# PLAN DE TRATAMIENTO DE RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

**CONTRALORÍA GENERAL DE BOYACÁ**
**DIRECCIÓN TÉCNICA DE SISTEMAS**
**TUNJA, BOYACÁ**
**2022**

| | | | | | |
|---|---|---|---|---|---|
| FIRMA | | FIRMA | | FIRMA | |
| ELABORÓ | | REVISÓ | | APROBÓ | |
| CARGO | | CARGO | | CARGO | |

## TABLA DE CONTENIDO



| | | | | | |
|---|---|---|---|---|---|
| FIRMA | | FIRMA | | FIRMA | |
| ELABORÓ | | REVISÓ | | APROBÓ | |
| CARGO | | CARGO | | CARGO | |

## INTRODUCCIÓN

La información es el pilar y activo intangible más importante de las organizaciones y por ello se deben consolidar estrategias que mejoren su seguridad, disponibilidad, y confidencialidad, dentro de la Entidad.

La digitalización de la información física a los sistemas de información y los inventarios documentales que se deben administrar por largos periodos de tiempo, estimados dentro de los procesos documentales institucionales obliga a que se establezcan políticas y procedimientos en los que todos los integrantes de la organización deben hacer aportes y tener responsabilidades definidas, además de velar por el correcto uso de los servicios y elementos dispuestos para la labor diaria en búsqueda del cumplimiento de los objetivos misionales y administrativos.

De igual forma la mayor dependencia de las TI, en todas las áreas que componen la entidad, para el cumplimiento de tareas, lleva a mejorar el conocimiento en las vulnerabilidades y amenazas que a diario se crean para afectar los procesos organizacionales, aprovechando el desconocimiento y el ocio de las personas y por lo cual se deben buscar las mejores estrategias para evitar riesgos de pérdida de información o riesgos de daño a hardware que impidan desarrollar las tareas y cumplimiento de compromisos institucionales personales y grupales.

Es importante destacar que a medida que mejora la tecnología, también aumentan las amenazas y riesgos, por lo cual se debe tener una retroalimentación de un buen uso de los servicios tecnológicos de la Entidad, con una sensibilización permanente de las posibles problemáticas y generando responsabilidad en el uso y confidencialidad de los datos.

Desde el MINTIC la implementación de mejores prácticas en el uso de la información y la importancia de tener entidades más transparentes al servicio de la comunidad basados en cuatro (4) ejes temáticos: TIC PARA GOBIERNO ABIERTO, TIC PARA SERVICIOS, TIC PARA GESTION y como eje transversal el de SEGURIDAD Y PRIVACIDAD DE LA INFORMACION, cuyo objetivo es el de garantizar la prestación

de servicios a la ciudadanía en general y la protección de la información de las entidades del Estado.

La evaluación permanente de estos elementos por parte de entes gubernamentales ha llevado a que en la Contraloría General de Boyacá mejore sus procesos en el desarrollo tecnológico, buscando una renovación de hardware y software, elementos indispensables en la implementación de herramientas de seguridad, con la adquisición de mejores servicios por parte de proveedores de servicios de internet y seguridad perimetral y el desarrollo de planes de contingencia que ante la eventualidad de problemáticas los tiempos de ausencia de servicios sean mínimos, así como propender por culturas responsables en la administración de la información, haciendo uso de herramientas de almacenamiento externo e información por malos hábitos de administración de datos, y uso exclusivo para actividades institucionales.

La Contraloría General de Boyacá, ha dispuesto servicios locales de sistemas de información para servicios de administración de información esencial de la Entidad, con servidores de cómputo ubicados en la Dirección Técnica de sistemas, dejando la custodia de la información y la administración técnica de las bases de datos, quien se encarga de mantener los sistemas de información funcionando para la prestación de servicios. Cualquier riesgo o falla sobre la infraestructura tecnológica que afecte el servicio ofrecido a través de los sistemas de información, es la Dirección Técnica de sistemas quien se encarga de garantizar la no suspensión total del servicio y por ende la encargada de restablecerlo, con estrategias que permitan continuidad de los servicios y mejoren la integridad y seguridad de la información.

# OBJETIVOS

## Objetivo General

Garantizar servicios de tecnología para el desarrollo de actividades de la Contraloría General de Boyacá, ante la posibilidad de presentar situaciones que alteren la normalidad de uso de los sistemas de información y servicios conexos, que ante la eventualidad de problemáticas externas e internas, se tengan habilitadas estrategias para minimizar la ausencia de servicio con planes de contingencia eficientes y eficaces minimizando los tiempos de inoperatividad.

## Objetivos Específicos

- Minimizar la perdida de información de los sistemas de información administrativa y financiera ante la posibilidad de errores humanos o fallas técnicas.

- Identificar y mitigar los riesgos a los que se encuentra expuesta la red de datos de la entidad.

- Mantener la disponibilidad de los servicios tecnológicos a los usuarios de la entidad.

- Restablecer el funcionamiento de los sistemas de información en el menor tiempo posible ante la presentación de ausencias de servicio que se puedan llegar a presentar.

- Mantener operativos los sistemas de información críticos de la entidad cuando son interrumpidos o paralizados por contingencias que afectan parcial o totalmente las instalaciones donde se procesan los sistemas y los servicios de datos de la Entidad.

## ALCANCE

El Plan de Contingencia de TI de la Contraloría General de Boyacá, busca mantener en operación la infraestructura de hardware y software de la Entidad, los equipos de comunicaciones elementos esenciales para la transaccionabilidad de la información digital y análoga y necesaria para la comunicación de la Entidad con entes de control y los sujetos y puntos de control que tiene a cargo en el Departamento de Boyacá. Sistemas de información esenciales como SYSMAN, SIDCAR, FLASH y herramientas externas al servicio de la Contraloría como son SIA OBSERVA, SIA CONTRALORIAS, SIREL y demás sistemas de información de carga y consulta que dependen de una red de datos eficiente con conexiones a internet agiles que deben estar siempre disponibles para el cumplimiento de compromisos organizacionales que tienen a la Entidad en una continua medición y cumplimiento de objetivos institucionales.

## CONSIDERACIONES

Se consideran los siguientes tipos de incidentes:

- Cualquier incidente externo o interno que pudiera potencialmente causar una interrupción de las operaciones del negocio, tales como la pérdida de los servicios de suministro eléctrico o de telecomunicaciones.
- Cualquier incidente que afecte al funcionamiento del hardware o del software y que suponga una interrupción superior a las 24 horas.
- Cualquier incidente interno que pudiera potencialmente causar o afectar la interrupción de las operaciones de los sistemas de información, como son la falla en los servidores o puntos de conexión.
- Cualquier incidente que suponga la paralización de actividades de la organización por motivos ajenos a la tecnología, tales como problemas laborales propios o del sector o problemas laborales que afecten al área geográfica donde se encuentra ubicada la organización.

Se descartan o son poco probables de suceder los siguientes tipos de incidentes:

- Los que causen un daño físico en las instalaciones o equipos, como fuego, humo o daños por agua.
- Los que afecten de forma indirecta la posibilidad de acceso a las instalaciones, como evacuación de emergencia por amenaza de bomba, o amenazas externas tales como incendios en instalaciones cercanas, fuga de gases tóxicos, etc.
- Desastres regionales no previstos o inesperados, que puedan causar daños en las instalaciones y equipos e impedir el acceso normal al personal encargado o quien haga sus funciones de las operaciones informáticas, aunque las instalaciones estén intactas, tales como inundaciones, huracanes entre otros.

## DEFINICIONES TÉCNICAS

- **Copias de seguridad (Backup):** una copia de seguridad o backup (su nombre en inglés) en tecnología de la información o informática es una copia de seguridad - o el proceso de copia de seguridad - con el fin de que estas copias adicionales puedan utilizarse para restaurar el original después de una eventual pérdida de datos. Disco duro: en informática, un disco duro o disco rígido (en inglés Hard Disk Drive, HDD) es un dispositivo de almacenamiento de datos no volátil que emplea un sistema de grabación magnética para almacenar datos digitales. Se compone de uno o más platos o discos rígidos, unidos por un mismo eje que gira a gran velocidad dentro de una caja metálica sellada. Sobre cada plato se sitúa un cabezal de lectura/escritura que flota sobre una delgada lámina de aire generada por la rotación de los discos.
- **Enrutador (router):** el enrutador (calco del inglés *router*), direccionador, ruteador o encaminador es un dispositivo de hardware para interconexión de red de ordenadores que opera en la capa tres (nivel de red). Un enrutador es un dispositivo para la interconexión de redes informáticas que permite asegurar el enrutamiento de paquetes entre redes o determinar la mejor ruta que debe tomar el paquete de datos.
- **Hardware:** corresponde a todas las partes físicas y tangibles de una computadora: sus componentes eléctricos, electrónicos, electromecánicos y mecánicos; sus cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado.
- **Hub**: Concentrador. Dispositivo capaz de enlazar físicamente varios ordenadores de forma pasiva, enviando los datos para todos los ordenadores que estén conectados, siendo éstos los encargados de discriminar la información.
- **LAN:** (Local Area Network - Red de Área Local). Interconexión de computadoras y periféricos para formar una red dentro de una empresa u hogar, limitada generalmente a un edificio.

- **Módem:** Un módem es un dispositivo que sirve para enviar una señal llamada *moduladora* mediante otra señal llamada *portadora*. Se han usado módems desde los años 60, principalmente debido a que la transmisión directa de las señales electrónicas inteligibles, a largas distancias, no es eficiente, por ejemplo, para transmitir señales de audio por el aire, se requerirían antenas de

gran tamaño (del orden de cientos de metros) para su correcta recepción. Es habitual encontrar en muchos módems de red conmutada la facilidad de respuesta y marcación automática, que les permiten conectarse cuando reciben una llamada de la RTPC (Red Telefónica Pública Conmutada) y proceder a la marcación de cualquier número previamente grabado por el usuario. Gracias a estas funciones se pueden realizar automáticamente todas las operaciones de establecimiento de la comunicación.

- **Plan de Contingencia:** Conjunto de estrategias, acciones, procedimientos planificados y responsabilidades definidas para minimizar el impacto de una interrupción imprevista de las funciones críticas y conseguir la restauración de las mismas, dentro de unos límites de tiempo establecidos. Sin que sea una regla general, se suele aplicar al plan circunscrito a las actividades de los departamentos de Sistemas de Información.
- **Red:** Una red de computadoras, también llamada red de ordenadores o red informática, es un conjunto de equipos informáticos conectados entre sí por medio de dispositivos físicos que envían y reciben impulsos eléctricos, ondas electromagnéticas o cualquier otro medio para el transporte de datos para compartir información y recursos. Este término también engloba aquellos medios técnicos que permiten compartir la información.
- **Software:** se conoce como software al equipamiento lógico o soporte lógico de una computadora digital; comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos del sistema, llamados hardware. Servidores: una aplicación informática o programa que realiza algunas tareas en beneficio de otras aplicaciones llamadas clientes. Algunos servicios habituales son los servicios de archivos, que permiten a los usuarios almacenar y acceder a los archivos de una computadora y los servicios de aplicaciones, que realizan tareas en beneficio directo del usuario final. Este es el significado original del término. Es posible que un ordenador cumpla simultáneamente las funciones de cliente y de servidor.
- **S.O.:** (Sistema Operativo): un Sistema operativo (SO) es un software que actúa de interfaz entre los dispositivos de hardware y los programas de usuario o el usuario mismo para utilizar un computador. Es responsable de gestionar, coordinar las actividades y llevar a cabo el intercambio de los recursos y actúa como intermediario para las aplicaciones que se ejecutan.

## ANÁLISIS DE LA SITUACIÓN ACTUAL

El Plan de Contingencia de Sistemas de Información implica un análisis de los posibles riesgos a cuáles pueden estar expuestos nuestros equipos de cómputo y sistemas de información en la CGB. Corresponde a la Dirección Técnica de Sistemas aplicar medidas de seguridad para proteger y estar preparados para afrontar contingencias y desastres de diversos tipos. El Plan de Contingencia de los Sistemas de Información de la CGB está orientado a establecer un adecuado sistema de seguridad lógica (firewall) en previsión de desastres, para establecer medidas destinadas a salvaguardar la información contra los daños producidos por hechos naturales, técnicos, organizacionales, proveedores, soporte, falla de hardware, errores humanos, entre otros. La información como uno de los activos más importantes de la Contraloría, es el fundamento más importante de este Plan.

El Plan se ha desarrollado sobre los siguientes supuestos:

- Sólo el área habitual de trabajo ha sido afectada por el incidente; todos los lugares alternativos pre designados están intactos.
- Los almacenes externos de archivos críticos de Backup e información están intactos y accesibles.
- El personal cualificado en cantidad suficiente está disponible para realizar los trabajos de recuperación.
- Las copias de seguridad y su correspondiente actualización se han realizado correctamente, y se ha corregido cualquier riesgo identificado.
- El Backup de las telecomunicaciones y las estrategias de recuperación identificadas en otros capítulos del presente plan, están completamente realizadas y comprobadas.
- Las estrategias de recursos y soluciones de recuperación (por ejemplo: soluciones de reposición de estaciones de trabajo) están disponibles, realizadas y comprobadas satisfactoriamente.
- Las organizaciones externas como proveedores, cooperarán razonablemente durante el periodo de los trabajos de recuperación.
- Se han realizado adecuadamente los programas de pruebas del Plan y las modificaciones pertinentes como consecuencia de su resultado.
- La revisión del Plan, mantenimiento, y actualizaciones están realizadas con periodicidad para asegurar que responde a las necesidades de cada momento.

## FUNCIONES DE LA DIRECCIÓN

Las funciones de la Dirección técnica de sistemas se limitan a la revisión y aprobación de cualquier acción que exceda de las estrategias de respuesta y recuperación planificadas y previamente aprobadas. Solo en los casos en que el incidente haya sobrepasado las previsiones se precisa la intervención directa de la Dirección. En esos casos, el responsable de reportar los incidentes debe preparar informes para la Dirección para ayudar a la gestión de cada día y a la toma de decisiones acerca de cuestiones no previstas en el plan.

## INFORME A DIRECCIÓN

En el supuesto de suceder cualquier incidente, la persona encargada de reportar, una vez atendidas las decisiones más urgentes descritas en el Plan de Contingencia, emitirá un informe a la Dirección con el siguiente contenido:

Estado de las actividades de respuesta a la emergencia:

- Evaluación de los daños a los sistemas de información.
- Respuesta de los organismos públicos.

Descripción del incidente:

- ¿Qué ocurrió?
- Localización del suceso.
- Hora del suceso.
- Supuesta causa.

Informe de daños a los servidores.

- Descripción del servidor.
- Nombre y estado de los daños al sistema del servidor.
- Daños potenciales adicionales.

Áreas afectadas:

- Áreas afectadas.
- Estado actual.
- Posibilidad de acceso a corto plazo a los sistemas de información.
- Impacto en las operaciones del negocio.

Plan de Acción:

- Localización del Centro de Control.

- Situación de las comunicaciones con los sistemas de información.
- ¿Qué se ha hecho hasta ahora?
- Planes a corto plazo.

La identificación de las posibilidades de riesgo interno y externo y la gradualidad del impacto es proporcionar la información necesaria para la toma de decisiones en el desarrollo de su estrategia de recuperación. Para ello, el Análisis de Impacto debe establecer el grado de criticidad de dichas funciones dentro de la Dirección técnica de Sistemas y la forma en la que se pueden minimizar los tiempos en la restauración del servicio, así como la identificación del posible origen de la problemática y como poder generar las tareas de contingencia minimizando las pérdidas asociadas a la información dentro de los sistemas y procederes y alternativas para dar continuidad de los servicios de la Contraloría hacia la comunidad y poder cumplir con los compromisos documentales tanto de análisis como de evaluación a entes externos.

Una vez identificadas los posibles problemáticas se deben enfocar los esfuerzos de la dirección y de la alta gerencia en localizar los objetivos de restauración como:

- Definir los tipos de impacto que se deberían considerar, (económico, operacional, de cumplimiento, etc.).
- Identificar las funciones críticas de la Contraloría General de Boyacá.
- Identificar el impacto causado a la Contraloría por la interrupción de cada una de ellas.
- Informar al Despacho del Contralor y Dirección Administrativa, de los resultados anteriores para que pueda fijar prioridades, definiendo cuáles son las funciones consideradas prioritarias y establecer los procedimientos de recuperación.
- Posibilitar la identificación de los recursos mínimos necesarios para una recuperación satisfactoria de las funciones definidas como críticas y justificar su adquisición.

## IMPACTOS MÁS COMUNES

Se debe tener en cuenta que pueden ocurrir fallos en la comunicación de la información de un evento o desastre, trayendo como resultado reacciones negativas graves, esto puede ser causado por situaciones tales como:

- Falta de compresión por parte de los funcionarios, judicantes, practicantes y demás personal sobre los acontecimientos.
- Sensación de incompetencia de la dirección percibida por usuarios externos, funcionarios, judicantes y practicantes.

**Caída o interrupción en el servicio de internet.**

- La ausencia de servicio de internet es una de las funciones que mayor impacto tienen en la Entidad y requiere de respuesta inmediata y oportuna generalmente no puede exceder su ausencia de pocos minutos, pero que generalmente la presentación de problemas no depende de la red local sino del proveedor del servicio y la solicitud al requerimiento no puede superar las ocho horas, en caso extremo donde por condiciones naturales o de infraestructura se ha afectado la fibra óptica por la cual se hace la transmisión de la señal.

Se debe tener en cuenta que pueden ocurrir fallos en la comunicación de la información de un evento o desastre, trayendo como resultado reacciones negativas graves, esto puede ser causado por situaciones tales como:

- Falta de compresión por parte de los funcionarios, judicantes, practicantes y demás personal sobre los acontecimientos.
- Sensación de incompetencia de la dirección percibida por usuarios externos, funcionarios, judicantes y practicantes.

**Caída o interrupción del sistema eléctrico**

- Riesgo externo. Corresponde al corte del servicio de energía eléctrica en la Contraloría General de Boyacá por parte de falla externa en el proveedor del servicio o fallo en la infraestructura del Edificio donde se encuentra las oficinas

de la Entidad. El corte eléctrico que genera interrupción del funcionamiento de los equipos donde se alojan los aplicativos críticos de la entidad, que puede dejar los servicios y aplicativos inoperantes. Tipo de riesgo: Tecnología.

**Caída del canal de internet**

- Riesgo externo. Consiste en las fallas técnicas por parte del proveedor del servicio de internet, lo que ocasionaría suspensión de los servicios de correo electrónico, Sistema de Gestión Documental SIDCAR y de los aplicativos críticos de la entidad. Tipo de riesgo: Tecnológico.

**Caída del Servicio Telefónico**

- Riesgo externo correspondiente a la suspensión del servicio analógico por daños o fallas del proveedor de servicio (MOVISTAR). Tipo de riesgo: Tecnológico

**Caída de servicios por virus informático**

- Riesgo externo. Es la posibilidad de infección de los equipos servidores y de cómputo que puede presentarse en la entidad por mala configuración del sistema antivirus o por ausencia de política de seguridad lo que genera la suspensión total o parcial del funcionamiento o de la prestación de un servicio de red, inoperancia o inestabilidad de los sistemas. Tipo de riesgo: Tecnológico.

**Suspensión del servicio por sismo, inundación o incendio**

- Riesgo externo. Hace referencia al riesgo que corre la entidad para que se presente un evento de sismo, inundación o incendio que afecte la infraestructura tecnológica de los sistemas de información, generando suspensión total o parcial del funcionamiento o de la prestación de un servicio de red, inoperancia de los sistemas o inestabilidad de los mismos. Tipo de riesgo: Operativo.

**Retrasos en el Proceso precontractual de la entidad en contratos relacionados con la infraestructura tecnológica de la entidad.**

- Riesgo interno que corresponde a retrasos en el proceso precontractual de la entidad en contratos relacionados con la infraestructura tecnológica de la entidad por deficiente planeación del proceso de contratación, falta de personal capacitado para realizar los estudios previos de contratación. Lo que puede ocasionar Inoperancia de los sistemas de información, desactualización de los sistemas de información. Tipo de riesgo: Operativo

**Contratación sin asistencia técnica, Soluciones Inadecuadas o Incompatibilidad frente a los Requerimientos y Recursos Disponibles**

- Riesgo interno que se relaciona con deficientes procesos de análisis, evaluación, planeación y toma de decisiones sobre la elección de las alternativas tecnológicas a ser implementadas y con el probable desconocimiento de las características y especificaciones técnicas de los recursos disponibles y las necesarias en cada una de las soluciones elegidas. Al materializarse el riesgo la infraestructura tecnológica puede generar inoperancia de los sistemas de información. Tipo de riesgo: Operativo.

**Falla técnica en equipos servidores, de escritorio o de comunicaciones**

- Riesgo interno que corresponde al daño físico o lógico de un equipo servidor, de escritorio o de comunicaciones que afecta el funcionamiento de un sistema de información crítico o de servicio por falta de mantenimiento preventivo a los equipos o por mal uso de los equipos por parte de los usuarios que hace que el servicio quede inoperante o Inestable. Tipo de riesgo: Tecnológico.

**Falla técnica en sistemas de información**

- Riesgo interno, corresponde al riesgo de presentarse errores de lógica en programación o incompatibilidad entre software que afectan a los sistemas de información que genera Inoperancia o inestabilidad de los sistemas de información. Tipo de riesgo: Tecnológico.

**Ausencia de personal de la Dirección Técnica de Sistemas para soporte y mantenimiento a los a los sistemas de información y estaciones de trabajo**

- Riesgo interno. Corresponde a la falta o inasistencia en un momento dado, de un ingeniero o técnico de la Dirección para realizar actividades de soporte a usuarios o de administración técnica sobre un sistema de información, lo que genera inoperancia o inestabilidad de los sistemas de información. Tipo de Riesgo: Operativo.

**Mal uso de hardware y/o software Institucional**

- Riesgo interno. Consiste en el riesgo que se puede presentar por un uso inadecuado de los equipos de cómputo, software y/o sistemas de información por parte de los funcionarios por deficiencias en el conocimiento y uso de las herramientas tecnológicas o por uso mal intencionado de los mismos lo que puede dejar generar interrupción del funcionamiento de los equipos donde se alojan los sistemas de información críticos de la entidad, que puede dejar los servicios y aplicativos inoperantes. Tipo de riesgo: Tecnología.

## ESTRATEGIA DE CONTINGENCIA

Para que mantener servicios se deben presentar alternativas para minimizar los problemas asociados a la ausencia de servicios informáticos y de TI, disminuyendo los tiempos de caída de servicios y se deben tener alternativas reales de contingencia, minimizando los costos por improductividad laboral asociadas al uso de servicios de TI.

## EMPRESAS PRESTADORAS DE SERVICIOS

Las empresas de servicios que se contratan para la disposición de servicios de internet tienen asociados la contratación de seguridad perimetral, servicios de hosting y ftp, esto dada la limitada infraestructura de almacenamiento con la que se cuenta y dentro de las posibilidades presupuestales se ha mejorado la adquisición de estos servicios. Estos elementos contratados permiten que la contingencia se terceriza al proveedor de servicios manteniendo esquemas de seguridad robustos y garantizando los datos de publicación web, y demás documentación institucional que se encuentra disponible a través de la web. De igual forma la configuración del firewall está acorde a las políticas de seguridad implementadas desde la dirección de sistemas y que está fundamentada en el buen uso de los recursos institucionales y la limitación de contenidos como redes sociales, contenidos ociosos y demás elementos que disminuyen la productividad laboral y generan tráfico a través de la red de datos.

Esto se complementa con las copias de seguridad realizadas desde el espacio FTP y que se desarrollan mensualmente como elemento integral en la administración de la información de la Entidad.

Para la prestación de servicio de internet, se tiene dentro de los estudios previos de adquisición la obligatoriedad de servicios de alta de calidad y con tiempos mínimos de ausencia de servicio y que después de 8 horas de ausencia son descontados de la facturación mensual, así mismo la supervisión eficiente del contrato permite generar exigencia para una prestación de servicio de alta calidad llegando al 97% de eficiencia.

## COMUNICACIONES ALTERNATIVAS

Con el fin de aminorar las problemáticas que se pueden presentar ante la ausencia de servicio por parte del canal principal de internet, se tiene contingencia a través de los servicios de telefonía fija, para las dependencias de mayor necesidad de uso y estaciones de trabajo ubicadas en la dirección técnica de sistemas que permiten evacuar consulta y navegación, evitando la ausencia total de servicio.

## PROCEDIMIENTO DE BACKUP O COPIA DE SEGURIDAD

La dirección de sistemas genera una sensibilización permanente a los usuarios de los servicios de TI para el almacenamiento de copias de seguridad en dispositivos extraíbles, clasificando la información esencial para el desarrollo de tareas y de igual forma a nivel institucional se desarrollan copias de seguridad diarias de los sistemas de información y bases de datos, y localizándolas en lugares externos con el fin de aminorar la perdida de información ante la posibilidad de fallos.

## PROCEDIMIENTO PARA RECUPERACIÓN DE DATOS

Los equipos de recuperación son grupos de personas que se encargan de una serie de actividades para conseguir un proceso de recuperación efectivo. En caso de daño este servicio es externo a la Entidad y los discos de almacenamiento son enviados con el fin de desarrollar los procedimientos que permitan hacer la recuperación de la información. Dentro de la Entidad se cuenta con herramientas de software generalmente versiones libres que desarrollan actividades de recuperación, teniendo efectividad aproximadamente en un 60% de las tareas que en el caso se han desarrollado. De las herramientas utilizadas para la recuperación de información esta RECUVA y EASY RECOVERY.

## PLAN DE ACCIÓN

El aspecto más importante de la continuidad del negocio es la inmediata notificación al responsable apropiado de cualquier suceso que pueda causar una interrupción en las operaciones informáticas, con independencia de su dimensión. Una de las problemáticas más significativas es la pérdida de tiempo ocasionado por la ausencia o inoperatividad de los recursos de TI. Cualquiera que sea el inconveniente presentado,

se le debe dar aviso a la Dirección Técnica de sistemas con el fin de evaluar la problemática y desarrollar las tareas de respuesta o contingencia. Al momento de recibir la notificación de un incidente, se desarrollará el Plan de acción según se especifica en la lista de actividades de la gestión del mismo, poniendo en marcha los procedimientos correspondientes.

## ANALISIS DE RIESGOS

De acuerdo a la evaluación y verificación de la posibilidad de ocurrencia de un evento que afecte la operatividad de la infraestructura de TI, se han evaluado a través de la matriz de riesgo, verificando su impacto y posibilidad de ocurrencia, así como el nivel de afectación dentro de la Entidad.

**La Calificación del Riesgo*:*** Se logra a través de la estimación de la probabilidad de su ocurrencia y el impacto que puede causar la materialización del riesgo. La primera representa el número de veces que el riesgo se ha presentado en un determinado tiempo o puede presentarse y la segunda se refiere a la magnitud de sus efectos.

| Probabilidad | Descripción | Frecuencia | Valor |
|---|---|---|---|
| Casi seguro | El evento probablemente ocurriría en la mayoría de los casos | Más de una vez al año | 5 |
| Probable | El evento probablemente ocurriría en la mayoría de los casos | Al menos una vez en el último año | 4 |
| Posible | El evento podría ocurrir en algún momento | Al menos una vez en los últimos dos años | 3 |
| Improbable | El evento podría ocurrir en algún momento | Al menos una vez en los últimos cinco años. | 2 |
| Raro | El evento podría ocurrir solo en circunstancias excepcionales | No se ha presentado en los últimos cinco (5) años | 1 |

Probabilidad: Posibilidad de ocurrencia del riesgo. Se puede medir con criterios de:

1. *Frecuencia*, si se ha materializado.
2. *Factibilidad* teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo.

La Evaluación del Riesgo*:* permite comparar los resultados de su calificación, con los criterios definidos para establecer el grado de exposición de la entidad al riesgo; de esta forma es posible distinguir entre los riesgos EXTREMOS, ALTOS, MODERADOS, BAJOS y fijar las prioridades de las acciones requeridas para su tratamiento.

| MATRIZ DE CALIFICACIÓN, EVALUACIÓN Y RESPUESTA A LOS RIESGOS | | | | | |
|---|---|---|---|---|---|
| **PROBABILIDAD** | **Insignificante (1)** | **Menor (2)** | **Moderado (3)** | **Mayor (4)** | **Catastrófico (5)** |
| **Casi Seguro (5)** | A | A | E | E | E |
| **Probable (4)** | M | A | A | E | E |
| **Posible (3)** | B | M | A | E | E |
| **Improbable (2)** | B | B | M | A | E |
| **Raro (1)** | B | B | M | A | A |

B: Zona de riesgo baja: Asumir el riesgo M: Zona de riesgo moderada: Asumir el riesgo, reducir el riesgo A: Zona de riesgo Alta: Reducir el riesgo, evitar, compartir o transferir E: Zona de riesgos extrema: Reducir el riesgo, evitar, compartir o transferir

.

- **Procedimientos de Riesgo Extremos.** Son actuaciones inmediatas al incidente que tratan de proteger la integridad de la infraestructura y la información, atajar la progresión del incidente y pararlo en la medida de lo posible, realizando la correspondiente evaluación de daños.

- **Procedimientos de Riesgo Moderado.** Son actuaciones de cada área o servicio que tienden a sustituir los procedimientos habituales de trabajo por otros alternativos que, aunque no reproduzcan totalmente las funcionalidades de cada área o servicio, permiten atender las necesidades más inmediatas y críticas de los mismos.

- **Procedimientos de recuperación.** Normalmente referidos a actividades de los sistemas de información, como son los procedimientos que permiten volver a utilizar datos, aplicaciones, sistemas operativos, etc.

Los riesgos que se tendrán en cuenta en este Plan de Contingencias de TI son los catalogados como EXTREMOS Y ALTOS, es decir aquellos que afectan en forma

drástica la operación de la entidad, la pérdida de información confidencial estratégica, la suspensión parcial o total del funcionamiento del hardware, software y/o sistemas de información, considerados como críticos; esta valoración se da en términos de las consecuencias que acarrearía dicha suspensión.

Los riesgos potenciales que pueden afectar la continuidad y operatividad normal del hardware, software y/o los sistemas de información de la entidad, son:

| TIPO RIESGO | Riesgo | Probabilidad | Impacto | Zona de Riesgo (Calificación) |
|---|---|---|---|---|
| Externo | Posibles cambios a la normatividad de control fiscal que afecten el funcionamiento de los sistemas de información. | 1 | 4 | ALTO |
| Externo | Incumplimiento al objeto contractual por parte de los contratistas. | 2 | 3 | MODERADO |
| Externo | Caída o interrupción del sistema eléctrico | 5 | 3 | EXTREMO |
| Externo | Caída del canal de internet | 5 | 3 | EXTREMO |
| Externo | Caída en el servicio telefónico | 4 | 2 | ALTO |
| Externo | Caída de servicios por virus informático | 2 | 3 | MODERADO |
| Externo | Suspensión del servicio por Sismo, inundación o incendio | 1 | 5 | EXTREMO |

| | | | | |
|---|---|---|---|---|
| Interno | Retrasos en el Proceso precontractual de la entidad en contratos relacionados con la infraestructura tecnológica de la entidad. | 3 | 3 | ALTO |
| Interno | Contratación sin asistencia técnica, Soluciones Inadecuadas o Incompatibilidad frente a los Requerimientos y Recursos Disponibles | 2 | 4 | ALTO |
| Interno | Pérdida de información considerada confidencial o de reserva por robo, alteración o extracción. | 5 | 4 | EXTREMO |
| Interno | Falla técnica en equipos servidores, de escritorio o de comunicaciones. | 5 | 3 | EXTREMO |
| Interno | Falla técnica en sistemas de información. | 5 | 4 | EXTREMO |

| | | | | |
|---|---|---|---|---|
| Interno | Ausencia de personal de la Dirección Técnica de Sistemas para soporte y mantenimiento de HW y sistemas de información. | 1 | 3 | MODERADO |
| Interno | Mal uso de hardware y/o software por parte de los funcionarios de la Contraloría de Bogotá | 5 | 3 | EXTREMO |

## INVENTARIO DE EQUIPOS Y SISTEMAS DE INFORMACION

### Equipos de cómputo y periféricos

| Cantidad | Descripción | Observación |
|---|---|---|
| 3 | Servidores físicos | |
| 65 | Equipos de cómputo | |
| 15 | Equipos portátiles | |
| 11 | Impresoras multifuncionales | |
| 7 | Impresoras B/N | |
| 1 | Impresoras COLOR | |
| 1 | Escáner | |
| 1 | impresora de etiquetas | |
| 2 | radios de comunicación Ubiquiti | |
| 3 | UPS | |
| 1 | Firewall FORTIGATE F110 C | ARRIENDO |
| 1 | CISCO | ARRIENDO |
| 3 | SISTEMAS DE INFORMACION (SYSMAN, SIDCAR, FLASH) | |
| 3 | SWITCH - 48 PUERTOS | |
| 8 | ACCES POINT | |
| 1 | PLANTA TELEFONICA – PANASONIC | |

**Software de Red**

| |
|---|
| Windows Server 2012 |
| SQL Server 2012 |
| Windows 8.1 |
| AVAST FREE |
| Windows server 2003 |

**Sistemas de Información**

| |
|---|
| SYSMAN (Nomina, Contabilidad, tesorería y presupuesto |
| SIDCAR - Sistema de Gestión documental |
| FLASH |
| CONSTRUCCION DE BASES DE DATOS MYSQL – JOOMLA INTRANET |

## ACTIVACIÓN DE PROCEDIMIENTOS DE EMERGENCIA

Ante la presencia de cualquier anomalía en el desarrollo normal de la red y de tareas asociadas a la utilización de elementos de TI, de debe informar a la dirección técnica de sistemas con el fin de evaluar la aplicación del plan de contingencia.

El plan de contingencia de los sistemas de información debe ser activado si una o más de las siguientes condiciones son verdaderas:

- Interrupción total de las operaciones de los equipos de comunicaciones ubicados en la oficina de la Dirección Técnica de Sistemas ubicada en el quinto piso del edificio de la lotería de Boyacá, donde se debe comenzar la verificación de la problemática y definir si el problema que se presenta esta por daños internos u obedece a condiciones externas y estimar la posibilidad de ausencia de servicio con el fin de hacer las notificaciones correspondientes a los funcionarios de la Entidad a través de los jefes de las Direcciones.

- Una vez evaluadas las causas del daño, comenzar con la verificación de estado de los equipos que no permiten establecer la conectividad de los servicios y desarrollar la comunicación correspondiente con proveedores de servicios si el problema es externo, con el fin de establecer los tiempos de restablecimiento

de servicio y conocer las posibles causas de la problemática. Si el problema es interno desarrollar la verificación correspondiente de equipos, verificando su estado y posibilidad de fallo en hardware o software, de esta manera poder establecer los procedimientos de recuperación y establecer los tiempos límites de operatividad.

- Otro criterio que se considere apropiado.

**Notificación de primera alerta**

Dependiendo de la naturaleza del incidente, el día, hora y ubicación, la notificación será descrita en estos ambientes. La respuesta inicial se dará con los procedimientos que tengan en la Contraloría General de Boyacá y la práctica operativa estándar, basada en la verificación de conectividad, estado de los equipos e inspección física de las instalaciones y equipos.

Los procedimientos siguientes muestran un flujo típico de las notificaciones y acciones iniciales del aviso de emergencia. Al momento de ser avisado o ser testigo del incidente, los pasos a seguir son los siguientes:

Dar aviso de lo sucedido a la persona encargada de sistemas, por vía escrita con la siguiente información.

- Nombre completo;
- Descripción del incidente;
- Informe preliminar de los daños presentados;
- Información acerca de cualquier intento de notificación anterior;
- La dirección de sistema decidirá las acciones a tomar, y de acuerdo a la situación de la problemática presentada poner en marcha el Plan de Contingencia o permanecer en alerta hasta nueva orden.
- Determinar QUIÉN podrá desarrollar la acción de mejora y restauración de servicio.
- Determinar el TIEMPO MÁXIMO permitido para la ejecución de la acción.
- En caso de no tener éxito en la acción, determinar QUIÉN debe ser avisado a continuación para hacerse cargo del problema y de su resolución.

- Si el tiempo pasa y las acciones de resolución del problema no tienen éxito, determinar en qué nivel de gravedad se encuentra la organización, por medio de un sistema de graduación de alertas.

**RESPONSABILIDAD**

De acuerdo al estado de inoperatividad se debe verificar el plan de contingencia y de acuerdo al daño y su significancia en la afectación de servicio se debe tratar por:

- Personal designado para ello en el Plan de Acción (personal capacitado
- Externo - personal interno de la Dirección).
- Personal no designado pero entrenado, o informado de los procedimientos de notificación.
- Si no hay nadie de los anteriores, cualquier persona que se encuentre con el problema.

**ACCIONES A EJECUTAR**

El personal de este en la capacidad de atender la situación deberá estar en la capacidad de:

- Verificarlo y solucionarlo si es su responsabilidad y está al alcance del conocimiento y experticia.
- Si no es su responsabilidad, intentar hacer la reparación si lo cree posible y no puede causar daños mayores o correr riesgos innecesarios.
- Informar A LA MAYOR BREVEDAD, al personal implicado en el Plan de Acción, y si no lo conoce, a sus superiores de la dirección a la que está asignado para desarrollar el plan de acción o contingencia pre establecido.

**INFORME DE EMERGENCIA**

Una vez que el Plan de Contingencia haya sido puesto en práctica y se hayan recuperado las funciones críticas, la dirección técnica de sistemas elaborará un informe con el siguiente formulario:

| |
|---|
| INFORME DE EMERGENCIA – DIRECCION TECNICA DE SISTEMAS<br>CONTRALORIA GENERAL DE BOYACÁ<br>ORDEN DE SERVICIO: Dependencia.<br>_____ _____<br>DETECTADA<br>POR:_____ HORA _____<br>FECHA _____ |
| EMERGENCIA DETECTADA |
| |
| |
| |
| ACCIONES REALIZADAS |
| |
| |
| |
| |

Se deben identificar las prioridades de restauración de los elementos dañados, informando qué registros vitales y equipos electrónicos son necesarios para restaurar las actividades de recuperación y cuáles podrían estar en daño y no pueden ser restaurados rápidamente, con el fin de cuantificar el valor de poner todo el sistema en operatividad y estabilizar la red minimizando el impacto negativo en las operaciones de la organización.

## PROCEDIMIETOS DE RESPUESTA

Los procedimientos de respuesta pueden ser activados muy rápidamente, pero usualmente son solo medidas de emergencia y, por lo general, no son suficientes para las operaciones del negocio a más largo plazo. Los procedimientos de respuesta están basados típicamente en equipos y facilidades utilizadas específicamente para ese fin. Son a menudo lo único que se requiere durante las interrupciones breves del servicio. Los servicios de TI serán valorados por funcionarios de la Dirección Técnica de Sistemas (hardware – software), así como la reubicación de dichos equipos. Además, esta área ayudará a las otras áreas afectadas en la recuperación de sus datos, estaciones de trabajo y red de comunicaciones.

El orden en el que se desarrollará la contingencia será el siguiente:

- Presentarse ante el Señor Contralor la problemática presentado, con el fin de poner al tanto de la ausencia de servicio y el tiempo estimado en la recuperación del servicio.
- Detalles específicos relacionados con el suceso, como tipo de suceso, lugar, duración, causa. Espacio físico potencialmente afectado, acceso al edificio y acceso potencial a corto plazo. Cualquier instrucción especial.
- Contactar inmediatamente con los proveedores de servicios para obtener apoyo en la evaluación del daño y actividades de restauración.

Si existen daños físicos en las instalaciones se deben coordinar las siguientes actividades

- Recopilar los datos necesarios de los siguientes elementos: Servidores.
- Estaciones de trabajo. Equipos de comunicaciones y líneas. Impresoras
- Computadores personales. Otros equipos.
- La dirección técnica de sistemas, dará la estimación del tiempo necesario para la puesta en servicio de la red de datos y procesamiento de datos.
- Revisar posibles alternativas de trabajar en canales y servicios alternativos.
- Coordinar con proveedores la posibilidad de recuperación de datos de acuerdo al daño de los equipos y discos de almacenamiento (hardware), regularizando la entrega de los datos de recuperación a las áreas afectadas.
- Proveer de estaciones de trabajo y espacios físicos alternativos para alojar un nuevo centro de proceso de datos, asegurarse de que las necesidades

particulares de la instalación son conocidas por los responsables de su contratación. Tener en cuenta los requisitos particulares siguientes:

Alimentación de energía eléctrica, condiciones de ventilación del centro de datos y Otros.

- Coordinar con el Señor Contralor como responsable del gasto de la Entidad, la sub dirección Financiera, la adquisición de computadores personales y servidores, además del software adecuado, según se especifica en la lista de recursos mínimos necesarios de cada área.
- Pedir estimación de costos y disponibilidad de los principales proveedores potenciales y canales de compra a través de Colombia compra eficiente y la tienda virtual.
- Ayudar a las direcciones afectadas en la recuperación de sus datos utilizando sus copias de seguridad.
- Coordinar la retirada de los elementos recuperables y su potencial arreglo con profesionales y entidades especializadas y los elementos que no tienen reparación dar el debido alistamiento para la baja de equipos y con entidades ambientales poder dar disponibilidad final de estos equipos, que en estado de chatarrización son altamente contaminantes, de igual forma con la subdirección de bienes y servicios poder hacer notificación a la compañía de seguros y poder hacer recuperación a través de la póliza global de amparos con la que cuenta la Entidad.
- Restablecer el acceso a la red de datos.
- Contactar inmediatamente con el proveedor de telecomunicaciones para obtener soporte presencial en el sitio para la evaluación de los daños y actividades de recuperación.

**PRUEBAS Y ACTUALIZACIÓN**

Con el fin de atender de una manera efectiva el plan de contingencia se deben tener en cuenta procedimientos actualizados y con una entrada en operación optima, lo que incurre en un conocimiento previo de la metodología a desarrollar y contar con los equipos y normatividad vigente para que sea efectivo los procedimientos y los tiempos de restauración sean mínimos.

El programa de pruebas y entrenamiento debe constar, como mínimo, de tres elementos:

- Revisiones periódicas.
- Ejercicios de entrenamiento.
- Pruebas técnicas.

Es aconsejable establecer una programación anual de estos tres ejercicios para asegurar su ejecución. Después de cada revisión o ejercicio, los diversos componentes del plan deben ser actualizados, si procede, con las experiencias obtenidas de los mismos.

**Revisiones periódicas**

Las revisiones deben comprobar los siguientes puntos:

- ¿Siguen siendo válidas las premisas de partida sobre las que se construyó el plan?
- ¿Están todavía disponibles los recursos de recuperación, incluyendo las copias de seguridad actualizadas en el almacenamiento externo?
- ¿Son todavía apropiados, en cantidades y umbrales de recuperación, los recursos críticos que se han definido?
- ¿Ha habido algún cambio en la criticidad de alguna información, que ahora la haga esencial para la recuperación?

**MANTENIMIENTO DEL PLAN**

- El Plan de Contingencia si se quiere efectividad para la recuperación. La dirección técnica de sistemas tiene como responsabilidad primaria el mantener el plan actualizado. Además, deben ser consideradas algunas premisas aparte de los planes de recuperación individuales. Es importante revisar elementos de orden presupuestal, normativo y técnico que aseguren la construcción del plan de contingencia es adecuada a las circunstancias institucionales y que dentro de los alcances se puede dar servicio de TI en tiempos mínimos que eviten una afectación de los procedimientos, procesos y cumplimientos de compromisos institucionales.

- Se deben actualizar los planes a la realidad institucionales y tener en consideración las amenazas globales que pueden afectar a la Entidad.
- Los cambios técnicos deben estar acordes a la actualidad tecnológica, con políticas de seguridad eficientes y sensibilización permanente a los funcionarios de la Entidad, elementos que permitirán desarrollar un plan de contingencia con menor posibilidad de retraso y fracaso.
- Distribuir roles dentro de la organización y generar responsabilidad en la administración de la información institucional personal, así como el cuidado de los inventarios de hardware y software asignadas para el desarrollo de tareas institucionales.
- Mantener al día el Plan de Contingencia, incluyendo todos los procedimientos, listado y registros del equipo actualizados. Actualizar este plan en cualquiera de las siguientes circunstancias:
    - Cambios en el personal de las dependencias y re-inducción permanente, con el fin de tener conocimiento de posibles amenazas y afectación de servicios por causa de mala operación de equipos y TI de la Entidad.

La información de este Plan de Contingencia estará de consulta permanente a través de la página web institucional www.cgb.gov.co y la intranet institucional. Se tiene a disposición de la dirección administrativa como elemento de inducción para el ingreso de personal a la Entidad y junto con las políticas de seguridad de los sistemas de información ponerlas en práctica y acatarlas según los requerimientos establecidos.