comités, funciones y responsabilidad, se encuentran definidos en la normativa asociada al Modelo Integrado de Planeación y Gestión del Copnia.
Los Líderes de Área o Líderes funcionales son responsables de establecer los roles, funciones y responsabilidades de operación y administración de los sistemas de información del Copnia, conforme a las funciones asignadas al área de desempeño. Los roles, funciones y responsabilidades, deberán estar debidamente documentados y distribuidos, conforme a lineamientos establecidos para el control documental de la entidad.

3.2 Gestión de Activos[2]

A continuación, se relacionan las directrices que orientan a los funcionarios los límites y procedimientos frente a la identificación, uso, administración y responsabilidad frente a los activos de información.

3.2.1 Identificación de activos

El Copnia es el dueño de la propiedad intelectual de los avances tecnológicos e intelectuales desarrollados por los funcionarios del Copnia y los contratistas, derivadas del objeto del cumplimiento de funciones y/o tareas asignadas, como las necesarias para el cumplimiento del objeto del contrato.

El Copnia es propietario de los activos de información y los administradores de estos activos son los funcionarios, contratistas o demás colaboradores del Copnia (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 y sistemas de información (TIC).

Es responsabilidad del área de Tecnologías de la Información y de las Comunicaciones nombrar los activos de cómputo del Copnia nomenclatura: CO más número de identificación único (placa de inventario), que permita administración de su ubicación y asignación final a los usuarios responsables. Ejemplo: CO160300036. Para realizar la actividad, es necesario que el activo de cómputo cuente con placa de inventario asignado por el área Administrativa.

En concordancia con los criterios de administración documental del Copnia, directrices para la creación y diseño de documentos, sistema de gestión de documentos electrónicos de archivo – SGDEA, mecanismos de autenticación y mecanismos de asignación de metadatos enfocados en el marco de la planeación que debe generar la entidad, los lineamientos de creación y actualización del registro de activos de información, se rige por las definiciones del Programa de Gestión Documental de la Entidad, cuyo desarrollo e implementación es responsabilidad del Área Administrativa de la Subdirección Administrativa y Financiera.

---

[1] Esta política tiene como finalidad establecer el comité directivo de la seguridad de la información.

[2] Este grupo de políticas deben hacer referencia a todas aquellas directrices mediante las cuales se indica a los funcionarios los límites y procedimientos frente a la identificación, uso, administración y responsabilidad frente a los activos de Información

Los usuarios y custodios de los activos de información del Copnia son responsables por el uso apropiado, la protección y privacidad de dichos activos.
Teniendo en cuenta que los activos de información son el conjunto de datos que la entidad genera, obtiene, adquiere, transforma o controla, se encuentra prohibido hacer uso de los recursos tecnológicos del Copnia para almacenar información que no corresponda a los procesos definidos para dar cumplimiento a la misionalidad institucional y por tanto es excluida de cualquier responsabilidad de la entidad.
Toda información que no sea de propósito estrictamente laboral conforme a las funciones del Copnia y que sea guardada en la infraestructura tecnológica de la entidad, estará supeditada a su inmediata eliminación, sin previo aviso a sus propietarios.

3.2.2 Clasificación y etiquetado de activos de información

La Entidad debe determinar la clasificación de los activos de información de acuerdo con la criticidad, sensibilidad y reserva de esta. Es responsabilidad del área Administrativa, conforme a lineamientos de gestión documental, liderar y definir las actividades tendientes a identificar y controlar los activos de información de acuerdo con su nivel de confidencialidad y reserva.

3.2.3 Devolución de activos

La devolución de activos fijos se encuentra enmarcada en el Procedimiento de manejo de bienes AB-pr-02. En el momento del retiro de la Entidad, el funcionario se pondrá en contacto con el encargado del área Administrativa, a fin de legalizar la entrega de los bienes que estaban a su cargo. Verificada la información por el encargado de almacén y la conformidad con el inventario, se entrega al funcionario su "Paz y salvo de inventarios".
Todos los funcionario, contratistas y terceros tienen la responsabilidad de devolver los activos de información que se encuentren a su cargo al terminar su empleo, contrato o vínculo con la Entidad.
Es responsabilidad de la Subdirección Administrativa y Financiera, a través de las áreas de Talento Humano y Administrativa, definir los procedimientos, formatos y paz y salvos, necesarios para la entrega de activos de información.
Es responsabilidad de los jefes de dependencias y líderes de áreas verificar el cumplimiento de procedimientos y actividades para la entrega y custodia de activos de información, conforme a los equipos de trabajo asignados a cada uno de ellos.

3.2.4 Gestión de medios removibles

Para facilitar el acceso a la información, el Copnia pone a disposición de sus funcionarios y contratistas autorizados, herramientas tecnológicas de trabajo colaborativo y en la nube, razón por la cual el uso de medios removibles de almacenamiento (cintas, discos duros removibles, CDs, DVDs y unidades de almacenamiento USB, entre otras) se encuentra restringido y regulado por los lineamientos de respaldo de activos de información y tablas de retención documental, emitidos por la Subdirección Administrativa y Financiera.
La responsabilidad de la información contenida en los medios removibles es del funcionario que está a cargo del activo, por lo tanto, la información que es almacenada en medios removibles y que debe estar disponible, debe ser protegida para evitar que ésta se vea afectada por el tiempo de vida útil del medio.

3.2.5 Disposición de los activos

Es responsabilidad del área de Tecnologías de la Información y de las Comunicaciones, planificar y dar a conocer las necesidades de recursos necesarios para generación y control de copias de respaldo y almacenamiento de sus activos de información contenidos en los sistemas de información y las bases de datos de la entidad.

Los puntos y tiempos óptimos de restauración son acordados contractualmente con los proveedores en 24 horas. Es responsabilidad de los supervisores de contrato verificar periódicamente el cumplimiento de esta condición.

La entidad pone a disposición de los funcionarios y contratistas, herramientas tecnológicas para el almacenamiento de la información. De acuerdo con lo anterior, todos los activos de información que se generen en herramientas ofimáticas deberán ser guardados en la carpeta de One Drive configurada en cada uno de los equipos asignados. Es responsabilidad de los funcionarios y contratistas realizar el respectivo backup en esta herramienta y cumplir los parámetros generales de uso descritos con anterioridad (abstenerse de guardar información ajena a la misionalidad institucional), conforme a instrucciones operativas impartidas por el área de Tecnologías de la Información y de las Comunicaciones.

3.2.6 Dispositivos móviles y portátiles

No está permitido a los funcionarios del área de Tecnologías de la Información y de las Comunicaciones reparar, desinstalar o instalar software, formatear, dar soporte preventivo o correctivo a equipos personales o que no hagan parte de los activos fijos del Copnia.

Es responsabilidad del área de Talento Humano informar la desvinculación o culminación de relación laboral de funcionarios, supernumerarios o planta temporal al área de Tecnologías de la Información y las Comunicaciones. Una vez recibida la comunicación, es responsabilidad del Área de Tecnologías de la Información y las Comunicaciones retirar todos los accesos a que haya lugar, incluidos dispositivos móviles.

Es responsabilidad de los supervisores informar la desvinculación o culminación de relación laboral de contratistas al área de Tecnologías de la Información y las Comunicaciones. Una vez recibida la comunicación, es responsabilidad del Área de Tecnologías de la Información y las Comunicaciones retirar todos los accesos a que haya lugar, incluidos dispositivos móviles.

En caso de requerir el retiro del dispositivo móvil es necesario informar al área Administrativa conforme a los procedimientos definidos para tal fin. De presentarse el extravió o hurto de un dispositivo móvil que contengan información de la entidad, el funcionario será el responsable de reportar de forma inmediata a la Subdirección Administrativa y Financiera y al área de Tecnologías de la Información y las Comunicaciones, quienes identificarán conforme la información contenida, las medidas de seguridad adecuadas para la protección de la información.

Los dispositivos móviles que manejen o administren información confidencial o crítica de la entidad, no se podrán conectar a una red pública, y deberán ser transportados y usados con extremos cuidados para evitar el daño o manipulación no autorizada de la información, así mismo, será necesario evitar dejar el equipo desatendido o debe ser asegurado con su respectiva guaya.

Se encuentra prohibido realizar instalaciones de aplicaciones que puedan afectar la confidencialidad, integridad y/o disponibilidad de la información almacenada o transmitida por el dispositivo. En todo caso las instalaciones realizadas en dispositivos móviles deberán realizarse por el área de Tecnologías de la Información y de las Comunicaciones, o con su consentimiento o bajo su supervisión.

Para los dispositivos móviles aplican todos los lineamientos emitidos en el presente manual.

3.2.7 Internet

El área de Tecnologías de la Información y de las Comunicaciones es responsable de la generación e implementación de lineamientos que permitan la navegación segura y el uso adecuado de este servicio por parte de los usuarios finales, evitando errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones WEB.

El servicio de internet del Copnia se encuentra disponible para la ejecución de las labores propias de la función de la entidad; de acuerdo con lo anterior, todos los ingresos establecidos a través de internet pueden ser controlados, monitoreados y reportados por el área de Tecnologías de la Información y de las Comunicaciones, sin previa autorización de los funcionarios o contratistas que tengan el respectivo acceso.

El área de Tecnologías de la Información y de las Comunicaciones se reservan el derecho de filtrar los contenidos que se reciban o envíen desde la red de internet del Copnia.

Los usuarios del servicio de internet son responsables de evitar prácticas o usos que comprometan la seguridad de la información de la entidad, tales como descargas de software no autorizado.

Los usuarios del servicio de internet del Copnia son responsables tanto del contenido de las comunicaciones como de cualquier otra información que se envíe desde la red de la entidad.
Se encuentra estrictamente prohibido hacer uso de los servicios tecnológicos del Copnia para el acceso a páginas relacionadas con pornografía, actividades criminales, terrorismo, crímenes computacionales, y en general todos aquellas páginas y aplicaciones que pongan en riesgo la seguridad y reputación de la entidad.

3.2.8 Correo electrónico, comunicaciones de texto, voz y video

El uso del servicio de correo electrónico está disponible para ingreso desde cualquier sitio con conexión a internet, por esta razón se debe ingresar a este servicio solo desde lugares con acceso a internet conocidos, no se recomienda ingresar a este servicio desde redes públicas.
No se deben usar las cuentas de correo empresariales para envío de correos masivos externos, toda vez que este proceso puede generar el ingreso del dominio copnia.gov.co en listas negras de Spam. De ser necesario enviar correos masivos diarios a usuarios externos que supere más de 1000 cuentas es necesario comunicarse con el área de Tecnologías de la Información y de las Comunicaciones.
Está prohibido el uso del correo electrónico o de Skype (comunicación de texto, voz o video) para el envío, reenvío o intercambio de mensajes no deseados o considerados SPAM (mensajes no solicitados, no deseados o con remitente no conocido), cadenas de mensajes o publicidad.
Se prohíbe el uso de los medios electrónicos de comunicación del Copnia para el envio o intercambio de mensajes con contenido que atente contra la integridad de las personas o instituciones, tales como: ofensivo, obsceno, pornográfico, chistes, información terrorista, cadenas de cualquier tipo, racista, o cualquier contenido que represente riesgo de virus.

En caso de recibir una comunicación o correo electrónico sospechoso deberá reportarse de inmediato, sin abrirlo, al correo electrónico de soporte del Copnia o a la mesa de ayuda.

El servicio de correo electrónico sólo estará vigente mientras los funcionarios o contratistas tengan relación laboral o contractual con el Copnia; una vez termine dicha relación, el área de Tecnologías de la Información y de las Comunicaciones eliminará los accesos conforme a comunicación del área de Gestión Humana o de los supervisores de contrato.

Se prohíbe hacer uso de los medios electrónicos del Copnia para el envío de mensajes en donde se divulgue, comente o exprese hechos, opiniones o asuntos internos del Copnia que puedan afectar la reputación, seguridad e imagen de la entidad.

Se prohíbe a los funcionarios suscribirse con su correo corporativo a listas de correo electrónico, mercadeo, entidades bancarias o grupos de noticias que divulguen información o mensajes ajenos a las funciones y deberes de la entidad.

Los funcionarios y contratistas a quienes se les haya asignado cuentas a medios electrónicos de comunicación de la entidad serán responsables ante la Copnia de todos los accesos y actividades que se puedan haber realizado con su usuario y contraseña.

La aplicación Skype debe ser utilizada exclusivamente para asuntos laborales, ya que está diseñada para facilitar la comunicación entre usuarios del Copnia. El uso de video conferencias implica ocupación del ancho de banda de la red y por esta razón se debe utilizar solo para aplicación en asuntos laborales.

3.2.9 Redes Sociales

La información que se publique o divulgue por cualquier medio de Internet, de cualquier funcionario, contratista o colaborador del Copnia, que sea creado a nombre personal en redes sociales como: twitter®, facebook®, youtube® likedink®, blogs, instagram, etc, se considera fuera del alcance del Sistema de Gestión de Seguridad de la Información – SGSI del Copnia, 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.

El área de Comunicaciones del Copnia es responsable de la creación y administración de redes sociales institucionales y su uso está restringido a la difusión de actividades relacionadas con la ejecución estratégica, misional, de apoyo y de evaluación de la entidad. Los contenidos que se desarrollan se encuentran bajo la supervisión y control de dicha dependencia.

Los funcionarios y contratistas del Copnia, no deben crear cuentas, abrir grupos, o publicar cualquier tipo de información escrita o audiovisual a nombre de la entidad.

3.2.10 Recursos tecnológicos

Todos los equipos de cómputo del Copnia deben estar enrolados con un usuario estándar de Windows en el dominio del Copnia, ningún equipo de propiedad del Copnia debe estar por fuera del dominio, no se permite usuarios de Windows como administradores locales o de dominio, los usuarios administradores solo están configurados para soporte de los equipos y administración de estos.

La infraestructura tecnológica del Copnia tal como, servidores, equipos activos, PBX y otro tipo de hardware de computador que no resida típicamente en escritorios de usuario o en un área de trabajo común, deben estar ubicados físicamente en un área segura, y se deben implementar los controles necesarios para la prevención contra riesgos ambientales y no ambientales, que puedan afectar la disponibilidad de los datos.

Es responsabilidad de los funcionarios del Copnia, hacer uso de los puntos de energía protegidos dispuestos por la entidad, para evitar daños en el hardware de computador.

El área de Tecnologías de la información y de las Comunicaciones debe garantizar que el cableado de telecomunicaciones que transporta los datos o soporta los servicios de información de la entidad se encuentren adecuadamente protegidos para evitar daño o mala manipulación.

La instalación de cualquier tipo de software en los equipos de cómputo del Copnia, es responsabilidad del área de Tecnologías de la Información y de las Comunicaciones y por tanto son los únicos autorizados para realizar o autorizar esta labor.

Es responsabilidad del área Administrativa presupuestar y programar los mantenimientos preventivos y correctivos para los equipos, de acuerdo con las especificaciones e intervalos de servicio recomendados por los fabricantes. El área de Tecnologías de la Información y de las Comunicaciones deberá mantener los registros de las fallas reportadas por los usuarios.

Se deben asegurar los equipos fuera de las instalaciones de la organización y su salida debe estar autorizada por el responsable del área a la cual esté asignada la máquina e informada al área Administrativa, conforme a procedimientos establecidos para tal fin.

Toda la información del Copnia tendrá que ser removida del equipo antes de su disposición o reutilización.

Antes de cualquier venta o donación, todos los medios de almacenamiento deben ser borrados de acuerdo con los mecanismos de eliminación de información que adopte la entidad.

Los usuarios no deben realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla definido por la Entidad. Estos cambios pueden ser realizados únicamente por el área de Tecnologías de la Información y de las Comunicaciones; para ello se debe disponer de un estándar de seguridad para estaciones de trabajo independientemente del sistema operativo.

El área de Tecnologías de la Información y de las Comunicaciones define e informa la lista actualizada de software y aplicaciones autorizadas que se encuentran permitidas para ser instaladas en las estaciones de trabajo de los usuarios; así mismo, realiza el control y verificación de cumplimiento del licenciamiento del respectivo software y aplicaciones asociadas.

El área de Tecnologías de la Información y de las Comunicaciones no prestará servicio de soporte técnico (revisión, mantenimiento, reparación, configuración y manejo e información) a equipos que no sean del Copnia

3.2.11 Escritorio y pantalla despejada

Los funcionarios, contratistas, personas en comisión, pasantes y terceros que tienen algún vínculo con el Copnia deben conservar su escritorio libre de información, propia de la entidad, que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.

Los usuarios de los sistemas de información y comunicaciones del Copnia deben 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.

Por política de seguridad de información en el dominio Copnia, se bloqueará automáticamente la pantalla después de 15 minutos de inactividad de la misma.

Los usuarios de los sistemas de información y comunicaciones del Copnia deben cerrar las aplicaciones y servicios de red cuando ya no los necesite.

Al imprimir documentos con información pública reservada y/o pública clasificada (semiprivada o privada), deben ser retirados de la impresora inmediatamente y no se deben dejar en el escritorio sin custodia.

No se debe utilizar fotocopiadoras, escáneres, periféricos, cámaras digitales y en general equipos tecnológicos que se encuentren desatendidos, es decir, equipos que no se encuentren administrados por el dominio Copnia.

3.2.12 Gestión de Hardware

Cualquier cambio que se requiera realizar en los equipos de cómputo de la entidad (cambios de procesador, monitor, teclado, mouse, adición de memoria o tarjetas) debe tener previamente una evaluación y autorización técnica del área de Tecnologías de la Información y de las Comunicaciones.

La reparación técnica de los equipos, que implique la apertura de estos, únicamente puede ser realizada por personal capacitado, previa autorización del supervisor del contrato de mantenimiento y del responsable del manejo de bienes.

Los equipos de cómputo (PC, servidores, comunicaciones, etc.) no deben moverse o reubicarse sin previa autorización de los responsables del manejo de bienes.

Todo funcionario está obligado a solicitar por escrito al responsable de manejo de bienes, cualquier movimiento o modificación que se lleve a cabo con los equipos.

El funcionario designado para supervisar los contratos de mantenimiento será el encargado de diseñar y ejecutar planes de mantenimiento preventivo a los equipos del Copnia.

3.2.13 Gestión de Software

Los líderes funcionales del Copnia son quienes determinan e informan al Área de Tecnologías de la Información y las Comunicaciones los permisos que cada uno de los funcionarios deben tener sobre las aplicaciones Copnia.

Los líderes funcionales son los únicos que pueden avalar cambios sobre los aplicativos, como actualizaciones, modificaciones, desarrollos, respaldos o dar de baja algún sistema de información.

Los líderes funcionales podrán requerir en cualquier momento al área de tecnología una matriz de roles y perfiles con los usuarios activos a la fecha, para que se determine si se requiere hacer algún cambio que debe ser oficializado según el procedimiento TIC-pr-01.

Cada funcionario es responsable del buen uso de su usuaria dentro de los aplicativos del Copnia, teniendo en cuenta que son ambientes productivos, por lo tanto, no debe ingresar información invalida, incorrecta, ficticia o de prueba.

Está prohibido realizar actualizaciones, modificaciones, inserciones o eliminaciones directamente en las bases de datos del Copnia, omitiendo la capa de aplicación y los registros de auditoria propios de los sistemas de información.
La administración de las bases de datos del Copnia es realizada únicamente por el Área de Tecnologías de la Información y las Comunicaciones, quienes en ninguna circunstancia pueden alterar la información allí contenida. Se podrán realizar actividades de soportes sobre la base de datos en caso de algún error de las aplicaciones o de alguna imposibilidad técnica, que debe estar reportado y documentado según el procedimiento TIC-pr-01.

No se pueden generar copias de las bases de datos sin una autorización escrita del profesional del Área de Tecnologías de la Información y las Comunicaciones, ni se deben entregar copias o accesos a terceros o proveedores sin la misma autorización.

Los cambios de software se realizarán siempre en un ambiente de pruebas dispuesto por la entidad; estos cambios deben ser avalados por escrito por el líder funcional del sistema de información o plataforma quien autorizara el paso a producción.

Una vez se superada etapa de pruebas, el Área de Tecnologías de la Información y las Comunicaciones documenta y coordina el paso a producción.

Todo cambio a un recurso informático de la plataforma tecnológica relacionado con modificación de accesos, mantenimiento de software o modificación de parámetros deberá realizarse sin la alteración de la seguridad.

El Área de Tecnologías de la Información y las Comunicaciones deberá verificar que los cambios sean propuestos por usuarios autorizados y se encuentren alineados a la licencia de uso y necesidades de la entidad.

El Área de Tecnologías de la Información y las Comunicaciones garantizará que la implementación de los cambios se lleve a cabo sin generar interrupción de las actividades operativas, de no ser posible por las actividades propias de los cambios, se debe programar una ventana de mantenimiento para informar de la hora de inicio y hora de finalización donde se encontrará indisponibilidad parcial o completa de los servicios.

Los responsables de los cambios deberán informar antes de la implementación de un cambio a las áreas o usuarios que puedan verse afectados, con el fin de evitar la alteración de los procesos y la operatividad de la entidad para el cumplimiento de la misión institucional.

3.2.14 Copias en estaciones de trabajo de usuario final

Teniendo en cuenta que el Copnia dispone de medios de almacenamiento en la nube, los funcionarios y contratistas de la entidad son los responsables de la información que reposa en sus equipos de cómputo.
Es responsabilidad del área de Tecnologías de la Información y de las Comunicaciones brindar soporte a los funcionarios y contratistas con el fin de garantizar el respaldo adecuado de la información que se encuentra alojada en las estaciones de trabajo.

3.3 Control de Acceso[3]

3.3.1 Control de accesos con usuarios y contraseñas

El área de Tecnologías de la Información y las Comunicaciones es responsable de que todos los usuarios sean identificados independientemente, con permisos de acceso específicos e individuales para el acceso a redes, aplicaciones, y sistemas de información del Copnia, autorizados por razones básicas de sus funciones, por el área de Talento Humano.

El área de Tecnologías de la Información y de las Comunicaciones suministrará a los usuarios autorizados por el área de Talento Humano, contraseñas o claves para el acceso a los servicios de red, sistemas de información y/o servicios TIC. Es responsabilidad de los usuarios cambiar la contraseña inicial, conforme a los parámetros definidos para cada servicio tecnológico y encargarse de su respectiva administración.

El Área de Tecnologías de la Información y las Comunicaciones suministrará una matriz de roles y perfiles para la gestión de permisos definidos por los líderes funcionales.

Los líderes de área o funcionales, determinan los permisos adicionales requeridos para la ejecución de labores y gestionan con el área de Tecnologías de la Información y de las Comunicaciones novedades como la modificación, activación o inactivación de usuarios, siguiendo el procedimiento de Atención de Incidencias y Requerimientos TIC-pr-01.

Los usuarios y contraseñas asignados a funcionarios, contratistas o terceros que tengan permisos de acceso a redes, aplicaciones y sistemas de información del Copnia, son de uso personal e intransferible, por lo cual no se permite compartirlos o prestarlos.

Ningún usuario deberá acceder a la red, sistemas de información o a los servicios TIC del Copnia, utilizando una cuenta de usuario o clave diferente a la asignada.

Para facilitar el acceso a las aplicaciones disponibles, mediante el uso de un número reducido de claves y contraseñas por usuario, el área de Tecnologías de la Información se encargará de que dichos accesos se realicen con vinculación directa de las credenciales de los usuarios de directorio activo.

---

[3] Este grupo de políticas deben hacer referencia a todas aquellas directrices mediante las cuales la Entidad determina los mecanismos de protección, los límites y procedimientos frente a la administración y responsabilidad, relacionados con los accesos a la información, sin importar si estos accesos sean electrónicos o físicos.

Las conexiones a servicios en la nube dispuestos por la entidad, tales como office 365, deben realizarse desde sitios seguros, evitando conexiones en lugares tales como café internet, equipos móviles desconocidos o sitios de bajo nivel de confianza, entre otros.

Es responsabilidad de los funcionarios y contratistas del Copnia realizar el cierre de cesiones por cada caso de ingreso a cualquiera de las aplicaciones o servicios tecnológicos que requieran acceso mediante usuarios y contraseña. La práctica de cierres de ventanas conlleva el riesgo de permitir el ingreso a los sitios del Copnia a personas no autorizadas.

El Área de Tecnologías de la Información y las Comunicaciones es responsable de fomentar y programar desconexiones por tiempo sin uso temporal de aplicaciones y computadores personales activos.

3.3.2 Suministro del control de acceso

Es responsabilidad del líder del área de Tecnologías de la Información y de las Comunicaciones suministrar, conservar y custodiar las claves de acceso otorgadas a funcionarios con usuarios con privilegios superiores utilizados para la administración de infraestructura, aplicaciones y sistemas de información de la entidad. Los usuarios con privilegios superiores y sus correspondientes contraseñas a consolas administrables, accesos a sistemas de información, servidores o infraestructura, se dejan en custodia al líder de Tecnologías de la Información y de las Comunicaciones, quien asignará accesos a los funcionarios del área, según funciones y niveles de responsabilidad.

El personal del área de Tecnologías de la Información y de las Comunicaciones debe emplear de manera obligatoria, las claves o contraseñas con el más alto nivel de complejidad disponible para cada aplicación, sistema de información o infraestructura, utilizando los servicios de autenticación fuerte disponibles para cada uno de ellos.

Los administradores de los sistemas de información deben seguir los lineamientos de gestión de contraseñas definidas en este documento y notificar cualquier cambio al líder del área de Tecnologías de la Información y de las Comunicaciones, quien se encargará de la custodia centralizada de las claves o contraseñas, en un sitio seguro.

Es responsabilidad de los funcionarios que cuenten con usuarios con privilegios superiores utilizados para la administración de infraestructura, aplicaciones y sistemas de información mantener informado al líder del área de Tecnologías de la Información y de las Comunicaciones, de cualquier cambio ocurrido en los usuarios y claves de acceso otorgados para la labor encomendada.

Es responsabilidad de los funcionarios del área de Tecnologías de la Información y de las Comunicaciones asegurarse que de que las contraseñas referentes a las cuentas "predefinidas o por default" incluidas en los sistemas, hardware o aplicaciones adquiridas que se encuentre bajo su responsabilidad sean desactivadas. De no ser posible su desactivación, las contraseñas serán cambiadas después de la instalación del producto. Las anteriores actividades deben ser informadas al líder del área de Tecnologías de la Información y las Comunicaciones.

Los usuarios y claves de los administradores de sistemas y del personal del área de Tecnologías de la Información y de las Comunicaciones son de uso personal e intransferible, por lo tanto, los funcionarios del área en mención no deben dar a conocer sus claves a terceros. En caso de ser requerido algún acceso o soporte que exija dar a conocer dicha información, se debe solicitar autorización del profesional de gestión del área, quien documentará e impartirá instrucciones especiales al respecto.

El Área de Tecnologías de la Información y las Comunicaciones define las reglas para asegurar un acceso controlado, físico o lógico, a la información y plataforma informática del Copnia.

La conexión remota a la red de área local del Copnia debe realizarse a través de una conexión VPN segura (Red privada virtual) suministrada por la entidad, la cual debe ser aprobada, registrada y monitoreada por el Área de Tecnologías de la Información y las Comunicaciones. El uso de esta herramienta está establecido solo para uso laboral. No se debe suministrar configuración de usuarios o datos de conexión a personas ajenas del Copnia ni se debe configurar la VPN en equipos ajenos a la entidad.

3.3.3 Gestión de contraseñas

La solicitud del restablecimiento de contraseñas solo puede ser realizado por el usuario titular de la cuenta o de su jefe inmediato, mediante requerimiento escrito, conforme a las directrices del procedimiento de Atención de Incidencias y Requerimientos TIC-pr-01. Es responsabilidad del funcionario del área de Tecnologías de la Información y de las Comunicaciones asignado para la labor, verificar el estricto cumplimiento del procedimiento, así como validar la identidad y competencia del solicitante, antes de proceder.

Es responsabilidad del área de Tecnologías de la Información y de las Comunicaciones configurar las contraseñas de los servicios de Directorio Activo y Correo, de tal forma que cumplan las siguientes reglas o condiciones:

- Las contraseñas deben tener mínimo ocho (8) caracteres alfanuméricos, de los cuales, por lo menos uno (1) debe ser una letra en mayúscula, uno (1) en minúscula y uno (1) numérico. Ej. Sinfonica07.
- Las contraseñas deben tener una vigencia de máximo 40 días. Transcurrido el periodo, los servicios deben requerir el cambio.
- Cada vez que se requiera un cambio, ya sea por requerimiento del usuario o expiración de las contraseñas, los servicios deberán validar que las nuevas contraseñas sean diferentes a las últimas cinco que hayan sido usadas por la cuenta.
- Los servicios deberán parametrizarse para que las contraseñas se bloqueen después de 3 intentos erróneos. En caso de que la situación descrita se presente, el desbloqueo de claves se realizará siguiendo el procedimiento de Atención de Incidencias y Requerimientos TIC-pr-01.

Se recomienda a los usuarios abstenerse de asignar contraseñas que contengan información personal tal como nombres propios, de familiares o de mascotas, apellidos y fechas de cumpleaños, entre otros, ya que estas prácticas pueden ser detectadas y usadas en contra de la seguridad de la información de la entidad.

3.3.4 Perímetro de seguridad

Las áreas dispuestas por la Entidad para la atención al público son las ventanillas de correspondencia de cada oficina, por lo cual no es permitido el acceso de visitantes a las oficinas de las diferentes áreas de la Entidad, a excepción de contratistas. En caso de que se requiera el acceso de personal diferente, este deberá ser autorizado por el profesional de gestión del área Administrativa o por el secretario seccional en los casos

correspondientes, para esto el funcionario que estará a cargo del visitante deberá solicitar autorización para el ingreso de este mediante correo electrónico a los funcionarios mencionados anteriormente según sea el caso.

Las áreas de comedores o cafetería son de uso exclusivo para los funcionarios de la Entidad, por lo cual no está permitido el ingreso de visitantes a estos espacios.

Todos los funcionarios deben garantizar que ninguna persona ajena a la Entidad se quede en las instalaciones sin acompañamiento o supervisión.

Todo ingreso de funcionarios y personal externo en horario no hábil deberá ser autorizada previamente por el profesional de gestión del área Administrativa o el secretario seccional cuando corresponda para lo cual, debe remitirse un correo electrónico por el funcionario o por el jefe del área quien deberá ser informado al respecto.

Las puertas de acceso a las oficinas deberán permanecer cerradas durante la jornada laboral y debidamente aseguradas en horario no laboral, es responsabilidad de todos los funcionarios garantizar el cierre de estas a su salida. Con el fin de salvaguardar los equipos de la Entidad estos deben estar asegurados en la medida de lo posible privilegiando el uso de guaya.

Al finalizar la jornada laboral deben quedar las ventanas de cada oficina cerradas y tanto las luces como los equipos apagados. Es responsabilidad de cada funcionario velar por estas condiciones haciendo uso razonable de los recursos de la Entidad.

Todos los funcionarios deberán portar su carné en un lugar visible mientras permanezcan dentro de las instalaciones del Copnia.
En las instalaciones del centro de datos o de los centros de cableado **no** está permitido:

a. Ingresar sin previa autorización del profesional de gestión del área de Tecnologías de la Información y de las Comunicaciones.
b. Fumar, introducir alimentos o bebidas dentro del Data Center.
c. Mover, desconectar y/o conectar equipo de cómputo sin autorización escrita del líder del área de Tecnologías de la Información y de las Comunicaciones.
d. Realizar algún cambio en las conexiones o configuración sin previa autorización escrita del líder o profesional de gestión del área de Tecnologías de la Información y las Comunicaciones.
e. Alterar software instalado en los equipos sin autorización escrita del líder o profesional de gestión del área de Tecnologías de la Información y las Comunicaciones.
f. Alterar o dañar las etiquetas de identificación de los sistemas de información o sus conexiones físicas.
g. Extraer información de los equipos en dispositivos externos.
h. Toda persona que ingrese a hacer mantenimiento o dar soporte en los centros de cableado o centros de datos, debe hacer uso únicamente de los equipos y accesorios que les sean asignados, para los fines que haya autorizado por escrito el líder o profesional de gestión del área de Tecnologías de la Información y de las Comunicaciones.

Es responsabilidad del profesional de gestión del área de Tecnologías de la Información y de las Comunicaciones mantener almacenadas y en custodia las llaves de ingreso a los centros de cableado y data center. No está permitido sustraer o prestar dichas llaves sin autorización.

3.4 No repudio[4]

3.4.1 Trazabilidad

El área de Tecnologías de la Información y de las Comunicaciones verifica que los sistemas informáticos del Copnia generen y mantengan trazabilidad apropiada con el fin de identificar usuarios y documentar las situaciones relacionadas con eventos de seguridad.
El área de Tecnologías de la Información y de las Comunicaciones, será la encargada de asegurar que los sistemas de información cuenten con los registros requeridos para realizar la trazabilidad de las acciones ejecutadas en el sistema, garantizando los campos básicos de: Usuario, fecha, acción.

3.4.2 Retención

El periodo de retención de la información de las acciones realizadas por el usuario será el mismo que opere para el ciclo de vida de utilización del sistema de información mencionado, una vez el sistema de información sea dado de baja por obsolescencia, en los archivos de disposición final que se extraen del mencionado sistema para custodia en el archivo de la entidad, deberán también ser transferidos los registros de trazabilidad.

3.4.3 Auditoría

Garantiza a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
Es responsabilidad de la Oficina de Control Interno programar auditorías periódicas al cumplimiento de los lineamientos estipulados en el presente manual, conforme los procedimientos definidos para el proceso de Evaluación y Control de la entidad.

3.4.4 Intercambio electrónico de información

La información del Copnia relacionada con la topología de la red, el direccionamiento interno, así como las configuraciones y demás datos relacionados con las redes y sistemas de comunicación de la entidad, deberá ser información confidencial.

Todo intercambio de información o interacción entre sistemas de información con otras entidades deberá estar soportado con un contrato o convenio formalizado y con el visto bueno del profesional de gestión del área de Tecnología de la Información y de las Comunicaciones.
Cuando se requiera conectar la red o los sistemas de información del Copnia con la red o sistemas de otra entidad, esta solicitud deberá ser estudiada y avalada por el profesional de gestión del área de Tecnologías de Información y de las Comunicaciones, incluyendo un análisis de los posibles riesgos asociados y posteriormente debe escalarse con la Dirección General para su respectiva aprobación, considerando siempre la necesidad de apoyar la misión del Copnia.
El área de Tecnologías de la Información y de las Comunicaciones es responsable de proteger la información involucrada (transporte por protocolo seguro) en transacciones en línea, para evitar la transmisión incompleta, rutas equivocadas, alteración y divulgación.
El Copnia establece los siguientes lineamientos para estos acuerdos o convenios de intercambio de información:

[4] La política de seguridad y privacidad comprende la capacidad de no repudio con el fin de que los usuarios eviten haber realizado alguna acción.

- El intercambio de información debe realizarse a través de protocolos seguros definidos por el profesional de gestión TIC de la entidad
- La información que se suministrara del Copnia a otra entidad, debe estar claramente detallada dentro del acuerdo o contrato, así como su disposición final y su tratamiento respectivo.
- Los repositorios finales de información, así como sus medios de trasmisión y presentación, deben contar con las características de seguridad exigidas por el profesional de gestión del Área de Tecnologías de la Información y las Comunicaciones.
- El consumo de información que se realiza al Copnia, debe contar con las características técnicas y de seguridad que se dispongan por parte del profesional de gestión del Área de Tecnologías de la Información y las Comunicaciones, lo cual es dependiente de la arquitectura que maneje determinado sistema de información.

3.5 Antivirus

El Área de Tecnologías de la Información y las Comunicaciones planificará las necesidades de recursos necesarios, que garanticen la protección de la información y los recursos de la plataforma tecnológica en donde se procesa y almacena, adoptando los controles necesarios para evitar la divulgación, modificación o daño permanente ocasionados por el contagio de software malicioso. Además, proporcionará los mecanismos para generar cultura de seguridad entre sus funcionarios y personal provisto por terceras partes frente a los ataques de software malicioso.

3.6 Privacidad y Confidencialidad[5]

El Copnia desarrolla lineamientos y acciones orientadas a la protección y tratamiento de los datos personales recolectados para fines misionales, contractuales y administrativos. Dichos lineamientos se desarrollan en la Política de Protección de Datos personales y en el Manual para la Protección de Datos Personales disponibles en el sitio Web y en la documentación del proceso de Atención al Ciudadano.

El área de Talento Humano es responsable de solicitar a funcionarios, supernumerarios y planta temporal, la firma de acuerdos de confidencialidad individuales en los que se comprometan a no divulgar información interna y externa que conozca en razón a la ejecución de actividades misional o desarrollo de labores administrativas. La firma del acuerdo implica que la información conocida por todo funcionario, en ninguna circunstancia deberá ser revelada por ningún medio electrónico, verbal, escrito u otro, ni total ni parcialmente.

El área de Contratación es responsable de incluir cláusulas de confidencialidad y no divulgación de tal forma que los proveedores de bienes o servicios se comprometan a no divulgar información interna y externa que conozca en razón a la ejecución de actividades misional o desarrollo de labores administrativas. La firma del acuerdo implica que la información conocida por todo contratista y/o tercero, en ninguna circunstancia deberá ser revelada por ningún medio electrónico, verbal, escrito u otro, ni total ni parcialmente.

[5] Este lineamiento contiene la descripción de las políticas de tratamiento y protección de datos personales que deben ser aplicados, conforme a lo establecido en la normatividad vigente

3.7 Integridad[6]

Los líderes de las dependencias y áreas del Copnia son responsables porque toda la información verbal, física o electrónica, sea entregada o transmitida integralmente, sin modificaciones o alteraciones, al destinatario correspondiente.
Es responsabilidad de todos los funcionarios del Copnia hacer uso de los activos de información de forma responsable, profesional, ética y legal.
Es responsabilidad de todos los funcionarios del Copnia, mantener la privacidad de las comunicaciones personales, en un nivel de servicio apropiado a la función que desempeñan en la entidad.
La información generada y recibida en el Copnia, debe ser usada para los propósitos misionales de la Entidad, conforme a las funciones propias de cada cargo y para responder requerimientos de entes de control o terceros, de acuerdo con procedimientos definidos para tal fin.
En el caso de vinculación contractual, el compromiso de administración y manejo integro e integral de la información interna y externa hará parte de las cláusulas del respectivo contrato, bajo la denominación de cláusula de integridad de la información. Es responsabilidad del Área de Contratación de la Subdirección Administrativa y Financiera, verificar la existencia de dicha cláusula.

3.8 Disponibilidad del Servicio e Información[7]

El área de Tecnologías de la Información y las Comunicaciones, es responsable de implementar las medidas necesarias para disminuir los posibles efectos de las interrupciones en los sistemas de información o el normal funcionamiento de la infraestructura tecnológica; de igual forma será la encargada de liderar la implementación de controles para asegurar la continuidad de los procesos críticos.

3.9 Registro y Auditoría[8]

Es responsabilidad del Área de Tecnologías de la información y las Comunicaciones verificar que los sistemas de información almacenen los registros de cualquier evento de seguridad, así como de establecer un adecuado mecanismo para la gestión de los eventos de seguridad.
Los registros de trazabilidad del sistema serán suministrados a la Oficina de Control Interno según lo requiera en el marco de las auditorias anuales que se realizan a los procesos de la entidad.

3.10 Gestión de Incidentes de Seguridad de la Información[9]

Es deber de los funcionarios reportar, a través del procedimiento Atención de Incidentes y Requerimientos, todo incidente de seguridad de información que atente en contra de las políticas consignadas en el presente

---

[6] Se refiere al manejo íntegro e integral de la información tanto interna como externa, conocida o administradas por los funcionarios y/o terceros que hacen parte de la Entidad.
[7] Contiene los lineamientos que le permiten a la Entidad asegurar, recuperar o restablecer la disponibilidad de los procesos que soportan el Sistema de Gestión de Seguridad de la Información y procesos misionales de la Entidad, ante el evento de un incidente de seguridad de la información.
[8] Esta política vela por el mantenimiento de las evidencias de las actividades y acciones que afectan los activos de información.
[9] Documenta los lineamientos para la gestión de eventos, incidentes y vulnerabilidades de seguridad de la información.

documento o que identifique un riesgo o evento factible para la integridad, disponibilidad y seguridad de la información del Copnia.

Es responsabilidad del área de Tecnologías de la Información y de las Comunicaciones categorizará el incidente como "Seguridad de la información" y tomará las acciones respectivas para eliminar o mitigar la amenaza. De ser necesario, el área de Tecnologías de la Información y de las Comunicaciones convocará al Subcomité de Seguridad de la Información para el análisis del incidente reportado.

3.11 Capacitación y Sensibilización en Seguridad de la Información[10]

La Subdirección Administrativa y Financiera, a través del área de Talento Humano, es responsable de incorporar en el Plan Institucional de Capacitación programas de uso y apropiación del presente manual, de tal manera que se promueva la apropiación de este, mediante una adecuada sensibilización, capacitación y comunicación.

3.12 Implementación de proyectos tecnológicos

Para la implementación de proyectos tecnológicos se requiere seguir los siguientes lineamientos:

- La arquitectura debe ser definida y aprobada por el Área de Tecnologías de la Información
- El modelo de seguridad (protocolos, transacciones, implementación de roles, perfiles, arquitectura, autenticación y autorización, entre otros) debe ser definido por el área de Tecnologías de la Información, acorde a la protección de los activos de información y su criticidad.
- El proceso de implementación de los proyectos tecnológicos debe ser acordado con el Área de Tecnologías de la Información, acorde con la segregación de ambientes (desarrollo, pruebas, producción).
- Las estrategias de migración y de salida a producción deben ser acordadas con el Área de Tecnologías de la Información, dependencia garante de minimizar los impactos y responsable de certificar la calidad de los productos entregados.

4. ANEXOS

N.A

5. CONTROL DE CAMBIOS

No.	Fecha	Descripción del cambio o modificación
1	Julio 2019	Primera emisión

[10] Lineamientos cuya finalidad es disminuir las vulnerabilidades y amenazas relacionadas con el recurso humano.

IVAN TORRES GONZÁLEZ	GLORIA MATILDE TORRES CRUZ	GLORIA MATILDE TORRES CRUZ
Profesional de gestión del área de Tecnología de la Información y de las Comunicaciones	Subdirectora de Planeación, Control y Seguimiento	Directora General (E)
ELABORÓ	**REVISÓ**	**APROBÓ**