RESOLUCION No. 039

30 DE ENERO DE 2023

"POR MEDIO DE LA CUAL SE ADOPTA EL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA CONTRALORÍA DEL DEPARTAMENTO DEL QUINDIO PARA LA VIGENCIA 2023"

LA CONTRALORA GENERAL DEL QUINDÍO, en uso de sus facultades Constitucionales y legales y,

CONSIDERANDO:

A. Que las Contralorías Departamentales son organismos de carácter técnico, dotadas de autonomía administrativa, presupuestal y contractual, de conformidad con lo dispuesto en el artículo 272 de la Constitución Política de Colombia (Modificado por el artículo 4° del Acto Legislativo 04 de 2019, concordante con el artículo 66 de la ley 42 de 1993 y el artículo 2 de la ley 330 de 1996).

B. Que el Plan de tratamiento de riesgos de seguridad y privacidad de la Información de la Contraloría General del Quindío, está orientado a crear una cultura de carácter preventivo, con el propósito de comprender el concepto de riesgo y planear acciones que minimicen la afectación a la Entidad en caso de la materialización de los mismos; así como buscar estrategias que permitan la identificación, análisis, control, evaluación y seguimiento de manera objetiva a dichos riesgos, adoptando buenas prácticas en el manejo de las tecnologías de la información y la comunicación.

C. Que el objetivo del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, es definir los parámetros para el tratamiento de los riesgos de seguridad y privacidad de la información a los que pueda estar expuesta la Contraloría General del Quindío, preservando la integridad, confidencialidad, seguridad y privacidad de la información.

D. Que a través de la implementación de este plan, se pretende hacer eficientemente la gestión y tratamiento de los riesgos de la seguridad y privacidad de la información, con el fin de llevar a cabo buenas prácticas que ayuden a prevenir o mitigar las eventualidades que de alguna manera afecten el cumplimiento de la misionalidad de la Entidad y el logro de sus objetivos, dando lineamientos que contribuyan a evidenciar, analizar, controlar, evaluar y minimizar la ocurrencia de riesgos.

E. Que corresponde a la Dirección Administrativa y Financiera de la Contraloría General del Quindío, aplicar las medidas de seguridad para proteger y estar preparados para afrontar contingencias y desastres de diversos tipos.

F. Que el Decreto 1083 del 26 de mayo de 2015 "*Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública*" adicionado por el artículo 1° del Decreto Nacional 612 de 2018, establece en su artículo 2.2.22.3.14:

"ARTÍCULO 2.2.22.3.14. Adicionado por el art. 1, Decreto Nacional 612 de 2018. <El texto adicionado es el siguiente> 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 publicarlos, 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 1757de 2015.

G. Que de acuerdo a la norma citada anteriormente, el PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN vigencia 2023, deberá estar integrado en el plan de acción y publicado a más tardar el 31 de enero de la presente vigencia

H. Que el Comité Institucional de Gestión y Desempeño de la Contraloría General del Departamento del Quindío, aprobó el PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN vigencia 2023.

Que en mérito de lo anterior, la Contralora General del Quindío;

RESUELVE:

ARTÍCULO PRIMERO: Adoptar el PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2023 de la Contraloría General del Quindío, conforme a la parte motiva y teniendo en cuenta el plan 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, el 30 de enero de 2023

PUBLÍQUESE Y CÚMPLASE

CLAUDIA CARDONA CAMPO
Contralora General del Quindío

	Nombre y apellido	firma	Fecha
Proyectado por	Aura María Álvarez Ciro	Aura Ma Alvarez Ciro	Enero 30 de 2023
Revisado por	Mario German Rodríguez Cifuentes		Enero 30 de 2023
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.			

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

VIGENCIA FISCAL
2023

CONTRALORIA GENERAL
DEL QUINDIO

Armenia, Quindío - Colombia
2023

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

VIGENCIA FISCAL 2023

CONTRALORIA GENERAL DEL QUINDIO

CLAUDIA CARDONA CAMPO
CONTRALORA GENERAL DEL QUINDÍO

MARIO GERMAN RODRÍGUEZ CIFUENTES
DIRECTOR ADMINISTRATIVO Y FINANCIERO

CLAUDIA LORENA LÓPEZ MURILLAS
ASESOR DE PLANEACION

DIANA MARCELA BERNAL OCHOA
PROFESIONAL UNIVERSITARIA – ING. DE SISTEMAS

ANGELICA YOHANA MONTOYA HERNANDEZ
TÉCNICO OPERATIVO – ADMINISTRADORA DE SISTEMAS

Contenido

1. ESTRUCTURA DE LA ENTIDAD

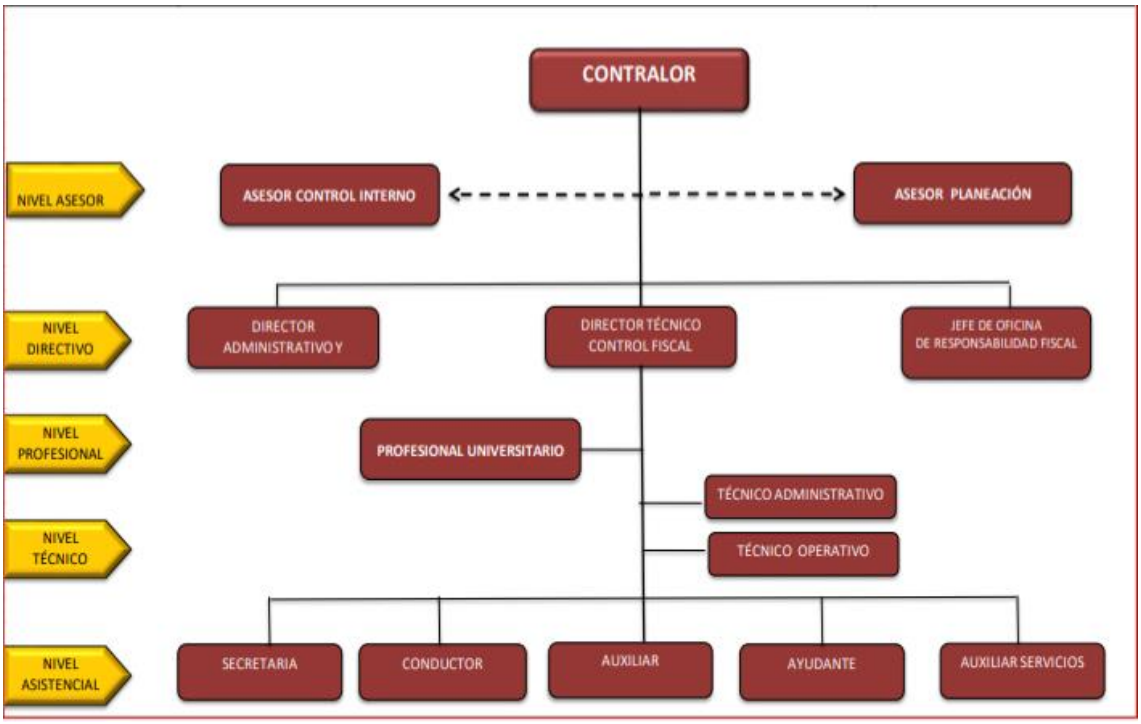

Ilustración 1. Estructura organizacional de la entidad

Estructura Organizacional

Ordenanza No. 037 del 20 de noviembre de 2012 - Planta de personal 38 cargos: 32 de carrera administrativa, 5 de libre nombramiento y remoción y 1 cargo de período fijo.

Ordenanzas No. 11 del 26 de julio de 2017 adoptada mediante resolución interna No. 193 del 26 de julio de 2017.

Mediante resolución No. 092 del 30 de marzo de 2022 julio 13 de 2020 se adoptó el Plan Estratégico Institucional 2022 – 2025 “Hacia un control fiscal oportuno, incluyente y ambiental”.

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 objetividad, en procura de que el manejo de los recursos públicos

sea administrado con eficiencia, eficacia y economía, reconociendo a la ciudadanía como principal destinataria de su gestión.

1.2. Visión

En el 2025, La Contraloría General del Quindío será reconocida a nivel departamental y nacional como un Órgano de Control Fiscal efectivo, que logra sus metas con base en los principios de integridad y calidad, fomentando así, un buen manejo de los recursos públicos por parte de las entidades vigiladas, lo cual proporcionará una mejor calidad de vida a todos los Quindianos.

2. INTRODUCCIÓN

El Plan de tratamiento de riesgos de seguridad y privacidad de la Información de la Contraloría General del Quindío, está orientado a crear una cultura de carácter preventivo, con el propósito de comprender el concepto de riesgo y planear acciones que minimicen la afectación a la Entidad, en caso de la materialización de los mismos. Así como buscar estrategias que permitan la identificación, análisis, control, evaluación y seguimiento de manera objetiva a dichos riesgos, adoptando buenas prácticas en el manejo de las tecnologías de la información y la comunicación.

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 la protección de los servicios de Tecnología y la información de 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.

3. OBJETIVOS

3.1. OBJETIVO GENERAL

Definir los parámetros para el tratamiento de los riesgos de seguridad y privacidad de la información a los que pueda estar expuesta la Contraloría General del Quindío, preservando la integridad, confidencialidad, seguridad y privacidad de la información.

3.2. OBJETIVOS ESPECÍFICOS

- Garantizar la continuidad de las operaciones de los principales elementos que componen los sistemas de información.
- Definir actividades para proteger la infraestructura tecnológica contra los daños y perjuicios producidos por corte de servicios, fenómenos naturales o humanos.
- Realizar un análisis de los posibles riesgos a los cuales puede estar expuesta la infraestructura tecnológica, para reducir su impacto y probabilidad de ocurrencia y reanudar los procesos, en caso de desastres, en el menor tiempo posible.

4. ALCANCE

A través de la implementación de este plan, se pretende hacer eficientemente la gestión y tratamiento de los riesgos de la seguridad y privacidad de la información, con el fin de llevar a cabo buenas prácticas que ayuden a prevenir o mitigar las eventualidades que de alguna manera afecten el cumplimiento de la misionalidad de la Entidad y el logro de sus objetivos, dando lineamientos que contribuyan a evidenciar, analizar, controlar, evaluar y minimizar la ocurrencia de riesgos.

5. DEFINICIONES

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).

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).

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.

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.

Riesgo*:* Es la vulnerabilidad de un activo o bien, ante un posible o potencial perjuicio o daño.

Vulnerabilidad: es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

Probabilidad: es la posibilidad de que la amenaza aproveche la vulnerabilidad para materializar el riesgo.

6. POLITICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

6.1. 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, 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 Entidad. 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.

6.2. 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 aquella que la adicione, modifique o derogue.

6.3. POLITICA DE ADMINISTRACION DE RIESGOS

La Contraloría General del Quindío se compromete a establecer los lineamientos para una eficiente gestión y tratamiento de los riesgos de la seguridad y privacidad de la información, mediante mecanismos y controles encaminados a la prevención y detección de sucesos que puedan poner en riesgo el cumplimiento de los objetivos estratégicos y la misionalidad de la Entidad, así como respuestas oportunas a la ocurrencia de los mismos.

Mediante la política de administración de riesgos se debe tener en cuenta cómo evitar, prevenir, reducir o mitigar y controlar la ocurrencia de los riesgos que afecten el normal funcionamiento de la Entidad.

7. ROLES Y RESPONSABILIDADES

Todos los funcionarios y contratistas 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 Entidad. Esta restricción se debe cumplir inclusive después de la terminación del vínculo laboral o 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.

7.1. OBLIGACIONES DE LOS USUARIOS

Todos los usuarios de nuestras redes, equipos de cómputo y 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 las leyes sobre las licencias de software o derechos de autor.

Estas pautas aplican para todos los funcionarios de la Entidad, contratistas, pasantes, judicantes 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. ANÁLISIS DE EVALUACIÓN DE RIESGOS Y ESTRATEGIAS

8.1. CRITERIOS DE ANÁLISIS

Para la clasificación de los riesgos de las Tecnologías de la Información de la Contraloría General del Quindío, se han considerado tres criterios:

Riesgos Naturales: como el mal tiempo, terremotos, etc.

Riesgos Tecnológicos: como fallas de energía y accidentes de transmisión y transporte de información.

Riesgos Sociales: como actos terroristas.

8.2. ANÁLISIS DEL RIESGO

El objetivo del análisis es establecer una valoración y priorización de los riesgos, con el fin de clasificarlos y proveer información para establecer su nivel y las acciones que se van a implementar. El análisis del riesgo dependerá de la información sobre el mismo, de su origen y la disponibilidad de los datos.

Para adelantarlo es necesario diseñar escalas que pueden ser cuantitativas o cualitativas o una combinación de las dos.

Se han establecido dos aspectos para realizar el análisis de los riesgos identificados:

Probabilidad: Es la posibilidad de ocurrencia del riesgo; puede ser medida con criterios de frecuencia (por ejemplo: número de veces en un tiempo determinado), o de factibilidad, teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque éste no se haya presentado nunca.

Impacto: Son las consecuencias que puede ocasionar a la entidad la materialización del riesgo en caso de sucederse.

8.3. ANÁLISIS CUALITATIVO

Se refiere a la utilización de formas descriptivas para presentar la magnitud de consecuencias potenciales y la posibilidad de ocurrencia. Se diseñan escalas ajustadas a las circunstancias de acuerdo con las necesidades particulares o el concepto particular del riesgo evaluado.

Escala de medida cualitativa de ***PROBABILIDAD DE OCURRENCIA:*** se deben establecer las categorías a utilizar y la descripción de cada una de ellas, para nuestro caso tomamos algunos parámetros establecidos por el Departamento Administrativo de la Función Pública, en la guía para administrar el riesgo. Por ejemplo:

NIVEL	DESCRIPTOR	DESCRIPCIÓN	FRECUENCIA
1	ALTA	El evento ocurrirá en la mayoría de las circunstancias	Al menos una vez en el último año

2	MEDIA	El evento podría ocurrir en algún momento	Al menos una vez en los últimos dos años
3	BAJA	El evento podría ocurrir en circunstancias excepcionales	Al menos una vez en los últimos cinco años

Ese mismo diseño puede aplicarse para la escala de medida cualitativa de ***IMPACTO,*** estableciendo las categorías y la descripción así:

NIVEL	DESCRIPTOR	DESCRIPCIÓN
1	ALTO	Si el hecho llegara a presentarse, tendría graves consecuencias o efectos.
2	MEDIO	Si el hecho llegara a presentarse tendría medio impacto o efecto en la Entidad
3	BAJO	Si el hecho llegara a presentarse tendría bajo impacto o efecto en la Entidad

8.4. ANÁLISIS CUANTITATIVO

Este análisis contempla valores numéricos. Básicamente se refiere a la construcción de indicadores que reflejen tanto la probabilidad de ocurrencia como el impacto que pueden causar. La forma en la cual la probabilidad y el impacto son expresados y las formas por las cuales ellos se combinan para proveer el nivel de riesgo, este puede variar de acuerdo con el tipo de riesgo.

Bajo este esquema y contando con los antecedentes de reclamaciones ante aseguradores, pérdidas de equipos, información u otro suceso que haya afectado en alguna medida la infraestructura tecnológica de la Entidad, se realizó un análisis de todos los elementos de riesgos a los que puede estar expuesta la infraestructura tecnológica de la Contraloría y la información procesada, identificando los siguientes como los activos más susceptibles dentro de las tecnologías de información de la Entidad:

8.5. ACTIVOS Y OTROS ELEMENTOS

- Hardware
- Software
- Datos e información
- Documentación
- Suministro de energía eléctrica
- Suministro de telecomunicaciones
- Cableado estructurado
- Internet
- Dispositivos móviles y equipos portátiles

8.6. PLANIFICACIÓN DE CONTINGENCIAS

Para la planificación de contingencias, la Contraloría General del Quindío, deberá identificar los procesos críticos y esenciales, sus repercusiones en caso de presentarse fallas o de no estar en funcionamiento, por lo cual se resalta la necesidad de contar con estrategias que permitan realizar: Análisis de Riesgos, de Prevención, de Emergencia, de Respaldo y recuperación para enfrentar de manera ágil y oportuna algún desastre.

8.7. DESCRIPCIÓN DE RIESGOS:

De acuerdo con la metodología establecida para análisis de los riesgos, se presenta el Mapa de Riesgos y Controles de los procesos de la entidad, que están disponibles en el aplicativo correspondiente por parte de la Contraloría. Esta herramienta tecnológica se constituye en el mecanismo más apropiado para el proceso de administración, control y tratamiento de los riesgos de la entidad.

8.7.1. PÉRDIDA Y FUGA DE LA INFORMACIÓN

Frecuencia	BAJA
Grado de Impacto	ALTO

Hace referencia a cuando la información confidencial de la Contraloría General del Quindío es accedida por personal no autorizado (terceros); cabe aclarar que debido a los procesos que la Entidad maneja, es de suma importancia proteger la información. El origen de la pérdida y/o fuga puede ser tanto interno como externo.

Acciones preventivas y correctivas

- Cada funcionario es responsable de realizar periódicamente el respaldo de su información la cual, puede ser guardada en uno de los discos duros externos con que cuenta la Entidad y se pueden acceder a ellos a través del Almacen de la entidad y en DVD, que debe ser custodiado por el funcionario. A través de la divulgación permanente y socialización se fomenta la prevención de malas prácticas como compartir contraseñas o información confidencial, es necesario fijar políticas de seguridad.
- Para el aplicativo financiero, el servidor cuenta con disco espejo. De igual forma, se ha establecido como prioridad, crear un respaldo en la nube. La información de la correspondencia de la Entidad es guardada en una copia en el servidor de Aplicativos.
- Los dispositivos y unidades de almacenamiento tienen instalado un software de antivirus.

- Los contratistas tienen inmerso dentro de sus obligaciones mantener la reserva profesional sobre la información que les sea suministrada para la ejecución de su contrato y tener total reserva con la información de las actuaciones fiscales y sancionatorias, contenidas en los expedientes sobre los que deba desarrollar actividades de proyección.
- Se sugiere como un periodo maximo de 15 dias entre copias de seguridad tanto para los funcionarios como para cada uno de los aplicativos usados dentro de la entidad.

8.7.2. DESASTRES NATURALES Y/O ANTRÓPICOS

Frecuencia	BAJA
Grado de Impacto	ALTO

Son los riesgos a los que está expuesta la Contraloría General del Quindío, en caso de un incendio, el alto riesgo que se tiene por estar ubicada en zona de gran actividad sísmica, constantes cambios climáticos, entre otros.

Acciones preventivas y correctivas

- Las instalaciones físicas en caso de un incendio, se encuentra protegido con aspersores de agua.
- En las instalaciones de la Contraloría General del Quindío se tienen tres extintores para cubrir los riesgos potenciales, ubicados estratégicamente, (área de sistemas y archivo, contabilidad, Administración).
- Se realizan copias de seguridad del servidor en el disco espejo.
- Existe protección permanente a los activos de la Entidad con las pólizas de seguros.
- Se cuenta con la señalización adecuada para la evacuación y las brigadas de emergencia en operación.

La previsión de desastres naturales sólo se puede hacer bajo el punto de vista de minimizar los riesgos necesarios en el área de sistemas, en la medida de no dejar objetos en posición tal que ante un movimiento telúrico pueda generar, mediante su caída y/o destrucción, la interrupción del proceso de operación normal. Además, bajo el punto de vista de respaldo, se debe tener en claro los lugares de resguardo, vías de escape y de la ubicación de los archivos, dispositivos de almacenamiento, discos con información vital, todo ello como soporte de aquellos que se encuentren aún en las instalaciones de la institución.

Analizando el riesgo de incendio, permite resaltar el tema sobre el lugar dónde almacenar las copias de seguridad. El incendio, a través de su acción calorífica,

es más que suficiente para destruir los Dispositivos de almacenamiento, tal como CD, DVD, discos duros. Para la mejor protección de los dispositivos de almacenamiento, se colocarán estratégicamente en lugares distantes, cerca de la salida de la Contraloría General del Quindío, en el cuarto contiguo a la recepción.

8.7.3. ERRORES HUMANOS O SABOTAJE

Frecuencia	BAJA
Grado de Impacto	ALTO

Se refiere a la transmisión accidental de datos erróneos, eliminación de archivos o cualquier acción en el sistema provocada por un funcionario accidentalmente, también a la manipulación de la información por parte de empleados para su destrucción.

Acciones preventivas y correctivas

- El servidor cuenta con clave de acceso restringida la cual sólo tiene acceso el (la) Ingeniero (a) de Sistemas.
- El servidor financiero comparte información con tres equipos de la Entidad; Dirección Administrativa y Financiera, Contabilidad y Pagaduría.
- Se maneja el correo institucional para el uso exclusivo de información de la Entidad.
- Restricción del uso de memorias USB, CD, DVD, Discos duros y/o otros dispositivos de almacenamiento digital por parte de terceros en equipos de uso institucional de la entidad.

8.7.4. FALLAS EN EL FUNCIONAMIENTO DE EQUIPOS

Frecuencia	BAJA
Grado de Impacto	BAJA

Indica el mal funcionamiento en los equipos de cómputo de la Contraloría General del Quindío, pueden ocasionar datos erróneos, pérdida de información, incumplimiento de metas, entre otros. Con relación a los equipos de cómputo portátiles, por su permanente traslado de un lugar a otro en el ejercicio del control fiscal y conexión a diferentes fuentes de energía, aumenta la posibilidad de daño y pérdida de información.

Acciones preventivas y correctivas

- Realizar mantenimiento preventivo y correctivo a todos los equipos de cómputo dos veces al año.
- Dentro de las capacitaciones por parte del área de tecnologías de la información se incluyen las recomendaciones para el buen uso de los equipos tecnológicos.
- Desde el área de tecnologías de la información se recuerda constantemente la realización por parte de los funcionarios la copia de seguridad de sus archivos en un periodo no mayor a 15 días.

8.7.5. SEGURIDAD / ROBO

Frecuencia	BAJA
Grado de Impacto	MEDIO

Hace referencia al robo de información, equipos de cómputo y software de la Contraloría General del Quindío. Divulgación de información a instancias fuera de la institución y que afecte su patrimonio estratégico, sea mediante Robo o Infidencia.Debido a los procesos que realiza la Entidad, los auditores deben desplazarse con sus equipos portátiles, lo cual genera un alto riesgo de robo de equipos y por ende pérdida de información.

Acciones preventivas y correctivas

- Desarrollar capacitación en riesgo público.
- Para reducir este riesgo, la Contraloría General del Quindío tiene una póliza de seguros contra todo riesgo para los equipos de cómputo.
- Se cuenta con una red de 14 cámaras de seguridad estratégicamente ubicadas en las instalaciones físicas de la Entidad que guarda un registro de los últimos tres meses en el disco duro del DVR.
- Se tiene como requisito el registro de entrada y salida de los equipos en la bitácora de la portería del edificio.
- El acceso a las aplicaciones fuentes de información es restringido, cada usuario tiene contraseña para tener la trazabilidad.
- El área de tecnología de la información cambia la clave para el acceso a la red inalámbrica mensualmente.

8.7.6. AUSENCIA DE PERSONAL DE PLANTA DE TIC

Frecuencia	MEDIA
Grado de Impacto	MEDIO

Se realiza apoyo a estas labores por parte de un contratista profesional ingeniero de sistemas adscrito a la Dirección Administrativa y Financiera; pero dada su

condición de contratista, se pueden presentar tiempos en los que no se cuente con su apoyo.

Acciones preventivas y correctivas

- Se tiene programado analizar la posibilidad de modificar perfiles profesionales para poder ubicar un profesional de sistemas de la Contraloría que responda por esta área.

8.7.7. OBSOLESCENCIA DE LA INFRAESTRUCTURA TECNOLÓGICA

Frecuencia	MEDIA
Grado de Impacto	MEDIO

Indica la interrupción del servicio de procesamiento de datos por desactualización en el Hardware o Software de la Contraloría General del Quindío.

Acciones preventivas y correctivas

- Recambio constante de equipos tecnológicos.
- Inclusión de nuevas formas en los procesos.
- Realizar el proceso de baja de equipos a dispositivos tecnológicos que previamente se habían identificado como obsoletos por el área de tecnología.

8.7.8. ATAQUES INFORMÁTICOS:

Frecuencia	BAJA
Grado de Impacto	ALTA

Estos tienen por objeto alterar el funcionamiento normal de los equipos de cómputo sin el consentimiento del usuario; el trabajo en la Contraloría General del Quindío, requiere de conexión a internet, traslado de archivos por medio de memorias, compartir información a través de la red, que pueden ocasionar daños en los sistemas, bloquear redes, dañar archivos, entre otros.

Acciones preventivas y correctivas

- La Contraloría General del Quindío cuenta con un programa de antivirus para todos sus equipos de cómputo, el cual se contrata para un periodo de un año y se realiza la actualización anual del mismo.

- El ingeniero (a) de sistemas es el encargado (a) de realizar la instalación del software en cada uno de los equipos de acuerdo con su necesidad.
- Se tiene acceso restringido al servidor por parte del (a) ingeniero (a) de sistemas que como administrador (a) de la red es el (la) encargado (a) de cambiar configuraciones y anexar nuevos equipos.
- Gestionar la adquisición de un dispositivo de tipo Firewall con la finalidad de monitorear el tráfico de red entrante y saliente el permitiendo tomar decisiones respecto al bloqueo o no de tráfico específico en función de un conjunto definido de reglas de seguridad.
- Tramitar el personal idóneo para la configuración del Firewall quien junto a el (la) Ingeniero (a) de Sistemas de la entidad llevaran a cabo la implementación del mismo en la Contraloría General del Quindío, al finalizar el proceso de implementarlo se deberá capacitar tanto a contratistas como personal de planta del área de tecnologías de la información con la finalidad de realizar ajustes posteriores a la políticas inicialmente establecidas.

Los virus y ataques informáticos han evolucionado de tal manera que hoy en día todos conocemos la importancia de tener un programa Antivirus en el computador y aún más importante es su actualización.

9. ADMINISTRACIÓN DE RIESGOS

Cualquier esfuerzo que se emprenda en torno a la valoración del riesgo llega a ser inútil, si no culmina en un adecuado manejo y control de los mismos definiendo acciones posibles y efectivas, tales como cambios físicos, entre otros, que hagan parte de un plan de manejo.

Para el manejo del riesgo se pueden tener en cuenta alguna de las siguientes opciones, las cuales pueden considerarse cada una de ellas independientemente, interrelacionadas o en conjunto.

Evitar el riesgo: es siempre la primera alternativa a considerar. Se logra cuando al interior de los procesos se genera cambios sustanciales de mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones emprendidas. Un ejemplo puede ser el mantenimiento preventivo de los equipos, desarrollo tecnológico, etc.

Reducir el riesgo: si el riesgo no puede ser evitado porque crea grandes dificultades operacionales, el siguiente paso es reducirlo al más bajo nivel posible. La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas

y difíciles. Se consigue mediante la optimización de los procedimientos y la implementación de controles. Ejemplo: Planes de contingencia.
Dispersar y atomizar el riesgo: Se logra mediante la distribución o localización del riesgo en diversos lugares. Es así como, por ejemplo, la información de gran importancia se puede duplicar y almacenar en un lugar distante y de ubicación segura, en vez de dejarla concentrada en un solo lugar.

Transferir el riesgo: Hace referencia a buscar respaldo y compartir con otro parte del riesgo como por ejemplo tomar pólizas de seguros; se traslada el riesgo a otra parte o físicamente se traslada a otro lugar.

Asumir el riesgo: Luego de que el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene, en este caso se acepta la pérdida residual probable y elabora planes de contingencia para su manejo.

Una vez establecidos cuales de los anteriores manejos del riesgo se van a concretar, estos deben evaluarse con relación al beneficio-costo para definir cuáles son susceptibles de ser aplicadas y elaborar el plan de manejo de riesgo, teniendo en cuenta el análisis hecho para cada uno de los riesgos de acuerdo con su impacto, probabilidad y nivel de riesgo.

Posteriormente se definen los ***responsables*** de llevar a cabo las acciones especificando el grado de participación de las dependencias en el desarrollo de cada una de ellas.

9.1. PLAN DE RECUPERACIÓN Y RESPALDO DE LA INFORMACIÓN

El costo de la recuperación en caso de desastres severos, como los de un terremoto que destruya completamente el interior del edificio y sus instalaciones, estará directamente relacionado con el valor de los equipos de cómputo e información que no fueron informados oportunamente y actualizados en la relación de equipos informáticos asegurados que obra en poder de la compañía de seguros.

El costo de recuperación en caso de desastres de proporciones menos severos, como los de un terremoto de grado inferior o un incendio controlable, estará dado por el valor no asegurado de equipos informáticos e información más el costo de oportunidad, es decir, el costo del menor tiempo de recuperación estratégica, si se cuenta con parte de los equipos de información recuperados. Este plan de restablecimiento estratégico del sistema de red, software y equipos informáticos será abordado en la parte de actividades posteriores al desastre.

El paso inicial en el desarrollo del plan contra desastres, es la identificación de las personas que serán las responsables de la ejecución del Plan de Contingencia. Por tanto, se definen los siguientes responsables:

Ingeniero (a) de sistemas: Será el responsable de llevar a cabo las acciones correctivas definidas anteriormente a fin de minimizar los riesgos establecidos.

La Dirección Administrativa y Financiera: Verificará la labor realizada por el (la) Ingeniero (a) de Sistemas.

Asesor de Control Interno: Evaluará la ejecución de acciones preventivas y correctivas a fin de minimizar los riesgos.

9.2. ACTIVIDADES MANTENIMIENTO EQUIPOS DE CÓMPUTO

- Informar a los jefes de área del inicio del proceso de mantenimiento correctivo para contar con la disposición y el tiempo para llevar a cabo este proceso.
- Verificar el estado actual del equipo, al momento de realizar el mantenimiento.
- Revisar que los equipos no tengan vigente la garantía de compra.
- Iniciar el proceso de limpieza eliminando residuos de polvo de cada una de las partes de los equipos de cómputo e impresoras
- Comprobar el estado del Antivirus, instalarlo o actualizarlo con el licenciamiento de la Contraloría General del Quindío, Luego eliminar virus y malware alojados en el equipo.
- Desinstalar todo software que no esté debidamente licenciado y autorizado por la Contraloría General del Quindío y dejar constancia de su desinstalación debidamente firmado por el funcionario responsable del equipo de cómputo.
- En caso de encontrar algún daño en el equipo que amerite remplazo o compra de alguna parte, realizar un informe técnico y solicitud de la parte que se debe adquirir.
- Por último, realizar las recomendaciones pertinentes sobre el uso adecuado de los equipos de cómputo al funcionario correspondiente.
- Como el trabajo que se realiza a cada equipo de cómputo es detallado, se estima un tiempo aproximado de dos (02) horas por equipo.

9.3. COPIAS DE SEGURIDAD

Dentro de las actividades realizadas se han generado copias de seguridad, las cuales están siendo alojadas en los discos duros externos de la Contraloría General del Quindío, en cuanto a las copias de seguridad del aplicativo financiero, son realizadas en el disco espejo del servidor, con el fin de poder

consultarla en caso de un siniestro. Igualmente, el Backup a la correspondencia enviada y recibida se guarda en el servidor de aplicativos.

9.4. ACTIVIDADES MANTENIMIENTO DE UPS

El proveedor se encarga de efectuar el mantenimiento durante los dos primeros años mientras durante la garantía de compra.

El mantenimiento preventivo de una UPS, lo realizamos mediante las siguientes actividades:

- Inspección del estado de carga de las baterías, mediante prueba funcional.
- Revisión interna de contactos, baterías y demás componentes.
- Revisión externa con comprobación de voltajes
- Comprobación de alarmas generadas por la UPS
- Limpieza general

9.5. IMPORTANCIA DEL MANTENIMIENTO

Es necesario realizar mantenimiento preventivo y correctivo con el fin de proporcionar un servicio de calidad a los funcionarios de la Contraloría General del Quindío, para prevenir y minimizar la probabilidad de fallas en los equipos debido a desgaste o uso de los mismos.

Un apropiado mantenimiento preventivo puede ayudar a extender la vida útil del equipo de cómputo, y mantenerlo operando más tiempo evitando costosas reparaciones.

Los equipos de cómputo presentan buen funcionamiento y están protegidos cuando reciben mantenimiento adecuado y oportuno; si no se limpian y se organizan con frecuencia, el disco duro se llena de información, el sistema de archivos se desordena y el rendimiento general disminuye, originando lentitud y poca capacidad para almacenar información.

Si no se realiza periódicamente un escaneo del disco duro para corregir posibles errores o fallas, una limpieza de archivos y la desfragmentación del disco duro, la información estará más desprotegida y será más difícil de recuperar.

El mantenimiento que se debe hacer, se puede resumir en tres aspectos básicos importantes, los cuales son:

- Diagnóstico.
- Limpieza.
- Desfragmentación.

Los equipos de cómputo trabajan más de lo que normalmente se cree. Está constantemente dando prioridad a las tareas, ejecutando órdenes y distribuyendo la memoria. Sin embargo, con el tiempo ocurren errores en el disco duro, los datos se desorganizan y las referencias se vuelven obsoletas; estos problemas se acumulan y generan lentitud en el sistema operativo, las fallas del sistema y software ocurren con más frecuencia y las operaciones de encendido y apagado se demoran más.

Para que el sistema funcione adecuadamente e incluso para que sobre todo no se ponga tan lento, se debe realizar un mantenimiento periódico, asegurándonos de incluir en la rutina del mantenimiento estas labores:

- Exploración del disco duro para saber si tiene errores y solucionar los sectores alterados.
- Limpieza de archivos.
- Desfragmentación el disco duro.

9.6. LIMPIEZA DE EQUIPO DE CÓMPUTO

Para garantizar un rendimiento óptimo y eficaz del equipo de cómputo, debemos mantenerlo limpio y bien organizado.

Debemos eliminar los programas antiguos, programas que no utilicemos y las unidades de disco para liberar la memoria y reducir la posibilidad de conflicto del sistema.

Un disco duro puede presentar diversas deficiencias, que casi siempre se pueden corregir, estas son:

- Poco espacio disponible.
- Espacio ocupado por archivos innecesarios.
- Alto porcentaje de fragmentación.

Se deben eliminar los archivos antiguos y temporales. Además, entre más pocos archivos innecesarios tenga el equipo de cómputo, estará más protegida de amenazas como el hurto de la identidad en Internet.

Cuando el espacio libre de un disco se acerca peligrosamente a cero, el equipo entra en una fase de funcionamiento deficiente, se torna excesivamente lento, emite mensajes de error (que en ocasiones no especifican la causa), algunas aplicaciones no se inician, o se cierran después de abiertas, etc.

Como factor de seguridad aceptable, el espacio vacío de un disco duro no debe bajar del 10% de su capacidad total, y, cuando se llega a este límite, deben borrarse archivos innecesarios, desinstalar aplicaciones que no se usen, borrar

archivos temporales, mantener limpia la papelera de reciclaje o comprimir archivos.

Debe obrar con mucho cuidado cuando haga esta "limpieza profunda" y si no hay plena seguridad de que un archivo en cuestión puede ser borrado, no debe eliminarlo de la papelera de reciclaje hasta comprobarlo, pudiendo reponerse a su ubicación original si resultara necesario.

En general lo que se debe realizar son estas labores:

- Eliminar los programas antiguos y archivos temporales.
- Eliminar la información obsoleta
- Asegurarnos de guardar de manera segura la información.
- Eliminar las entradas de registro inválidas y los accesos directos dañados.
- Ejecutar la herramienta de Windows “CHKDSK” mediante línea de comandos para detectar errores en los discos de datos de cada equipo de cómputo.

9.7. DESFRAGMENTACIÓN

De todos los componentes de un Equipo de Cómputo, el disco duro es el más sensible y el que requiere un cuidadoso mantenimiento.

La detección precoz de fallas puede evitar a tiempo un desastre con pérdida parcial o total de información (aunque este evento no siempre puede detectarse con anticipación).

Alto porcentaje de fragmentación: Durante el uso de un Equipo de Cómputo existe un ininterrumpido proceso de borrado de archivos e instalación de otros nuevos. Estos se instalan a partir del primer espacio disponible en el disco y si no cabe se fracciona, continuando en el próximo espacio vacío.

Un índice bajo de fragmentación es tolerable e imperceptible, pero en la medida que aumenta, la velocidad disminuye en razón del incremento de los tiempos de acceso al disco ocasionado por la fragmentación, pudiendo hacerse notable.

Todas las versiones de Windows incluyen el desfragmentador de disco.

El proceso de desfragmentación total consume bastante tiempo (en ocasiones hasta horas), y aunque puede realizarse como tarea de fondo no resulta conveniente la ejecución simultanea de otro programa mientras se desfragmenta el disco, debiendo desactivarse también el protector de pantalla.