PLAN DE TRATAMIENTO DE RIESGO DE SEGURIDAD DE LA INFORMACIÓN VIGENCIA 2025

Tabla de contenido

INTRODUCCIÓN

La Lotería del Quindío en concordancia con las actividades de la estrategia de gobierno digital y la elaboración del modelo de seguridad y privacidad de la información elabora este documento, con el fin de tener una línea base durante el análisis y el recorrido de la construcción del modelo de seguridad y privacidad de la información, con el fin de proteger los bienes, activos, servicios, derechos y dependientes del estado.
Teniendo en cuenta lo anterior la Lotería 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.

1. OBJETIVOS

Planear e implementar en la Lotería del Quindío los procedimientos y elementos mínimos requeridos para afrontar alguna contingencia relacionada con un eventual cese de actividades, inoperatividad de equipos causado por razones de fuerza mayor y de diferente índole.

1.1 Objetivos específicos

- Identificar y solucionar de manera rápida y eficaz cualquier problema que se presente con los sistemas información de la Lotería del Quindío.

- Proteger y conservar los activos informáticos de la Lotería del Quindío contra riesgos, desastres naturales o actos malintencionados.

- Garantizar la operatividad de la red interna de la Lotería 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.

2. ALCANCE

La necesidad de implementar un plan de contingencias, 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 LOTERIA 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 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 áreas y de los recursos disponibles (capacitación, recursos técnicos, presupuesto, etc.).

3. ROLES Y RESPONSABILIDADES

3.1 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.

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

3.2 Talento Humano

El profesional especializado de gestión administrativa y gestión financiera, designara a un auxiliar administrativo cumplirá la función de notificar a todo el personal que se vincula por nombramiento o contractualmente con la Lotería 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.

3.3 Recursos Físicos

El profesional especializado de Tesorería y Bienes 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 Lotería del Quindío.

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

3.4 Administrativa y Gestión Financiera

El área Administrativa y Gestión Financiera, en conjunto con el área de Recursos Tecnológicos, cumplirá la función de darle continuidad al modelo de seguridad y privacidad de la información (MSPI), así como también de proponer cambios en dicho modelo, generar el plan de continuidad del negocio, asignar responsabilidades dentro de la matriz de riesgos de la entidad y especificar los planes de respuesta al riesgo ante alguna eventualidad que pueda llegar a suceder.

3.5 Recursos Tecnológicos

El profesional especializado de Recursos Tecnológicos cumplirá 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. También velará por el cumplimiento de las políticas de la información en la Lotería 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.

El profesional especializado de Recursos Tecnológicos junto con el encargado del área jurídica, 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 Lotería del Quindío y que manejen datos susceptibles de la entidad.

3.6 Jurídica

El profesional especializado encargado del área de Jurídica, 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.

3.7 Gestión Control y Evaluación (Control Interno)

El profesional especializado de control interno cumplirá la función de vigilar y ejercer los controles disciplinarios necesarios para que los funcionarios de la Lotería del Quindío cumplan a cabalidad lo dispuesto en el documento de políticas de seguridad de la información.

4. IDENTIFICACION Y ANALISIS DE RIESGOS

4.1 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 Lotería.
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.

4.2 Análisis de Riesgos

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

4.2.1 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 Lotería 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.

4.2.2 Riesgos por incidencia interna

- Perdida de la información: Hace referencia a la seguridad de la información que maneja la Lotería 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.

- Falla en servidores: Los servidores que se encuentran en la oficina de Recursos Tecnológicos de la Lotería del Quindío, pueden llegar a presentar fallas de configuración, provocando que se paren los aplicativos esenciales con los que trabajan los funcionarios, como SIL y MI CORRESPONDENCIA.

- 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 Lotería de Quindío.

- Calentamiento del Rack de Comunicaciones: Este riesgo está asociado a la probabilidad de que se incremente la temperatura del Rack de Comunicaciones por encima de los mínimos permitidos por el área de Recursos Tecnológicos, cabe aclarar que en el Rack de Comunicaciones se encuentran los Switch principales de la red interna y las UPS, 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 el área de Recursos tecnológicos.

- 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.

- 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 SIL, Mi Correspondencia, Pagina Web ,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 Lotería del Quindío.

- Accesos no autorizados a los sistemas de información: Hace referencia a accesos a las bases de datos no autorizados de los diferentes aplicativos misionales de la entidad y de computadores que manejen información confidencial de la misma.

- Equivocaciones humanas: Riesgo permanente que se genera por el desconocimiento, descuido, o mal uso de un sistema de información o aplicativo de la entidad.

- Activos de la información desactualizados: La no actualización de los activos de la información por parte del área de Recursos Tecnológicos, genera un riesgo inherente a la pérdida de la información y/o desconocimiento de lo que se encuentra instalado en cada equipo de la entidad.

- Equipos de red (Switch) conectados a puntos de red a la vista de funcionarios y de fácil acceso: Riesgo

asociado a equipos de red identificados en diferentes pisos de la entidad, los cuales tienen acceso cualquier funcionario o persona ajena a la entidad, pudiéndose conectar a internet.

4.3 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:

4.3.1 Desastres naturales

Aunque realmente un desastre natural no se puede evitar, la Lotería 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 Lotería, no cuenta con una estructura sismo resistente, debido a que es un edificio antiguo, teniendo en cuenta este factor se implementa el software libre OwnCloud que permite realizar copias automáticas a los equipos conectados a la red y los almacena en la nube; adicional a esto, se cuentan con copias realizadas en discos duros de la información y que están por fuera de la entidad y el servicio en la nube por parte de la empresa Lapoint Ict SAS ubicado en la zona franca de Antioquia, que ayuda a que en caso de terremoto ayuda a salvaguardar la información.

Por otra parte, la red interna de la Lotería del Quindío, está respaldada con UPS, para evitar que los Switch se dañen en caso de tormentas eléctricas, con este mismo respaldo cuentan los servidores de la Lotería.

4.3.2Interrupción del fluido eléctrico

La red interna de la Lotería del Quindío se encuentra respaldada con UPS, para que esta siga su funcionamiento normalmente durante más de 15 minutos de interrupción, esto con el fin de tener tiempo para apagar los servidores de una manera correcta, evitando un mayor traumatismo.

4.3.3 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.

4.3.4 Pérdida de Información

La Lotería del Quindío, cuenta con una política de respaldo de la información de los servidores de la Lotería, este respaldo se realiza todos los días en discos duros externos que se encuentran en la oficina de recursos físicos.

4.3.5 Falla de equipos electrónicos

Para tratar de mitigar este riesgo, la Lotería del Quindío a través del área de Recursos Tecnológicos, Realiza anualmente mantenimiento preventivo y correctico.

4.3.6 Falla en servidores

Los servidores se actualizan constantemente con las últimas actualizaciones de seguridad.

4.3.7 Virus informáticos

Contra los virus informáticos, la Lotería 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 con el mantenimiento preventivo y correctivo que se realiza cada año, incluye mantenimiento de software y sistema operativo (desinfección).

4.3.8 Seguridad o Robo

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

4.3.9 Calentamiento del Rack de Comunicaciones

Este riesgo tiene una baja probabilidad de ocurrencia, debido a que la Lotería del Quindío ha implementado procedimientos para su mitigación, tales como: La implementación del Rack de Comunicaciones (piso 1) un Sistema de Temperatura autorregulada, provisto de un sistema de aire acondicionado.

4.3.10 Copias de seguridad sistemas de información

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

4.3.11 Falta de actualización de la infraestructura tecnológica

La Lotería 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.

4.3.12 Incumplimiento de los contratistas

Dentro de los procesos de contratación que tiene la Lotería 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.

4.3.13 Retrasos en Procesos Administrativos

La Lotería del Quindío tiene como prioridad el resguardo de la seguridad de la información, por tal motivo se intenta contar como primer lugar con todos los proveedores y personal capacitado para el área de recursos tecnológicos.

4.3.14 Procesos de capacitación constante del personal TI

El área de recursos tecnológicos, capacita en el manejo de los sistemas de información a todo el personal que ingresa a la dependencia, 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 Lotería.
Por otra parte, a través de la estrategia de gobierno en línea, se capacita constantemente a su personal en implementación de la misma.

4.3.15 Accesos no autorizados a los sistemas de información

Como parte de las políticas de seguridad de la información aprobada, la entidad cuenta con una política de bloqueo de cesión e ingresar con contraseña. Lo anterior con el fin de evitar accesos no autorizados a los sistemas cuando el funcionario responsable del equipo no se encuentre en el sitio de trabajo.
Por otra parte, y con el fin de evitar acceso no autorizado a los sistemas de información por parte de personas tanto internas como externan a la Lotería del Quindío; La entidad cuenta con un firewall instalado y con un sistema de antivirus licenciado que brindan seguridad a la hora de bloquear intentos de ataques o accesos a sistemas de información de la entidad.

4.3.16 Equivocaciones humanas

Si bien es cierto que este riesgo es difícil de mitigar, es importante resaltar que el área de recursos tecnológicos brinda capacitaciones a los funcionarios de la entidad, sobre el manejo de los aplicativos de la entidad, además de eso, desde el área se generan copias de seguridad diarias de las bases de datos de los aplicativos de la entidad, lo anterior con el fin restaurar la información, ante cualquier perdida o daño que se haga en una base de datos.

4.3.17 Activos de la información desactualizados

Dentro de los planes y controles que la oficina se está construyendo en la actualidad, se tiene establecido el catálogo de servicios tecnológicos y la arquitectura de servicios TI, los cuales deben de tener actualizados los activos de la información para su correspondiente actualización anual.

Equipos de red (Switch) conectados a puntos de red a la vista de funcionarios y de fácil acceso Como parte del levantamiento de los diagramas de red y activos de la información de IPV6, se verifico que la entidad no

tiene puntos de red no autorizados, gracias a la infraestructura del lugar y a que el número de empleados y funcionarios no superan las 30 personas, es más fácil ejercer un control sobre este tipo de situaciones.

5. 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.

5.1 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

- 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 profesional especializado de Recursos Tecnológicos de Lotería, 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 Lotería del Quindío dispone de una base de datos con todas las contraseñas de los servidores de la Lotería del Quindío y que contiene información para restablecimiento de la información en caso de pérdida o robo, desastre natural, etc.

5.2 Recuperación del desastre: plan de acción

El Plan presupone que debe utilizarse un Centro de Cómputo alterno externo al edificio sede de la Lotería 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.

5.3 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 (data center de la entidad), debe implantarse inmediatamente los procedimientos de emergencia implementados por el grupo de Salud Ocupacional o prevención de desastres de la Lotería del Quindío, previa notificación a uno de sus integrantes.

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

- Inicializar procedimientos de emergencia organizacional estándar
- Ejecutar procedimientos de apagado para los servidores y demás dispositivos del Rack de Comunicaciones.

5.4 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 sistemas 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.

5.4.1 Acciones a tomar

Dentro de las 6 horas siguientes al desastre se debe:

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

Dentro de las 24 horas siguientes al desastre debe:

- Contactar con el proveedor y ordenar el soporte tanto de hardware como de aplicativos como SIL, Mi Correspondencia, página web, etc.
- Iniciar y coordinar los procedimientos de preparación del lugar para el data center Alterno.
- Montar data center alterno.

- Notificar a los proveedores las configuraciones de Hardware nuevas y alistar los requerimientos que surjan de esas configuraciones.
- Confirmar el soporte dado por el proveedor.
- Inicializar las preparaciones ambientales en el data center o Centro de Respaldo. (Eléctrica, protección contra incendio, extractores).
- Ordenar los circuitos para comunicación de datos en el data center, si es necesario.

Dentro de los 5 días siguientes al desastre:

- El data center alterno de la Lotería debe estar totalmente preparado para operar llevar el inventario de los medios magnéticos, los listados y otra documentación en el Centro Alterno.
- Recibir en el data center suficientes suministros, muebles y equipo relacionado.
- Establecer un catálogo de procesamiento de las aplicaciones críticas.

Dentro de los 7 días siguientes al desastre debe:

- Completar la preparación ambiental del Centro Alterno
- Recibir la documentación y el medio magnético de los lugares de almacenamiento en el data center alterno.
- Asegurar el ambiente físico en el data center alterno y establecer la seguridad de los datos.
- Restablecer los backups de datos.
- Evaluar los sistemas en línea, para verificar la operación y validez de los datos restaurados.
- Notificar a los usuarios el estado de la recuperación. Dentro de los 15 días siguientes al desastre:
- Asegurar la operación total de los sistemas críticos.
- Continuar la implantación por fases de la red de comunicación de datos Dentro de los 30 días siguientes al desastre:
- Restauración completa de la red de comunicación de datos y de las operaciones.

5.5 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.

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

5.6 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 del comité de la seguridad de la información. El Plan será auditado para ver que estos detalles sean actualizados rutinariamente en el plan y en todas sus copias.

6. 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 los servidores de la Lotería 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 profesional especializado del área de Recursos Tecnológicos de la Lotería 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 por la entidad, bajo un acta del Comité de MIPG.

CAROLINA JARAMILLO QUINTERO
Gerente de la Lotería del Quindío

CARLOS BAUTISTA OSORIO
P.E Gestión Recursos Tecnológicos