RESOLUCIÓN No. 2 1 1

27 JUL 2018

*"POR MEDIO DE LA CUAL SE ADOPTA EL PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2018 DE LA CONTRALORÍA GENERAL DEL QUINDÍO"*

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

CONSIDERANDO:

A. El Plan de Tratamiento de Riesgos de Seguridad y Privacidad, tiene como objetivo principal realizar un análisis de los posibles riesgos a los cuales puede estar expuesta la infraestructura tecnológica, para reducir su impacto y probabilidad, reanudando los sistemas en el menor tiempo posible.

B. El Plan de Seguridad y Privacidad de la Información de la Contraloría General del Quindío, busca realizar un análisis de los riesgos a los cuales están expuestos los equipos de cómputo y sistemas de información, aplicando las medidas de seguridad para proteger y afrontar las contingencias y desastres de diversos tipos.

C. Que el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2018 de la Contraloría General del Quindío fue aprobado por el Comité Institucional de Gestión y Desempeño, el 27 de julio de 2018.

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

RESOLUCIÓN No. 2 1 1 3

27 JUL 2018

RESUELVE:

**ARTÍCULO PRIMERO:** Adoptar el **PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2018** 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 a los 27 JUL 2018

PUBLÍQUESE Y CÚMPLASE

GERMAN BARCO LÓPEZ
Contralor General del Quindío

| | Nombre y apellido | firma | fecha |
|---|---|---|---|
| Proyectado por | Aura María Álvarez C. | Aura Ma. Alvarez C. | 23 JULIO 2018 |
| Aprobado por | Juan Manuel Rodríguez B. | | |
| 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 2018

Armenia, Quindío
Colombia.

2018

## CONTRALORIA GENERAL DEL QUINDIO

Dirección: Calle 20 Nro. 13-22 piso 3 Edif. Gobernación del Quindio
Email: contactenos@contraloria-quindio.gov.co
Teléfonos: 7444940 – 7444840 – 7445142 Telefax: 7440016
Linea Gratuita: 018000963123

# CONTRALORIA GENERAL DEL QUINDIO



**GERMAN BARCO LOPEZ**
CONTRALOR GENERAL DEL QUINDÍO

**JUAN MANUEL RODRIGUEZ BRITO**
DIRECTOR ADMINISTRATIVO Y FINANCIERO

**CARLOS ANDRES QUINTERO SEGURA**
ASESOR DE PLANEACION

## CONTENIDO

1. INTRODUCCIÓN 5
2. OBJETIVOS ..... 6
2.1. OBJETIVO GENERAL ..... 6
2.2. OBJETIVOS ESPECIFICOS ..... 7
3. IMPORTANCIA ..... 7
4. ALCANCE ..... 7
5. DEFINICIONES ..... 8
6. ROLES Y RESPONSABILIDADES FRENTE A LA ADMINISTRACIÓN DEL RIESGO ..... 9
6.1. Obligaciones de los usuarios ..... 10
6.2. Capacitación en seguridad informática ..... 10
6.3. Sanciones ..... 10
7. ANÁLISIS DE EVALUACIÓN DE RIESGOS Y ESTRATEGIAS ..... 10
7.1. CRITERIOS DE ANÁLISIS ..... 10
7.1.1. Análisis del riesgo ..... 11
7.2. ACTIVOS Y OTROS ELEMENTOS ..... 13
7.3. POSIBLES DAÑOS ..... 13
7.4. FUENTES DE DAÑO ..... 13
7.5. PLANIFICACIÓN DE CONTINGENCIAS ..... 14
7.6. DESCRIPCIÓN DE RIESGOS: ..... 14
7.6.1. PÉRDIDA DE LA INFORMACIÓN: ..... 14
7.6.2. DESASTRES NATURALES Y/O ANTRÓPICOS: ..... 15
7.6.3. ERRORES HUMANOS O SABOTAJE: ..... 17
7.6.4. FALLAS DE EQUIPOS DE CÓMPUTO: ..... 17
7.6.5. SEGURIDAD / ROBO: ..... 18
7.6.6. AUSENCIA DEL PERSONAL DE SISTEMAS: ..... 19
7.6.7. DESACTUALIZACIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA: ..... 19



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

VIRUS INFORMÁTICOS: ..... 20

8. ADMINISTRACIÓN DEL RIESGOS: ..... 20

9. PLAN DE MANEJO DE RIESGOS. ..... 22

10. PLAN DE RECUPERACIÓN Y RESPALDO DE LA INFORMACIÓN ..... 22

10.1. ACTIVIDADES PREVIAS AL DESASTRE ..... 23

10.2. ACTIVIDADES DURANTE EL DESASTRE (PLAN DE EMERGENCIAS) ..... 25

10.3. ACTIVIDADES DESPUÉS DEL DESASTRE ..... 26

10.4. EVALUACIÓN DE RESULTADOS ..... 28

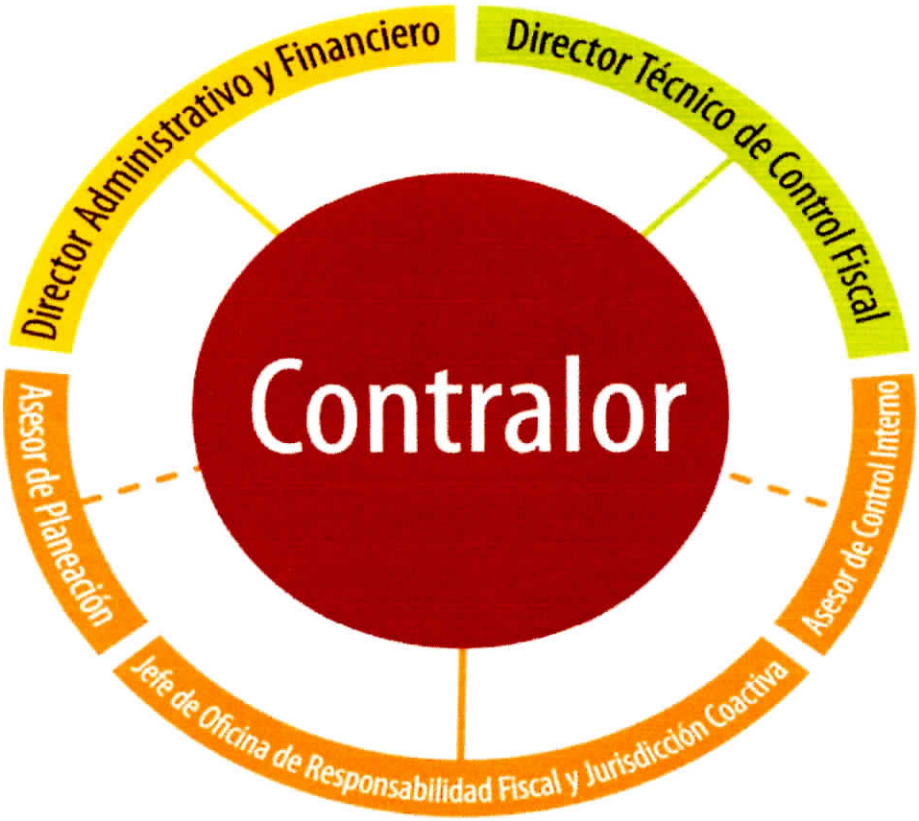
10.5. RETROALIMENTACIÓN DE ACTIVIDADES ..... 28

11. RECOMENDACIONES ..... 28



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

## 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.

## Misión

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



## Visión

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

## 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 de la Ingeniera de Sistemas, 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. La información, como uno de los activos más importantes de la Contraloría General del Quindío, es el fundamento para este Programa.

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 del problema. Los problemas menores o mayores sirven para retroalimentar los requisitos para el buen uso de la infraestructura tecnológica.

## OBJETIVOS

### 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.

## OBJETIVOS ESPECIFICOS

- 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.



## 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 implementacion de este programa, genera la capacidad de una respuesta oportuna que permita la continuidad del cumplimiento de la misión institucional.

## 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.

## 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[1] en el modelo de seguridad y privacidad de la información, las cuales son:



- **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
- **Análisis de Riesgo:** Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).
- **Auditoría:** Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (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.

## 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,

[1] Modelo de seguridad y privacidad de la información emitido por MINTC

mediante conversaciones o situaciones que puedan poner en riesgo la seguridad o el buen nombre de la CGQ. Esta restricción se debe cumplir inclusive después de la terminación del vínculo laboral y contractual y debe estar incluida en los Acuerdos de Confidencialidad establecidos por la CGQ.

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



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

### Obligaciones de los usuarios

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

### 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 de que se le declare culpable de un delito informático.

## ANÁLISIS DE EVALUACIÓN DE RIESGOS Y ESTRATEGIAS

### 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.



## Análisis del riesgo

El objetivo del análisis es el de 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 |
|---|---|---|---|
| Es 1 | ALTA | El evento ocurrirá en la mayoría de las circunstancias | Al menos una vez en el último año |
| e 2 | MEDIA | El evento podría ocurrir en algún momento | Al menos una vez en los últimos dos años |
| mi 3 | BAJA | El evento podría ocurrir en circunstancias excepcionales | Al menos una vez en los últimos cinco años |

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

| 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 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:



## ACTIVOS Y OTROS ELEMENTOS

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

## 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.

## 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).



## PLANIFICACIÓN DE CONTINGENCIAS

Para la planificación de contingencias, la Contraloría General del Quindío debe identificar los procesos críticos o esenciales y 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.

## DESCRIPCIÓN DE RIESGOS:

De acuerdo con el análisis de los riesgos realizado y documentado en el formato FO-AF-03 – Mapa de Riesgos y Mapa de Controles, que forman parte de este documento como anexo, se detallan los riesgos evaluados.

## 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.



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 de la Profesional Universitaria, ingeniera de sistemas y en DVD, que debe ser custodiado por el funcionario.

- Para el aplicativo financiero, el servidor cuenta con disco espejo y tres copias mensuales en DVD, dos de las cuales son custodiadas fuera de las instalaciones de la Contraloría. 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.

## 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 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 diarias del servidor en el disco espejo y de forma mensual, almacenada en DVD.

- 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.

## 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.

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

## 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.



## 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.

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.

## AUSENCIA DEL PERSONAL DE SISTEMAS:

| | |
|---|---|
| Frecuencia | MEDIA |
| Grado de Impacto | MEDIO |

Se realiza apoyo a estas labores por parte de un funcionario adscrito a la Dirección Técnica de Control Fiscal; teniendo en cuenta que su labor misional está orientada a la elaboración de auditoría a la línea de las TIC´s su capacidad de respuesta ante requerimientos del sistema pueda verse afectada por la disponibilidad de la profesional.

## DESACTUALIZACIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA:

| | |
|---|---|
| Frecuencia | MEDIO |
| Grado de Impacto | ALTO |

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

Acciones correctivas:

- La Contraloría General del Quindío tiene un plan de compras en el cual está incluida la adquisición de equipos tecnológicos así como de la actualización de los mismos. En la actualidad los integrantes del equipo auditor cuentan con equipo portátil nuevo.

## VIRUS INFORMÁTICOS:

| | |
|---|---|
| Frecuencia | BAJA |
| Grado de Impacto | ALTO |



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 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.

- La ingeniera de sistemas es la encargada 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.

Los Virus 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.

## 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.



## 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.

## 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 edificios e 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 personas que serán las responsables de la ejecución del Plan de contingencia. Por tanto 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:

## 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:

- Si
  stemas de Información Equipos de Cómputo
- O

btención y almacenamiento de los Respaldos de Información (BACKUPS).

**Sistemas de Información**

La Entidad cuenta con una relación de los Sistemas de Información, tanto los de desarrollo propio, como los desarrollados por empresas externas.

**Equipos de Cómputo**



Se debe tener en cuenta la relación del Hardware, impresoras, scanner, módems, fax y otros, detallando su ubicación (software que usa, ubicación y nivel de uso institucional).

Se debe emplear los siguientes criterios sobre identificación y protección de equipos:

- Pólizas de seguros comerciales, como parte de la protección de los activos institucionales y considerando una restitución por equipos de mayor potencia, teniendo en cuenta la depreciación tecnológica.

- Identificación de los computadores de acuerdo con la importancia de su contenido y valor de sus componentes, para dar prioridad en caso de evacuación.

- Mantenimiento actualizado del inventario de los equipos de cómputo requerido como mínimo para el funcionamiento permanente de cada sistema en la Entidad.

**Obtención y almacenamiento de Copias de Seguridad (Backup)**

Se debe contar con procedimientos para la obtención de las copias de seguridad de todos los elementos de software necesarios para asegurar la correcta ejecución de los sistemas en la institución. Las copias de seguridad son las siguientes:

Backup del Sistema Operativo: Todas las versiones de sistema operativo instalados en la Red. (Periodicidad – Semestral).

Backup de los datos (Base de datos, password y todo archivo necesario para la correcta ejecución del software aplicativos de la institución). (Periodicidad – Mensual).

## ACTIVIDADES DURANTE EL DESASTRE (PLAN DE EMERGENCIAS)

Presentada la contingencia o desastre se debe ejecutar las siguientes actividades planificadas previamente:



**Plan de Emergencias**

Son las actividades a realizar durante el desastre o siniestros, se debe tener en cuenta la probabilidad de su ocurrencia durante: el día, noche o madrugada. Este plan debe incluir la participación y actividades a realizar por todas y cada una de las personas que se pueden encontrar presentes en el área donde ocurre el siniestro, descritas a continuación:

- B

uscar Ayuda de Otros Entes

- E

s de tener en cuenta que sólo se debe realizar acciones de resguardo de equipos en los casos en que no se pone en riesgo la vida de personas. Normalmente durante la acción del siniestro es difícil que las personas puedan afrontar esta situación debido a que no están preparadas o no cuentan con los elementos de seguridad, por lo que las actividades para esta etapa del proyecto de prevención de desastres deben estar dedicados a buscar ayuda inmediatamente para evitar que la acción del siniestro causen más daños o destrucciones.

Se debe tener en toda oficina los números de teléfono y direcciones de organismos e instituciones de ayuda.

- Todo el personal debe conocer la localización de vías de Escape o Salida y éstas deben estar señalizadas.

- Instruir a los funcionarios de la Entidad respecto a evacuación ante sismos, a través de simulacros, esto se realiza acorde a los programas de seguridad organizadas por la Gobernación y los brigadistas.

- Ubicar y señalizar los elementos contra el siniestro: tales como extintores, zonas de seguridad, puntos de encuentro.

- Secuencia de llamadas en caso de siniestro: tener a la mano elementos de iluminación, pito, lista de teléfonos de los funcionarios y de las instituciones como: Compañía de Bomberos, Cruz Roja, Hospitales, Centros de Salud, Ambulancias, Seguridad.



**Formación de Equipos**

Se debe establecer los equipos de trabajo, con funciones claramente definidas que deberán realizar en caso de desastre. En caso de que el siniestro lo permita (al estar en un inicio o estar en un área cercana, etc.), se debe formar 02 equipos de personas que actúen directamente durante el siniestro, un equipo para combatir el siniestro y el otro para salvamento de los equipos informáticos, teniendo en cuenta la clasificación de prioridades. Estas actividades están bajo la responsabilidad de los brigadistas.

**Entrenamiento**

Se debe establecer un programa de prácticas periódicas con la participación de todo el personal en la lucha contra los diferentes tipos de siniestro, de acuerdo con los roles que se hayan asignado en los planes de evacuación del personal o equipos. Es importante que el personal tome conciencia que los siniestros (incendios, inundaciones, terremotos, apagones, etc.) Pueden realmente ocurrir; y tomen con seriedad y responsabilidad estos entrenamientos; para estos efectos es conveniente que participen los Directivos, dando el ejemplo de la importancia que la Alta Dirección otorga a la Seguridad Institucional.

## ACTIVIDADES DESPUÉS DEL DESASTRE

Estas actividades se deben realizar inmediatamente después de ocurrido el

siniestro, son las siguientes:

**Evaluación de daños**



El objetivo es evaluar la magnitud del daño producido, es decir, qué sistemas se afectaron, qué equipos han quedado inoperativos, cuáles se pueden recuperar y en cuanto tiempo. En el caso de la Entidad, se deben atender los procesos de Contabilidad, Tesorería, Presupuesto y demás Sistemas de Información primordiales para el funcionamiento de la Entidad, por la importancia estratégica. La recuperación y puesta en marcha de los servidores que alojan dichos sistemas, es prioritario.

**Priorizar Actividades**

La evaluación de los daños reales nos dará una lista de las actividades que se deben realizar, preponderando las actividades estratégicas y urgentes de nuestra institución. Las actividades comprenden la recuperación y puesta en marcha de los equipos de cómputo y los Sistemas de Información, compra de accesorios dañados, etc.

**Ejecución de actividades**

La ejecución de actividades implica la colaboración de todos los funcionarios, creando Equipos de Trabajo, asignando actividades. Cada uno de estos equipos deberá contar con un líder que deberá reportar el avance de los trabajos de recuperación y en caso de producirse un problema, reportarlo de inmediato al Directivo, brindando posibles soluciones.

Los trabajos de recuperación se iniciarán con la restauración del servicio usando

los recursos de la institución, teniendo en cuenta que en la evaluación de daños se contempló y gestionó la adquisición de accesorios dañados. La segunda etapa es volver a contar con los recursos en las cantidades y lugares propios del Sistema de Información, debiendo ser esta última etapa lo suficientemente rápida y eficiente para no perjudicar la operatividad de la institución y el buen servicio de nuestro sistema e Imagen Institucional.



## EVALUACIÓN DE RESULTADOS

Una vez concluidas las labores de Recuperación de los sistemas que fueron afectados por el siniestro, debemos de evaluar objetivamente, todas las actividades realizadas, con qué eficacia se hicieron, qué tiempo tomaron, qué circunstancias modificaron (aceleraron o entorpecieron) las actividades, cómo se comportaron los equipos de trabajo, etc. De la evaluación de resultados y del siniestro, deberán obtenerse dos tipos de recomendaciones, una la retroalimentación del Plan de Contingencias y Seguridad de Información, y otra una lista de recomendaciones para minimizar los riesgos y perdida que ocasionaron el siniestro.

## RETROALIMENTACIÓN DE ACTIVIDADES

Con ésta se pueden mejorar las actividades que tuvieron algún tipo de dificultad y reforzar los elementos que funcionaron adecuadamente.

## RECOMENDACIONES

Hacer de conocimiento general el contenido el programa de Contingencias y Seguridad de Información, con la finalidad de instruir adecuadamente al personal de la Contraloría General del Quindío.

Adicionalmente, al plan de contingencias se deben desarrollar las acciones correctivas planteadas para minimizar los riesgos identificados.

Es importante tener actualizados los contratos de garantía y licencias tanto de hardware como de software, así como pólizas de seguro.

En ausencia del administrador de la red, se recomienda capacitar a una persona que pueda hacer lo mínimo indispensable para levantar todos los servicios, a fin de que la operación básica de la Entidad no se vea interrumpida.



**GERMAN BARCO LOPEZ**
Contralor General Del Quindío

**JUAN MANUEL RODRIGUEZ BRITO**
Director Administrativo y Financiero

Original Firmado
**CARLOS ANDRES QUINTERO SEGURA**
Asesor de Planeación

| CONTRALORÍA GENERAL DEL QUINDÍO | CONTRALORÍA GENERAL DEL QUINDÍO<br>ACTA COMITÉ INSTITUCIONAL DE DESEMPEÑO | Código: FO-GC-03<br>Fecha: 16/07/2013<br>Versión: 2<br>Pagina 1 do2 |
|---|---|---|

| Número de acta: | 00 | Tema de la reunión: Resoluciones y Adopciones | Comité institucional de desempeño | | |
|---|---|---|---|---|---|
| Fecha: | 27/07/2018 | Hora: | 8:00 a.m. | Lugar: | Sala De Juntas |

| ASISTENTE | FIRMA | ASISTENTE | FIRMA |
|---|---|---|---|
| German Barco Lopez – Contralor General del Quindío | | | |
| Juan Manuel Rodríguez Brito - Director Administrativo | | | |
| Claudia Patricia González Q – Directora Técnica de Control Fiscal | | | |
| Carlos Andrés Quintero Segura- Asesor de Planeación | Carlos A. Quintero | | |
| Alexandra Zuluaga Londoño Jefe Proceso Responsabilidad Fiscal y Jurisdicción Coactiva | | | |

TEMAS

1- Adopcion de todos los planes institucionales según decreto 612 de 2018, 2- Autorizacion para realizar Resoluciones de estos planes, 3- Autorizacion de Modificaciones al Plan de Accion 2018, 4- Insercion de todos los Planes segun Decreto 612 al Plan de Accion 2018, 5- Publicacion de todos los Planes cumpliendo con el Decreto 612 de 2018,

DESARROLLO DE LOS TEMAS

1- El Doctor Juan Manuel Rodriguez hace presentacion y entrega al Contralor General y al Doctor Carlos Andres quintero Segura de todos Los Planes Institucionales según decreto 612 de 2018 para que sean adoptados y aprobados por este comité, El comité Aprueba

2- El Doctor Juan Manuel Rodriguez y el Contralor colocan como fecha el 30 de julio para nueva reunion con el fin de revisar que todos los planes esten con su respectiva resolucion para cumplir con el decreto 612 del DAFP y Publicados en la pagina.

3- El Doctor Carlos Andres Quintero Solicita autorizacion para realizar unas modificaciones al Plan de Accion 2018 Para el Normal cumplimiento de este. El Comité Aprueba

4- El Contralor Solicita que todos los planes nuevos institucionales según decreto 612 de 2018 sean integrados al Plan de Accion 2018

5- El Doctor Juan Manuel Rodriguez solcita que todos los Planes sean Publicados con su respectiva resolucion y acta de adopcion, El comité aprueba

6- El Doctor Carlos Andres Quintero Solicita que todos los planes según decreto 612 de 2018 con su respectiva resolucion y acta de adopcion sean enviados a la Ingeniera de sistemas para su publicacion en pagina

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

COMPROMISOS

| No. | Tarea / Acción / Compromiso | Responsable | Fecha Compromiso |
|---|---|---|---|
| 1 | Resoluciones Totalemente terminadas | Aura Maria Alvarez | 30-jul-18 |
| 2 | Cumplimiento Decreto 612 del DAFP | Todas Las Dependencias | 31-jul-18 |
| 3 | Modificaciones Del Plan de Accion | Planeacion | 30-jul-18 |
| 4 | Publicacion de todos los Planes en Pagina | Planeacion y Sistemas | 30-jul-18 |