RESOLUCIÓN No. 231

02 SEP 2019

"POR MEDIO DE LA CUAL SE ADOPTA EL MANUAL DE POLÍTICAS DE PRIVACIDAD Y SEGURIDAD INFORMÁTICA PARA LA CONTRALORÍA GENERAL DEL QUINDÍO"

EL DIRECTOR ADMINISTRATIVO Y FINANCIERO con delegación de funciones de CONTRALOR GENERAL DEL QUINDÍO según Resolución No. 224 del 26 de agosto de 2019, en uso de sus atribuciones Constitucionales y Legales, en especial las conferidas por la Ley 489 de 1998, y,

CONSIDERANDO:

A. Que la Ley 1273 de 2009 por medio de la cual se modificó el Código Penal, se creó un nuevo bien jurídico tutelado denominado *"De la protección de la información y de los datos"*- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones; tipificando penalmente las conductas contra la confidencialidad, la integridad y la disponibilidad de los datos de los sistemas informáticos.

B. Que la ley 1712 de 2014 reglamentada por el Decreto 103 de 2015, por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la información Pública en las Instituciones del Estado, estableció los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información.

C. El Decreto 1078 de 2015 dispone que las entidades que conforman la administración pública deberán acatar el cumplimiento de las políticas y los lineamientos de la estrategia de gobierno en línea, estableciendo en su artículo 2.2.9.1.2.1 como uno de sus cuatro componentes el de la seguridad y privacidad de la información, comprendido por las acciones transversales a los componentes de TIC para servicios, TIC para Gobierno abierto y TIC para la Gestión, tendientes a proteger la información y los sistemas de información, acceso, uso, divulgación, interrupción o destrucción no autorizada.

D. Que por medio de CONPES 3854 de 2016 se fijó la política Nacional de seguridad digital, para que las entidades del Estado constituyan mecanismos para la gestión de los riesgos digitales.

E. Que conforme a la normatividad citada surge la necesidad de adoptar una política institucional de privacidad y seguridad de la información, con la que se busca establecer en el interior de la Entidad una cultura de calidad operando en una forma confiable.

F. Que mediante reunión de comité institucional de desempeño del 16 de agosto de 2019, se estudió y aprobó la adopción del Manual de Políticas de Privacidad y Seguridad Informática para la Contraloría General del Quindío.

G. La Contraloría General del Quindío reconoce el valor de su información como uno de sus activos más valiosos y es consciente de la necesidad de su custodia, conservación, disponibilidad, integridad, accesibilidad y confidencialidad en los casos que corresponda, generando una cultura de protección y uso adecuado a través dé la implementación y mejora continua de un sistema de gestión de seguridad de la información, con un enfoque de administración y tratamiento de riesgos asociados y el cumplimiento de todos los requisitos propios de su actividad, legales, reglamentarios y contractuales, que permitan asegurar la confianza de las partes interesadas.

H. Que en atención a lo anteriormente relacionado, se hace necesario adoptar el Manual de Políticas de Privacidad y Seguridad Informática; con el fin de generar una cultura y apropiación de trabajo enfocada a la toma de conciencia para la protección y el uso adecuado de la información por parte de los servidores públicos.

Con base en lo anterior el Director Administrativo y Financiero con delegación de funciones de Contralor General del Quindío,

RESUELVE:

ARTÍCULO PRIMERO: Adoptar el **MANUAL DE POLÍTICAS DE PRIVACIDAD Y SEGURIDAD INFORMÁTICA** de la Contraloría General del Quindío, conforme a la parte motiva y teniendo en cuenta el manual anexo que hace parte integral de la presente Resolución.

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 02 SEP 2019

PUBLÍQUESE Y CÚMPLASE

JUAN MANUEL RODRÍGUEZ BRITO
Director Administrativo y Financiero
Con delegación de funciones de Contralor General del Quindío

	Nombre y apellido	firma	fecha
Proyectado por:	Verónica Cifuentes	Veronica Cifuentes A.	Septiembre 2-2019.
Revisado por:	Aura María Álvarez C.	Aura Mª Alvarez C.	Sep 2/2019
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.			

Manual de Políticas de Privacidad y Seguridad Informática

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: 018000963123

TABLA DE CONTENIDO

1. INTRODUCCIÓN

Con la definición de las políticas de privacidad y seguridad informática se busca establecer en el interior de la Entidad una cultura de calidad operando en una forma confiable. La seguridad informática, es un proceso donde se deben evaluar y administrar los riesgos apoyados en políticas y estándares que cubran las necesidades de la Contraloría General del Departamento de Córdoba en materia de seguridad. Para el desarrollo de este manual se busca estructurarlo en base a ciertos criterios tales como:

- Seguridad Institucional
- Seguridad física y del medio ambiente
- Manejo y control Centro de Computo
- Control de usuarios
- Lineamientos legales

2. OBJETIVO

El objetivo de este documento es establecer las políticas de privacidad y seguridad informática de la Contraloría General del Quindío, con el fin de regular la gestión de la seguridad de la información al interior de la entidad.

3. ALCANCE

Las políticas de privacidad y seguridad de la información cubren todos los aspectos administrativos y de control que deben ser cumplidos por los directivos, funcionarios y terceros que laboren o tengan relación con la Contraloría General del Quindío, para conseguir un adecuado nivel de protección de las características de seguridad y calidad de la información relacionada.

4. JUSTIFICACIÓN

El presente plan de seguridad de la información se define en cumplimiento a sus propósito y obligaciones internos como sectoriales en cuanto a la contribución a la construcción de un estado más eficiente, transparente y participativo a través de la definición del MSPI, al igual que

a lo establecido en el componente de seguridad y privacidad de la información de la estrategia de Gobierno Digital.

5. PRESENTACIÓN DE LA ENTIDAD

MISIÓN

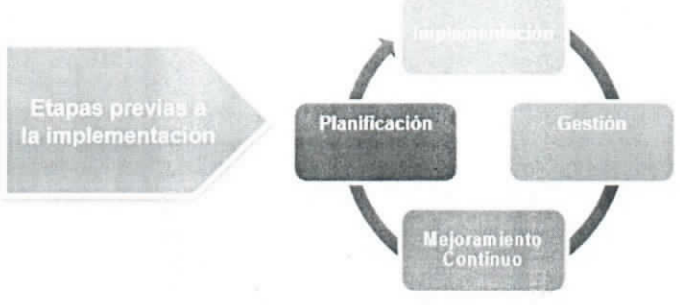
La **Contraloría General del Quindío** en cumplimiento del mandato constitucional y legal, vigila la gestión fiscal y ambiental de los sujetos de control, con transparencia y visibilidad, en procura del correcto manejo de los recursos administrados por las entidades públicas, reconociendo a la ciudadanía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

VISIÓN

La **Contraloría General del Quindío** para el 2019 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.

6. DESCRIPCIÓN DETALLADA DEL MODELO DE SEGURIDAD

Para la etapa inicial de los propósitos de diseño del sistema de gestión de seguridad de la información, se identificó la necesidad de definir las 5 fases que orientarían el ejercicio para los propósitos de protección de la información de la Entidad bajo un modelo sostenible; las fases del ciclo de operación se definen de la siguiente manera basadas en una fase inicial de diagnóstico:



7. FASE PREVIA DE DIAGNOSTICO DEL MANUAL DE POLITICAS DE PRIVACIDAD Y SEGURIDAD INFORMATICA

En esta fase y mediante el uso de herramientas de diagnóstico, se desarrollan actividades de reconocimiento y valoración del estado de gestión, cumplimento de requisitos y lineamientos de seguridad de la información basado con el Modelo de Seguridad y Privacidad de Información de la estrategia de Gobierno Digital del Gobierno Nacional (u otros modelos de seguridad de la información aplicables y reconocidos), y de la implementación de controles de seguridad de la información con visión de mitigar todo tipo de escenario de riesgo asociado que pudiese generar un impacto indeseado a la Entidad.

El resultado de la evaluación de diagnóstico permitirá establecer el nivel de madurez del ciclo de operación del modelo de seguridad y privacidad de la información en la Contraloría General del Quindío y el mapa de ruta para las actividades claves de las fases de diseño y establecimiento del mismo modelo.

8. FASE PLANEACIÓN

Para el desarrollo de esta fase y basado con el resultado de la evaluación de diagnóstico y el análisis de contexto de la Contraloría General del Quindío, se identificarán los aspectos claves que definan y orienten las actividades para los propósitos de seguridad y privacidad de la información, entre ellos, la justificación, el alcance, la política y los objetivos del Modelo de Seguridad y Privacidad de la Información.

9. ALCANCE DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El plan de seguridad y privacidad de la información y lineamientos asociados como directriz de la Contraloría General del Quindío, será de aplicabilidad e implementación para todos los procesos y aspectos administrativos de la organización y de cumplimiento por parte de todos aquellos servidores públicos y terceros que presten sus servicios o tengan algún tipo de relación con la Entidad.

El alcance del Modelo de Seguridad y Privacidad de la Información permitirá a la Contraloría General del Quindío definir los límites sobre los cuales se implementará la seguridad y privacidad de la información, por tanto, deberá tener en cuenta, los procesos que impactan directamente la consecución de los objetivos misionales, procesos, servicios, sistemas de información, ubicaciones físicas, terceros relacionados e interrelaciones del Modelo de Seguridad y Privacidad de la Información con otros procesos.

10. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La política de seguridad de información es la declaración general que representa la posición de la Contraloría General del Quindío frente a la necesidad de protección de su información, al igual que de la preservación de aquellos activos de información que la soportan, por tal motivo define que:

La Contraloría General del Quindío reconoce el valor de su información como uno de sus activos más valiosos y es consciente de la necesidad de su custodia, conservación, disponibilidad, integridad, accesibilidad y confidencialidad en los casos que corresponda, generando una cultura de protección y uso adecuado a través de la implementación y mejora continua de un sistema de gestión de seguridad de la información, con un enfoque de administración y tratamiento de riesgos asociados y el cumplimiento de todos los requisitos propios de su actividad, legales, reglamentarios y contractuales, que permitan asegurar la confianza de las partes interesadas.

11. OBJETIVOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

En beneficio del apoyo y cumplimiento de los propósitos de la política estratégica de seguridad de la información en la Contraloría General del Quindío, se declaran los siguientes objetivos generales:

- Establecer las directrices y lineamientos relativos a seguridad de la información.
- Generar una cultura y apropiación de trabajo enfocada a la toma de conciencia para la protección y el uso adecuado de la información por parte de los servidores públicos.
- Implementar mecanismos de control para la protección de los datos, la información y los recursos asociados que los soportan.
- Asegurar que los riesgos asociados a seguridad de la información se mantienen en un nivel aceptable.
- Mantener un enfoque de cumplimiento estricto de los requisitos legales, normativos o contractuales aplicables y relativos al tratamiento y protección de la información.

12. COMPROMISO DE LA DIRECCIÓN ADMINISTRATIVA

El Contralor General del Quindío aprueba la política de seguridad de la información como muestra de su compromiso y apoyo a las actividades de diseño, implementación, mantenimiento

y mejora continua de políticas y lineamientos consecuentemente orientados a la salvaguardar la confidencialidad, integridad y disponibilidad de la información de la Entidad.

Su compromiso se demostrará a través de:

- La revisión y aprobación de políticas y lineamientos de seguridad de la información.
- La promoción de una cultura de seguridad y protección de la información.
- El apoyo para la divulgación de los propósitos y lineamientos de seguridad de la información a los servidores públicos y partes interesadas.
- La asignación de los recursos necesarios para la implementación y mantenimiento del sistema de gestión de seguridad de la información.
- La realización de actividades de verificación y evaluación del desempeño del sistema de gestión de seguridad de la información de manera periódica.

13. ROLES Y RESPONSABILIDADES DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Contraloría General del Quindío, definirá una estructura de roles y asignación formal de responsabilidades orientados a la seguridad y privacidad de la información en diferentes niveles de la Entidad para permitir la adecuada y oportuna toma de decisiones enfocados al cumplimiento de los objetivos de seguridad y privacidad de la información de la Entidad.

13.1 Asignación De Roles Y Responsabilidades.

Está asociada con la definición de los actores responsables en su actuar y función de la seguridad de la información, cuya asignación no sólo generará las dinámicas propias de un proceso, sino que ampliará la cobertura de la seguridad sobre todos los activos de información en la entidad.

Se identifican responsabilidades en las siguientes áreas:

Dirección Administrativa y Financiera
Dirección Técnica Control Fiscal
Oficina de Planeación
Oficina de Control Interno
Oficina de Contabilidad

Oficina de Pagaduría
Oficina de Responsabilidad Fiscal
Ventanilla de Gestión Documental
Archivo
Oficina Jurídica
Recepción

Responsables de la coordinación de la ejecución del Plan de Acción para implementar el Modelo de Seguridad y Privacidad de la Información:

Dirección Administrativa y Financiera
Oficina de Planeación
Oficina de Control Interno
Oficina Jurídica

14. SEGURIDAD INSTITUCIONAL

Todo el personal usuario de la infraestructura tecnológica de la CONTRALORÍA GENERAL DEL QUINDÍO debe aceptar las condiciones de confidencialidad, de uso adecuado de los bienes informáticos y de la información, así como cumplir y respetar al pie de la letra las directrices impartidas en el presente Manual de Políticas de Privacidad y Seguridad Informática para Usuarios.

Los funcionarios nuevos de la entidad, deberán ser notificados a la Dirección Administrativa y Financiera, que es el área encargada de agregar y eliminar el personal de planta y contratistas y de esta manera asignarle los derechos correspondientes: Equipo de Cómputo, Creación de Usuario para la Red, Perfil de usuario en el Directorio Activo, creación de cuenta de correo institucional o en caso de retiro del funcionario, anular y cancelar los derechos otorgados como usuario informático.

15. POLITICAS Y DIRECTRICES DE SEGURIDAD DE LA INFORMACIÓN

- Lineamientos que describen los principios de seguridad y privacidad de la información definida y ajustada a las necesidades de la Contraloría General del Quindío, en orientación de los propósitos asociados a la protección de la confidencialidad, integridad y disponibilidad de la información y activos que la soportan.

ACCESO Y USO DE INFORMACIÓN.

- Todo servidor público o persona entenderá y asumirá su responsabilidad de protección de la información a través de su acceso y uso apropiados.
- La Contraloría General del Quindío será la dueña de la propiedad intelectual de los avances tecnológicos e intelectuales desarrollados por los servidores públicos o terceros, derivados del objeto y en cumplimiento de las funciones o tareas asignadas bajo acuerdo contractual.
- Todos los servidores públicos o terceros deberán firmar el acuerdo de confidencialidad y transparencia, en el cual se establece la responsabilidad de confidencialidad de la información de la Entidad bajo su responsabilidad.
- Todo servidor público o tercero previo a recibir su cuenta de acceso a los sistemas de información de La Contraloría General del Quindío, deberá firmar y aceptar una declaración de responsabilidad sobre el uso y acciones realizadas con dichas cuentas.
- Los usuarios no deberán almacenar información en discos duros de los equipos de cómputo o virtuales disponibles, archivos de video, música, fotos o cualquier tipo de archivo que no sea de carácter institucional.

CLASIFICACIÓN DE LA INFORMACIÓN

- Toda información al interior de la Contraloría General del Quindío deberá recibir el nivel de clasificación apropiado de acuerdo con las necesidades de protección de la misma y a los riesgos potenciales asociados
- Toda Información clasificada deberá recibir el sistema de etiquetado con la identificación del nivel de clasificación asignado.

MANEJO DISPOSICIÓN DE INFORMACIÓN, MEDIOS Y EQUIPOS

La Dirección Administrativa y Financiera establecerá las directrices necesarias para el manejo de la información, medios y equipos de acuerdo con las labores desempeñadas. Cada una de las dependencias de la Contraloría General del Quindío realizara las respectivas solicitudes de acuerdo a cada una de sus necesidades. De esta manera se realizaran las siguientes acciones:

- Se establecerán controles para evitar la divulgación, modificación, el retiro o la destrucción no autorizada de información almacenada en los medios proporcionados, velando por la disponibilidad y confidencialidad de la información.

- Los medios y equipos donde se almacena la información deberán mantenerse con las medidas de protección físicas y lógicas aplicables, se deberán generar planes de mantenimiento preventivo y correctivo que se requieran.

- Para el retiro de equipos de cómputo por su estado de obsolescencia y/o daño, se deberá garantizar la aplicación del procedimiento de saneamiento, es decir llevar acabo buenas prácticas para la eliminación y/o destrucción de la información con herramientas automáticas que aseguren que la misma no pueda en ningún caso ser recuperada.

- Toda aquella información que por su obsolescencia se encuentre en medio físico papel y ésta no sea confidencial, deberá ser eliminada mediante la técnica de rasgado o picado mediante el uso de equipo especializado.

USO Y PROTECCIÓN DE EQUIPO DE CÓMPUTO

- En equipo de cómputo de propiedad de la Entidad, únicamente se podrá instalar y utilizar software o programas, sistemas de información, herramientas de software que sean licenciados y autorizados por la Entidad.

- Los equipos de cómputo no podrán ser utilizados para actividades de divulgación, propagación o almacenamiento de contenido personal o comercial de publicidad, promociones, ofertas, programas destructivos (virus), propaganda política, material religioso, o cualquier otro uso que no esté autorizado.

USO DE CORREO ELECTRÓNICO

- La Contraloría General del Quindío tendrá el derecho a realizar monitoreo o seguimiento del uso del correo electrónico a todos funcionarios y/o contratistas a quienes se les conceda una cuenta de correo corporativa.

- Los usuarios no deberán participar en correo electrónico que incite o incentive el envío de cadenas o publicidad que no sean interés o estén relacionados con la administración de la Contraloría General del Quindío

- No se deberán realizar el envío o distribución de información catalogada como confidencial, interna o privada dentro o fuera de la Contraloría General del Quindío (sin la autorización correspondiente).

- No se podrá hacer uso de lenguaje ofensivo, inapropiado o con declaraciones de blasfemia, obscenidad, ilegales, incitadores a infringir la ley, hostigamiento basado en sexo, raza, nacionalidad, contenido despectivo o difamatorio en cualquier mensaje electrónico para con sus compañeros, clientes, proveedores u otros; su uso inadecuado, se considerará fuera del alcance y responsabilidad Contraloría General del Quindío, por lo tanto, los daños y perjuicios que pueda llegar a causar, serán de completa responsabilidad del propietario de la cuenta de correo electrónico que la haya generado.

- Se prohíbe el envío de correos masivos al interior de la organización; sólo los usuarios autorizados por el área de comunicaciones podrán enviar dichos correos.

- Está prohibido utilizar el correo electrónico para el intercambio de información o de software que violen las leyes de derechos de autor.

- Es responsabilidad de los usuarios de correo electrónico hacer mantenimiento a su buzón de correo: eliminar mensajes de la bandeja de entrada, archivar mensajes.

USO DE IMPRESORA Y SERVICIO DE IMPRESIÓN

Estas políticas son necesarias con el fin de Asegurar la operación correcta y segura de las impresoras y del servicio de impresión.

Controles

- Es responsabilidad del usuario conocer el adecuado manejo de los equipos de impresión (escáner y fotocopiado) para que no se afecte su correcto funcionamiento.

- Los documentos que se impriman en las impresoras de la Contraloría General del Quindío deberán ser de carácter institucional.

- Labores de reparación o mantenimiento de las impresoras es exclusivo de ejecución por parte de la Dirección Administrativa y ningún otro funcionario o persona podrá realizar dicha actividad.

USO DE INTERNET

La Contraloría General del Quindío consciente de la importancia de Internet como una herramienta para el desempeño de labores, proporcionará los recursos necesarios para asegurar

su disponibilidad a los usuarios que así lo requieran para el desarrollo de sus actividades diarias en la entidad.

Se tendrá en cuenta los siguientes controles para el uso del internet:

- El acceso a internet deberá encontrarse protegido por filtros para disminuir sitios peligrosos que contengan códigos maliciosos o que se encuentren ajenos al servicio, Permitiendo de esta manera aumentar la velocidad de acceso a los sitios necesarios y disminuir el riesgo de virus.
- No navegar por sitios no confiables.
- Se prohíbe el uso de sitios de radios online a excepción de sitios institucionales.
- Se prohíbe el uso de intercambio de archivos a través de sistemas o programas de internet, sin que estos cuenten con la debida acreditación y controles de seguridad.
- Se prohíbe el uso de internet para actividades ilícitas.
- Se prohíbe la descarga que no cumpla con la normativa vigente de copyright y similar.
- Se prohíbe el acceso a los sitios o páginas Web que contengan materiales amenazadores, pornográficos, racistas, sexistas o cualquier otro que degrade la calidad del ser humano, salvo aquellas requeridas por la naturaleza de las funciones institucionales del usuario.
- No compartir sus claves para ingresar a sitios que lo requiera (Bancos, Correo, etc)
- No permitir que el navegador de internet recuerde la contraseña automáticamente.
- Evitar participar en juegos de entretenimiento en línea.
- Si no está navegando por internet, cierre todas las ventanas abiertas.
- Cualquier archivo que se reciba o descargue de internet deberá revisarse con el antivirus para asegurar que no tenga virus.
- Si requiere navegar en algún sitio bloqueado se deberá solicitar a la Dirección administrativa.
- Se reserva el derecho de realizar monitoreo o seguimiento de los accesos a sitios en internet realizados por parte de los funcionarios públicos.

- Se permitirá el acceso a servicios de internet, con lineamientos que garanticen la navegación y uso controlados de componentes del servicio.
- Se restringirá toda posibilidad de descarga de software no autorizado o código malicioso en los equipos de cómputo de la Contraloría General del Quindío a través de internet, así mismo.

- El acceso y uso del servicio de internet se concederá solo para propósitos laborales o fines particulares definidos y aprobados por la Contraloría General del Quindío.
- Para los propósitos de almacenamiento de archivos e información, se dispone del servicio en la nube Drive, al igual que se tiene un espacio en el servidor para realizar las copias.
- Se restringirá el acceso a sitios web dedicados a compartir material audiovisual fotos, videos, streaming tales como Facebook, Youtube, Netflix, etc.
- No se permitirá el acceso a sitios web con contenidos que están en contra de la ley, principios de ética moral de la Contraloría General del Quindío tales como, pornografía, terrorismo, contenidos obscenos, discriminación racial o similar.

16. SEGURIDAD FÍSICA Y DEL MEDIO AMBIENTE

El acceso a los sitios y áreas restringidas se debe notificar a la Dirección Administrativa y Financiera para la autorización correspondiente, y así proteger la información y los bienes informáticos de la entidad.

El usuario o al funcionario deberán reportar de forma inmediata a la Dirección Administrativa y Financiera cuando se detecte riesgo alguno real o potencial sobre equipos de cómputo o de comunicaciones, tales como caídas de agua, choques eléctricos, caídas o golpes o peligro de incendio.

El usuario o funcionario tienen la obligación de proteger las unidades de almacenamiento que se encuentren bajo su responsabilidad, aun cuando no se utilicen y contengan información confidencial o importante.

Es responsabilidad del usuario o funcionario evitar en todo momento la fuga de información de la entidad que se encuentre almacenada en los equipos de cómputo personal que tenga asignados.

17. POLITICA PARA USO DE CONEXIONES REMOTAS

La Contraloría General del Quindío establecerá las circunstancias y requisitos para el establecimiento de conexiones remotas; así mismo, suministrará las herramientas y controles necesarios para que dichas conexiones se realicen de manera segura.

- La Dirección Administrativa y Financiera debe implantar los métodos y controles de seguridad para establecer conexiones remotas. Además restringir las conexiones remotas a los recursos; únicamente se deben permitir estos accesos a personal autorizado y por periodos de tiempo establecidos, de acuerdo con las labores desempeñadas. Se debe verificar la efectividad de los controles aplicados sobre las conexiones remotas a los recursos de manera permanente.

- La Oficina de Control Interno debe, dentro de su autonomía, realizar auditorías sobre los controles implantados para las conexiones remotas. Para realizar estas auditorías la contraloría deberá contar una red VPN que garantice la seguridad en el envió y recepción de la información para evitar la fuga y filtración de información.

- Los usuarios que realizan conexión remota deben contar con las aprobaciones requeridas para establecer dicha conexión a los dispositivos y acatar las condiciones de uso establecidas para dichas conexiones.

18. POLITICA DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACION

La Dirección Administrativa debe proveer medidas de seguridad en sistemas de información desde la fase de requerimientos, y deben ser incorporados en las etapas de desarrollo, implementación y mantenimiento.

- Requerimientos de seguridad de los sistemas: La Dirección Administrativa debe asegurar que todas las actividades relacionadas con el desarrollo y mantenimiento de sistemas de información, consideren la administración de los riesgos de seguridad. Todos los requerimientos de seguridad se deben identificar durante la etapa de requerimientos, al igual que justificar, acordar y documentarse, como parte del manual de políticas de privacidad y seguridad informática.

- Seguridad de las aplicaciones del sistema: Se deben desarrollar estándares que indiquen cómo se deben asegurar los diferentes sistemas y aplicaciones, para minimizar la aparición de errores, pérdidas y modificaciones no autorizadas o usos indebidos en la información de las aplicaciones.

Se deben diseñar controles adecuados en las aplicaciones, para garantizar un correcto procesamiento. Se debe incluir la validación de los datos introducidos, el procesamiento interno y los datos resultantes.

- Seguridad de los sistemas de archivos. Se debe controlar el acceso al sistema de archivos y al código fuente de los programas. La actualización del software aplicativo, las aplicaciones y las librerías, sólo debe ser llevada a cabo por los administradores.

- Seguridad de los procesos de soporte. Se requiere de un control estricto en la implementación de cambios. Los procedimientos de control de cambios deben validar que los procesos de seguridad y control no estén comprometidos; igualmente se debe de cerciorar que los proveedores de apoyo posean acceso sólo a las partes en el sistema necesario para desarrollar su trabajo, que dichos cambios sean aprobados con un procedimiento adecuado y con la documentación correspondiente.

Se deberán estructurar pautas y lineamientos de control de seguridad de la información para las actividades de adquisición, desarrollo y mantenimiento de los sistemas de información de la Contraloría General del Quindío, para las cuales se promulgue la confidencialidad, integridad y disponibilidad como parte integral de los mismos.

19. POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La Contraloría General del Quindío asegurará que tanto los eventos como los incidentes de seguridad de la información sean registrados, analizados y atendidos de manera oportuna, bajo la definición de un protocolo establecido, el cual oriente en las actividades a realizar y en la toma de decisiones oportunas para una mitigación o reducción de impactos indeseados sobre la Entidad.

El procedimiento en cualquiera de estos casos se debe registrar teniendo en cuenta los siguientes pasos:

En caso de falla de un activo se debe:

- Enviar un correo electrónico desde el correo institucional de la oficina al correo de la Dirección Administrativa, donde especifique:

a) nombre del usuario

b) dependencia donde labora

c) datos de contacto celular, teléfono o extensión

d) la falla que se va a reportar siendo muy claros sobre esta.

- En caso de no poder enviar el correo debe comunicarse en su defecto al número del Director Administrativo para la asignación de la persona a cargo de las TI.

- En caso de no ser factible ninguna de las opciones anteriores, también puede comunicarse con la persona encargada de las TI para tomar el servicio.

Es de vital importancia comunicar los fallos a tiempo ya que de esto depende su pronta resolución.

Para el caso de realizar mantenimiento el preventivo semestral:

- Se debe pasar el cronograma de actividades de los mantenimientos donde se especifique la dependencia sobre la cual se van a realizar, así como la fecha en que estos se van a efectuar. Lo anterior con la previa autorización de la Dirección Administrativa.

- En caso de algún cambio en el hardware o software del equipo, este debe ser colocado en la hoja de vida del equipo de cómputo.

20. POLITICA DE GESTION DE PROVEEDORES

La Contraloría General del Quindío identificará pautas para establecer y mantener relaciones claras y fortalecidas con aquellos terceros con quien se establezca una relación contractual bien sea de servicios o de productos, que aseguren el adecuado cumplimiento de los acuerdos establecidos, donde se garantice la aplicación de medidas de seguridad de la información en cumplimiento de los objetivos de la Entidad.

Desde el año 1998 La Contraloría General del Quindío cuenta con el software a la medida para la entidad del Sistema Administrativo y Gerencial "XENCO". Durante los 21 años de funcionamiento, el software ha cumplido a cabalidad con todas las expectativas que se han requerido durante este tiempo, obteniendo como resultado fidelidad al sistema, obtenido capacitaciones a personal, actualización del software, asistencia inmediata a fallos (presencial y remota). el cual contiene los módulos de:

- Contabilidad
- Tesorería
- Presupuesto
- Nomina
- Recursos Humanos

- Activos Fijos
- Bienes e Inmuebles
- Suministros y Mantenimiento de Vehículos y Maquinaria.

El software nos permite tener unas características externas que nos permite realizar más fácil el trabajo que se requiere en el momento de una auditoria, contando con la posibilidad de:

- Sistema en línea que permite la actualización inmediata de la información
- Consulta de Informes por pantalla e Impresora
- Manejo de múltiples usuarios e impresoras
- Manejo amplio de niveles de acceso por aplicación, programa y documentos
- Almacenamiento de información hasta por 99 años
- Capacidad de configuración por el usuario de planes de cuentas, códigos de artículos, terceros y otros, según requerimientos propios.
- Sistema de control de auditoría que registra la fecha, hora, usuario estación de trabajo y modificación efectuada
- Calculadora y libreta dentro del programa
- Alto nivel de validación de datos
- Copias de seguridad, rutinas de mantenimiento y recuperación de archivos desde el menú
- Exportación de datos a otros ambientes o entre módulos
- Importación de datos de otros módulos
- Importación de datos de otros ambientes
- Adaptación a todas las exigencias fiscales y tributarias de la legislación colombiana
- Funcionamiento en forma integrada o modular de cada una de las aplicaciones
- Ayuda en línea y manual de usuario
- Manejo y control de centro de costos en todos los módulos

21. EVALUACION DE DESEMPEÑO DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Con el propósito de conocer los estados de cumplimiento de los objetivos de seguridad de la información, se mantendrán esquemas de seguimiento y medición al cumplimiento de aspectos del modelo de seguridad y privacidad de información que permitan contextualizar una toma de decisiones de manera oportuna.

SEGUIMIENTO Y MEDICIÓN

Para las actividades de seguimiento y medición, la Entidad definirá procedimientos que permitan:

- Definir y orientar actividades para la identificación de situaciones de eventos o incidentes de seguridad y privacidad de la información.
- Definir los esquemas de atención a los eventos e incidentes de seguridad de la información, en beneficio de prevenir y mitigar escenarios de impacto a la Entidad.
- Emprender revisiones regulares de la eficacia del MSPI (que incluyen el cumplir de la política de seguridad de la información, los objetivos, los controles) teniendo en cuenta los resultados de las auditorías de seguridad, incidentes, medición de la eficacia sugeridas y la retroalimentación de las partes interesadas.
- Revisar las valoraciones de riesgos de manera regular, asegurando que los niveles de riesgos residuales son comprendidos y aceptados.
- Realizar ejercicios de auditoría interna del MSPI.
- Realizar actividades de revisión del MSPI por parte de la Alta Dirección de la Entidad.

IDENTIFICACIÓN, VALORACIÓN Y TRATAMIENTO DE RIESGOS.

La identificación de los riesgos en la seguridad de la información permite conocer y entender los riegos de la Contraloría General del Quindío a los que se expone en cada momento. Estos riesgos se clasifican en:

Actos originados por la criminalidad común:

- Sabotaje (ataque físico y electrónico)
- Daños por vandalismo
- Fraude / Estafa

- Robo / Hurto (físico)
- Robo / Hurto de información electrónica
- Virus / Ejecución no autorizado de programas
- Violación a derechos de autor

Riesgos por sucesos de origen físico:

- Incendio
- Inundación
- Sismo
- Polvo
- Falta de ventilación
- Sobrecarga eléctrica
- Falla de corriente (apagones)
- Falla de sistema / Daño disco duro

Negligencia de usuarios/as y decisiones institucionales:

- Falta de inducción, capacitación y sensibilización sobre riesgos
- Mal manejo de sistemas y herramientas
- Utilización de programas no autorizados / software ilegal
- Falta de pruebas de software nuevo con datos productivos
- Perdida de datos
- Infección de sistemas a través de unidades portables sin escaneo
- Manejo inadecuado de datos críticos (codificar, borrar, etc.)
- Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas)
- Compartir contraseñas o permisos a terceros no autorizados
- Transmisión de contraseñas por teléfono
- Acceso electrónico no autorizado a sistemas externos

FORMATO DE DECLARACION Y RESPONSABILIDAD

Ciudad___, Fecha

Doctor
JUAN MANUEL RODRIGUEZ BRITO
Director Administrativo y Financiero
Armenia, Quindío

Certifico

Yo _____ , identificado con cedula de ciudadanía _____conozco y acepto plenamente las obligaciones, compromisos y reglamento de la confidencialidad de la información, uso adecuado de los bienes informáticos y de la información, así como cumplir y respetar al pie de la letra las directrices impartidas en el presente Manual de Políticas de Privacidad y Seguridad Informática.

Atentamente,

_____
JUAN MANUEL RODRIGUEZ BRITO
Director Administrativo y Financiero

_____
NOMBRE Y APELLIDOS
CARGO

CONTRALORÍA GENERAL DEL QUINDÍO	CONTRALORÍA GENERAL DEL QUINDÍO ACTA COMITÉ INSTITUCIONAL DE DESEMPEÑO	Código: FO-GC-03 Fecha: 16/07/2013 Versión: 2 Pagina 1 de2

Número de acta:	010	Tema de la reunión: temas varios	Comité institucional de desempeño

Fecha:	16/08/2019	Hora:	2:30 a,m.	Lugar:	Sala De Juntas

German Barco Lopez - Contralor General			
Juan Manuel Rodriguez- Director Administrativo y Financiero			
Claudia Patricia Gonzales– Directora Técnica de Control Fiscal			
Carlos Andrés Quintero Segura-Asesor de Planeación			
Cielo Muñoz - Asesora de Control Interno			
Claudia Patricia Fernandez Jefe Proceso Responsabilidad Fiscal y Jurisdicción Coactiva			

TEMAS

1. Aprobación Política de seguridad de la información,
2, Aprobacin Esquema de líneas de defensa de la contraloría,
3, Retirar la lnea 1,11 y la 2,5 del plan de acción y plan estratégico, 3, Modificar la línea 2,7 del plan de acción y plan estratégico,
4, Solicitar resolución para retiros y modificaciones.

DESARROLLO DE LOS TEMAS

1- La Doctora Cielo Muñoz Muñoz Solicita la aprobación de la política de seguridad de la información y actualizar la política de riesgos de la entidad, el comité aprueba,

2- La Doctora Cielo Muñoz Muñoz solicita aprobar el Esquema de líneas de defensa de la Contraloría General del Quindío y se Compromete a realizar la capacitacion a los funcionarios, el comité Aprueba,

3- El Señor Contralor propone retirar del plan de acción y plan estratégico la línea 1,11 Preparaciòn de Propuesta de una Metodologia para el Control Fiscal, en razón a que se esta esperando la nueva guía de auditoría GAT para las entidades territoriales, el comité aprueba,

4- El Señor Contralor Solicita se retire la línea 2,5 Promover una reestructuraciòn Administrativa del plan de acción y plan estratégico, teniendo en cuenta la ley de garantías y tiempos previstos para dejar esta acción al próximo Contralor, sin dejar aparte que se dejó todos los estudios pertinentes para cumplirla, El comité Aprueba

5- El Doctor Juan Manuel Rodríguez Brito, Solicita modificar la línea 2,7 Implemetaciòn de un Sistema de Gestiòn Documental, del plan de acción y plan estratégico quedando asé: Gestionar la implementación del SIA ATC con la Auditoría General de la República, El comité aprueba

6- El señor Contralor Solicita se envie todos los planes a los Jefes de Oficina para su revisión respectiva.

7- El señor Contralor Solicita realizar las Resoluciones correspondientes y modificaciones necesarias al plan de acción y plan estratégico, El Comité Aprueba

COMPROMISOS

1	Subir a la Nube La Política de seguridad de la información	control interno	30-ago-19
2	Subir a la Nube el esquema de líneas de defensa de la CGQ	control interno	30-ago-19
3	Retirar la línea 1,11 y 2,5 del plan de acción y plan estratégico	Planeacion	20-ago-19
4	Modificar la línea 2,7 del Plan de Acción y Plan Estratégico	Planeacion	20-ago-19
5	Realizar la Resolución Correspondiente a los cambios Solicitados	Juridica	20-ago-19

Manual de Políticas de Privacidad y Seguridad Informática

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: 018000963123

TABLA DE CONTENIDO

1. INTRODUCCIÓN

Con la definición de las políticas de privacidad y seguridad informática se busca establecer en el interior de la Entidad una cultura de calidad operando en una forma confiable. La seguridad informática, es un proceso donde se deben evaluar y administrar los riesgos apoyados en políticas y estándares que cubran las necesidades de la Contraloría General del Departamento de Córdoba en materia de seguridad. Para el desarrollo de este manual se busca estructurarlo en base a ciertos criterios tales como:

- Seguridad Institucional
- Seguridad física y del medio ambiente
- Manejo y control Centro de Computo
- Control de usuarios
- Lineamientos legales

2. OBJETIVO

El objetivo de este documento es establecer las políticas de privacidad y seguridad informática de la Contraloría General del Quindío, con el fin de regular la gestión de la seguridad de la información al interior de la entidad.

3. ALCANCE

Las políticas de privacidad y seguridad de la información cubren todos los aspectos administrativos y de control que deben ser cumplidos por los directivos, funcionarios y terceros que laboren o tengan relación con la Contraloría General del Quindío, para conseguir un adecuado nivel de protección de las características de seguridad y calidad de la información relacionada.

4. JUSTIFICACIÓN

El presente plan de seguridad de la información se define en cumplimiento a sus propósito y obligaciones internos como sectoriales en cuanto a la contribución a la construcción de un estado más eficiente, transparente y participativo a través de la definición del MSPI, al igual que

a lo establecido en el componente de seguridad y privacidad de la información de la estrategia de Gobierno Digital.

5. PRESENTACIÓN DE LA ENTIDAD

MISIÓN

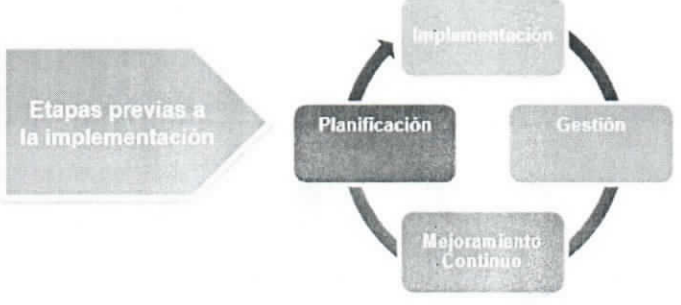
La **Contraloría General del Quindío** en cumplimiento del mandato constitucional y legal, vigila la gestión fiscal y ambiental de los sujetos de control, con transparencia y visibilidad, en procura del correcto manejo de los recursos administrados por las entidades públicas, reconociendo a la ciudadanía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

VISIÓN

La **Contraloría General del Quindío** para el 2019 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.

6. DESCRIPCIÓN DETALLADA DEL MODELO DE SEGURIDAD

Para la etapa inicial de los propósitos de diseño del sistema de gestión de seguridad de la información, se identificó la necesidad de definir las 5 fases que orientarían el ejercicio para los propósitos de protección de la información de la Entidad bajo un modelo sostenible; las fases del ciclo de operación se definen de la siguiente manera basadas en una fase inicial de diagnóstico:



7. FASE PREVIA DE DIAGNOSTICO DEL MANUAL DE POLITICAS DE PRIVACIDAD Y SEGURIDAD INFORMATICA

En esta fase y mediante el uso de herramientas de diagnóstico, se desarrollan actividades de reconocimiento y valoración del estado de gestión, cumplimento de requisitos y lineamientos de seguridad de la información basado con el Modelo de Seguridad y Privacidad de Información de la estrategia de Gobierno Digital del Gobierno Nacional (u otros modelos de seguridad de la información aplicables y reconocidos), y de la implementación de controles de seguridad de la información con visión de mitigar todo tipo de escenario de riesgo asociado que pudiese generar un impacto indeseado a la Entidad.

El resultado de la evaluación de diagnóstico permitirá establecer el nivel de madurez del ciclo de operación del modelo de seguridad y privacidad de la información en la Contraloría General del Quindío y el mapa de ruta para las actividades claves de las fases de diseño y establecimiento del mismo modelo.

8. FASE PLANEACIÓN

Para el desarrollo de esta fase y basado con el resultado de la evaluación de diagnóstico y el análisis de contexto de la Contraloría General del Quindío, se identificarán los aspectos claves que definan y orienten las actividades para los propósitos de seguridad y privacidad de la información, entre ellos, la justificación, el alcance, la política y los objetivos del Modelo de Seguridad y Privacidad de la Información.

9. ALCANCE DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El plan de seguridad y privacidad de la información y lineamientos asociados como directriz de la Contraloría General del Quindío, será de aplicabilidad e implementación para todos los procesos y aspectos administrativos de la organización y de cumplimiento por parte de todos aquellos servidores públicos y terceros que presten sus servicios o tengan algún tipo de relación con la Entidad.

El alcance del Modelo de Seguridad y Privacidad de la Información permitirá a la Contraloría General del Quindío definir los límites sobre los cuales se implementará la seguridad y privacidad de la información, por tanto, deberá tener en cuenta, los procesos que impactan directamente la consecución de los objetivos misionales, procesos, servicios, sistemas de información, ubicaciones físicas, terceros relacionados e interrelaciones del Modelo de Seguridad y Privacidad de la Información con otros procesos.

10. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La política de seguridad de información es la declaración general que representa la posición de la Contraloría General del Quindío frente a la necesidad de protección de su información, al igual que de la preservación de aquellos activos de información que la soportan, por tal motivo define que:

La Contraloría General del Quindío reconoce el valor de su información como uno de sus activos más valiosos y es consciente de la necesidad de su custodia, conservación, disponibilidad, integridad, accesibilidad y confidencialidad en los casos que corresponda, generando una cultura de protección y uso adecuado a través de la implementación y mejora continua de un sistema de gestión de seguridad de la información, con un enfoque de administración y tratamiento de riesgos asociados y el cumplimiento de todos los requisitos propios de su actividad, legales, reglamentarios y contractuales, que permitan asegurar la confianza de las partes interesadas.

11. OBJETIVOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

En beneficio del apoyo y cumplimiento de los propósitos de la política estratégica de seguridad de la información en la Contraloría General del Quindío, se declaran los siguientes objetivos generales:

- Establecer las directrices y lineamientos relativos a seguridad de la información.
- Generar una cultura y apropiación de trabajo enfocada a la toma de conciencia para la protección y el uso adecuado de la información por parte de los servidores públicos.
- Implementar mecanismos de control para la protección de los datos, la información y los recursos asociados que los soportan.
- Asegurar que los riesgos asociados a seguridad de la información se mantienen en un nivel aceptable.
- Mantener un enfoque de cumplimiento estricto de los requisitos legales, normativos o contractuales aplicables y relativos al tratamiento y protección de la información.

12. COMPROMISO DE LA DIRECCIÓN ADMINISTRATIVA

El Contralor General del Quindío aprueba la política de seguridad de la información como muestra de su compromiso y apoyo a las actividades de diseño, implementación, mantenimiento

y mejora continua de políticas y lineamientos consecuentemente orientados a la salvaguardar la confidencialidad, integridad y disponibilidad de la información de la Entidad.

Su compromiso se demostrará a través de:

- La revisión y aprobación de políticas y lineamientos de seguridad de la información.
- La promoción de una cultura de seguridad y protección de la información.
- El apoyo para la divulgación de los propósitos y lineamientos de seguridad de la información a los servidores públicos y partes interesadas.
- La asignación de los recursos necesarios para la implementación y mantenimiento del sistema de gestión de seguridad de la información.
- La realización de actividades de verificación y evaluación del desempeño del sistema de gestión de seguridad de la información de manera periódica.

13. ROLES Y RESPONSABILIDADES DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Contraloría General del Quindío, definirá una estructura de roles y asignación formal de responsabilidades orientados a la seguridad y privacidad de la información en diferentes niveles de la Entidad para permitir la adecuada y oportuna toma de decisiones enfocados al cumplimiento de los objetivos de seguridad y privacidad de la información de la Entidad.

13.1 Asignación De Roles Y Responsabilidades.

Está asociada con la definición de los actores responsables en su actuar y función de la seguridad de la información, cuya asignación no sólo generará las dinámicas propias de un proceso, sino que ampliará la cobertura de la seguridad sobre todos los activos de información en la entidad.

Se identifican responsabilidades en las siguientes áreas:

Dirección Administrativa y Financiera
Dirección Técnica Control Fiscal
Oficina de Planeación
Oficina de Control Interno
Oficina de Contabilidad

Oficina de Pagaduría
Oficina de Responsabilidad Fiscal
Ventanilla de Gestión Documental
Archivo
Oficina Jurídica
Recepción

Responsables de la coordinación de la ejecución del Plan de Acción para implementar el Modelo de Seguridad y Privacidad de la Información:

Dirección Administrativa y Financiera
Oficina de Planeación
Oficina de Control Interno
Oficina Jurídica

14. SEGURIDAD INSTITUCIONAL

Todo el personal usuario de la infraestructura tecnológica de la CONTRALORÍA GENERAL DEL QUINDÍO debe aceptar las condiciones de confidencialidad, de uso adecuado de los bienes informáticos y de la información, así como cumplir y respetar al pie de la letra las directrices impartidas en el presente Manual de Políticas de Privacidad y Seguridad Informática para Usuarios.

Los funcionarios nuevos de la entidad, deberán ser notificados a la Dirección Administrativa y Financiera, que es el área encargada de agregar y eliminar el personal de planta y contratistas y de esta manera asignarle los derechos correspondientes: Equipo de Cómputo, Creación de Usuario para la Red, Perfil de usuario en el Directorio Activo, creación de cuenta de correo institucional o en caso de retiro del funcionario, anular y cancelar los derechos otorgados como usuario informático.

15. POLITICAS Y DIRECTRICES DE SEGURIDAD DE LA INFORMACIÓN

- Lineamientos que describen los principios de seguridad y privacidad de la información definida y ajustada a las necesidades de la Contraloría General del Quindío, en orientación de los propósitos asociados a la protección de la confidencialidad, integridad y disponibilidad de la información y activos que la soportan.

ACCESO Y USO DE INFORMACIÓN.

- Todo servidor público o persona entenderá y asumirá su responsabilidad de protección de la información a través de su acceso y uso apropiados.
- La Contraloría General del Quindío será la dueña de la propiedad intelectual de los avances tecnológicos e intelectuales desarrollados por los servidores públicos o terceros, derivados del objeto y en cumplimiento de las funciones o tareas asignadas bajo acuerdo contractual.
- Todos los servidores públicos o terceros deberán firmar el acuerdo de confidencialidad y transparencia, en el cual se establece la responsabilidad de confidencialidad de la información de la Entidad bajo su responsabilidad.
- Todo servidor público o tercero previo a recibir su cuenta de acceso a los sistemas de información de La Contraloría General del Quindío, deberá firmar y aceptar una declaración de responsabilidad sobre el uso y acciones realizadas con dichas cuentas.
- Los usuarios no deberán almacenar información en discos duros de los equipos de cómputo o virtuales disponibles, archivos de video, música, fotos o cualquier tipo de archivo que no sea de carácter institucional.

CLASIFICACIÓN DE LA INFORMACIÓN

- Toda información al interior de la Contraloría General del Quindío deberá recibir el nivel de clasificación apropiado de acuerdo con las necesidades de protección de la misma y a los riesgos potenciales asociados
- Toda Información clasificada deberá recibir el sistema de etiquetado con la identificación del nivel de clasificación asignado.

MANEJO DISPOSICIÓN DE INFORMACIÓN, MEDIOS Y EQUIPOS

La Dirección Administrativa y Financiera establecerá las directrices necesarias para el manejo de la información, medios y equipos de acuerdo con las labores desempeñadas. Cada una de las dependencias de la Contraloría General del Quindío realizara las respectivas solicitudes de acuerdo a cada una de sus necesidades. De esta manera se realizaran las siguientes acciones:

- Se establecerán controles para evitar la divulgación, modificación, el retiro o la destrucción no autorizada de información almacenada en los medios proporcionados, velando por la disponibilidad y confidencialidad de la información.

- Los medios y equipos donde se almacena la información deberán mantenerse con las medidas de protección físicas y lógicas aplicables, se deberán generar planes de mantenimiento preventivo y correctivo que se requieran.

- Para el retiro de equipos de cómputo por su estado de obsolescencia y/o daño, se deberá garantizar la aplicación del procedimiento de saneamiento, es decir llevar acabo buenas prácticas para la eliminación y/o destrucción de la información con herramientas automáticas que aseguren que la misma no pueda en ningún caso ser recuperada.

- Toda aquella información que por su obsolescencia se encuentre en medio físico papel y ésta no sea confidencial, deberá ser eliminada mediante la técnica de rasgado o picado mediante el uso de equipo especializado.

USO Y PROTECCIÓN DE EQUIPO DE CÓMPUTO

- En equipo de cómputo de propiedad de la Entidad, únicamente se podrá instalar y utilizar software o programas, sistemas de información, herramientas de software que sean licenciados y autorizados por la Entidad.

- Los equipos de cómputo no podrán ser utilizados para actividades de divulgación, propagación o almacenamiento de contenido personal o comercial de publicidad, promociones, ofertas, programas destructivos (virus), propaganda política, material religioso, o cualquier otro uso que no esté autorizado.

USO DE CORREO ELECTRÓNICO

- La Contraloría General del Quindío tendrá el derecho a realizar monitoreo o seguimiento del uso del correo electrónico a todos funcionarios y/o contratistas a quienes se les conceda una cuenta de correo corporativa.

- Los usuarios no deberán participar en correo electrónico que incite o incentive el envío de cadenas o publicidad que no sean interés o estén relacionados con la administración de la Contraloría General del Quindío

- No se deberán realizar el envío o distribución de información catalogada como confidencial, interna o privada dentro o fuera de la Contraloría General del Quindío (sin la autorización correspondiente).

- No se podrá hacer uso de lenguaje ofensivo, inapropiado o con declaraciones de blasfemia, obscenidad, ilegales, incitadores a infringir la ley, hostigamiento basado en sexo, raza, nacionalidad, contenido despectivo o difamatorio en cualquier mensaje electrónico para con sus compañeros, clientes, proveedores u otros; su uso inadecuado, se considerará fuera del alcance y responsabilidad Contraloría General del Quindío, por lo tanto, los daños y perjuicios que pueda llegar a causar, serán de completa responsabilidad del propietario de la cuenta de correo electrónico que la haya generado.
- Se prohíbe el envío de correos masivos al interior de la organización; sólo los usuarios autorizados por el área de comunicaciones podrán enviar dichos correos.
- Está prohibido utilizar el correo electrónico para el intercambio de información o de software que violen las leyes de derechos de autor.
- Es responsabilidad de los usuarios de correo electrónico hacer mantenimiento a su buzón de correo: eliminar mensajes de la bandeja de entrada, archivar mensajes.

USO DE IMPRESORA Y SERVICIO DE IMPRESIÓN

Estas políticas son necesarias con el fin de Asegurar la operación correcta y segura de las impresoras y del servicio de impresión.

Controles

- Es responsabilidad del usuario conocer el adecuado manejo de los equipos de impresión (escáner y fotocopiado) para que no se afecte su correcto funcionamiento.
- Los documentos que se impriman en las impresoras de la Contraloría General del Quindío deberán ser de carácter institucional.
- Labores de reparación o mantenimiento de las impresoras es exclusivo de ejecución por parte de la Dirección Administrativa y ningún otro funcionario o persona podrá realizar dicha actividad.

USO DE INTERNET

La Contraloría General del Quindío consciente de la importancia de Internet como una herramienta para el desempeño de labores, proporcionará los recursos necesarios para asegurar

su disponibilidad a los usuarios que así lo requieran para el desarrollo de sus actividades diarias en la entidad.

Se tendrá en cuenta los siguientes controles para el uso del internet:

- El acceso a internet deberá encontrarse protegido por filtros para disminuir sitios peligrosos que contengan códigos maliciosos o que se encuentren ajenos al servicio, Permitiendo de esta manera aumentar la velocidad de acceso a los sitios necesarios y disminuir el riesgo de virus.
- No navegar por sitios no confiables.
- Se prohíbe el uso de sitios de radios online a excepción de sitios institucionales.
- Se prohíbe el uso de intercambio de archivos a través de sistemas o programas de internet, sin que estos cuenten con la debida acreditación y controles de seguridad.
- Se prohíbe el uso de internet para actividades ilícitas.
- Se prohíbe la descarga que no cumpla con la normativa vigente de copyright y similar.
- Se prohíbe el acceso a los sitios o páginas Web que contengan materiales amenazadores, pornográficos, racistas, sexistas o cualquier otro que degrade la calidad del ser humano, salvo aquellas requeridas por la naturaleza de las funciones institucionales del usuario.
- No compartir sus claves para ingresar a sitios que lo requiera (Bancos, Correo, etc)
- No permitir que el navegador de internet recuerde la contraseña automáticamente.
- Evitar participar en juegos de entretenimiento en línea.
- Si no está navegando por internet, cierre todas las ventanas abiertas.
- Cualquier archivo que se reciba o descargue de internet deberá revisarse con el antivirus para asegurar que no tenga virus.
- Si requiere navegar en algún sitio bloqueado se deberá solicitar a la Dirección administrativa.
- Se reserva el derecho de realizar monitoreo o seguimiento de los accesos a sitios en internet realizados por parte de los funcionarios públicos.

- Se permitirá el acceso a servicios de internet, con lineamientos que garanticen la navegación y uso controlados de componentes del servicio.
- Se restringirá toda posibilidad de descarga de software no autorizado o código malicioso en los equipos de cómputo de la Contraloría General del Quindío a través de internet, así mismo.

- El acceso y uso del servicio de internet se concederá solo para propósitos laborales o fines particulares definidos y aprobados por la Contraloría General del Quindío.
- Para los propósitos de almacenamiento de archivos e información, se dispone del servicio en la nube Drive, al igual que se tiene un espacio en el servidor para realizar las copias.
- Se restringirá el acceso a sitios web dedicados a compartir material audiovisual fotos, videos, streaming tales como Facebook, Youtube, Netflix, etc.
- No se permitirá el acceso a sitios web con contenidos que están en contra de la ley, principios de ética moral de la Contraloría General del Quindío tales como, pornografía, terrorismo, contenidos obscenos, discriminación racial o similar.

16. SEGURIDAD FÍSICA Y DEL MEDIO AMBIENTE

El acceso a los sitios y áreas restringidas se debe notificar a la Dirección Administrativa y Financiera para la autorización correspondiente, y así proteger la información y los bienes informáticos de la entidad.

El usuario o al funcionario deberán reportar de forma inmediata a la Dirección Administrativa y Financiera cuando se detecte riesgo alguno real o potencial sobre equipos de cómputo o de comunicaciones, tales como caídas de agua, choques eléctricos, caídas o golpes o peligro de incendio.

El usuario o funcionario tienen la obligación de proteger las unidades de almacenamiento que se encuentren bajo su responsabilidad, aun cuando no se utilicen y contengan información confidencial o importante.

Es responsabilidad del usuario o funcionario evitar en todo momento la fuga de información de la entidad que se encuentre almacenada en los equipos de cómputo personal que tenga asignados.

17. POLITICA PARA USO DE CONEXIONES REMOTAS

La Contraloría General del Quindío establecerá las circunstancias y requisitos para el establecimiento de conexiones remotas; así mismo, suministrará las herramientas y controles necesarios para que dichas conexiones se realicen de manera segura.

- La Dirección Administrativa y Financiera debe implantar los métodos y controles de seguridad para establecer conexiones remotas. Además restringir las conexiones remotas a los recursos; únicamente se deben permitir estos accesos a personal autorizado y por periodos de tiempo establecidos, de acuerdo con las labores desempeñadas. Se debe verificar la efectividad de los controles aplicados sobre las conexiones remotas a los recursos de manera permanente.

- La Oficina de Control Interno debe, dentro de su autonomía, realizar auditorías sobre los controles implantados para las conexiones remotas. Para realizar estas auditorías la contraloría deberá contar una red VPN que garantice la seguridad en el envió y recepción de la información para evitar la fuga y filtración de información.

- Los usuarios que realizan conexión remota deben contar con las aprobaciones requeridas para establecer dicha conexión a los dispositivos y acatar las condiciones de uso establecidas para dichas conexiones.

18. POLITICA DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACION

La Dirección Administrativa debe proveer medidas de seguridad en sistemas de información desde la fase de requerimientos, y deben ser incorporados en las etapas de desarrollo, implementación y mantenimiento.

- Requerimientos de seguridad de los sistemas: La Dirección Administrativa debe asegurar que todas las actividades relacionadas con el desarrollo y mantenimiento de sistemas de información, consideren la administración de los riesgos de seguridad. Todos los requerimientos de seguridad se deben identificar durante la etapa de requerimientos, al igual que justificar, acordar y documentarse, como parte del manual de políticas de privacidad y seguridad informática.

- Seguridad de las aplicaciones del sistema: Se deben desarrollar estándares que indiquen cómo se deben asegurar los diferentes sistemas y aplicaciones, para minimizar la aparición de errores, pérdidas y modificaciones no autorizadas o usos indebidos en la información de las aplicaciones.

Se deben diseñar controles adecuados en las aplicaciones, para garantizar un correcto procesamiento. Se debe incluir la validación de los datos introducidos, el procesamiento interno y los datos resultantes.

- Seguridad de los sistemas de archivos. Se debe controlar el acceso al sistema de archivos y al código fuente de los programas. La actualización del software aplicativo, las aplicaciones y las librerías, sólo debe ser llevada a cabo por los administradores.

- Seguridad de los procesos de soporte. Se requiere de un control estricto en la implementación de cambios. Los procedimientos de control de cambios deben validar que los procesos de seguridad y control no estén comprometidos; igualmente se debe de cerciorar que los proveedores de apoyo posean acceso sólo a las partes en el sistema necesario para desarrollar su trabajo, que dichos cambios sean aprobados con un procedimiento adecuado y con la documentación correspondiente.

Se deberán estructurar pautas y lineamientos de control de seguridad de la información para las actividades de adquisición, desarrollo y mantenimiento de los sistemas de información de la Contraloría General del Quindío, para las cuales se promulgue la confidencialidad, integridad y disponibilidad como parte integral de los mismos.

19. POLÍTICA DE GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La Contraloría General del Quindío asegurará que tanto los eventos como los incidentes de seguridad de la información sean registrados, analizados y atendidos de manera oportuna, bajo la definición de un protocolo establecido, el cual oriente en las actividades a realizar y en la toma de decisiones oportunas para una mitigación o reducción de impactos indeseados sobre la Entidad.

El procedimiento en cualquiera de estos casos se debe registrar teniendo en cuenta los siguientes pasos:

En caso de falla de un activo se debe:

- Enviar un correo electrónico desde el correo institucional de la oficina al correo de la Dirección Administrativa, donde especifique:

a) nombre del usuario

b) dependencia donde labora

c) datos de contacto celular, teléfono o extensión

d) la falla que se va a reportar siendo muy claros sobre esta.

- En caso de no poder enviar el correo debe comunicarse en su defecto al número del Director Administrativo para la asignación de la persona a cargo de las TI.

- En caso de no ser factible ninguna de las opciones anteriores, también puede comunicarse con la persona encargada de las TI para tomar el servicio.

Es de vital importancia comunicar los fallos a tiempo ya que de esto depende su pronta resolución.

Para el caso de realizar mantenimiento el preventivo semestral:

- Se debe pasar el cronograma de actividades de los mantenimientos donde se especifique la dependencia sobre la cual se van a realizar, así como la fecha en que estos se van a efectuar. Lo anterior con la previa autorización de la Dirección Administrativa.

- En caso de algún cambio en el hardware o software del equipo, este debe ser colocado en la hoja de vida del equipo de cómputo.

20. POLITICA DE GESTION DE PROVEEDORES

La Contraloría General del Quindío identificará pautas para establecer y mantener relaciones claras y fortalecidas con aquellos terceros con quien se establezca una relación contractual bien sea de servicios o de productos, que aseguren el adecuado cumplimiento de los acuerdos establecidos, donde se garantice la aplicación de medidas de seguridad de la información en cumplimiento de los objetivos de la Entidad.

Desde el año 1998 La Contraloría General del Quindío cuenta con el software a la medida para la entidad del Sistema Administrativo y Gerencial "XENCO". Durante los 21 años de funcionamiento, el software ha cumplido a cabalidad con todas las expectativas que se han requerido durante este tiempo, obteniendo como resultado fidelidad al sistema, obtenido capacitaciones a personal, actualización del software, asistencia inmediata a fallos (presencial y remota). el cual contiene los módulos de:

- Contabilidad
- Tesorería
- Presupuesto
- Nomina
- Recursos Humanos

- Activos Fijos
- Bienes e Inmuebles
- Suministros y Mantenimiento de Vehículos y Maquinaria.

El software nos permite tener unas características externas que nos permite realizar más fácil el trabajo que se requiere en el momento de una auditoria, contando con la posibilidad de:

- Sistema en línea que permite la actualización inmediata de la información
- Consulta de Informes por pantalla e Impresora
- Manejo de múltiples usuarios e impresoras
- Manejo amplio de niveles de acceso por aplicación, programa y documentos
- Almacenamiento de información hasta por 99 años
- Capacidad de configuración por el usuario de planes de cuentas, códigos de artículos, terceros y otros, según requerimientos propios.
- Sistema de control de auditoría que registra la fecha, hora, usuario estación de trabajo y modificación efectuada
- Calculadora y libreta dentro del programa
- Alto nivel de validación de datos
- Copias de seguridad, rutinas de mantenimiento y recuperación de archivos desde el menú
- Exportación de datos a otros ambientes o entre módulos
- Importación de datos de otros módulos
- Importación de datos de otros ambientes
- Adaptación a todas las exigencias fiscales y tributarias de la legislación colombiana
- Funcionamiento en forma integrada o modular de cada una de las aplicaciones
- Ayuda en línea y manual de usuario
- Manejo y control de centro de costos en todos los módulos

21. EVALUACION DE DESEMPEÑO DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Con el propósito de conocer los estados de cumplimiento de los objetivos de seguridad de la información, se mantendrán esquemas de seguimiento y medición al cumplimiento de aspectos del modelo de seguridad y privacidad de información que permitan contextualizar una toma de decisiones de manera oportuna.

SEGUIMIENTO Y MEDICIÓN

Para las actividades de seguimiento y medición, la Entidad definirá procedimientos que permitan:

- Definir y orientar actividades para la identificación de situaciones de eventos o incidentes de seguridad y privacidad de la información.
- Definir los esquemas de atención a los eventos e incidentes de seguridad de la información, en beneficio de prevenir y mitigar escenarios de impacto a la Entidad.
- Emprender revisiones regulares de la eficacia del MSPI (que incluyen el cumplir de la política de seguridad de la información, los objetivos, los controles) teniendo en cuenta los resultados de las auditorías de seguridad, incidentes, medición de la eficacia sugeridas y la retroalimentación de las partes interesadas.
- Revisar las valoraciones de riesgos de manera regular, asegurando que los niveles de riesgos residuales son comprendidos y aceptados.
- Realizar ejercicios de auditoría interna del MSPI.
- Realizar actividades de revisión del MSPI por parte de la Alta Dirección de la Entidad.

IDENTIFICACIÓN, VALORACIÓN Y TRATAMIENTO DE RIESGOS.

La identificación de los riesgos en la seguridad de la información permite conocer y entender los riegos de la Contraloría General del Quindío a los que se expone en cada momento. Estos riesgos se clasifican en:

Actos originados por la criminalidad común:

- Sabotaje (ataque físico y electrónico)
- Daños por vandalismo
- Fraude / Estafa

- Robo / Hurto de información electrónica
- Virus / Ejecución no autorizado de programas
- Violación a derechos de autor

Riesgos por sucesos de origen físico:

- Incendio
- Inundación
- Sismo
- Polvo
- Falta de ventilación
- Sobrecarga eléctrica
- Falla de corriente (apagones)
- Falla de sistema / Daño disco duro

Negligencia de usuarios/as y decisiones institucionales:

- Falta de inducción, capacitación y sensibilización sobre riesgos
- Mal manejo de sistemas y herramientas
- Utilización de programas no autorizados / software ilegal
- Falta de pruebas de software nuevo con datos productivos
- Perdida de datos
- Infección de sistemas a través de unidades portables sin escaneo
- Manejo inadecuado de datos críticos (codificar, borrar, etc.)
- Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas)
- Compartir contraseñas o permisos a terceros no autorizados
- Transmisión de contraseñas por teléfono
- Acceso electrónico no autorizado a sistemas externos

FORMATO DE DECLARACION Y RESPONSABILIDAD

Armenia, Septiembre 2 de 2019

Doctor
GERMAN BARCO LÓPEZ
Contralor General del Quindío
Armenia, Quindío

Certifico

Yo JUAN MANUEL RODRIGUEZ BRITO, identificado con cedula de ciudadanía 18.471.146, conozco y acepto plenamente las obligaciones, compromisos y reglamento de la confidencialidad de la información, uso adecuado de los bienes informáticos y de la información, así como cumplir y respetar al pie de la letra las directrices impartidas en el presente Manual de Políticas de Privacidad y Seguridad Informática.

Atentamente,

JUAN MANUEL RODRIGUEZ BRITO
Director Administrativo y Financiero