PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

VIGENCIA FISCAL 2020

CONTRALORIA GENERAL DEL QUINDIO

Armenia, Quindío - Colombia 2020

ITEM	NOMBRE Y APELLIDO	FIRMA	FECHA
Aprobado por:	Rosmira Rodríguez Díaz		
Revisado por:	María Patricia Medina Urrea		
Proyectado por:	Astrid Yaneth Hernández Jaramillo / Fabián Herrera Carmona		

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

VIGENCIA FISCAL 2020

CONTRALORIA GENERAL DEL QUINDIO

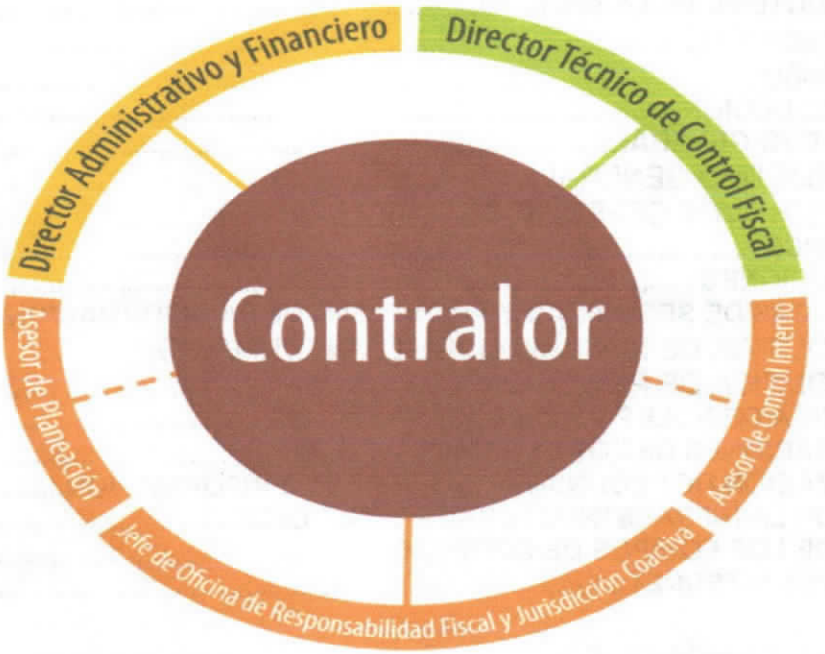
JUAN MANUEL RODRIGUEZ BRITO (E)
CONTRALOR GENERAL DEL QUINDÍO

ROSMIRA RODRIGUEZ DIAZ
DIRECTORA ADMINISTRATIVA Y FINANCIERA

MARIA PATRICIA MEDINA URREA
ASESORA DE PLANEACION

Contenido

1. 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.

1.1. 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.

1.2. Visión

"Para el 2021 la Contraloría General del Quindío, 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".

1. INTRODUCCIÓN

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

2. OBJETIVO GENERAL

2.1. 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.

2.2. OBJETIVOS ESPECÍFICOS

- 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.

3. ALCANCE

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

4. DEFINICIONES

Para el desarrollo de este plan, es importante tener en cuenta las definiciones establecidas en el Plan, las cuales son:

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 alguna de las definiciones estipuladas por el Ministerio de Tecnologías de la Información y Comunicaciones – MINTIC[1] 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.

5. POLITICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

5.1. POLITICA DE SEGURIDAD DE LA INFORMACIÓN

Esta política consiste en que toda persona que ingresa como usuario nuevo de la Contraloría General del Quindío para utilizar equipos de cómputo y hacer uso de servicios informáticos debe aceptar las condiciones de confidencialidad, de uso adecuado de los bienes informáticos y de la información, así como también, debe cumplir y respetar cada una de las directrices impartidas.

La Contraloría General del Quindío, se compromete a otorgar los recursos necesarios para garantizar los tres (3) pilares fundamentales de la Seguridad como son la disponibilidad, integridad y confidencialidad de la información, con el fin de dar cumplimiento a los objetivos institucionales, la estrategia y misión de la CGQ. De igual manera se compromete a velar por la aplicación y cumplimiento adecuado de la presente política de seguridad de la información y todas las que se deriven de ella, por parte de todos los Funcionarios, Colaboradores y Terceros de la CGQ.

5.2. POLITICA DE PRIVACIDAD

La Contraloría General del Quindío establece que el único medio autorizado para el tratamiento de datos personales es el dueño de la información, de acuerdo a la Ley de protección de datos personales 1581 de 2012 decreto 1377 o la que la adicione, modifique o derogue.

6. 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.

7. 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

obtener accesos no autorizados, respetar los derechos de los otros usuarios y respetar las leyes sobre las licencias de software.
Estas pautas aplican para todos los funcionarios de la Entidad, contratistas, pasantes, judicantes y que hagan uso de los recursos de la Contraloría General del Quindío. Quien de forma deliberada o reiterada haga caso omiso de lo expuesto, se podrán ver sujetos a las actuaciones disciplinarias que enmarca la ley.

8. UTILIZACIÓN DE RECURSOS Y SISTEMAS DE INFORMACIÓN

- Todo tipo de Software que se instale en los equipos de cómputo de la Contraloría General del Quindío, debe tener vigente la respectiva licencia que permita su uso de manera legal.

- Los servidores públicos de la Contraloría, no pueden realizar ningún tipo de cambio en la configuración de los aplicativos instalados en los equipos que tienen a su cargo.

- No se debe instalar ningún tipo de aplicación descargada de internet sin previa autorización de la Dirección Administrativa y Financiera o la persona encargada de sistemas, quienes deben verificar la necesidad y conveniencia de dicha instalación.

- Corresponde a la Dirección Administrativa y Financiera, y al profesional universitario encargado de sistemas, realizar la supervisión del software que se encuentra instalado en los equipos de cómputo de la Entidad.

- El acceso de los usuarios a los sistemas de información, será únicamente a los requeridos para desarrollar su trabajo.

- Los aplicativos de la Contraloría deben tener un usuario responsable de su administración.

- Es responsabilidad del usuario de cada equipo verificar que el software antivirus se encuentre en ejecución y vigente en forma permanente.

- La creación, edición inactivación y eliminación de usuarios y contraseñas para el acceso a los aplicativos COVI, SIA y SIA OBSERVA de las entidades sujetas a control, está bajo la responsabilidad del profesional universitario encargado de sistemas con previa autorización de la Dirección Técnica de Control Fiscal.

- Cuando un servidor público se retire de su cargo definitivamente, el Ingeniero de sistemas encargado de los sistemas, debe inactivar sus cuentas y el ingreso a los aplicativos institucionales.

- Las licencias de paquetería de software deben ser custodiadas por el Ingeniero de Sistemas.

- La configuración de los equipos es realizada por la Ingeniero de Sistemas encargado y no deberá ser modificada por los usuarios.

- Cada servidor público es responsable del respaldo de su información de acuerdo con sus necesidades, en caso de las aplicaciones cliente – servidor, el profesional universitario ingeniero de sistemas será el responsable de los respaldos como administrador de la red.

- Se debe realizar copias de Seguridad del Aplicativo XENCO el cual contiene Los procesos de Contabilidad, Nomina, Tesorería y Presupuesto, respaldando con copias internas y externas para minimizar el riesgo de pérdida de la información, así mismo, el servidor cuenta con un disco espejo en el cual se generan copias de seguridad diariamente.

- 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.

9. USO DE LA INFRAESTRUCTURA TECNOLOGICA

- La Dirección Administrativa y Financiera, y el Ingeniero de Sistemas 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 Ingeniero de Sistemas 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 Ingeniero de Sistemas encargado de sistemas, velaran 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 malintencionado como virus, troyano, spam, etc.

10. 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.

11. 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:

- Dejar sesiones de trabajo abiertas.

- Utilizar los recursos para llevar a cabo actividades fuera de la ley.

- Utilizar los recursos para fines particulares en horario laboral.

- Distribuir datos o información confidencial.

- 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.

El Ingeniero 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.

JUAN MANUEL RODRIGUEZ BRITO (E)
CONTRALOR GENERAL DEL QUINDÍO

ROSMIRA RODRIGUEZ DIAZ
DIRECTORA ADMINISTRATIVA Y FINANCIERA

MARIA PATRICIA MEDINA URREA
ASESORA DE PLANEACION