Contraloría Municipal de Neiva Neiva Bajo Control Compromiso de Todos !	**FORMATO**
	CONTEXTO ESTRATEGICO

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

CONTRALORIA MUNICIPAL DE NEIVA

VIGENCIA 2020

1. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Política de Seguridad Informática proporciona la base para la aplicación de controles de seguridad que reduzcan los riesgos y las vulnerabilidades del sistema.

El propósito de estructurar Políticas de Seguridad Informática es, por tanto, garantizar que los riesgos para la Seguridad Informática sean conocidos, asumidos, gestionados y minimizados.

La entidad, considera la información como uno de los activos más importantes de la organización que representa la Contraloría Municipal de Neiva (CMN) con respecto a (los funcionarios, contratistas, terceros, la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, frente a la generación y publicación de sus políticas, procedimientos e instructivos, de la misma manera como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

La Contraloría Municipal de Neiva debe revisar periódicamente la vigencia y la aplicabilidad de las siguientes políticas específicas de la información y efectuar los ajustes necesarios sobre ellas para que sean funcionales y se pueda seguir exigiendo su cumplimiento por parte de todos los funcionarios y personal suministrado por terceras partes que provean servicios a la Contraloría Municipal de Neiva.

POLITICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

1. ORGANIZACION DE LA SEGURIDAD

a) La Contraloría Municipal de Neiva ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, amparado en lineamientos claros alineados a las necesidades de la entidad, y a los requerimientos regulatorios que le aplican a su naturaleza.

b) La Contraloría Municipal de Neiva garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

c) La Contraloría Municipal de Neiva garantiza la disponibilidad de sus procesos de la entidad y la continuidad de su operación basada en el impacto que pueden generar los eventos.

d) La Contraloría Municipal de Neiva 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.

e) La Contraloría Municipal de Neiva garantiza que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

f) La Contraloría Municipal de Neiva implementa controles de acceso a la información, sistemas y recursos de red.

g) La Contraloría Municipal de Neiva controla la operación de sus procesos de la entidad garantizando la seguridad de los recursos tecnológicos y las redes de datos.

h) La Contraloría Municipal de Neiva protege las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

i) La Contraloría Municipal de Neiva protege su información de las amenazas originadas por parte del personal.

j) La Contraloría Municipal de Neiva protege la información creada, procesada, transmitida o resguardada por sus procesos de la entidad, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

k) Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros.

Nota. El incumplimiento a la política de Seguridad y Privacidad de la Información, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

2. SEGURIDAD EN EL RECURSO HUMANO

El objetivo es asegurar que los funcionarios, contratistas, pasantes y demás colaboradores de la CMN entiendan sus responsabilidades y funciones, con el fin de reducir el riesgo de hurto, fraude o uso inadecuado de la información.

a. La Contraloría cuenta con discos duros para almacenar la información que cada usuario considere importante y sobre ella se garantizará la disponibilidad en caso de un daño en el equipo asignado. Es de aclarar que cada usuario debe copiar la información necesaria en la carpeta destinada para tal fin.

b. La Contraloría no se hará responsable por las copias no autorizadas de programas instalados o ejecutados en los equipos asignados a sus funcionarios o contratistas.

c. El uso de dispositivos de almacenamiento externo (dispositivos móviles, DVD, CD, memorias USB, celulares, etc.) pueden ocasionalmente generar riesgos para la entidad al ser conectados a los computadores ya que son susceptibles de transmisión de virus informáticos o pueden ser utilizados para la extracción de información no autorizada.

d. Los recursos tecnológicos y de software asignados a los funcionarios de la Contraloría son responsabilidad de cada uno.

e. Los usuarios son los responsables de la información que administren en sus equipos y deberán abstenerse de almacenar en ellos información no institucional.

f. Es responsabilidad de cada usuario de proteger la información que esta contenida en documentos, formatos, listados, etc., los cuales son el resultado de los procesos informáticos.

g. El software licenciado y registrado como software adquirido será únicamente instalado en equipos y servidor de propiedad de la Contraloría.

3. SEGURIDAD PARA WEBMASTER

El objetivo es proteger la integridad de la página web institucional y la información contenida.

a. Los responsables de la información a publicar deben depurar la información de su Dependencia, revisar y corregir la ortografía, redacción e imagen corporativa de la información a publicar.

b. El administrador de la página web debe publicar oportunamente la información, llevar registro de la información publicada y almacenarla.

c. El administrador de la página web deberá realizar copias de seguridad.

4. SEURIDAD EN EL USO DE INTERNET

a. La navegación en internet debe realizarse de forma razonable y con propósitos laborales.

b. No se permite la navegación a sitios con contenidos contrarios a la ley o a las políticas de la Contraloría o que representen peligro para la entidad como: pornografía, terrorismo, etc.

c. La descarga de archivos de internet debe ser con propósitos laborales y de forma razonable para no afecta el servicio de internet.

5. SEGURIDAD FÍSICA

a. Mantener Áreas seguras para la gestión, almacenamiento y procesamiento de información en el Contraloría Municipal de Neiva. Las áreas deben contar con protecciones físicas y ambientales acordes con el valor y la necesidad de aseguramiento de los activos que se protegen, incluyendo la definición de perímetros de seguridad, controles de acceso físicos, seguridad para protección de los equipos, seguridad en el suministro eléctrico y cableado, condiciones ambientales adecuadas de operación y sistemas de contención, detección y extinción de incendios.

b. Las oficinas administrativas y operativas que cuenten con equipos de cómputo debe contar con mecanismos de control de acceso tales como puertas de seguridad, sistema de alarmas o controles biométricos; sistemas de detección y extinción automáticas de incendios, control de inundación y alarmas en caso de detectarse condiciones inapropiadas, estar separado de áreas que tengan líquidos inflamables o estén en riesgo de inundaciones e incendios.

c. Las oficinas e instalaciones donde haya atención al público no deben permanecer abiertas cuando los funcionarios se levantan de sus puestos de trabajo, así sea por periodos cortos de tiempo.

d. La seguridad de los equipos de cómputo fuera de las instalaciones será responsabilidad de cada funcionario y contratista asignado, junto con una autorización del jefe inmediato.

e. La documentación física generada, recibida y en general, manipulada por los funcionarios de la Entidad y los funcionarios provistos por terceras partes debe estar ubicada en archivos o repositorios con condiciones de temperatura y humedad adecuadas, de acuerdo con las Directrices de la función archivística de la entidad.

f. Los trabajos de mantenimiento de redes eléctricas, cableados de datos y voz, deben ser realizados por el personal especialista y debidamente autorizado e identificado.

6. Objetivo

Definir los mecanismos y todas las medidas necesarias por parte de la Contraloría Municipal de Neiva, tanto técnica, lógica, física, legal y ambiental para la protección de los activos de información, los recursos y la tecnología de la entidad, con el propósito de evitar accesos no autorizados, divulgación, duplicación, interrupción de sistemas, modificación, destrucción, pérdida, robo, o mal uso, que se pueda producir de forma intencional o accidental, frente a amenazas internas o externas, asegurando el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

7. Alcance

Este Plan de Seguridad y Privacidad de la Información y su política, son aplicables a todos los funcionarios de la Contraloría Municipal de Neiva, a sus recursos, procesos y procedimientos tanto internos como externos, así mismo al personal vinculado a la entidad y terceras partes, que usen activos de información que sean propiedad de la entidad.

8. Responsabilidades

Es responsabilidad de la Alta Dirección de la Contraloría Municipal de Neiva, establecer y mantener las Políticas de Seguridad Informática, las normas, directrices y procedimientos de la Organización. La Alta Dirección está integrada por la Señora Contralora, Secretaría General, Directores Técnicos y Asesor de Control Interno.

Las siguientes son las principales responsabilidades de Seguridad Informática, dentro de la Entidad:

a. Garantizar que la seguridad de la información forma parte integral del proceso de planeación estratégica de la organización.
b. Establecer las funciones y responsabilidades específicas de seguridad de la información para la Contraloría.
c. Establecer y respaldar los programas de concientización de la Contraloría en materia de seguridad y protección de la información.
d. Establecer, evaluar y aprobar el presupuesto designado para el tema de seguridad de la información.
e. Evaluar la adecuación, coordinación y la implementación de los controles de seguridad específicos para nuevos servicios o sistemas de información.
f. Promover explícitamente el apoyo institucional a la seguridad de la información en toda la organización.
g. Supervisar y controlar los cambios
h. Los funcionarios, además de ser responsables de la información, serán también los encargados de administrarla. En consonancia con lo anterior serán responsables todos aquellos que manejen información en los computadores asignados para llevar a cabo sus actividades o que tengan acceso a cualquier aplicación o sistema que sirva de apoyo a sus labores.

9. Cumplimiento

El cumplimiento de la Política de Seguridad y Privacidad de la Información es obligatorio. Si los funcionarios de la entidad o terceros violan este plan, la Contraloría Municipal de Neiva se reserva el derecho de tomar las medidas correspondientes.

10. Comunicación

Mediante socialización a todos los funcionarios de la Contraloría Municipal Neiva se dará a conocer el contenido del documento de las políticas de seguridad, así mismo se deberá informar a los contratistas y/o terceros en el

momento que se requiera con el propósito de realizar los ajustes y la retroalimentación necesaria para dar cumplimiento efectivo al plan.

Todos los funcionarios, contratistas y/o terceros de la entidad deben conocer la existencia de las políticas, la obligatoriedad de su cumplimiento, la ubicación física del documento estará a cargo del Sistema de Gestión Integrado para que sean consultados en el momento que se requieran, igualmente estarán alojados en el Portal Web de la entidad www.contralorianeiva.gov.co.

11. MONITOREO

Se crearán los mecanismos y los indicadores correspondientes a la política de seguridad con el fin de determinar el cumplimiento de las mismas para establecer qué modificaciones o adiciones deben hacerse, este monitoreo debe realizarse como mínimo una vez al año o cuando sea necesario.

12. CONTROL DEL ACCESO

La Contraloría usa controles de acceso y otras medidas de seguridad para proteger la confidencialidad, integridad y disponibilidad de la información manejada por computadores y sistemas de información.

Para mantener estos objetivos la Contraloría se reserva el derecho y la autoridad de: 1. Restringir o revocar los privilegios de cualquier usuario; 2. Inspeccionar, copiar, remover cualquier dato, programa u otro recurso que vaya en contra de los objetivos planteados; y, 3. Tomar cualquier medida necesaria para manejar y proteger los sistemas de información de La Contraloría.

Los funcionarios responsables de la información deberán almacenarla, implementar los controles de acceso (para prevenir la divulgación no autorizada) y periódicamente hacer copias de respaldo y así evitar la pérdida de información crítica.

Los funcionarios no deben utilizar ninguna estructura o característica de contraseña que podría dar como resultado una contraseña que sea predecible o deducible con facilidad, incluyendo entre otras las palabras de un diccionario, derivados de los identificadores de usuario, secuencias de caracteres comunes, detalles personales o cualquier parte gramatical.

La longitud mínima de las contraseñas será igual o superior a ocho caracteres y estarán constituidas por combinación de caracteres alfabéticos, numéricos y especiales.

Los usuarios finales no deben configurar, instalar y eliminar software de los equipos de cómputo de la Contraloría Municipal Neiva.

Los usuarios con acceso al sistema de información o a la red informática o telemática de la entidad disponen de una única autorización de acceso compuesta de identificador de usuario y contraseña, son los responsables de las acciones realizadas por el usuario que ha sido asignado.

Previo al acceso a un activo de información cada usuario debe demostrar su identidad utilizando el medio establecido, autorizado y provisto por la Contraloría.

El acceso a la información la Contraloría, deberá ser otorgado sólo a Usuarios autorizados, basados en lo que es requerido para realizar las tareas relacionadas con su responsabilidad.

El escritorio virtual de cada equipo de cómputo independiente del sistema operativo que use, debe mantenerte despejado, no debe contener archivos de ningún tipo salvo los accesos directos a aplicaciones necesarias en la labor del empleado.

El personal debe bloquear el equipo de cómputo con protector de pantalla que exija la contraseña de acceso a la sesión ante la ausencia temporal del puesto de trabajo.

13. CONTROL DE ACTIVOS DE INFORMACIÓN

La información que se encuentra en documentos físicos debe ser protegida, a través de controles de acceso físico y las condiciones adecuadas de almacenamiento y resguardo.

Tanto los funcionarios como el personal provisto por terceras partes deben asegurarse que en el momento de ausentarse de su puesto de trabajo, sus escritorios se encuentren libres de documentos y medios de almacenamiento, utilizados para el desempeño de sus labores; estos deben contar con las protecciones de seguridad necesarias de acuerdo con su nivel de clasificación.

Los usuarios deben tener en cuenta estas consideraciones cuando impriman, escaneen, saquen copias y envíen faxes: verificar las áreas adyacentes a impresoras, escáneres, fotocopiadoras y máquinas de fax para asegurarse que no quedaron documentos relacionados o adicionales; asimismo, recoger de las impresoras, escáneres, fotocopiadoras y máquinas de fax, inmediatamente los documentos confidenciales para evitar su divulgación no autorizada o mal intencionada.

Los usuarios deben acatar los lineamientos guía de clasificación de la Información para el acceso, divulgación, almacenamiento, copia, transmisión, etiquetado y eliminación de la información contenida en los recursos tecnológicos, así como de la información física de la entidad.

14. GESTIÓN DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La Contraloría Municipal de Neiva debe asegurar que se establecen y ejecutan procedimientos para identificar, analizar, valorar y dar un tratamiento adecuado a los incidentes, y que se hace una adecuada evaluación del impacto en el negocio de los incidentes de seguridad de la información.

Los usuarios de la información de la Contraloría Municipal de Neiva deben reportar los incidentes de seguridad que se presenten, según el procedimiento de gestión de incidentes que se implementes a través de los formatos respectivos adoptados por la entidad.

15. CUMPLIMIENTO

La Contraloría Municipal de Neiva, gestiona la seguridad de la información de tal forma que se dé cumplimiento adecuado a la legislación vigente. Para esto, analiza los requisitos legales aplicables a la información, incluyendo entre otros los derechos de propiedad intelectual, protección de datos personales, los tiempos de retención de registros, la privacidad, los delitos informáticos, el uso inadecuado de recursos de procesamiento.

Cumplimiento de la normatividad y los controles relacionados con la seguridad de la información y los que son técnicamente compatibles con los diferentes ambientes o tecnologías de la entidad.

Los productos de Software que se adquieran e instalen en los equipos de cómputo de la Contraloría deben contar con su respectiva licencia de uso.

Realización de auditorías internas, para verificar la eficacia de los controles y asegurar la administración de los riesgos de seguridad de la información.

Las políticas junto con el Sistema de Gestión de Seguridad de la Información que se implementen por parte de la Contraloría Municipal de Neiva, debe ser auditados anualmente para verificar su nivel, actualidad, aplicación, completitud y cumplimiento.

Contraloría Municipal de Neiva Neiva Bajo Control Compromiso de Todos !	**FORMATO**
	CONTEXTO ESTRATEGICO