RESOLUCIÓN No. 038

30 ENE 2020

"POR MEDIO DE LA CUAL SE ADOPTA EL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN PARA LA VIGENCIA 2020 DE LA CONTRALORÍA GENERAL DEL QUINDÍO"

EL CONTRALOR GENERAL DEL DEPARTAMENTO DEL QUINDÍO ENCARGADO, en uso de sus facultades Constitucionales y legales y,

CONSIDERANDO:

A. El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la información expone las actividades a desarrollar a partir de la definición del contexto estratégico, la identificación de los riesgos, su análisis, valoración y la definición de la opciones de manejo y soluciones que se puedan requerir la para mitigar el daño y para garantizar una adecuada gestión del riesgo.

B. Igualmente, el objetivo de la Contraloría General del Quindío con el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, es 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 corte de servicios, desastres o errores humanos en el menor tiempo posible.

C. Corresponde a la Dirección Administrativa y Financiera, con la asesoría y acompañamiento de del ingeniero (a) de sistemas de la Entidad, aplicar las medidas de seguridad para proteger y estar preparados para afrontar contingencias y desastres de diversos tipos.

D. 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*" establece en su ARTÍCULO 2.2.22.3.14, el cual fue adicionado por el artículo 1 del Decreto Nacional 612 de 2018 lo siguiente:

*"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

RESOLUCIÓN No. 0 38

30 ENE 2020

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.*

ARTÍCULO 2.2.22.3.15. *Adicionado por el art 1, Decreto Nacional 612 de 2018. <El texto adicionado es el siguiente>* ***Adopción de equipos transversales.*** *Adoptar como instancias para facilitar la coordinación en la aplicación de las políticas de gestión y desempeño institucional, los equipos transversales que organice e integre el Departamento Administrativo de la Función Pública."*

E. Que de acuerdo a la norma citada anteriormente, entre los planes que deben estar integrados al plan de acción y que debe estar publicado al 31 de enero de cada año, se encuentra presente el **PLAN DE TRATAMIENTO DE RIESGOS SE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN** vigencia 2020.

F. Que en la Contraloría General del Quindío, a través de su Comité Institucional de Gestión y Desempeño, en reunión del 28 de enero de 2020 aprobaron el PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN vigencia 2020.

Que en mérito de lo anterior, el Contralor General del Quindío Encargado,

RESUELVE:

ARTÍCULO PRIMERO: Adoptar el **PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2020** 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.

RESOLUCIÓN No. 0 38

30 ENE 2020

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 ENE 2020

PUBLÍQUESE Y CÚMPLASE

JUAN MANUEL RODRIGUEZ BRITO
Contralor General del Quindío Encargado

	Nombre y apellido	Firma	fecha
Proyectado por:	Julián Daniel Murillas Marín	Julian Daniel Murillas Marin	Enero 30/2020
Revisado por :	Aura María Álvarez Ciro	Aura M. Alvarez C.	ENERO 30/2020
Aprobado por:	Rosmira Rodríguez Díaz		ENERO 30/2020
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 2020

CONTRALORIA GENERAL DEL QUINDIO

Armenia, Quindío - Colombia 2020

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

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

VIGENCIA FISCAL 2020

CONTRALORIA GENERAL DEL QUINDIO

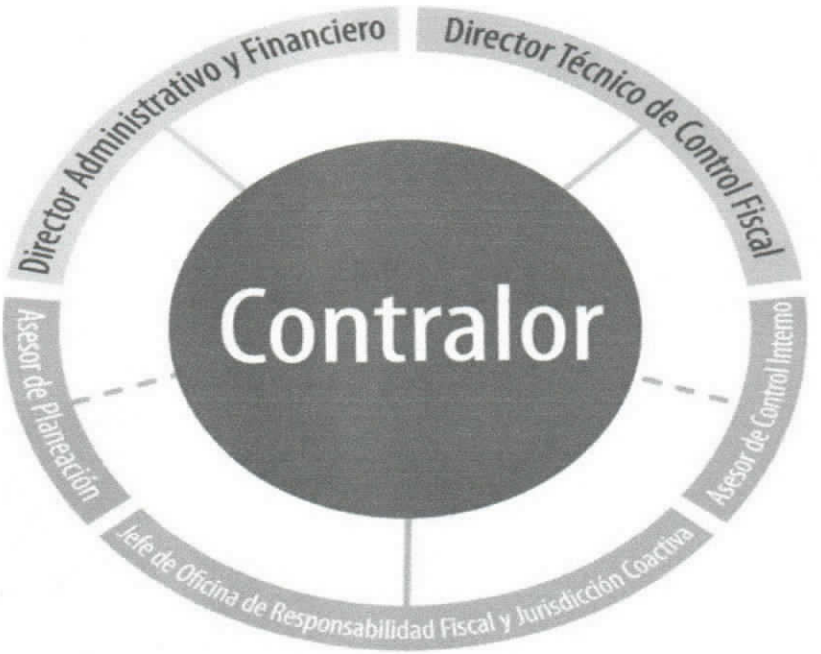
JUAN MANUEL RODRIGUEZ BRITO (E)
CONTRALOR GENERAL DEL QUINDÍO

ROSMIRA RODRIGUEZ DIAZ
DIRECTORA ADMINISTRATIVA Y FINANCIERA

MARIA PATRICIA MEDINA URREA
ASESORA DE PLANEACION

Contenido

1. ESTRUCTURA DE LA ENTIDAD



Estructura circular
(Ordenanza No. 037 - 20/11/12) **Planta de Personal 38 cargos:**
***32 Carrera administrativa/ *5 libre nombramiento y remoción/**
***1 cargo de período fijo.**
Ordenanzas No. 11 - 26/07/17 / Adoptada Resolución internas No. 193 – 26/07/17.

1.1. Misión

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

1.2. Visión

"Para el 2021 la Contraloría General del Quindío, será una entidad reconocida en la efectividad del Control Fiscal con independencia en la ejecución de los recursos públicos, en la preservación y cuidado del medio ambiente, en el cumplimiento de las políticas públicas por parte de los sujetos de control con presencia activa de la comunidad".

1. INTRODUCCIÓN

El Plan de Seguridad y Privacidad de la Información de la Contraloría General del Quindío, involucra un análisis de los riesgos a los cuales pueden estar expuestos los equipos de cómputo y sistemas de información. Corresponde a la Dirección Administrativa y Financiera, con la asesoría y acompañamiento del Ingeniero (a) de Sistemas de la entidad, aplicar las medidas de seguridad para proteger y estar preparados para afrontar contingencias y desastres de diversos tipos.

La infraestructura informática está conformada por el hardware, software y elementos complementarios que soportan la información o datos críticos para la función de la Contraloría General del Quindío.

Los procedimientos relevantes a la infraestructura informática, son aquellas tareas que realizan los funcionarios frecuentemente al interactuar con la plataforma tecnológica (ingreso de datos, generación de reportes, consultas, etc.). Este Plan está orientado a establecer un adecuado sistema de seguridad física y lógica en previsión de desastres, con el fin de establecer medidas destinadas a salvaguardar la información contra los daños producidos por hechos naturales o por el hombre; como uno de los activos más importantes de la Contraloría General del Quindío.

Frente a cualquier evento, la celeridad en la determinación de la gravedad del problema depende de la capacidad y la estrategia a seguir para señalar con precisión la fuente dela dificultad. Los inconvenientes menores o mayores sirven para retroalimentar los requisitos para el buen uso de la infraestructura tecnológica.

2. OBJETIVO GENERAL

2.1. OBJETIVO GENERAL

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.

2.2. 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.

3. IMPORTANCIA

- Garantiza la seguridad física, la integridad de los activos lógicos y materiales de un sistema de información de datos.
- Permite realizar un conjunto de acciones con el fin de evitar el fallo, o en su defecto, disminuir las consecuencias que de el se puedan derivar.
- Permite realizar un análisis de riesgos, respaldo de los datos y su posterior recuperación.
- La implementación de este programa, genera la capacidad de una respuesta oportuna que permita la continuidad del cumplimiento de la misión institucional.

4. ALCANCE

Este plan, suministra los métodos establecidos por la Contraloría General del Quindío, para la administración y gestión de los riesgos a nivel de procesos; orienta acerca de las actividades a desarrollar desde la definición del contexto estratégico, la identificación de los riesgos, su análisis, valoración y la definición de las opciones de manejo que pueden requerir la formulación de acciones adicionales para garantizar una adecuada gestión del riesgo.

5. DEFINICIONES

Para el desarrollo de este plan, es importante tener en cuenta las definiciones establecidas en el Plan de Seguridad y Privacidad de la información, las cuales son:

MSPI: Modelo de Seguridad y Privacidad de la Información.
INTEGRIDAD: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
DISPONIBILIDAD: Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.
CONFIDENCIALIDAD: La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
INFORMACIÓN: Es un conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.
DATO: Es una representación simbólica (numérica, alfabética, algorítmica, espacial, etc.) de un atributo o variable cuantitativa o cualitativa.
COPIAS DE RESPALDO: Es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.
SERVIDOR: Es una aplicación en ejecución (software) capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia.
ACTIVO: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización. (ISO/IEC 27000).

ACTIVO DE INFORMACIÓN: Es todo aquello que en la CGQ es considerado importante o de alta validez para la misma ya que puede contener información importante como son en las Bases de Datos con usuarios, contraseñas, números de cuentas, etc.
RIESGO: Es la posibilidad de que una amenaza se produzca, dando lugar a un ataque al equipo. Esto no es otra cosa que la probabilidad de que ocurra el ataque por parte de la amenaza.

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

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).
Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).
Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).
Ciberespacio: Ámbito o espacio hipotético o imaginario de quienes se encuentran inmersos en la civilización electrónica, la informática y la cibernética. (CONPES 3701, Tomado de la Academia de la lengua Española).
Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

6. ROLES Y RESPONSABILIDADES FRENTE A LA ADMINISTRACIÓN DEL RIESGO

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

Obligaciones de los usuarios

Es responsabilidad de los usuarios de bienes y servicios informáticos, cumplir las Políticas y Estándares de Seguridad Informática para Usuarios.

Capacitación en seguridad informática

Todo servidor o funcionario nuevo en la Contraloría General del Quindío deberá contar con la inducción sobre las Políticas y Estándares de Seguridad Informática,

Manual de Usuarios, donde se den a conocer las obligaciones para los usuarios y las sanciones en que pueden incurrir en caso de incumplimiento.

Sanciones
Se consideran violaciones graves; el robo, daño, divulgación de información reservada o confidencial de cualquier dependencia, o a quien se declare culpable de un delito informático.

7. ANÁLISIS DE EVALUACIÓN DE RIESGOS Y ESTRATEGIAS

7.1. CRITERIOS DE ANÁLISIS

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

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

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

Riesgos Tecnológicos: tales como incendios eléctricos, fallas de energía y accidentes de transmisión y transporte.

Riesgos Sociales: como actos terroristas y desordenes.

7.2. 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: La posibilidad de ocurrencia del riesgo; esta 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: Consecuencias que puede ocasionar a la entidad la materialización del riesgo en caso de sucederse.

Algunos ejemplos de las escalas que pueden implementarse para analizar los riesgos.

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

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:

7.3. ACTIVOS Y OTROS ELEMENTOS

- Hardware
- Software y utilitarios
- Datos e información
- Documentación
- Suministro de energía eléctrica
- Suministro de telecomunicaciones

7.4. POSIBLES DAÑOS

- Imposibilidad de acceso a los recursos debido a problemas físicos en las instalaciones.
- Eliminación o borrado físico/lógico de información clave.
- Divulgación de información a instancias fuera de la institución y que afecte su patrimonio estratégico, sea mediante Robo o Infidencia.

7.5. FUENTES DE DAÑO

- Acceso no autorizado
- Ruptura de las claves de acceso a los sistema computacionales
- Desastres Naturales (Movimientos telúricos, Inundaciones, Fallas en los equipos de soporte causadas por el ambiente, la red de energía eléctrica o el no acondicionamiento atmosférico necesario).
- Fallas de Personal Clave (Enfermedad, Accidentes, Renuncias, Abandono de sus puestos de trabajo y Otros).

- Fallas de Hardware (Falla en los Servidores o Falla en el hardware de Red Switches, cableado de la Red, Router, FireWall).

7.6. 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.

7.7. DESCRIPCIÓN DE RIESGOS:

De acuerdo con el análisis de los riesgos realizado
– Mapa de Riesgos y Mapa de Controles, que forman parte de este documento como anexo, se detallan los riesgos evaluados.

7.8. PÉRDIDA DE LA INFORMACIÓN:

Frecuencia	BAJA
Grado de Impacto	ALTO

Hace referencia a la seguridad de la información de la Contraloría General del Quindío, ya que en gran parte, debido a los procesos que la Entidad maneja, debe conservarse de manera confidencial, y así evitar que sea entregada accidentalmente, o bien, que sea objeto de pérdida o robo.

7.8.1. Acciones 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 Alñmacen de la entidad y en DVD, que debe ser custodiado por el funcionario.

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.

7.9. 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.

7.9.1. Acciones correctivas

- El edificio, 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 al cuarto contiguo a la recepción.

7.10. 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 o hurto.

7.10.1. Acciones correctivas

- El servidor cuenta con clave de acceso restringida la cual sólo tiene acceso el Profesional Universitario Ingeniero 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.
- Copias de seguridad periódicas

7.11. FALLAS DE EQUIPOS DE CÓMPUTO

Frecuencia	MEDIA
Grado de Impacto	MEDIO

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.

7.12. 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. 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.

7.12.1. Acciones 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.

7.13. AUSENCIA DEL PERSONAL DE SISTEMAS:

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; dada su condición de contratista, se pueden presentar tiempos en los que no se cuente con su apoyo, supliendo el soporte o requerimientos la profesional adscrita a la Dirección Técnica de Control Fiscal que su labor misional está orientada a la elaboración de auditoría a la línea de las TIC´s.

7.14. DESACTUALIZACIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA:

Frecuencia	MEDIA
Grado de Impacto	MEDIO

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

7.15. VIRUS 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.

7.15.1. Acciones 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 de la ingeniera de sistemas que como administradora de la red es la encargada de cambiar configuraciones y anexar nuevos equipos.

LosVirusinformáticoshanevolucionadodetalmaneraquehoyendíatodosconocemos la importancia de tener un programa Antivirus en el computador y aún más importan te es su actualización.

8. ADMINISTRACIÓN DEL 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 adopción de procedimientos y 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. Así mismo, es importante construir indicadores, entendidos como los elementos que permiten determinar de forma práctica el comportamiento de las variables de riesgo, que van a permitir medir el impacto de las acciones.

8.1. PLAN DE MANEJO DE RIESGOS

Para elaborar el plan de manejo de riesgos es necesario tener en cuenta si las acciones propuestas reducen la materialización del riesgo y hacer una evaluación jurídica, técnica, institucional, financiera y económica, es decir considerar la viabilidad de su adopción. La selección de las acciones más convenientes para la Entidad se puede realizar con base en los siguientes factores:

- Nivel del riesgo
- Balance entre el costo de la implementación de cada acción contra el beneficio de la misma.

Una vez realizada la selección de las acciones más convenientes se debe preparar e implementar el plan, identificando responsabilidades, programas, resultados esperados, medidas para verificar el cumplimiento y las características del monitoreo.

8.2. 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 de edificio se 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 e 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 personasqueserán lasresponsablesdelaejecucióndelPlandecontingencia.Portanto se definen los siguientes responsables:

Ingeniero 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 la Profesional Universitario Ingeniero de Sistemas.

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

Un Plan de Recuperación de Desastres se clasifica en tres etapas:

8.3. ACTIVIDADES PREVIAS AL DESASTRE

Se considera las actividades de resguardo de la información, en busca de un proceso de recuperación con el menor costo posible para la Entidad. Se establece los procedimientos relativos a:

- Sistemas de Información Equipos de Cómputo
- Obtención y almacenamiento de los Respaldos de Información(BACKUPS).

JUAN MANUEL RODRIGUEZ BRITO (E)
CONTRALOR GENERAL DEL QUINDÍO

ROSMIRA RODRIGUEZ DIAZ
DIRECTORA ADMINISTRATIVA Y FINANCIERA

MARIA PATRICIA MEDINA URREA
ASESORA DE PLANEACION