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

GOBERNACIÓN DEL QUINDIO

2018

Gobernación del Quindío
Calle 20 No. 13-22
www.quindio.gov.co
Armenia, Quindío

PBX: 7 417700 EXT: 250
tecnologia@quindio.gov.co

Tabla de contenido

Gobernación del Quindío
Calle 20 No. 13-22
www.quindio.gov.co
Armenia, Quindío

PBX: 7 417700 EXT: 250
tecnologia@quindio.gov.co

Gobernación del Quindío
Calle 20 No. 13-22
www.quindio.gov.co
Armenia, Quindío

PBX: 7 417700 EXT: 250
tecnologia@quindio.gov.co

INTRODUCCION

Desde los inicios de los sistemas de información se sabe que los riesgos forman parte de los mismos, ya que como es sabido las amenazas a la información pueden presentarse de diferentes formas, tanto de origen natural (terremotos, tormentas eléctricas, etc), como de origen humano (huelgas, competencia entre compañeros, problemas laborales, etc) de origen técnico (fallas de hardware, software, suministro de energía, etc.) Y es casi siempre una situación no prevista la que regularmente provoca una crisis y las consecuencias de la misma, según su impacto y extensión, pueden ser catastróficas para los intereses de cualquier organización. Conscientes de ello, se pretende definir en este documento, el plan más asertivo aplicable a la gobernación del Quindío en materia de recuperación de la normalidad para aquellas eventualidades presentadas en las que algún recurso informático se afecte.

Teniendo en cuenta lo anterior la gobernación del Quindío considera que la información es el patrimonio principal de toda la Institución, por lo que planifica y toma medidas de seguridad para protegerla y estar preparados para afrontar contingencias y desastres de diversos tipos.

Gobernación del Quindío
Calle 20 No. 13-22
www.quindio.gov.co
Armenia, Quindío

PBX: 7 417700 EXT: 250
tecnologia@quindio.gov.co

OBJETIVOS

OBJETIVO GENERAL

Plantear y dotar a la gobernación del Quindío de los procedimientos y elementos mínimos requeridos para afrontar algún riesgo relacionado con el eventual cese de actividades, privacidad de la información e inoperatividad de equipos causada por razones de fuerza mayor y de diferente índole.

Objetivos específicos

- Identificar y solucionar de manera rápida y eficaz cualquier problema que se presente con los sistemas información de la gobernación del Quindío.
- Proteger y conservar los activos informáticos de la gobernación del Quindío contra riesgos, desastres naturales o actos malintencionados.
- Garantizar la operatividad de la red interna de la gobernación del Quindío, cuando se presente alguna eventualidad.
- Evaluar los riesgos de los procedimientos de contingencia requeridos cuando se presenta una interrupción de las operaciones, de forma que sólo se inviertan los recursos necesarios.
- Minimizar la posible pérdida de información en el evento inesperado, previendo procedimientos de recuperación efectivos y eficientes.

Gobernación del Quindío
Calle 20 No. 13-22
www.quindio.gov.co
Armenia, Quindío

PBX: 7 417700 EXT: 250
tecnologia@quindio.gov.co

ALCANCE

La necesidad de desarrollar un plan de tratamiento de riesgos de seguridad y privacidad de la información, está relacionada con el impacto potencial que provoca la interrupción parcial o total de los servicios electrónicos y procesamiento de la información, sobre el normal desarrollo de las actividades de la GOBERNACION DEL QUINDIO; específicamente, para afrontar la contingencia relacionada con el eventual cese de actividades e inoperatividad de equipos

Lo que supone que los procedimientos planteados en este documento, contemplan solamente las acciones a realizar con relación al Hardware, software, equipos electrónicos, información y redes involucrados en los procesos críticos definidos en el plan.

Adicionalmente, se consideran los riesgos y soluciones del ambiente físico, relacionados con la operación de los procesos principales de los equipos de cómputo y la red interna

Las actividades y procedimientos, están relacionados con las funciones que competen a cada uno de los usuarios y dependen de la diligencia y colaboración de las dependencias y de los recursos disponibles (capacitación, recursos técnicos, presupuesto, etc.).

Este plan constituye parte fundamental del Plan de Recuperación de Desastres DRP de la Gobernación del Quindío.

ROLES Y RESPONSABILIDADES

Comité de Seguridad de la Información

- Garantizar la existencia de una dirección y apoyo gerencial que soporte la administración y el desarrollo de iniciativas sobre seguridad de la información, a través de compromisos y uso adecuado de los recursos en el organismo.

Gobernación del Quindío
Calle 20 No. 13-22
www.quindio.gov.co
Armenia, Quindío

PBX: 7 417700 EXT: 250
tecnologia@quindio.gov.co

- Formular y mantener una política de seguridad de la información que aplique a toda la organización conforme con lo dispuesto por la gobernación del Quindío.

Director de Talento Humano

El Director de Talento Humano cumplirá la función de notificar a todo el personal que se vincula por nombramiento o contractualmente con la Gobernación del Quindío, de las obligaciones respecto del cumplimiento de la política de seguridad de la Información y de todos los estándares, procesos, procedimientos, prácticas y guías que surjan del sistema de gestión de la seguridad de la Información.

De igual forma, será responsable de la notificación de la presente política y de los cambios que en ella se produzcan a todo el personal, a través de la suscripción de los compromisos de confidencialidad y de tareas de capacitación continua en materia de seguridad según lineamientos dictados por el Comité de Seguridad de la Información.

Director de Recursos Físicos

El Director de Recursos Físicos cumplirá la función de vigilar y mantener la infraestructura física de la entidad, con el fin de salvaguardar la información. Será el encargado de implementar controles físicos, con el fin de minimizar los riesgos de amenazas físicas y ambientales como robos, incendios, agua, vandalismo, etc.

Por otra parte deberá implementar los controles que crea necesarios a las instalaciones sensibles a accesos de información, tales como el data center de la Gobernación del Quindío.

Por ultimo deberá ejercer control físico y/o electrónico sobre todas las personas que ingresan a las instalaciones de la Gobernación del Quindío, dichos controles abarcan desde empleados de planta pasando por contratistas y visitantes.

Gobernación del Quindío
Calle 20 No. 13-22
www.quindio.gov.co
Armenia, Quindío

PBX: 7 417700 EXT: 250
tecnologia@quindio.gov.co

Secretaria Administrativa

La Secretaria Administrativa en conjunto con el Director TIC cumplirán la función de darle continuidad a las políticas de información aquí generada, así como también proponer cambios en dichas políticas, generar el plan de continuidad del negocio, asignar responsabilidades dentro de la matriz d riesgos de la entidad y especificar los planes de respuesta al riesgo ante alguna eventualidad que se identifique.

Director de TIC

El Director TIC junto con el Director de Asuntos Jurídicos, Conceptos y Revisiones tendrá la responsabilidad de generar los acuerdos de confidencialidad, tratamiento de la información y demás documentación legal a los que se haga responsable tanto empleados, contratistas y/o empresas que presten los servicios a la Gobernación del Quindío y que manejen datos susceptibles de la entidad.

Director de Sistemas

El Director de Sistemas velará por el cumplimiento de las políticas de la información en la Gobernación del Quindío, ejercerá los controles que crea necesarios en los sistemas informáticos de la entidad, propondrá nuevos controles y será el encargado de darle seguimiento a las políticas de seguridad relacionados con la protección digital de los datos de la entidad.

Director de Asuntos Jurídicos, Conceptos y Revisiones

El Director de Asuntos Jurídicos, Conceptos y Revisiones verificará el cumplimiento de la presente política en la gestión de todos los contratos, acuerdos u otra documentación de la entidad con empleados y con terceros. Así mismo, asesorará en materia legal a la entidad en lo que se refiere a la seguridad de la información.

Jefe de Oficina de Control Interno de Gestión

El Jefe de Oficina de Control Interno de Gestión cumplirá la función de vigilar y ejercer los controles necesarios para que los funcionarios de la Gobernación del

Gobernación del Quindío
Calle 20 No. 13-22
www.quindio.gov.co
Armenia, Quindío

PBX: 7 417700 EXT: 250
tecnologia@quindio.gov.co

Quindío cumplan a cabalidad lo dispuesto en el documento de políticas de seguridad de la información.

IDENTIFICACION Y ANALISIS DE RIESGOS

Definición: La matriz de riesgos es una confrontación analítica de los posibles riesgos a los que se encuentra sometida el área tecnológica, este análisis nos permitirá evaluar la probabilidad de ocurrencia de los distintos riesgos para diseñar los controles preventivos y correctivos, los que se considera más críticos y causan más impacto para la gobernación.

En esta etapa se desarrolla la probabilidad de ocurrencia, posibilidades de mitigación, el Impacto y probabilidades de los riesgos, finalmente las alternativas de corrección de la anomalía.

Análisis de Riesgos: Los diferentes riesgos a los que puede encontrarse sometida el área tecnológica se pueden agrupar de la siguiente forma:

Riegos por incidencia externa

- **Desastre natural:** Hace referencia a los riesgos a los que está expuesta cualquier entidad pública, en caso de incendio, terremoto, tormenta eléctrica, etc.
- **Interrupción del fluido eléctrico:** Esto es la capacidad que tiene la gobernación del Quindío para reaccionar ante el corte parcial del fluido eléctrico, por daños inesperados por parte de la empresa prestadora del servicio.
- **Modificaciones a la constitución política**: Ya sea por asamblea constituyente, referendo, consulta popular, plebiscito o mediante leyes orgánicas, reestructuración o supresión de entidades.

Gobernación del Quindío
Calle 20 No. 13-22
www.quindio.gov.co
Armenia, Quindío

PBX: 7 417700 EXT: 250
tecnologia@quindio.gov.co

Riesgos por incidencia interna

- **Perdida de la información:** Hace referencia a la seguridad de la información que maneja la gobernación del Quindío, ya que debido a los procesos que la entidad maneja, esta debe conservarse de manera confidencial, y así evitar que sea entregada accidentalmente, o bien, que sea objeto de robo.

- **Falla de equipos electrónicos:** Como cualquier equipo electrónico los computadores son susceptibles a fallos en cualquier momento, pudiendo llegar a provocar perdida de la información y retrasos en procesos administrativos.

- **Virus informáticos:** Los virus informáticos tienen por objeto alterar el funcionamiento normal de los equipos de cómputo, además tienen la facilidad de propagarse con facilidad con el uso de memorias USB, correo electrónico, etc.

- **Seguridad o Robo:** hace referencia al hurto de la información, de los mismos equipos de cómputo o equipos de red con los que cuenta la gobernación de Quindío.

- **Calentamiento de la Sala de Cómputo (Data center):** Este riesgo está asociado a la probabilidad de que se incremente la temperatura del data center por encima de los mínimos permitidos por la dirección Tic, cabe aclarar que en el data center se encuentran los servidores de la gobernación del Quindío y switchs principales de la red interna, los cuales generan que se incremente la temperatura dentro del cuarto.

- **Copias de seguridad sistemas de información:** Riesgo asociado a la falta de copias de seguridad de las bases de datos de los sistemas de información con los que cuenta la entidad, dichas copias se deben realizar diariamente y por la dirección TIC.

- **Falta de Actualización de la infraestructura tecnológica**: se refiere a la falta de adquisición y/o actualización de equipos que se van quedando obsoletos por su tiempo de uso.

Gobernación del Quindío
Calle 20 No. 13-22
www.quindio.gov.co
Armenia, Quindío

PBX: 7 417700 EXT: 250
tecnologia@quindio.gov.co

- **Incumplimiento de los contratistas**: Este riesgo puede ocurrir a causa del posible atraso en la contratación, ejecución o trasgresión del de los contratos de actualización, modificación, mantenimiento, que se asumen durante la vigencia, contratos como licenciamiento de antivirus, mantenimiento correctivo de equipos, red de acceso a internet, sistemas de información como PCT, Sevenet, Ventani la única virtual Quindío, Siscar, etc.

- **Retrasos en Procesos Administrativos:** La implementación de los procesos tecnológicos relacionados con la ejecución de los contratos, implica el desarrollo de trámites administrativos, los cuales se puede llegar a retrasar por exigencias en el cumplimiento de requisitos.

- **Procesos de capacitación constante del personal TI:** Riesgo asociado a la falta de actualización y capacitación de los conocimientos en sistemas de información de la gobernación del Quindío

Mitigación del riesgo

Consiste en el establecimiento, desarrollo de estrategias y procedimientos previos a la posible materialización del riesgo u ocurrencia de la emergencia, tendientes a la mitigación de los mismos, haciéndolos menos graves, reduciendo al máximo las consecuencias o posibles pérdidas.

Los cuales se resumen a continuación:

Desastres naturales

Aunque realmente un desastre natural no se puede evitar, la gobernación del Quindío puede llegar a prevenir algunas de las consecuencias que este tipo de siniestro pueda llegar a tener sobre la infraestructura tecnológica.

El edificio de la gobernación, cuenta con una estructura sismo resistente, que ayuda a que en caso de terremoto este pueda seguir en pie o en consecuencia, con muchos menos daños que otros edificios.

Gobernación del Quindío
Calle 20 No. 13-22
www.quindio.gov.co
Armenia, Quindío

PBX: 7 417700 EXT: 250
tecnologia@quindio.gov.co

Por otra parte la red interna de la gobernación del Quindío, está respaldada con UPS, para evitar que los Switchs se dañen en casa de tormentas eléctricas, con este mismo respaldo cuentan los servidores de la gobernación que se encuentran en el data center.

Interrupción del fluido eléctrico

Como se dijo anteriormente la red interna de la Gobernación del Quindío se encuentra respaldada con UPS, para que esta siga su funcionamiento normalmente durante más de 20 minutos de interrupción. Además de que los servidores se encuentran respaldados.

Modificaciones a la constitución política

Leyes, decretos, resoluciones, ordenanzas, etc. Que expida el gobierno nacional a cargo del ministerio de Tecnologías de la información y comunicaciones MinTic, sobre el trato, seguridad y manejo de la información que tienen los entes gubernamentales.

Pérdida de Información

La Gobernación del Quindío, cuenta con una política de respaldo de la información de los servidores de la gobernación, este respaldo se realiza todos los días en discos duros externos que se encuentran en el data center.

Falla de equipos electrónicos

Para tratar de mitigar este riesgo, la gobernación del Quindío a través de la dirección TIC y con el apoyo de la empresa contratista a cargo de los mantenimientos preventivos y correctivos, viene realizando y ejecutando un plan de mantenimiento preventivo, el cual incluye un cronograma de actividades y que es ejecutado durante todo el año.

Gobernación del Quindío
Calle 20 No. 13-22
www.quindio.gov.co
Armenia, Quindío

PBX: 7 417700 EXT: 250
tecnologia@quindio.gov.co

Virus informáticos

Contra los virus informáticos, la gobernación del Quindío, cuenta con antivirus en todos los equipos de cómputo de la misma, que protegen los equipos en tiempo real. Además de lo anterior, cabe destacar que a través del año, se está ejecutando el mantenimiento preventivo el cual incluye mantenimiento de software y sistema operativo (desinfección).

Seguridad o Robo

Para reducir el riesgo de robo la gobernación del Quindío se encuentra en proceso de adquisición de cámaras de seguridad para el edificio, además de esto la gobernación cuenta con vigilantes las 24 horas del día, para reforzar la seguridad del mismo.

Calentamiento de la Sala de Cómputo (Data center)

Este riesgo tiene una baja probabilidad de ocurrencia, debido a que la gobernación del Quindío ha implementado procedimientos para su mitigación, tales como: La implementación en el centro de cómputo principal (piso 1) de un Sistema de Temperatura autorregulada, provisto de un sistema de aire acondicionado, con sensores ambientales para el control y monitoreo de temperatura.

Copias de seguridad sistemas de información

La Gobernación del Quindío, cuenta con una política de respaldo de la información de los servidores de la gobernación, este respaldo se realiza todos los días en discos duros externos que se encuentran en el data center.

Falta de actualización de la infraestructura tecnológica

La Gobernación del Quindío cuenta con un plan de compras, en el cual se tiene proyectado siempre la adquisición de equipos y/o dispositivos que ayuden a actualizar la infraestructura tecnológica de la misma.

Incumplimiento de los contratistas

Dentro de los procesos de contratación que tiene la gobernación del Quindío, con los proveedores de sistemas de información, se cuenta con pólizas de cumplimiento y responsabilidad que ayudan a mitigar el riesgo inherente al incumplimiento.

Gobernación del Quindío
Calle 20 No. 13-22
www.quindio.gov.co
Armenia, Quindío

PBX: 7 417700 EXT: 250
tecnologia@quindio.gov.co

Retrasos en Procesos Administrativos

La gobernación del Quindío tiene como prioridad el resguardo seguro de la información, por tal motivo se intenta contar como primer lugar con todos los proveedores y personal capacitado para la dirección TIC

Procesos de capacitación constante del personal TI

La dirección TIC, capacita en el manejo de los sistemas de información a todo el personal que ingresa a la dependía, se realiza un proceso de aprendizaje en el cual el ingeniero, técnico o tecnólogo aprende a dominar las herramientas tecnológicas que se tienen en la gobernación.
Por otra parte a través de la estrategia de gobierno en línea, la dirección TIC capacita constantemente a su personal en implementación de la misma.

MATRIZ DE RIESGOS

A continuación se relaciona matriz de probabilidad e impacto de los riesgos relacionados con anterioridad

Matriz de Riesgos.xlsx

Ver archivo de Excel matriz de riesgos

Gobernación del Quindío
Calle 20 No. 13-22
www.quindio.gov.co
Armenia, Quindío

Paisaje Cultural Cafetero
Patrimonio de la Humanidad
Declarado por la UNESCO

PBX: 7 417700 EXT: 250
tecnologia@quincio.gcv.co

FASE DE RECUPERACIÓN

Permite restablecer las condiciones originales y operación normal del sistema. El cual contempla:

- Definición de las políticas (parámetros, límites, horas de recuperación).
- Definición de los objetivos y requerimientos de la continuidad.
- Definiciones, términos y suposiciones.

Responsabilidades de la fase de recuperación.

- Mantener y mejorar los procedimientos de recuperación de desastres del grupo de operaciones del computador.
- Evaluar la instalación del software del sistema (al momento de la recuperación) y de los datos con la asistencia del grupo de soporte técnico y de las aplicaciones en producción, en la forma usual.
- Mantener la configuración de la red para todos los sistemas de comunicación de datos.
- Mantener un plano de la configuración de la red a ser implementada en el evento de un desastre.
- Evaluar los procedimientos de backup's para establecer los servicios de comunicación de datos en el evento de un desastre.

Cabe anotar que el director de sistemas de la gobernación, tiene a cargo estas responsabilidades y debe estar presto a restablecer el servicio en el menor tiempo posible con la ayuda de los demás ingenieros de la Dirección TIC, esto dependiendo del tipo de riesgo que se llegase a producir.

Como herramientas de recuperación para algún tipo de desastre, en primer lugar está el restablecer la información guardada mediante copias de seguridad en el menor tiempo posible.
El equipo de sistemas de la gobernación del Quindío dispone de una base de datos con todas las contraseñas de los equipos de cómputo y servidores de la gobernación del Quindío y que contiene información para restablecimiento de la información en caso de pérdida o robo, desastre natural, etc.

Gobernación del Quindío
Calle 20 No. 13-22
www.quindio.gov.co
Armenia, Quindío

PBX: 7 417700 EXT: 250
tecnologia@quindio.gov.co

Recuperación del desastre: plan de acción

El Plan presupone que debe utilizarse un Centro de Cómputo alterno externo al edificio sede de la Gobernación del Quindío, si la emergencia afecta en forma general (en un 60% o más) las instalaciones físicas y técnicas con que se cuenta. Los siguientes procedimientos se circunscriben a dichos hechos o casos.

PRIMERA FASE: Procedimientos Iniciales de Respuesta/Notificación

Los siguientes deben ser los procedimientos a ser implantados en el momento del desastre, dichos procedimientos que deben continuar hasta que se restauren los servicios de procesamiento de datos en el sitio original u otro permanente.
En el caso de incendio, explosión u otro desastre mayor en el Centro de Cómputo, debe implantarse inmediatamente los procedimientos de emergencia implementados por el grupo de Salud Ocupacional o prevención de desastres de la gobernación del Quindío, previa notificación a uno de sus integrantes.

Procedimientos de Emergencia en la Sala de Computadores

Si la naturaleza del desastre no da tiempo para apagar y evacuar, la prioridad más alta es la seguridad de las personas. Ellos deben salir inmediatamente del Centro de Cómputo o área afectada. En un caso de éstos, el siguiente paso es notificar inmediatamente al grupo de administración de emergencia (Grupo de Salud Ocupacional o gestión de riesgos de la gobernación del Quindío).

Si hay tiempo para apagar, se deben realizar las siguientes actividades, en el orden especificado:

1. Inicializar procedimientos de emergencia organizacional estándar (los establecidos por el Grupo de Salud Ocupacional gestión de riesgos de la gobernación del Quindío).
2. Ejecutar procedimientos de apagado para los servidores y demás dispositivos del data center.
3. Apagar extractores.
4. Apagar luces y bajar tacos en las cajas de distribución.

Gobernación del Quindío
Calle 20 No. 13-22
www.quindio.gov.co
Armenia, Quindío

PBX: 7 417700 EXT: 250
tecnologia@quindio.gov.co

SEGUNDA FASE: Procedimientos para el proceso de restauración.

Tan pronto como se haya declarado un desastre, los líderes de grupo serán llamados para implantar el plan a tomar en el desarrollo del Plan de Contingencias.
El grupo de Centro de Cómputo junto con el grupo de atención a usuarios establecerá un centro de control y empezarán la coordinación para la restauración de los sistemas que hayan sido afectados.

Acciones a tomar

Dentro de las 6 horas siguientes al desastre se debe:

1. Notificar a los usuarios la interrupción del servicio.
2. Efectuar una evaluación de daños e identificar que equipos se pueden reusar para transferirlo al data center alterno.
3. Seleccionar y catalogar las oficinas de servicio para el procesamiento de los reportes de respaldo.

Dentro de las 24 horas siguientes al desastre debe:

1. Contactar con el proveedor y ordenar el soporte tanto de hardware como de aplicativos como siscar, sevenet, PCT, intranet, pagina web, etc.
2. Iniciar y coordinar los procedimientos de preparación del lugar para el data center Alterno.
3. Montar data center alterno.
4. Notificar a los proveedores las configuraciones de Hardware nuevas y alistar los requerimientos que surjan de esas configuraciones.
5. Confirmar el soporte dado por el proveedor.
4. Inicializar las preparaciones ambientales en el data center o Centro de Respaldo. (Eléctrica, protección contra incendio, extractores).
5. Ordenar los circuitos para comunicación de datos en el data center, si es necesario.

Dentro de los 5 días siguientes al desastre:

1. El data center alterno de la gobernación debe estar totalmente preparado para operar llevar el inventario de los medios magnéticos, los listados y otra documentación en el Centro Alterno.
2. Recibir en el data center suficientes suministros, muebles y ecuipo relacionado.

Gobernación del Quindío
Calle 20 No. 13-22
www.quindio.gov.co
Armenia, Quindío

PBX: 7 417700 EXT: 250
tecnologia@quindio.gov.co

3. Establecer un catálogo de procesamiento de las aplicaciones críticas.

Dentro de los 7 días siguientes al desastre debe:

1. Completar la preparación ambiental del Centro Alterno
2. Recibir la documentación y el medio magnético de los lugares de almacenamiento en el data center alterno.
3. Asegurar el ambiente físico en el data center alterno y establecer la seguridad de los datos.
4. Restablecer los backups de datos.
5. Evaluar los sistemas en línea, para verificar la operación y validez de los datos restaurados.
6. Notificar a los usuarios el estado de la recuperación.

Dentro de los 15 días siguientes al desastre:

1. Asegurar la operación total de los sistemas críticos.
2. Continuar la implantación por fases de la red de comunicación de datos

Dentro de los 30 días siguientes al desastre:

1. Restauración completa de la red de comunicación de datos y de las operaciones.

TERCERA FASE: Recuperación en el sitio original o alterno

Mientras que las operaciones se estén ejecutando en el data center alterno, se harán planes para la recuperación total en el sitio original. Si hay un desastre mayor, o si está dentro de los planes de la organización, se puede realizar la recuperación en un sitio alterno improvisado.

Los siguientes son los componentes procedimentales importantes de las actividades en esta fase:

- Decisiones en el tiempo y equipo de recuperación.
- Preparar restauración del lugar.
- Desarrollo de los procedimientos de recuperación para la localización permanente.
- Repetir los procedimientos de recuperación.
- Asegurar el ambiente físico y establecer la seguridad de los datos.

Gobernación del Quindío
Calle 20 No. 13-22
www.quindio.gov.co
Armenia, Quindío

PBX: 7 417700 EXT: 250
tecnologia@quindio.gov.co

- Montaje de los sistemas.
- Evaluación de los sistemas-
- Realizar auditoría post-desastre.
- Preparar reclamación de los seguros.
- Reportar a la gobernación.

CUARTA FASE: Mantenimiento

Parte del mantenimiento del Plan será la Programación de sistemas requeridos para mantener los programas con los cambios sobre el tiempo, del hardware, software y aplicaciones. Esta es obviamente la clave para el futuro exitoso del plan.

La actualización de nombres, responsabilidades y números telefónicos de los participantes claves de la dirección TIC y la secretaria Administrativa es además críticamente importante.

El Plan será auditado para ver que estos detalles sean actualizados rutinariamente en el plan y en todas sus copias.

Gobernación del Quindío
Calle 20 No. 13-22
www.quindio.gov.co
Armenia, Quindío

PBX: 7 417700 EXT: 250
tecnologia@quindio.gov.co

IMPLEMENTACION DEL PLAN

Para la implementación del Plan, deben estar formalmente documentados, y en operación, los siguientes procedimientos:

- Retención y respaldo de archivos permanente y corriente de los aplicativos que se manejan en el data center de la gobernación del Quindío.
- Recuperación de errores y fallas del sistema.
- Seguridad física y lógica.
- Seguimiento al plan de mantenimiento preventivo y correctivo de equipos por parte del supervisor del contrato de dicho mantenimiento.
- Administración de personal en lo referente a las emergencias.
- En primera instancia, el presente plan debe ser puesto a consideración, revisión y aprobación por parte del director TIC y el director de sistemas de la gobernación del Quindío.
- En segunda instancia, desarrollar un programa de entrenamiento a los sujetos y áreas directamente involucradas, aquellas que asumen responsabilidades y funciones dentro del plan.
- Finalmente, debe adoptarse a nivel institucional mediante Acto Administrativo, es decir, reglamentado por Resolución.

CATALINA GÓMEZ RESTREPO
Secretaria Administrativa
Departamento del Quindío

JAIME ALBERTO LLANO CHAPARRO
Director TIC
Departamento del Quindío

Elaboró: Jaime Alberto Llano Chaparro – Director TIC

Gobernación del Quindío
Calle 20 No. 13-22
www.quindio.gov.co
Armenia, Quindío

PBX: 7 417700 EXT: 250
tecnologia@quindio.gov.co