República de Colombia

CONSEJO PROFESIONAL NACIONAL DE TOPOGRAFÍA

Ley 70 / 79

RESOLUCIÓN No. 02 de 2022

(11 de marzo de 2022)

"Por medio de la cual se crea la política de seguridad de la información del Consejo Profesional Nacional de Topografia CPNT"

LA JUNTA DEL CONSEJO PROFESIONAL NACIONAL DE TOPOGRAFÍA

en ejercicio de sus funciones establecidas en la Ley 70 de 1979, y en especial las conferidas por el reglamento interno en los literales c), f), i) de la Resolución 11 de 2012 y

CONSIDERANDO

1. Que el Consejo Profesional Nacional De Topografía -CPNT, es un órgano sui géneris, autónomo e independiente, creado por la Ley 70 de 1979, de derecho público, sin personería jurídica, de conformación mixta, que forma parte de la administración pública y en tenor en lo preceptuado en el artículo 26 de la Constitución Política de Colombia, ejerce las funciones públicas permanentes de inspección, vigilancia y control del ejercicio de la profesión del topógrafo, con fundamento en la función de policía administrativa, apoya y promueve el ejercicio legal de la profesión de topografía protegiendo a la población de eventuales malas prácticas que puedan implicar riesgo social; es el responsable de expedir las licencias profesionales, resoluciones, y demás actos administrativos que autorizan al profesional ejercer la profesión en todo el territorio colombiano.

2. Que el artículo 269 de la Constitución Política de Colombia, establece la obligatoriedad por parte de la autoridad correspondiente en cada entidad pública de diseñar y aplicar, según la naturaleza de sus funciones, métodos y procedimientos de control interno de conformidad con lo que disponga la Ley.

3. Que de conformidad con lo establecido en el artículo 8 de la Ley 70 de 1979, en sus literales *a), f), i)* y *j)*, cuenta con autonomía administrativa para su organización interna y asignación de funciones y atribuciones a través de sus propios reglamentos.

4. Que entre las funciones de la junta del CPNT según lo dispuesto en la Resolución 11 de 2012 (reglamento interno del CPNT), se encuentra:

a) *Los actos o decisiones adoptadas por la junta del CPNT quedarán consignados en Resoluciones y serán suscritas por el presidente y el (la) secretario (a) de la sesión respectiva. Estos actos se comunicarán, notificaran y/o publicaran de acuerdo con la naturaleza de la decisión que contengan y contra estos procederán únicamente el recurso de reposición interpuesto por escrito*

ante el CPNT, dentro del término establecido en el Código Contencioso Administrativo. Su numeración será consecutiva en cada año calendario, con indicación del día, mes y año en que se aprueben. Su archivo y custodia están a cargo de la Dirección Ejecutiva.

5. Que artículo 15 de la constitución política de Colombia establece el derecho a la intimidad personal y familiar y el buen nombre que debe garantizar el estado, sobre la política en particular a través de buenas prácticas informáticas que materialicen este derecho fundamental.

6. Que la ley 1341 de 2009, indico los principios y directrices sobre la sociedad de la información y la organización de las tecnologías de la información y de las comunicaciones.

7. Que la ley 527 de *1999* estableció y reglamento el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y estableció las entidades de certificación

8. Que la ley 1273 de2009, modifico y regulo el Código Penal creando un nuevo bien jurídico tutelado - denominado "*de la protección de la información y de los datos*"- con el fin de establecer los límites al acceso de la información en formato digital contenida en sistemas informáticos.

9. Que la ley 1581 de 2012 y su decreto reglamentario 1377 de 2013, establecieron las normas generales en la protección de datos personales., norma que tiene alcance en la data contenida en sistemas de información.

10. Que la ley 1712 de 2004, creo la ley de trasparencia y el derecho de acceso a la información pública nacional y su procedimiento de conformidad al principio de publicidad peto también de intimidad a que tiene derecho los colombianos.

11. Que el decreto 2573 de 2014, reglamento los lineamientos generales de la estrategia de gobierno en línea y en desarrollo de este definió los instrumentos para su implementación.

12. Que el manual para la implementación de Gobierno Digital, versión 5 de agosto de 2018, estableció la seguridad de la información como un elemento trasversal habilitador de política de gobierno digital

13. Que la Norma técnica NTC-ISO-IEC colombiana 27001:2013, es un reconocido marco internacional de las mejores prácticas para un sistema de gestión de seguridad de la información. Le ayuda a identificar los riesgos para su información importante y pone en su lugar los controles apropiados para ayudarle a reducir el riesgo.

14. Que el día 11 de marzo de 2022, la junta directiva del CPNT una vez revisado el contenido de la presente resolución emitió aval para su expedición de lo cual se dejó registro en el acta No. 3 de la misma fecha, como una buena práctica en la adopción de la Norma técnica NTC-ISO-IEC colombiana 27001:2013

En mérito de lo expuesto,

RESUELVE

GENERALIDADES DE LA POLITICA DE SEGURDAD DE LA INFORMACIÓN

ARTÍCULO PRIMERO: Crear la Política de Seguridad de la Información del Consejo Profesional Nacional de Topografia *(en adelante CNPT)*, con sujeción a las disposiciones legales y reglamentarias del estado colombiano.

ARTÍCULO SEGUNDO: Definiciones y Conceptos: Establecidos para el adecuado y objetivo entendimiento de la presente política.

2.1 **Activo de información:** Información representada en registros de tipo físico o digital que tienen valor para el CPNT.
2.2 **Amenaza:** Evento que puede ser la causa de un hecho que comprometa la confidencialidad, integridad o disponibilidad de algún activo de información del CPNT
2.3 **Análisis de riesgo:** Diagnóstico para identificar los riesgos de los mecanismos de protección de los activos de información con el fin de optimizar dichos mecanismos y facilitar su monitoreo.
2.4 **Confidencialidad:** Garantía que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.
2.5 **Control**: Medida utilizada para garantizar la confidencialidad, integridad y disponibilidad de un activo de la información.
2.6 **Responsable de la información**: Cargo o grupo de trabajo encargado de mantener las medidas de protección establecidas sobre los activos de información confiados.
2.7 **Accesibilidad:** Garantizar que el personal autorizado podrá acceder a la información cuando lo requieran.
2.8 **Efectividad**: Capacidad de lograr el resultado esperado en la gestión informática.
2.9 **Eficiencia:** Capacidad de conseguir un objetivo deseado con el menor gasto posible de recursos en la gestión informática.
2.10 **Evaluación del riesgo**: Determina el valor de los activos de información, identifica las amenazas aplicables y las vulnerabilidades que existen (o pueden existir), identifica los controles existentes y sus efectos en el riesgo identificado, determina los efectos potenciales y finalmente prioriza los riesgos derivados y los ordena contra el conjunto de criterios de valoración del riesgo en el contexto establecido.
2.11 **Tratamiento de activos**: Conjunto de actividades que consisten en la clasificación de los activos identificados, gestión de riesgo y seguimiento de los controles aplicados con el fin de garantizar la confidencialidad, integridad y confidencialidad de los activos de información que forman parte del SGSI.
2.12 **Tratamiento de incidentes:** Conjunto de actividades y recursos con los que se manejan los eventos que afectan la confidencialidad, integridad y disponibilidad de la información del CPNT.
2.13 **Tratamiento de vulnerabilidades:** Conjunto de actividades que consiste en detectar y controlar el riesgo generado por las vulnerabilidades mediante el uso de controles.

2.14 **Hardware**: Elementos físicos de la infraestructura informática del CPNT. Ejemplo: computador, servidor, switch, router, teclado, pantalla.

2.15 **Eventualidad de seguridad de la información:** Evento no deseado o inesperado con una probabilidad significativa de comprometer operaciones de negocio, divulgación de datos confidenciales o de uso interno del CPNT o datos personales de los cuales la entidad es responsable, tal que desencadene en repercusiones sobre aspectos financieros, operativos o en su reputación. Ejemplos de incidentes de seguridad de la información son: Pérdida de servicio en equipos, instalaciones o conexiones, incumplimiento de las políticas o directrices referentes a seguridad de la información, ataques de Phishing, infecciones de código malicioso (virus, malware, etc.), entre otros.

2.16 **Impacto**: Grado en que se ve afectado un activo de información e incluso el CPNT por la materialización de un riesgo.

2.17 **Información**: Datos relacionados que tienen significado para el CPNT. Estos datos pueden presentarse en formato digital o en documentos físicos.

2.18 **Integridad:** Propiedad o atributo de la información que indica que la información no debe tener modificaciones por parte de personas o procesos que no cuenten con la debida autorización.

2.19 **Medio removible**: Componente extraíble de hardware utilizado para el almacenamiento de información. Por ejemplo, cintas, CDs, DVDs, unidades de almacenamiento USB o discos duros extraíbles

2.20 **Phishing:** Técnica utilizada para obtener información confidencial (nombres de usuario, contraseñas, etc.) mediante el envío de comunicaciones electrónicas aparentemente confiables

2.21 **Propietario de un activo de información:** Parte designada por la entidad (un cargo, proceso o grupo de trabajo) que tiene la responsabilidad de garantizar que la información y los activos asociados con el proceso se clasifican adecuadamente. También se encargan de definir y revisar periódicamente las restricciones y clasificaciones del acceso. El propietario decide sobre la finalidad, contenido y uso del activo de información y es responsable de la seguridad del activo.

2.22 **Riesgo:** Es una combinación de los efectos que pueden seguir a la ocurrencia de un evento no deseado y de la probabilidad de la ocurrencia del evento. La evaluación del riesgo describe cualitativamente el riesgo y permite a la dirección ejecutiva priorizar los riesgos de acuerdo con su percepción de la gravedad u otros criterios establecidos.

2.23 **Seguridad de la información**: Es la preservación de la confidencialidad, integridad y disponibilidad de los activos de información a través de la gestión de riesgos.

2.24 **Seguridad informática**: Implementación y mantenimiento de herramientas y controles a nivel de hardware, software y decisiones organizacionales para garantizar la seguridad de la infraestructura tecnológica.

2.25 **SGSI**: Sistema de Gestión de Seguridad de la Información

2.26 **Sistema de información:** Componente de software desarrollado por el CPNT o por un fabricante externo que requiere la interacción de uno o más activos de información para efectuar sus tareas.

2.27 **Software malicioso**: Programa que tiene como objetivo infiltrarse o dañar la infraestructura tecnológica. Los objetivos más comunes son los sistemas operativos, redes de datos o los sistemas de información.

2.28 **Tercero**: Persona jurídica o natural que tienen relaciones contractuales o de otro tipo con el CPNT y que no son empleados., Ejemplo: Proveedores, contratistas y consultores.

2.29 **Vulnerabilidad**: Debilidad frente a una amenaza. Generalmente responde a la ausencia o deficiencia de controles que permiten que una amenaza materialice un riesgo.

MARCO DE APLICACIÓN DE LA POLITICA DE SEGURDAD DE LA INFORMACIÓN

ARTÍCULO TERCERO: Alcance: La presente política es vinculante para todos los activos de información del el CPNT, así como a los propietarios de la información y terceros con relación u ocasión a la misma.

ARTÍCULO CUARTO: Principios Orientadores: La política de seguridad informática acoge los principio de la función administrativa consagradas en el artículo 209, artículo 3 de la ley 1437 de 2011 y acogidas por la ley 80 de 1993 para su debida ejecución a saber: Coordinación, Eficacia: Economía, Celeridad, Transparencia, Responsabilidad, Debido Proceso, Igualdad, Imparcialidad, Buena Fe, Moralidad, Participación, Planeacion a fin de articular estas disposiciones con el desarrollo diario de actividades del CNPT.

ARTICULO QUINTO: Responsables: Todo empleado y tercero que tenga acceso a los activos de información de del CNPT debe conocer, aceptar de manera expresa y cumplir con las disposiciones de esta Política. Además, debe utilizar la información sólo para los fines permitidos por la Ley, esta entidad y/o los titulares de los datos personales, según el caso, y garantizar la reserva y confidencialidad de la misma cuando no sea de carácter público y, por lo tanto, abstenerse de suministrarla a personas no autorizadas. Es responsabilidad del Grupo de Seguridad de la Información supervisar el cumplimiento de la Política, evaluar periódicamente la aplicabilidad de los controles y fomentar una cultura de seguridad de la información para todas las partes involucradas.

OBJETO DE LA POLITICA DE SEGURDAD DE LA INFORMACIÓN

ARTICULO SEXTO: General: Orientar y dar lineamientos de seguridad de la información sobre los activos del CPNT , con el fin de garantizar que los riesgos son identificados valorados y administrados de una forma estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en el entorno, en las tecnologías de información.

ARTICULO SEPTIMO: Específicos: Se establecen los siguientes objetivos en el marco de la política:

7.1 Definir, implementar, mantener y mejorar el Sistema de Gestión de Seguridad de la Información.

7.2 Velar por la confidencialidad, integridad y disponibilidad de la información de manera que esté protegida de acuerdo con las necesidades organizacionales, incluyendo los datos personales que por su naturaleza debe manejar el CPNT.

7.3 Garantizar la continuidad de las operaciones críticas del CPNT frente a incidentes que puedan resultar en interrupción o afectación.

7.4 Mantener la confianza de sus colaboradores, usuarios, contratistas, proveedores y entes reguladores en cuanto a seguridad de la información.

7.5 Garantizar el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas en cuanto a seguridad de la información.
7.6 Fortalecer la cultura de seguridad de la información en toda la comunidad topográfica, como medida para proteger la información como un activo crítico.

ARTICULO OCTAVO: Actualización de la Política: La dirección Ejecutiva o quien esta designe se encargará de revisar el presente documento como mínimo una vez al año o cada vez que se presenten cambios significativos en la estrategia del CPNT, en el contexto organizacional o el entorno tecnológico.

ARTICULO NOVENO: Socialización de la Política: La dirección Ejecutiva o quien esta designe se encargará de la divulgación de la Política respecto a los colaboradores y terceros que tengan acceso a los activos de información del CPNT cada vez que se realice una actualización o cuando ingrese nuevo personal.

MARCO ESTRATEGICO DE LA POLITICA

ARTICULO DECIMO: Gestión de activos de información: Los activos de información de CPNT deben ser identificados y clasificados de acuerdo con su grado de confidencialidad. Así mismo, deben tener un propietario designado, quien tiene la responsabilidad de garantizar que se clasifican adecuadamente, revisar las restricciones de acceso y la seguridad del activo.
Todos los colaboradores del CPNT tienen la responsabilidad de proteger y usar adecuadamente los activos de información.

ARTICULO DECIMO PRIMERO: Los activos de información se categorizarse según la siguiente clasificación:

10.1 Confidencial: Información que puede ser conocida y utilizada por personas autorizadas POR EL CPNT, pero no puede ser divulgada sin autorización del propietario.
10.2 De uso interno: Información que puede ser utilizada por empleados de la entidad con la debida autorización del propietario.
10.3 Pública: Información conocida y utilizada por cualquier persona.

PARÁGRAFO: El etiquetado, manejo, procesamiento, almacenamiento y comunicación de todos los activos de información se dará de acuerdo con la clasificación asignada.

ARTICULO DECIMO SEGUNDO: El CPNT, incorpora elementos de seguridad de la información en su relación con los colaboradores y contratistas antes, durante y después de la relación contractual, de acuerdo con el nivel de riesgo identificado.

Todos los colaboradores y terceros deben conocer y dar cumplimiento a la política de seguridad.

Así mismo, con el fin de propender por una cultura sólida en seguridad de la información, el CPNT define y ejecuta periódicamente programas de sensibilización y capacitación en seguridad de la información de acuerdo con las necesidades identificadas.

ARTICULO DECIMO TERCERO: **Control de acceso**. El acceso a la información, los sistemas y redes del CPNT, incluyendo recursos como carpetas compartidas, se otorgará con base en el principio de "necesidad de saber", es decir, con una justificación de la entidad.

Se deben seguir los procedimientos establecidos para la gestión de usuarios y contraseñas, velando siempre por mantener los accesos mínimos requeridos y cambiando las claves una vez por mes de lo cual se deberá informar al director ejecutivo de la entidad.

Cada colaborador y demás personas a quienes se asignen permisos para el acceso a la información debe mantener confidenciales e intransferibles sus credenciales de acceso.

Los escritorios o puestos de trabajo de los colaboradores y contratistas deben mantenerse limpios y sin documentos fuera del horario de trabajo o en ausencia prolongada del sitio.

ARTICULO DECIMO CUARTO: **Cifrado.** La elaboración y actualización de la política relacionada con el uso de controles criptográficos debe ser consecuente con una evaluación de riesgos previa, la cual ayudará a determinar el nivel de protección que debe recibir la información.

ARTICULO DECIMO QUINTO: **Seguridad física y del entorno**: Respecto de las áreas seguras es responsabilidad de los líderes de los procesos identificar las áreas usadas para almacenar y procesar información confidencial y de uso interno.
Los equipos de procesamiento de información, así como sus elementos de soporte, deben contar con medidas de protección de acuerdo con la sensibilidad del activo.

ARTICULO DECIMO SEXTO: **Seguridad en las operaciones**:

16.1 **Documentación de los sistemas:** Debe existir documentación para los procedimientos operativos y estar disponible para todos los individuos con una necesidad legítima de conocerlos. La Dirección Ejecutiva o a quien esta designe es responsable del mantenimiento de esta documentación.

16.2 **Gestión de cambios:** Todo cambio que tenga o pueda tener algún tipo de influencia sobre los sistemas de información o la infraestructura tecnológica que lo soporta, debe ser sometido a análisis y aprobación por un proceso formal de control de cambio.

16.3 **Gestión de la capacidad:** Para cada sistema de información del CPNT, la Direccion Ejecutiva deberá determinar regularmente el nivel de utilización de sus recursos, así como la respectiva demanda. Esta información permitirá establecer proyecciones sobre la capacidad de los recursos del sistema.

16.4 **Separación de los ambientes de desarrollo, pruebas y producción**: Todo sistema en producción debe tener por lo menos un ambiente de desarrollo que permita probar cualquier cambio y reducir el riesgo de acceso no autorizado. Deben existir mecanismos que garanticen el control de acceso a los ambientes de desarrollo y producción.

16.5 **Protección ante software malicioso:** Se debe contar con mecanismos de detección de código malicioso en la infraestructura tecnológica del CPNT., se deben realizar campañas de divulgación con el objetivo de informar a los usuarios acerca de medios de prevención y protección ante software malicioso.

16.6 **Copias de seguridad:** Toda información de la CPNT debe ser respaldada por copias de seguridad tomadas de acuerdo con los requerimientos aplicables, tanto legales como organizacionales. Una vez por semana el último día y hora hábil de la misma. Así mismo, los registros de copias de seguridad deben ser guardados en una base de datos creada para tal fin siendo responsabilidad de la Dirección Ejecutiva o quien esta designe.

16.7 **Seguimiento:** El CPNT ha establecido mecanismos para detectar actividades no autorizadas en los sistemas de información, como la activación de los registros de auditoría (logs).

16.8 Los repositorios o almacenamientos donde se guarden los registros deberán estar protegidos contra accesos no autorizados y/o alteraciones. Las actividades de usuarios operadores y administradores en los sistemas de procesamiento de información o sus componentes, están condicionadas a monitoreo. Debe acordarse una fuente segura para la sincronización de todos los relojes de sistemas que controlen accesos o generen registros de auditoría.

16.9 **Control de software operacional:** Todo software que se ejecute en los equipos de cómputo de la CPNT debe originarse de fuentes confiables, para evitar alteraciones no autorizadas. La Direccion Ejecutiva es responsable de verificar las fuentes del software antes de proceder con la instalación.

16.10 **Gestión de vulnerabilidades técnicas**: Se deberá mantener una constante revisión de las vulnerabilidades técnicas que son detectadas por la comunidad de seguridad de la información que tengan relación con el software utilizado por el CPNT.

16.11 **Dispositivos móviles:** Los dispositivos móviles que fueren asignados a los colaboradores del CPNT con una finalidad específica, por lo cual sólo deben ser utilizados por los usuarios autorizados según su rol y para tal fin. Además, los dispositivos móviles corporativos deben contar con software legalmente licenciado y mecanismos de protección adecuados para mitigar los riesgos identificados.

16.12 **Uso de correo electrónico y mensajería Web:** El uso del correo electrónico, servicio de mensajería Web y demás recursos que comprende (calendario, gestión de tareas, entre otros), es proporcionado para fines laborales para el caso de colaboradores y terceros. Por lo que debe entenderse., que la cuenta que se asigne por parte del CPNT es personal e intransferible y se compromete a salvaguardar la contraseña asignada, a cambiarla con frecuencia o cada vez que sea solicitado y a no compartirla con otros usuarios.

16.13 El CPNT se reserva el derecho de proveer este servicio directamente o mediante un proveedor, de establecer la ubicación física de la información y de hacer los cambios que considere pertinentes.

16.14 **Uso de Internet:** El CPNT provee acceso a Internet para colaboradores con el objetivo de facilitar el logro de la misión de la entidad En consecuencia, todos los usuarios deben acogerse a los lineamientos de esta política.

16.15 El CPNT se reserva el derecho de restringir el acceso a sitios que puedan afectar la productividad de la institución, la seguridad de su información o su personal. Los usuarios deberán abstenerse de visitar sitios restringidos por la CPNT de manera directa o indirecta. Así mismo, toda actividad relacionada con navegación en Internet puede ser registrada por el CPNT, quien podrá revelar cualquier acceso cuando una autoridad judicial así lo requiera.

16.16 **Uso de medios removibles (Memorias USB, discos externos, CDs, DVDs, tarjetas SD/mini SD/microSD):** El uso de medio removibles debe seguir el procedimiento definido para tal fin por la Direccion Ejecutiva.

16.17 **Manejo de incidentes de seguridad**: Todo colaborador y tercero debe reportar cualquier acto sospechoso o expuesto que pueda afectar la confidencialidad, integridad o disponibilidad de algún activo de información del CPNT.

ARTICULO DECIMO SEPTIMO: **Seguridad en las comunicaciones**: Toda conexión hacia las redes de la entidad, que provenga o pase a través de redes inseguras o desconocidas deberá contar con mecanismos de protección (ej. autenticación, cifrado y manejo de la integridad), de acuerdo con los riesgos identificados.

Todas las redes del CPNT deben contar con mecanismos de segregación acordes a la sensibilidad de la información Deben establecerse medidas que restrinjan el acceso a puertos remotos de diagnóstico o configuración, sin una autorización apropiada.

ARTICULO DECIMO SEPTIMO: Relación con terceros: El CNPT debe identificar los riesgos de seguridad de la información relacionados con sus terceros, determinar las medidas apropiadas a adoptar y hacer el respectivo seguimiento de su adecuada implementación.
En caso de otorgársele acceso a información confidencial, de uso interno o a un activo de información tecnológico a un usuario externo, el mismo debe aceptar por escrito que conoce, entiende y acepta esta política de seguridad.

ARTICULO DECIMO OCTAVO: Cumplimiento. Deben identificarse y documentarse las legislaciones, normativas y requerimientos contractuales asociados con la seguridad de la información.
Se deben definir e implementar procedimientos que garanticen el cumplimiento de los derechos de autor sobre el software que esté protegido por las regulaciones aplicables., En ellos debe mencionarse que únicamente se podrán utilizar aplicaciones con licencia de manera que no se infrinjan las leyes de Propiedad Intelectual.
Para proteger los registros De la entidad, todos los colaboradores del CPNT deben firmar un Compromiso de Confidencialidad. El Grupo de Seguridad de la Información establecerá la gravedad de las infracciones a esta Política. El proceso investigativo y posible sanción seguirán lo establecido EN EL Reglamento Interno de Trabajo, según corresponda. En caso de ser necesario, se contactará a las autoridades competentes.

ARTICULO DECIMO NOVENO: **Coordinación para la ejecución de la política.** La Direccion Ejecutiva es la dependencia responsable de coordinar la promoción, implementación, seguimiento y autoevaluación de la política de seguridad de la información con el concurso de todas las áreas misionales y de apoyo.

ARTIUCLO VIGESIMO: La presente resolución rige a partir de la fecha de su expedición.

PUBLÍQUESE, COMUNÍQUESE Y CÚMPLASE

Dada en Bogotá, D. C., a los once (11) días del mes de marzo de 2022

WILMAR DARÍO FERNÁNDEZ GÓMEZ
Presidente

LUIS ALEJANDRO ZAFRA JARAMILLO
Director Ejecutivo

Elaboró: Sebastian Camilo Rios Sanchez- Abogado