	<p align="center">"CONTROL FISCAL CON CREDIBILIDAD"</p>	Código: FO-GC-29
		Fecha: 19/02/18
		Versión: 1
		PÁGINA 1 de 3

RESOLUCIÓN No. 025

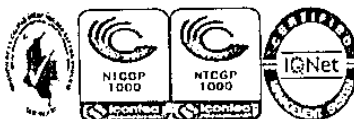
31 ENE 2019

"POR MEDIO DE LA CUAL SE ADOPTA EL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN PARA LA VIGENCIA 2019 DE LA CONTRALORÍA GENERAL DEL QUINDÍO"

EL DIRECTOR ADMINISTRATIVO Y FINANCIERO con delegación de funciones como CONTRALOR GENERAL DEL QUINDÍO según Resolución No. 020 del 28 de enero de 2019, en uso de sus facultades Constitucionales y legales y,

CONSIDERANDO:

- A. El Plan de Seguridad y Privacidad de la Información busca establecer directrices e implementar los procedimientos que se requiere en la Entidad, para el buen uso de los elementos que conforman la infraestructura tecnológica, por parte del personal de la Contraloría General del Quindío.
- B. El manejo y cuidado de los equipos y programas de la Entidad, es uno de los objetivos institucionales, con el fin de conseguir el mayor provecho de las herramientas informáticas, para un buen desempeño de las funciones determinadas en cada cargo.
- C. Igualmente, es necesario proveer a todos los funcionarios, colaboradores y terceros de la Contraloría General del Quindío la guía para el uso adecuado y responsable de la infraestructura tecnológica con la que cuenta la Entidad.
- D. El Plan de Seguridad y Privacidad de la Información busca establecer en la Contraloría General del Quindío una cultura de calidad y seguridad, que permita operar de forma confiable con medidas y estándares técnicos de administración y organización de toda la plataforma tecnológica de la Entidad.
- E. Que el Decreto 1078 de 2015, en su artículo 2.2.9.1.2.2 contempló los instrumentos para implementar la Estrategia en Línea, dentro de los



RESOLUCIÓN No. 0 2 5

31 ENE 2019

cuales se exige la elaboración del Plan de Seguridad y Privacidad de la Información.

- F. Que el Decreto 648 del 4 de abril de 2018 artículo 1º adicionó al capítulo 3 del Título 22 de la parte 2 del libro 2 del Decreto 1083 de 2015 “Único Reglamentario de Función Pública”, los siguientes artículos:

Artículo 1. Adicionar al Capítulo 3 del Título 22 de la Parte 2 del Libro 2 del Decreto 1083 de 2015, Único Reglamentario del Sector de Función Pública, los siguientes artículos:

“2.2.22.3.14, Integración de los planes institucionales y estratégicos al Plan de Acción. Las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011,

deberán integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlo, en su respectiva página web, a más tardar el 31 de enero de cada año:

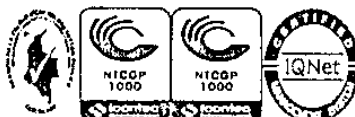
1. Plan Institucional de Archivos de la Entidad –PINAR
2. Plan Anual de Adquisiciones
3. Plan Anual de Vacantes
4. Plan de Previsión de Recursos Humanos
5. Plan Estratégico de Talento Humano
6. Plan Institucional de Capacitación
7. Plan de Incentivos Institucionales
8. Plan de Trabajo Anual en Seguridad y Salud en el Trabajo
9. Plan Anticorrupción y de Atención al Ciudadano
10. Plan Estratégico de Tecnologías de la Información y las Comunicaciones – PETI
11. Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información
12. Plan de Seguridad y Privacidad de la Información


Parágrafo 1. La integración de los planes mencionados en el presente artículo se hará sin perjuicio de las competencias de las instancias respectivas para formularlos y adoptarlos.

Cuando se trate de planes de duración superior a un (1) año, se integrarán al Plan de Acción las actividades que correspondan a la respectiva anualidad.

Parágrafo 2. Harán parte del Plan de Acción las acciones y estrategias a través de las cuales las entidades facilitarán y promoverán la participación de las personas en los asuntos de su competencia, en los términos señalados en la Ley 1757 de 2015.

- G. Entre los planes que deben estar integrados al plan de acción y que debe estar publicado al 31 de enero de cada año, es el presente plan de seguridad y privacidad de la información vigencia 2019.
- H. Que en la Contraloría General del Quindío, a través de su Comité Institucional de Gestión y Desempeño, en reunión del 24 de enero de 2019 aprobaron el PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2019.



 CONTRALORÍA GENERAL DEL QUINDÍO	"CONTROL FISCAL CON CREDIBILIDAD"	Código: FO-GC-29
		Fecha: 19/02/18
		Versión: 1
		PÁGINA 3 de 3

RESOLUCIÓN No. 0253

31 ENE 2019

Que en mérito de lo anterior, el Director Administrativo y Financiero con delegación de Funciones como Contralor General del Quindío,

RESUELVE:

ARTÍCULO PRIMERO: Adoptar el PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN PARA LA VIGENCIA 2019 DE LA CONTRALORÍA GENERAL DEL QUINDÍO, conforme a la parte motiva de esta resolución y el anexo que hace parte integral de la misma.

ARTÍCULO SEGUNDO: La presente Resolución, será publicada por la Dirección Administrativa y Financiera en la página web institucional.

ARTÍCULO TERCERO: La presente Resolución rige a partir de su expedición.

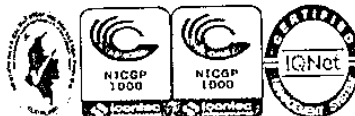
Dada en Armenia, Quindío a los **31 ENE 2019**

PUBLÍQUESE Y CÚMPLASE

JUAN MANUEL RODRIGUEZ-BRITO
 Director Administrativo y Financiero
 Con delegación de funciones como Contralor General del Quindío

	Nombre y apellido	firma	fecha
Proyectado por	Verónica Cifuentes Arias	Veronica Cifuentes A.	31-enero-2019.
Revisado por	Aura María Álvarez C.	Aura M. Álvarez C.	31 ENE 2019

Los arriba firmantes declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales vigentes y por lo tanto, bajo nuestra responsabilidad lo presentamos para la firma.





Control Fiscal con Credibilidad

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION 2019

CONTRALORIA GENERAL DEL QUINDIO

Dirección: Calle 20 Nro. 13-22 piso 3 Edif. Gobernación del Quindío
Email: contactenos@contraloria-quindio.gov.co
Teléfonos: 7444940 - 7444840 - 7445142 Telefax: 7440016
Línea Gratuita: 018000963023

GERMAN BARCO LOPEZ

Contralor General Del Quindío

JUAN MANUEL RODRIGUEZ BRITO

Director Administrativo y Financiero

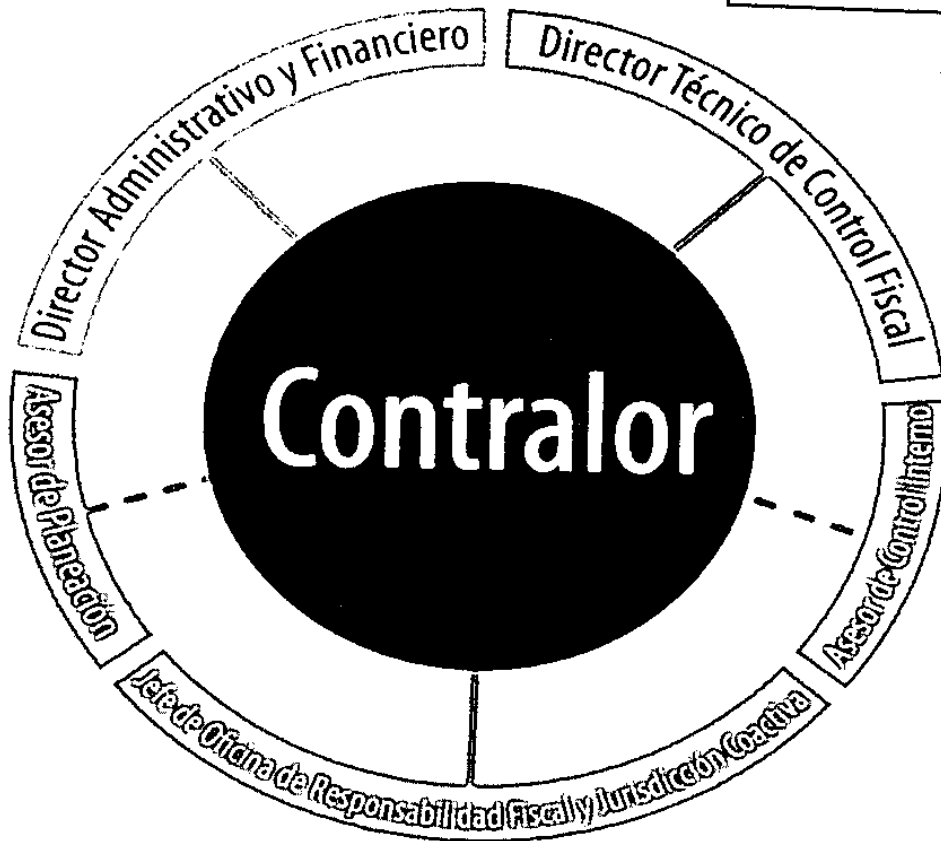
CARLOS ANDRES QUINTERO SEGURA

Asesor De Planeación



Contenido	
Contenido.....	1
Misión.....	3
Visión.....	5
INTRODUCCION.....	5
OBJETIVOS.....	6
OBJETIVO GENERAL.....	7
OBJETIVOS ESPECIFICOS:.....	7
ALCANCE.....	7
DEFINICIONES.....	7
POLITICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION	
10	
POLITICA DE SEGURIDAD DE LA INFORMACIÓN.....	10
POLITICA DE PRIVACIDAD.....	10
POLITICA DE ROLES Y RESPONSABILIDADES.....	11
OBLIGACIONES DE LOS USUARIOS.....	11
UTILIZACIÓN DE RECURSOS Y SISTEMAS DE INFORMACIÓN.....	12
USO DE LA INFRAESTRUCTURA TECNOLÓGICA.....	14
USO DE LOS EQUIPOS DE CÓMPUTO.....	15
USO DEL INTERNET.....	16

ESTRUCTURA DE LA ENTIDAD



Estructura circular

(Ordenanza No. 037 - 20/11/12).

Planta de Personal 38 cargos

*32 Carrera administrativa.

*5 libre nombramiento y remoción.

*1 cargo de período fijo.

Ordenanzas No. 11 - 26/07/17

Adoptada Resolución internas

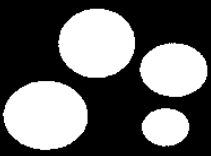
No. 193 - 26/07/17.

Dirección: Gallo 20 Nro. 13-22 piso 3 Edif. Gobernación del Quindío

Email: contactenos@contraloria-quindio.gov.co

Teléfonos: 7444940 - 7444840 - 7445142 Telefax: 7440016

Línea Gratuita: 018000968123



Misión

La Contraloría General del Quindío en cumplimiento del mandato constitucional y legal, vigila la gestión fiscal y ambiental de los sujetos de control, con transparencia y visibilidad, en procura del correcto manejo de los recursos administrados por las entidades públicas, reconociendo a la ciudadanía como principal destinataria de su gestión.

Visión

La Contraloría General del Quindío Para el 2019 será una entidad reconocida en la efectividad del Control Fiscal con independencia en la ejecución de los recursos públicos, en la preservación y cuidado del medio ambiente, en el cumplimiento de las políticas públicas por parte de los sujetos de control con presencia activa de la comunidad.



INTRODUCCION

El plan de Seguridad y Privacidad de la Información busca implantar en la Contraloría General del Quindío, una cultura de calidad y seguridad, que permita operar en una forma confiable con medidas y estándares técnicos de administración y organización de toda la plataforma tecnológica de la entidad, comprometido en el uso de los servicios informáticos proporcionados a los funcionarios por el proceso de Administración de Recursos informáticos de la Dirección de Talento Humano y Servicios de Apoyo a La Gestión.

La seguridad informática, es un asunto donde se deben evaluar y administrar los riesgos apoyados en políticas y estándares que cubran las necesidades de la Contraloría General del Quindío en materia de seguridad. Por este motivo, lo que se busca es fortalecer el aseguramiento de los servicios de Tecnología y la información suministrada o relacionada con la entidad, y cumplir con los estándares de seguridad de los sistemas de información, garantizando la confidencialidad de datos (información y de hardware) en los servicios ofrecidos como en los servicios internos a la CGQ, de acuerdo a lo estipulado en la norma ISO 27001.

Para el desarrollo de este manual se busca estructurarlo con base a ciertos criterios tales como:

- Seguridad Institucional
- Seguridad física y del medio ambiente
- Manejo y control de los equipos informáticos
- Control de usuarios
- Lineamientos legales



OBJETIVOS

OBJETIVO GENERAL

Establecer directrices e implementar los procedimientos necesarios para el uso adecuado de los elementos que componen la infraestructura tecnológica, por parte de los servidores públicos de la Contraloría General del Quindío.

OBJETIVOS ESPECIFICOS:

- Dar un manejo adecuado a los equipos y programas con que cuenta la Entidad, además de obtener el máximo provecho de las herramientas informáticas para el buen desempeño de las funciones.
- Proveer a todos los servidores públicos de la Contraloría de una guía para el uso responsable de la infraestructura tecnológica.

ALCANCE

Aplica para todos los Funcionarios, Colaboradores y Terceros de LA CONTRALORIA GENERAL DEL QUINDIO.

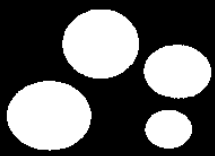
DEFINICIONES

MSPI: Modelo de Seguridad y Privacidad de la Información

- **INTEGRIDAD:** Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.



- **DISPONIBILIDAD:** Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.
- **CONFIDENCIALIDAD:** La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados. Información: Es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.
- **DATO:** Es una representación simbólica (numérica, alfabética, algorítmica, espacial, etc.) de un atributo o variable cuantitativa o cualitativa.
- **COPIAS DE RESPALDO:** Es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.
- **SERVIDOR:** Es una aplicación en ejecución (software) capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia.
- **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/IEC 27000).
- **ACTIVO DE INFORMACIÓN:** Es todo aquello que en la CGQ es considerado importante o de alta validez para la misma ya que puede contener información importante como son en las Bases de Datos con usuarios, contraseñas, números de cuentas, etc.
- **RIESGO:** Es la posibilidad de que una amenaza se produzca, dando lugar a un ataque al equipo. Esto no es otra cosa que la probabilidad de que ocurra el ataque por parte de la amenaza.



Adicionalmente, es importante tener en cuenta algunas de las definiciones estipuladas por el Ministerio de Tecnologías de la Información y Comunicaciones – MINTIC¹ en el modelo de seguridad y privacidad de la información, las cuales son:

- **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).
- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).
- **Ciberseguridad:** Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).
- **Ciberespacio:** Ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización electrónica, la informática y la cibernética. (CONPES 3701, Tomado de la Academia de la lengua Española).
- **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.

POLITICA DE ROLES Y RESPONSABILIDADES

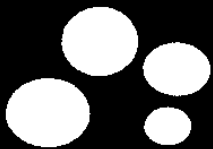
Todos los Funcionarios, Colaboradores y Terceros de la Contraloría General del Quindío deben usar de manera correcta la información que se genera del desempeño de sus funciones laborales y bajo ninguna circunstancia podrán divulgar información con categoría CONFIDENCIAL o RESERVADA en espacios públicos o privados, mediante conversaciones o situaciones que puedan poner en riesgo la seguridad o el buen nombre de la CGQ. Esta restricción se debe cumplir inclusive después de la terminación del vínculo laboral y contractual y debe estar incluida en los Acuerdos de Confidencialidad establecidos por la CGQ.

El proceso de la Administración de Recursos Informáticos, define Roles y Responsabilidades para cada activo de sistemas de información e infraestructura tecnológica, con el fin de crear el procedimiento de solicitud, modificación, eliminación y/o inactivación de usuarios privilegiados.

De igual manera, se debe capacitar a todos los usuarios solicitantes de accesos a componentes tecnológicos sobre el uso y la responsabilidad que implica contar con esos privilegios.

OBLIGACIONES DE LOS USUARIOS

De acuerdo a lo estipulado en esta política de Roles y Responsabilidades, los usuarios de nuestras redes y nuestros sistemas de información deben respetar la integridad de los recursos basados en los sistemas de información, evitar actividades destinadas a



- Los respaldos de información deberán ser almacenados en la caja fuerte de la Entidad al igual que en sitios externos y libres de cualquier daño o posible extracción por terceros.
- Los respaldos se utilizarán únicamente en casos especiales, ya que su contenido es de suma importancia para la Contraloría.

USO DE LA INFRAESTRUCTURA TECNOLOGICA

- La Dirección Administrativa y Financiera, y el Profesional Universitario encargado de sistemas deben realizar un monitoreo permanente a la UPS de la cual depende el sistema eléctrico regulado de la Entidad, al igual que al aire acondicionado del cuarto de datos y de las redes de voz y datos.
- Los puntos de corriente o energía regulados siempre van diferenciados por colores en las tomas eléctricas, esto permitirá identificar fácilmente los puntos protegidos contra variaciones de voltaje.
- La Dirección Administrativa y Financiera y el Profesional Universitario encargado de sistemas tienen la responsabilidad de controlar y llevar un inventario detallado de la infraestructura tecnológica de La Contraloría.
- La Dirección Administrativa y Financiera y el Profesional Universitario encargado de sistemas, velarán por la ejecución oportuna del cronograma de mantenimiento.

- Todos los equipos de cómputo deben estar protegidos por un antivirus, con el fin de minimizar riesgos por ataques de software malintencionados como virus, troyanos, spam, etc.

USO DE LOS EQUIPOS DE CÓMPUTO


- El servidor público al cual se le asigne un equipo de cómputo de la contraloría, es responsable de hacer buen uso del mismo y de la información que este bajo su cargo.
- No ingerir alimentos y bebidas en el área donde utilice el equipo de cómputo.
- No apagar el equipo, sin antes salir adecuadamente del sistema
- Hacer buen uso de los recursos de cómputo
- Realizar respaldos de información crítica periódicamente
- Consultar con el personal de soporte técnico (Ingeniera de sistemas), cualquier duda o situación que se presente relacionada con los equipos informáticos.
- Cuidar las condiciones físicas de limpieza donde se encuentre el equipo
- Los usuarios NO pueden instalar ningún tipo de software en los equipos de propiedad de la Contraloría General del Quindío. Esta actividad es competencia únicamente del equipo de soporte técnico previa verificación de la existencia del licenciamiento.
- Informar a la Dirección Administrativa y Financiera oportunamente sobre las fallas que se puedan presentar en algún equipo de cómputo con el fin de que se lleven a cabo las acciones necesarias para corregirlas.



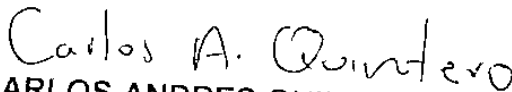
USO DEL INTERNET

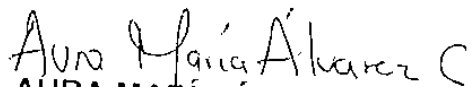
- El usuario es responsable de seguir las instrucciones para el buen uso de los recursos y servicios informáticos evitando cualquier práctica o uso inapropiado que los pueda poner en peligro y a la información de la Entidad. Se considera inapropiado:
 - o Dejar sesiones de trabajo abiertas.
 - o Utilizar los recursos para llevar a cabo actividades fuera de la ley.
 - o Utilizar los recursos para fines particulares en horario laboral.
 - o Distribuir datos o información confidencial.
 - o Utilizar el internet para consulta de páginas con contenidos obscenos.
- Evitar la descarga de programas que no cuentan con las respectivas licencias en la Entidad.
 - Se recomienda con frecuencia cambiar las claves y contraseñas.
 - Abstenerse de abrir correos electrónicos de contenido dudoso.
- La Profesional Universitaria - Ingeniera de Sistemas - podrá restringir el acceso a páginas web no seguras para la Entidad o no necesarias para el cumplimiento de las funciones del usuario.

ORIGINAL FIRMADO


GERMAN BARCO LOPEZ
Contralor General del Quindío

JUAN MANUEL RODRIGUEZ BRITO
Director Administrativo y Financiero


CARLOS ANDRES QUINTERO SEGURA
Asesor de Planeación


AURA MARÍA ÁLVAREZ CIRO
Profesional Universitario-Despacho del Contralor