ALCALDIA MUNICIPAL DE SAN GIL - SANTANDER

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

ADOPTADO MEDIANTE RESOLUCION N° 100-33-028-2020 DEL 30 DE ENERO

VERSIÓN: 0.1

SAN GIL

AÑO 2020

TABLA DE CONTENIDO

INTRODUCCIÓN

La Alcaldía de San Gil, en su compromiso con la calidad ha venido incorporando dentro de sus políticas de calidad el resguardo y protección de la información, ya que la información es el patrimonio principal de toda Institución, por lo que se deben aplicar medidas de seguridad para protegerla y estar preparados para afrontar contingencias y desastres de diversos tipos.

El literal "a" del Artículo 2º. de la Ley 87 de Noviembre 29 de 1993 indica que uno de los objetivos fundamentales del Sistema de Control Interno, consiste en proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afecten. Así mismo señala en su literal "e", la adopción de normas para la protección y utilización racional de los recursos. Como complemento, asesorar a la dirección en la continuidad del proceso administrativo como parte de su gestión y haciendo adherencia a la definición indicada en el artículo 9º. de la misma ley.

Esta exigencia legal sugiere que las dependencias de Informática y/o telemática de las entidades del orden Distrital (para nuestro caso), definan y documenten planes, normas y procedimientos que permitan la adecuada continuidad de las operaciones en caso de presentarse contingencias o situaciones de emergencia en los sistemas informáticos de las entidades gubernamentales.

El Plan está basado en un proceso dinámico y continúo que incluye no sólo las actividades a realizarse en el evento de una interrupción de la capacidad de procesamiento de datos; sino además, en las actividades realizadas anticipando dicho evento.

Una actividad principal del plan, es evaluar, mantener y mejorar los procedimientos de recuperación, que permitan mitigar los daños potenciales antes que un "desastre" ocurra.

Otra actividad es facilitar la recuperación en el evento de un desastre. Para lo cual, la fase de recuperación provee tres propósitos:

1. Los roles individuales (de ejecución, coordinación y toma de decisiones) deben ser entendidos y atendidos en el contexto de todo el plan.
2. Existe la necesidad de establecer y mantener las descripciones de los procedimientos a ser realizados en el evento inesperado.
3. El plan permite un repaso administrativo, al evaluar la perfección y exactitud de cada proceso y repasa los procedimientos de recuperación sobre la marcha.

En ese sentido, **Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información** se convertirá en la carta de navegación, contemplando:

- La estructura de una organización jerárquica paralela para administrar las emergencias, con mecanismos de notificación claramente definidos.
- Definición de escenarios.
- Diseños de programas de almacenamiento y estrategias.
- Detalle de la administración general del Plan.
- Establecimiento de procedimientos contingentes, organización de grupos de trabajo, funciones y responsabilidades, involucrando usuarios y administradores.

1. OBJETIVOS

Plantear y dotar a la Alcaldía de San Gil de los procedimientos y elementos mínimos requeridos para afrontar la contingencia relacionada con el eventual cese de actividades, inoperatividad de equipos causada por razones de fuerza mayor.

Proveer una solución para mantener operativos los sistemas de información y electrónicos fundamentales de la institución, que permitan reducir el impacto en las operaciones normales cuando son interrumpidos o paralizados por contingencias que afectan parcial o totalmente las instalaciones donde se procesan aplicaciones automatizadas y los servicios de procesamiento de datos de la entidad.

Cuantificar la exposición a pérdidas asociadas a cada sistema de información automatizado y/o recursos informáticos con que cuenta la entidad, permitiendo un análisis de riesgos comprensible de los sistemas, que sirva como guía durante la ejecución del plan.

Minimizar la posible pérdida financiera y operativa en el evento inesperado, previendo procedimientos de recuperación efectivos y eficientes. Así mismo, reducir las consecuencias de la posible pérdida de información relacionada con el evento inesperado, en un nivel aceptable, al ejecutar procedimientos de respaldo apropiados.

Mantener la prestación del servicio a los usuarios, en el nivel aceptable.

Restablecer las operaciones del Centro de Cómputo en menos de 5 días hábiles, seguidos de cese, dependiendo de la anomalía que se presente.

Asegurar la concordancia con otras regulaciones locales, distritales y estatales.

2. VENTAJAS POTENCIALES

El hecho de tener estructurado el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para el área de informática y los sistemas de información de la Alcaldía de San Gil, tiene algunas ventajas potenciales que ayudan a prevenir o a disminuir el impacto de los siniestros. Algunas de estas ventajas permiten:

- Determinar acciones preventivas que reduzcan el grado de vulnerabilidad; por el conocimiento que se tiene de los sistemas automatizados de información.
- Cuantificar los riesgos potenciales a que están expuestos los sistemas de información.
- Facilitar la oportuna toma de decisiones ante anomalías o fallas.
- Contribuir a generar una cultura de seguridad y control en las áreas de sistemas e institucionalmente, haciendo énfasis en el manejo de la información.
- Asegurar la estabilidad operativa y de la organización, frente a la evidencia de un siniestro.
- Medir el grado de seguridad en los sistemas de información institucionales.

3. 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 Alcaldía de San Gil; 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 y Equipos electrónicos 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 del Centro de Cómputo principal de la entidad.

Las actividades y procedimientos, están relacionados con las funciones que competen a cada uno de los grupos contingentes establecidos para la ejecución del Plan, y dependen de la diligencia y colaboración de las dependencias usuarias y de los recursos disponibles (capacitación, recursos técnicos, presupuesto, etc.).

El desarrollo de las actividades y proyectos, está condicionado a la aprobación de los mismos por parte de la Secretaría TICS a través del Secretario o de quien haga sus veces.

4. METODOLOGÍA

Si las operaciones y procesos más importantes se encuentran automatizados en la Alcaldía de San Gil, significa que el área de informática es de gran relevancia para el funcionamiento de la misma, lo cual obliga a la consideración de los siguientes aspectos:

El tiempo durante el cual la entidad puede funcionar sin sus recursos computacionales en operación.

La identificación de las amenazas potenciales sobre la capacidad de procesamiento automatizado de la información en la entidad.

La identificación de las aplicaciones críticas que deben ser procesadas mientras se restablecen las operaciones normales en la entidad.

Identificación de las consecuencias operativas, estratégicas, legales o de servicio, por la carencia del servicio automatizado.

El valor de la inversión en el desarrollo del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información que asegure su continuidad y normal funcionamiento. El Plan se ha estructurado en tres grandes Fases, a saber:

1) **Fase de Mitigación:** La Alcaldía, asegura la conservación de su información vital y determina donde procesar sus trabajos críticos de procesamiento de datos, sistemas o aplicaciones automáticas críticas, en caso de falla de sus equipos o de los mismos aplicativos.
2) **Fase de Emergencia:** Contiene las acciones detalladas que deben ser llevadas a cabo durante el siniestro o emergencia.
3) **Fase de Recuperación:** Permite restablecer las condiciones originales y operación normal de los sistemas de información en su conjunto.

Los cuales implican el desarrollo de las siguientes Etapas:

1) Revisión: comprende la determinación de vulnerabilidad del área, inventario de recursos y limitaciones de la misma.

2) Valuación del impacto por interrupción del servicio: comprende la estimación de las pérdidas que involucraría la suspensión parcial o total de las operaciones. Esta valuación se da en términos de las consecuencias que acarrearía dicha suspensión. En esta etapa se desarrolla el análisis de

riesgos.

3) **Implementación:** se realizan actividades específicas para la reducción y eliminación de riesgos que proponen las medidas de acción, en caso de presentarse alguna situación de emergencia.

   a) **Cronograma:** El diseño de un cronograma de trabajo provee la oportunidad de registrar los logros de cada tarea, verificar si las actividades han sido cumplidas o no en el tiempo previsto, y analizar cuáles han sido los principales inconvenientes que se han presentado si se detectan desviaciones importantes en el cronograma inicial, antes de la ejecución de las pruebas.

   b) **Documentación:** Se prepararán y archivarán todos los documentos donde se registren las actividades, logros e inconvenientes, programas, objetivos, cronograma, procedimientos, planillas y todo aspecto fundamental referente a las acciones generadas durante el desarrollo del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, creando un historial de referencia.

4) **Simulación o simulacro:** se define el cronograma de simulacros, así como se designa a los responsables de dar inicio a las pruebas, ambientar el personal y los recursos, controlar los eventos, documentar las acciones y evaluar el resultado en su conjunto.

5) **Ejecución:** se sigue el desarrollo de:
   a) Medidas de protección planificadas por cada segmento afectado.
   b) Iniciación de las acciones destinadas, por prioridad, a controlar la situación durante los primeros instantes de la emergencia.
   c) Consideración de las responsabilidades extraordinarias que el comité directivo del plan tendría que asumir a fin de ofrecer protección y seguridad a los elementos materiales y humanos del área.
   d) Evaluación del estado del área de informática, poniendo en operación los procedimientos planificados para la recuperación total del servicio.

5. IDENTIFICACIÓN Y ANÁLISIS DE RIESGOS

5.1 DEFINICIÓN

RIESGO es la probabilidad de ocurrencia de un evento inesperado. Proximidad a un daño, contingencia, peligro, inseguridad, azar o exposición.

5.2 DESCRIPCIÓN Y ANÁLISIS DE RIESGOS

El siguiente análisis de riesgos implica la valuación del impacto por interrupción del servicio, el cual comprende la estimación de las pérdidas que involucraría la suspensión parcial o total de las operaciones; esta valuación se da en términos de las consecuencias que acarrearía dicha suspensión. 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.

Los riesgos potenciales que pueden afectar la continuidad y operatividad normal de los sistemas de información con que cuenta la Entidad, son entre otros:

5.3 Riesgos con Incidencia Externa

5.3.1 Políticos

Modificaciones a la constitución política ya sea por asamblea constituyente, referendo, consulta popular, plebiscito o mediante leyes orgánicas, reestructuración o supresión de entidades.

5.3.2 Riesgos con Incidencia Interna

5.3.2.1 Posible incumplimiento de los contratistas

Este riesgo puede ocurrir a causa del posible atraso en la ejecución o trasgresión del clausulado de los contratos de actualización, modificación, mantenimiento que deriven de los procesos de compra y actualización de sistemas informáticos y tecnológicos de la Administración Municipal.

5.3.2.2 Posibles retrasos en Procesos Administrativos

La implementación de los procesos tecnológicos relacionados con la ejecución de los contratos, implica el desarrollo de trámites administrativos con exigencia en el cumplimiento de requisitos, ampliando el tiempo de ejecución de las actividades del Plan Emergente, de manera imprevista.

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

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, de manera compatible.

5.3.2.4 Posible pérdida de información

Este riesgo tiene baja probabilidad de ocurrencia, si se tiene en cuenta que el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información. incluye un proceso de respaldo, que permite la mitigación del riesgo, efectuando copias de seguridad (backups), tanto a los archivos de trabajo (Word, Excel, PowerPoint, otros) como a los archivos de bases de datos y resultados de las aplicaciones específicas en producción para cada una de las dependencias de la Entidad.

5.3.2.5 Posible falla de equipos electrónicos y Hardware fuera de inventario

Este riesgo se presenta por la Falta de Previsión, con la no inclusión de soluciones para aspectos de baja prioridad o al excluir elementos de los inventarios, por desconocimiento o por no haber sido reportados a tiempo a la Dirección de Informática.

5.3.2.6 Posibles Fallas en el Flujo de Energía Eléctrica

Este riesgo está relacionado con amenazas externas al control de la Entidad. Sin embargo, se han implementado equipos para la mitigación del riesgo de corte temporal de energía eléctrica, dado que la Alcaldía de San Gil está provista de UPS (Unidad de Poder In-interrumpido) en cada una de las redes de área local, para tener la posibilidad de salvaguardar la información durante aproximadamente 20 (viente) minutos. Si el corte es más prolongado, se debe acudir a los procedimientos de procesamiento en el centro alterno externo y en segunda instancia los procesos manuales establecidos como contingencia, hasta

tanto no se solucionen la falla.

5.3.2.7 Posible Calentamiento de la Sala de Cómputo

Que se tiene para evitar posible recalentamiento del centro de datos la sala de cómputo ya que en ella se encuentran los servidores locales y agregado a ello los rack y de cableado estructurado.

5.3.2.8 Posible Falla del Servicio Telefónico o de Internet

Este riesgo está relacionado con amenazas externas al control de la Entidad, la Alcaldía no puede efectuar mitigación de este riesgo. Sin embargo, se puede planear las posibles alternativas a implementar ante las posibles fallas del servicio Telefónico o de Internet. La probabilidad de ocurrencia sólo es manejable por la entidad proveedora del servicio.

El impacto sobre las operaciones de la Alcaldía de San Gil es de nivel bajo para la telefonía pero alto para Internet, ya que la Entidad posee una Infraestructura de Comunicación de datos y Redes locales implementadas sobre cableado estructurado que trabajan con el ISP.

Es fundamental para le entidad tener servicios de internet 24/7 ya que

El análisis del Centro de Computo de la Alcaldía de San Gil, se desarrolló un análisis del medio y los procedimientos de seguridad y control existentes.

El análisis indicó que la Entidad está arrojo:

1. El edificio no se encuentra en una zona que pueda presentar inundación.
2. El centro de cómputo está ubicado estratégicamente en el piso 2 del edificio sede.
3. No posee detectores de humo y fuego que accionan un sistema de alarmas y de descarga automática de gases que apagan las llamas originadas en el salón de la UPS y cuarto de computadores.
4. El acceso al software es restringido y se encuentra almacenado en un lugar seguro y adecuado.
5. El cielo raso y pisos del centro de cómputo no son de material no combustibles.
6. El centro de cómputo está provisto de una Temperatura autorregulada y cuenta con UPS.

6. IDENTIFICACION DE PROCESOS CRITICOS

6.1 CRITERIOS PARA IDENTIFICACIÓN DE PROCESOS CRÍTICOS

Los planes de contingencia se consideran "requeridos" para todos los sistemas de prioridad 1, "recomendables" para todos los sistemas de prioridad 2 y "sugeridos" para todos los sistemas de prioridad 3.

6.1.1 Prioridad 1

- Todos los sistemas vitales de la organización

6.1.2 Prioridad 2

- Sistemas con múltiples interfaces.
- Sistemas o dispositivos que no pueden ser sometidos a pruebas.
- Sistemas que alimentan datos a los sistemas vitales.

6.1.3 Prioridad 3

- Sistemas cuya falla causa molestias menores

6.2 FACTORES CRÍTICOS A CONSIDERAR

6.2.1 Aplicaciones en Producción

1 Nivel de importancia de la aplicación en la entidad
2 Impacto operativo, financiero o contable
3 Oportunidad de procesamiento
4 Programas críticos
5 Comunicaciones: entrada y salida de datos
6 Implicaciones para el usuario en caso de ausencia del recurso aplicativo.
7 Documentación del sistema: manuales de usuario y operación.
8 Procedimientos de respaldo y recuperación a nivel aplicativo.

6.2.2 Personal

1 Funcionarios de posición clave y personal de dirección
2 Personal con alta dependencia en los sistemas automatizados
3 Personal de respaldo
4 Entrenamiento

6.3.3 Parque computacional y aplicaciones en uso

1. Servidores, computadores personales, impresoras, periféricos, etc.
2. Líneas de comunicación y equipos relacionados.
3. Sistemas operativos y programas producto.
4. Suministros: papel, formas continuas, medios magnéticos y formas especiales.
5. Archivos maestros y de movimiento considerados críticos de respaldo de los mismos.

6.4 NIVELES DE PRIORIDAD Y CRITICIDAD DE LOS RECURSOS INFORMÁTICOS

Teniendo en cuenta los criterios y factores enunciados anteriormente, se han definido los siguientes niveles de prioridad y criticidad de los recursos informáticos con que cuenta la Alcaldía de San Gil:

6.4.1 Prioridad Alta

Corresponde a todas aquellas herramientas de la Alcaldía, que en el caso de no ser adaptadas oportunamente a las exigencias, generarían graves problemas que pueden llevar inclusive a paralizar toda la entidad.

6.4.2 Prioridad Media

Se le asigna a todas aquellas herramientas de la Alcaldía, que aunque son importantes para el desarrollo normal de las actividades administrativas, operativas y de control, cuentan con procedimientos alternativos preestablecidos.

6.4.3 *Prioridad Baja*

Se le asigna a todas aquellas herramientas de la Alcaldía, cuya falta de adaptación no representa graves traumatismos y sus modificaciones pueden aplazarse para la última parte del proyecto.

6.4.4 Criticidad A: (Máxima)

No puede permanecer interrumpido(a) por un período mayor de 24 a 48 horas

6.4.5 Criticidad B: (Intermedia)

No puede permanecer interrumpida(o) por un período mayor a 5 días hábiles. Puede sustituirse parcialmente por un período, por un proceso manual.

6.4.6 Criticidad C: (Mínima)

Puede permanecer interrumpida(o) por un período entre 15 días y 30 días hábiles. Puede sustituirse temporalmente por un proceso manual.

6.4.7 PROCESOS CRÍTICOS

Con base en lo anterior, se establecieron los Procesos Críticos de la Alcaldía de San Gil descritos en la siguiente relación de recursos informáticos señalando la prioridad y las acciones a seguir para cada problemática en particular.

6.4.8 SOFTWARE

6.4.8.1 Aplicaciones de Desarrollo Externo

Se determinó que las aplicaciones en producción que presentan un alto riesgo de pérdida de información y que pueden provocar parálisis en los procedimientos administrativos (en caso de no ser debidamente adecuadas), son aquellas elaboradas e implementadas a través de procesos contractuales; por lo tanto, serán objeto de inmediata solución.

6.4.9 HARDWARE

6.4.9.1 Microcomputadores

La Alcaldía cuenta con 33 portátiles y 104 pc, 6 Servidores, 4 Rack, 8 Swith, 3 microtik, 34 cantidad de Cámaras, 4 cantidades de discos de respaldo 3 de una Tera y uno de 512 GB, 32 Scanner, 28 Impresoras láser, 4 Impresoras de Tinta distribuidos como se presenta en el siguiente cuadro:

Cuadro 1
DISTRIBUCIÓN DE EQUIPOS DE CÓMPUTO POR DEPENDENCIA

Dependencia	Sistema Operativo	Impresoras	Scaner	Equipos de computo	Total Equipos
Agricultura	Windows 8.1 Windows 7	1	1	7	9
Almacén	Windows 7	2	1	2	5
Archivo	Windows 7	1	1	3	5
Bono Pensional	Windows 7 Windows XP	1		2	3
Contratación	Windows 7	2	1	6	9
Control Interno	Windows 7	1	1	2	4

Dependencia	Sistema Operativo	Impresoras	Scaner	Equipos de computo	Total Equipos
Control Interno Disciplinario	Windows 7	1		2	3
Familias en Acción	Windows 8 /7	1	1	4	6
Hacienda	Windows 7	12	6	19	34
Inspección de Policía	Windows 7 Windows 8.1	2		5	7
Jefe de Centro	Windows 7	1		1	2
Jurídica	Windows 7 Windows 8.1 Windows Xp	2	1	9	12
Oficina Administrativa	Windows 8	1	1	4	6
Oficina Personal	Windows 7	2	1	2	5
Periodismo	Windows 8.1			2	
Personería	Windows 7	2	1	3	6
Planeación	Windows 7 Windows XP Windows 10	2	2	15	19
Psicología	Windows 7			2	2
Policía de Infancia	Windows 7 Windows 8	1		2	3
Salud Publica	Windows 7 Windows 8.1	3	3	5	11
Sec.Desarrollo	Windows 7	1	1	2	4
Sec.Educ	Windows 8	1	1	3	5
Sec.Educ	Windows 7	1	1	3	5
Primera Dama	Windows 7	1		1	2
Sec.privada	Windows 7	1	1	3	5
Sec. Salud	Windows 7 Windows 8.1	4	3	5	12
Sec. Interior	Windows 7	1	1	1	3
Sistemas	Windows 10				24
Sisben	Windows 8 / 7	2	1	5	8
Terminal	Windows 7			10	
Transito	Windows 7	8	2	14	24
UAI	Windows 7			5	
Ventanilla	Windows 8	1	1	3	5
Victimas	Windows 8.1	1		2	3

6.4.9.2 Equipos Servidores

DIAGRAMA DE RED ALCALDIA DE SAN GIL

A continuación se muestra la actualización de infraestructura tecnológica de servidores que hacen parte de la red de la Contraloría.

SERVIDOR GD CORRESPONDENCIA Y ARCHIVO

- **Características**
  - HP Proliam Ml110
  - Procesador Intel Xeon CTU X3434 2.4 GHz
  - 6 GB RAM
  - 1 TB HD
  - SO: Windows Server 2008 Enterprise
- **Servicios**
  - Servidor de Correspondencia
  - Servidor de Archivo

SERVIDOR GD CORRESPONDENCIA Y ARCHIVO

- **Características**
  - Ecs G3IT-M7
  - Procesador ntel core 2 duo 2.8 GHz
  - 2 GB RAM
  - 512 TB HD
  - SO: Windows Xp profesional Servipack 3
- **Servicios**
  - Cámara de Comercio

SERVIDOR GD CORRESPONDENCIA Y ARCHIVO

- **Características**
  - IBM System x3500
  - Procesador Intel Dual core XEON 4.4 GHz
  - 4 GB RAM
  - 1 TB HD
  - SO: LINUX Semptos 7
- **Servicios**
  - Servidor de Backups

6.4.10 EQUIPOS ELECTRÓNICOS

Los equipos electrónicos no-informáticos con que cuenta el centro de cómputo que requieren ser ajustados o reemplazados, o son necesarios:

- UPS: No se tiene ups de respaldo para los sistemas solo para los Servidores del centro de cómputo.
- Sistemas de Alarmas: El sistema de alarma contra incendios no se posee ningún centro con lo cual en caso de un incendio no se tendría un sistema de respuesta inmediata que permita mitigar el daño.

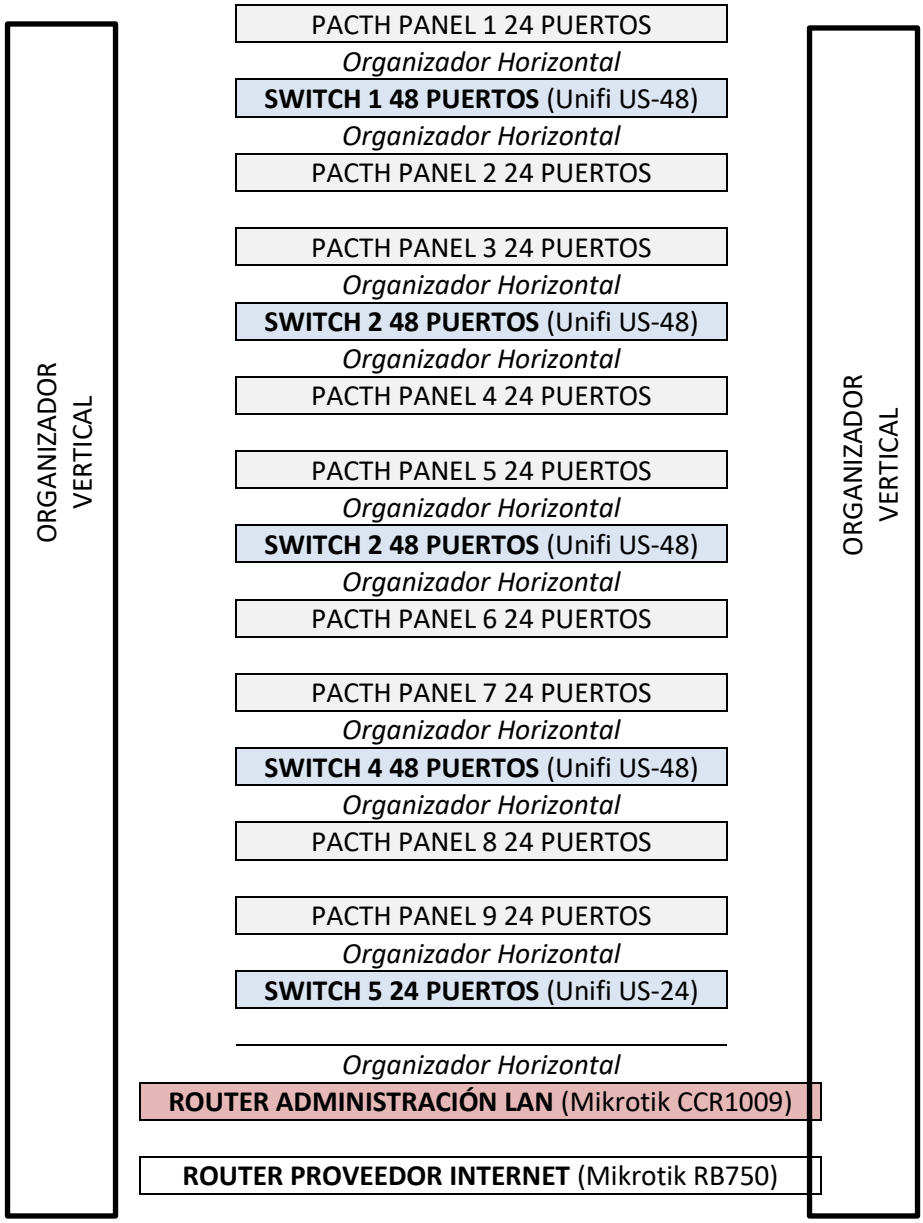
6.4.11 EQUIPOS DE COMUNICACIONES

6.4.11.1 Infraestructura de Redes

Descripción de la red

La estructura de la red maneja cableado UTP nivel 5 y 6a donde el cuarto de la sede central tiene los racks y servidores, se realizó el cambio del cableado estructurado se eliminaron de conexiones puentes y subredes que generaban cuellos de botella.

DEPENDENCIA	CANT	CONECTADOS	LIBRES	TOTAL
PISO 1				**213**
PLANEACION	29	19	10	
HACIENDA	31	19	12	
PORTERÍA	1		1	
SALUD	9	6	3	
SALUD PUBLICA	5	4	1	
BONO PENSIONAL	3	2	1	
ARCHIVO	8	5	3	
IGAC	2		2	
TOTAL	***88***	*55*	*33*	
PISO 2				
OFICINA ALCALDE	3		3	
OFICINA GESTORA SOCIAL	3		3	
SECRETARÍA PRIVADA	5	1	4	
RECPECÓN DESPACHO	4	2	2	
SECRETARÍA INTERIOR	8	4	4	
OFICINA ADMINISTRATIVA	4	1	3	
OFICINA DE PERSONAL	4	2	2	
COMUNICACIÓN SOCIAL	4	2	2	
SISTEMAS	5	3	2	
JURIDICA	17	8	9	
CONTROL INTERNO	4	2	2	
SANEAMIENTO	2	1	1	
CONTRATACIÓN	13	6	7	
DESARROLLO SOCIAL	4	2	2	
ALMACEN	4	2	2	
EDUCACIÓN	7	3	4	
OFICINA VACÍA	1		1	
TOTAL	***92***	*39*	*53*	
PISO 3				
AGRICULTURA	6	5	1	
ASOJUNTAS	2	2		
EDUCACIÓN RURAL	5	5		
DESARROLLO NUCLEO EDUCATIVO	2	2		
CONTROL INTERNO DISCIPLINARIO	2	2		
ATENCIÓN A VICTIMAS	2	1	1	
AUDITORIO	3		3	
CUARTO ARCHIVO 1	2		2	
CUARTO ARCHIVO 2	2		2	
TOTAL	***26***	*17*	*9*	
ACCESO INALAMBRICO (WIFI)				
WIFI	7	7		
TOTAL	***7***	*7*		


ORGANIZADOR VERTICAL
ORGANIZADOR VERTICAL
PACTH PANEL 1 24 PUERTOS
Organizador Horizontal
SWITCH 1 48 PUERTOS (Unifi US-48)
Organizador Horizontal
PACTH PANEL 2 24 PUERTOS
PACTH PANEL 3 24 PUERTOS
Organizador Horizontal
SWITCH 2 48 PUERTOS (Unifi US-48)
Organizador Horizontal
PACTH PANEL 4 24 PUERTOS
PACTH PANEL 5 24 PUERTOS
Organizador Horizontal
SWITCH 2 48 PUERTOS (Unifi US-48)
Organizador Horizontal
PACTH PANEL 6 24 PUERTOS
PACTH PANEL 7 24 PUERTOS
Organizador Horizontal
SWITCH 4 48 PUERTOS (Unifi US-48)
Organizador Horizontal
PACTH PANEL 8 24 PUERTOS
PACTH PANEL 9 24 PUERTOS
Organizador Horizontal
SWITCH 5 24 PUERTOS (Unifi US-24)
Organizador Horizontal
ROUTER ADMINISTRACIÓN LAN (Mikrotik CCR1009)
ROUTER PROVEEDOR INTERNET (Mikrotik RB750)

6.4.11.2 Hardware de Comunicaciones

En el siguiente cuadro se muestra el Consolidado de Recursos por Sede, relacionando los puntos de red, enlaces de radiofrecuencia y switches de cada uno de los edificios:

Cuadro 2
DISTRIBUCIÓN DE DISPOSITIVOS DE COMUNICACIONES

SEDE	PUNTOS DE RED	ANTENAS RADIOFRECUENCIA	SWITCHES
Principal	218	1	**8**
Centro de Convivencia	20	1	**4**
Tránsito y transporte	20	1	**1**
Terminal	**8**	**1**	**2**

Fuente: Oficina de Sistemas

7. DEFINICION Y CONFORMACION DEL GRUPO DE TRABAJO

Para dar cumplimiento al desarrollo del plan de Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información en las áreas de sistemas de la entidad, es necesario tratarlo como un proyecto. Por esta razón, se conformarán el comité directivo y el grupo de desarrollo, ambos responsables del plan. Se sugiere la estructuración del grupo encargado del desarrollo, implantación y mantenimiento del plan de Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

7.1 COMITÉ DIRECTIVO

Conformado por funcionarios de nivel directivo de la Alcaldía de San Gil quienes participan en el Comité de Informática:

- Alcalde Municipal
- Secretario del Interior
- Secretario del Educación y Tic
- Secretario Jurídico
- Jefe de Sistemas
- Secretario de Planeación
- Secretario de Hacienda
- Secretario de Salud
- Secretario de Desarrollo Social
- Secretario de Transito
- Secretario de Agricultura
- Directora de Oficina de Personal
- Control Interno

7.1.1 Responsabilidades

- Definir los lineamientos del plan de Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para las áreas de informática de la Alcaldía de San Gil.
- Orientar y evaluar el desarrollo e implantación del plan.
- Ejercer un control documentado y un seguimiento formal al proyecto.
- Estudiar, evaluar y decidir sobre los requerimientos que se presenten en el desarrollo e implantación del plan.

- Recomendar acerca de la adquisición o el mantenimiento de equipos, programas e instalaciones.
- Coordinar el desarrollo, implantación y mantenimiento del plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.
- Supervisar el cumplimiento de las labores asignadas al grupo de desarrollo del plan.
- Estudiar, evaluar y decidir sobre los requerimientos o recomendaciones planteadas por el grupo de desarrollo.
- Efectuar seguimiento y controlar los costos que se incurren en el desarrollo, implantación y mantenimiento del plan.
- Aprobar el establecimiento de convenios, contratos o adquisición de recursos para el plan.
- Organizar y disponer los recursos para el grupo de desarrollo del plan.

7.2 COOORDINADOR DEL PLAN DE PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Coordinador del Plan es el Canal de Comunicación entre el Grupo de Desarrollo del plan y el Comité Directivo, a través del cual se transmitirán las decisiones tomadas en torno a las acciones del plan de Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información los niveles de ejecución del Plan y el estado de los Recursos Informáticos que cubre el Plan.

Así mismo, debe encargarse de monitorear y asegurar el cumplimiento estricto del Plan y del mantenimiento de los canales de comunicación entre los diferentes grupos de trabajo. Proveer los recursos necesarios y notificar las decisiones a los funcionarios delegados.

El Coordinador del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información es el Encargado de la Oficina de Informática de la Alcaldía de San Gil y en su ausencia el Ingeniero que delegue, integrante de la Oficina de Sistemas y perteneciente al Grupo de Trabajo dela Oficina de Sistemas, dado el tipo de labores especificas a desarrollar dentro del plan (realización de copias de seguridad y restauración de las mismas) labores que son compatibles con las tareas cotidianas que desarrolla este grupo.

7.3 GRUPO DE DESARROLLO DEL PLAN

Está conformado por funcionarios de nivel medio, responsables de la ejecución de las áreas definidas dentro del plan. El grupo estará conformado por personal de las áreas administrativas y operativas de sistemas automatizados (funcionarios usuarios finales encargados del manejo de aplicaciones y equipos de cómputo), el grupo de soporte técnico de la Alcaldía de San Gil. Ellos han sido delegados y encargados por los niveles directivos de cada una de las áreas usuarias. Grupo de Desarrollo del Plan, en ella se define la asignación específica de cada funcionario en el subgrupo que le corresponda.

Funciones

- Ejecutar, en tiempo y forma, cada una de las actividades planeadas.
- Documentar y formalizar de Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.
- Ordenar la documentación inherente y los papeles de trabajo del proyecto.
- Diseñar planes de entrenamiento para los funcionarios de la entidad, a todo nivel, para que se involucren en las tareas del plan.
- Diseñar cronogramas y apoyar logísticamente las pruebas de cada segmento del plan.
- Mantener operativo y debidamente actualizado Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

.

El Coordinador del Plan y los funcionarios de la Oficina de Informática, elaborarán el plan de trabajo para el desarrollo e implantación del proyecto.

Así mismo, se conformarán los siguientes subgrupos de trabajo para la ejecución del Plan

7.3.1 Subgrupo de Atención de Emergencias

Conformado por un representante dela Oficina de Personal, el jefe de Sede del área afectada o su suplente y el responsable (o su suplente) del procedimiento a seguir según el aspecto afectado; estas personas son las designadas por el Encargado de la Oficina de Sistemas y de Personal. Este grupo se encargará de activar las medidas necesarias para salvaguardar los recursos humanos y materiales en caso de emergencias.

7.3.2 Subgrupo de supervisión

Conformado como mínimo, por personal del área afectada encargados de la operación de sistemas, el cual prestará apoyo e información al grupo de atención de emergencias, si así lo amerita. Encargándose, así mismo, de supervisar la situación del segmento no afectado por el siniestro en el momento de la contingencia y de informar al ingeniero de la Oficina de Informática coordinador de los sistemas afectados, para que apoye las labores de supervisión, dirija, participe en la ejecución del plan y el soporte técnicamente.

7.3.3 Subgrupo de evaluación de daños

Conformado por los mismos funcionarios del subgrupo de supervisión con el apoyo de los ingenieros del grupo de soporte de la Oficina de sistemas, quienes se encargarán de la revisión de la planta física, identificando los daños físicos y lógicos (Hardware y Software) originados durante la contingencia, para luego, informar los resultados al grupo de desarrollo.

7.3.4 Subgrupo de Reorganización

Conformado por los funcionarios del área; que forman parte del grupo de desarrollo, el cual se encargará de la evaluación de los daños y de la toma de decisiones pertinentes encaminadas al rescate progresivo de las funciones del área afectada.

7.3.5 Grupo de Seguimiento y Control

Conformado por los funcionarios representantes de la Oficina de Control Interno apoyados por el ingeniero coordinador de las labores del área afectada y que hace parte del grupo de desarrollo; quienes se encargaran de hacer seguimiento y control a las labores que se ejecuten, velando por el respeto del plan y la seguridad en su efectiva aplicación, así como la coherencia y consistencia en la aplicación de los procedimientos establecidos..

8. PLAN DE MITIGACION

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:

8.1 PROCESO DE RESPALDO

El Proceso de Respaldo establecido como procedimiento de Mitigación, a través del cual la Alcaldía de San Gil asegura la conservación de su información vital y determina donde realizar sus trabajos críticos de procesamiento de datos en caso de falta o falla de sus equipos.

El diseño del proceso de respaldo incluye los cinco (5) principales componentes de un sistema de información, a saber:

- Los datos
- La documentación
- Los programas (software)
- Los procedimientos
- Los equipos (hardware)

8.1.1 Proceso de Respaldo Externo

Como sitio de respaldo externo se entiende una instalación diferente a la sede principal de la entidad donde se almacena una copia de los archivos de backups de la entidad, para que ante cualquier eventualidad que se presente en la sede principal se pueda reiniciar labores con los archivos almacenados en el sitio de respaldo externo.

En la entidad no cuenta con un una instalación externa que conserve los backup de la información generada por la entidad, al igual que no tiene un servidor en la nube para los backups, considerando esto una riesgo de seguridad para la entidad, y que se debe mejorar con suma urgencia ya que en caso de emergencia en el cual haya daño a la planta física de la entidad se podría en riesgo por la continuidad de la operación de la entidad, ya que hay procesos que se llevan de manera local.

8.1.2 Plan de Backups y Equipos de Respaldo

Un backup es una copia de seguridad de la información en un segundo medio (cinta - cartridge) que nos garantiza recuperar la información contenida en nuestras maquinas en caso de que se presente alguna falla en el disco duro, un borrado accidental o un accidente imprevisto.

Estos backup deben ser ejecutados por:

1 El administrador de la oficina de Sistemas
2 Usuarios con privilegios para realizar copias de seguridad designada por la Oficina de Sistemas.

La Alcaldía adecuo un Servidor de backup al igual que un plan de Backups semanales para realizar las copias de seguridad de la Entidad.

8.1.2.1 Definición de Niveles de Backup

Los niveles de backup que se han establecido como política en la dirección de Informática son los siguientes:

ANUAL: Debe realizarse al final de cada año (último día del año), es un backup total en Discos que se guardan indefinidamente.

SEMESTRAL: Debe realizarse al final de cada semestre un backup total (último día de cada semestre exceptuando el último día del año). Estas cintas se pueden denominar semestre1, semestre2 y se reutilizan anualmente.

MENSUAL: Debe realizarse al final de cada mes un backup total (último día de cada mes exceptuando el último día del año). Estas cintas se pueden denominar mes1, mes2, mes3,…. mes12 y se reutilizan anualmente.

SEMANAL: Se debe realizar al final de la semana (último día de la semana), es un backup total en cintas. Estas cintas se pueden denominar semana1,….semana4 y se reutilizan mensualmente.

EN LINEA: Este backup se hace siempre y cuando se posea la infraestructura para copiar los archivos o directorios considerados como información vital al disco duro de un servidor remoto.

8.1.3 Procedimiento para Efectuar Backup's o Copias de Respaldo a la Información de las Dependencias

Este procedimiento se realiza según lineamientos de la Oficina de Sistemas

MATRIZ PARA LA DESCRIPCION DEL PROCEDIMIENTO:

No	RESPONSABLE	ACTIVIDAD	REGISTRO	OBSERVACIONES
1	Profesional Oficina de Sistemas	Determina de acuerdo a la periodicidad establecida si el backup a realizar es semanal, mensual o semestral.		**Existe un grupo de Equipos para backups semanales, mensuales y semestrales**
		Verifica en la Planilla de Control de Backups el número del Equipo correspondiente y registra la fecha de ejecución.	Planilla de Control de Backups	
		Selecciona El Equipo correspondiente y prepara en el servidor (el) (los) archivo(s) a respaldar.		
		Ejecuta la acción adecuada para respaldar (el)(los) archivo(s).		
		Finalizada la copia de (el)(los) archivo(s) se regresa la procede a copiarlos en el Servidor de Backups a su lugar de origen.		
2	Director de la oficina de Sistemas	Envía memorando al Alcalde, Secretarios de Despacho, Jefes de Dependencia, Contratistas informando acerca del plan de backup de información institucional	Memorando	
3	Alcalde, Secretarios de Despacho, Jefes de Dependencia, ContratistasJefes de Oficinas Asesoras y Grupo de Actuaciones Especiales	Solicita a todos sus funcionarios que seleccionen los archivos que ameriten ser conservados en copia de seguridad, en su última versión y preferiblemente establecer nombres cortos, combinado con fechas para definir los nombres de estos.		
		Asigna un funcionario para que realice la compilación de los archivos en el equipo seleccionado.		
4	Profesional y/o técnico de la Dependencia	Diseña en el computador seleccionado y dentro del directorio DT##### la estructura con los subdirectorios contenidos y copia en ella los archivos relevantes de la dependencia.		
	Contralor,	Envía a la Oficina de Informática memorando informando que el directorio asignado para incluir los archivos que ameriten mantenerse en backup se encuentra conformado donde se indique:		

No	RESPONSABLE	ACTIVIDAD	REGISTRO	OBSERVACIONES
5	Contralor Auxiliar, Directores Técnicos, Jefes de Oficinas Asesoras y Grupo de Actuaciones especiales	- Nombre y código de la Dependencia - Nombre del responsable del backup en la Dependencia - Ubicación e identificación en la red del computador que contiene la información - Nombre del directorio principal - Estructura gráfica del directorio principal completa.	Memorando	
6	Profesional Oficina de Sistemas	Ubica a través de la red el directorio principal de cada una de las dependencias y procede a copiar la información en un servidor del Centro de Cómputo asignado para tal fin. Registra la acción realizada en un planilla de control de backup institucional	Planilla de control de Backup Institucional	
		Una vez centralizada toda la información en el servidor.		
7	Alcalde, Secretarios de Despacho, Jefes de Dependencia, Contratistas Jefes de Oficinas Asesoras y Grupo de Actuaciones Especiales	Envía memorando a la Oficina de Sistemas solicitando la recuperación de un backup o parte de este, indicando la fecha y ubicación de la información en la estructura de directorios de la respectiva dependencia.	Memorando	
8	Director de Oficina De Sistemas.	Asigna profesional para realizar la tarea correspondiente		
9	Profesional de Oficina de Sistemas	Ubica el Backup correspondiente y restaura la información en el disco duro del servidor para luego enviarla vía red a la dependencia solicitante.		
		Proyecta respuesta para la firma del Director de la Oficina de Sistemas, informando fecha y ubicación donde fueron restaurados los datos solicitados.		

9. FASE DE EMERGENCIA

Presenta las acciones detalladas que deben ser llevadas a cabo durante la emergencia. Provee una serie de instrucciones a las áreas Operativas y Administrativas, en caso de materializarse el riesgo.

Las soluciones que deben ser implementadas para mantener la continuidad de los procesos críticos en el momento de la materialización de los riesgos son las siguientes, para cada proceso crítico asociado a un riesgo, se define una acción o procedimiento a seguir.

9.1 SOFTWARE

9.1.1 Aplicaciones Críticas en Producción

9.1.1.1 De Desarrollo Externo

La alcaldía cuenta con varios Sistema de Información desarrollados por GD, También tiene de la Cámara de Comercio el cual tiene su propio servidor en la nube para algunos programas y hace respaldos su servidor remoto, otros funcionan en servidor local y se deben hacer respaldo en los propios servidores

9.1.1.1.1 Software Financiero

Aplicación: GD (Tesorería, Contabilidad, Industria, Recaudo Predial, EcoFinanciero)

Estado Actual: Se contrató con el proveedor la actualización, mantenimiento y soporte técnico del sistema financiero GD software integrado por los módulos

Proveedores: GD

Usuario: (Tesorería, Contabilidad, Industria, Recaudo Predial, EcoFinanciero)

Riesgos Asociados: Posible incumplimiento de los contratistas, Posibles Retrasos en Procesos Administrativos, Mal funcionamiento de las aplicaciones críticas o de los Equipos en donde están instaladas.

Soluciones en contingencia: Ante la posible materialización de los riesgos o

falla de las aplicaciones actuales se plantea las siguientes o soluciones:

1) Se deben realizar revisión a las copias de seguridad mensualmente, a fin de saber que estas funcionan íntegramente.

- Solicitar que el contratista presente el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y niveles de seguridad e integridad de las copias a fin de establecer un plan conjunto con el área de sistemas para continuidad del negocio en condiciones de desastre.

9.1.1.1.2 *Software de PQRSD*

Aplicación: GD Correspondencia

Estado Actual: En la actualidad, el sistema se usa para la recepción de quejas y reclamos de la Alcaldía y funciona en un servidor local

Proveedor: GD

Usuario: Ventanilla Única

Riesgos Asociados: Posible incumplimiento de los contratistas, Posibles Retrasos en Procesos Administrativos, Mal funcionamiento de las aplicaciones críticas o de los Equipos en donde están instaladas, Contratación o aplicación de Soluciones Inadecuadas o Incompatibles con los Recursos Disponibles.

Soluciones en contingencia: Ante la posible materialización de los riesgos o falla de las aplicaciones actuales se plantea la Implementación y puesta en producción de las siguientes soluciones:

1) Seguir con la ejecución del contrato de mantenimiento con GD y exigir Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

2) al contratista para adecuarlo al de la Administración

3) Asignar un ingeniero de la oficina de sistemas que se encargue de realizar las copias de seguridad del Sistema en servicios de la nube y en disco externos.

4) Contratar un servicio en la nube para que el software funcione en la nube y se prevengan riesgo de pérdida de información.

9.1.1.1.2 *Software de Gestión Documental*

Aplicación: GD

Estado Actual: En la actualidad, el sistema se usa para el manejo de la gestión documental de la Alcaldía y funciona en un servidor local.

Proveedor: GD

Usuario: Archivo

Riesgos Asociados: Mal funcionamiento de las aplicaciones críticas o de los Equipos en donde están instaladas.

Soluciones en contingencia: Ante la posible materialización de los riesgos o falla de las aplicaciones actuales se plantea la Implementación y puesta en producción de las siguientes aplicaciones o soluciones:

1) Seguir con la ejecución del contrato de mantenimiento con GD y exigir Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información al contratista para adecuarlo al de la Administración.

1) Se plantea la implementación de un aplicativo de nivel bajo (sencillo), en hoja electrónica o base de datos, para garantizar la continuidad de los procesos críticos de presentación de información a las entidades externas.

2) Realizar una copia Mensual de la base de datos que maneje el servidor en servicios en la nube y realizar copias en disco externo.

3) Propender por tener el programa en la nube

9.1.1.1.4. Cámara *de Comercio*

Estado Actual:

Usuarios:

Riesgos Asociados: Mal funcionamiento de las aplicaciones críticas o de los Equipos en donde están instaladas, o caída del servidor.

Soluciones en contingencia: Ante la posible materialización de los riesgos o falla de la aplicación actual, se presenta las siguientes soluciones:

Soluciones en Contingencia: Backup de los servidores y los funcionarias harían las liquidaciones manualmente en Excel.

En el momento en que se presente la emergencia, para cualquiera de las aplicaciones críticas citadas anteriormente, los grupos de trabajo deben iniciar y seguir los siguientes pasos:

PASO	ACCION	RECURSO NECESARIO	DURACIÓN	RESPONSABLE
1	Reporte de la falla al funcionario encargado de los sistemas, que pertenece a la dependencia y que hace parte del grupo de desarrollo.	Teléfono. WhatsApp Reporte de Errores	Inmediato	**Usuario**
2	Inhabilitar el uso del equipo o equipos que utilizan dicha aplicación y advertencia a los usuarios para no desarrollar ninguna actividad relacionada.	Listado de usuarios, medio de comunicación.	Inmediato, Máximo 15 minutos	**Funcionario Encargado de la Dependencia**
3	Reporte de la falla a la Línea de Atención a Usuarios	Teléfono o WhatsApp Reporte de Errores	Inmediato, Máximo 30 minutos	**Funcionario Encargado de la Dependencia**
4	Dirigirse a la dependencia en donde se ha presentado la falla	Medio de transporte, reporte de errores, orden de servicio	Máximo 30 minutos, dependiendo del lugar donde se halla presentado la falla	**Ingeniero de la Oficina de Sistemas y Técnico de Soporte encargados de la vigilancia y soporte de la aplicación reportada en emergencia.**
5	Identificación, Diagnóstico y Análisis de las fallas y su alcance.	Fuentes, documentación soporte de la aplicación, equipo de soporte y pruebas	Dependiendo del nivel de criticidad de la falla (alta, media, baja), pero no mayor de 1 hora.	**Ingeniero de la Oficina de Sistemas, Funcionario delegado en la dependencia y Técnico de Soporte**

PASO	ACCION	RECURSO NECESARIO	DURACIÓN	RESPONSABLE
		(herramientas y medios magnéticos)		**encargados de la vigilancia y soporte de la aplicación reportada en emergencia**
6	Reporte al Coordinador del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.	Teléfono, WhatsApp y documento de diagnóstico de la falla	Inmediatamente se haya terminado el diagnóstico respectivo, máximo 15 minutos después.	**Ingeniero de la Oficina de Sistemas**
7	Notificación al Director de la Oficina de Sistemas para que se tomen la decisión de liberar y poner en ejecución el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información., si así lo amerita.	Teléfono, WhatsApp, Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y documento de diagnóstico de la falla.	Inmediato, máximo 15 minutos.	**Coordinador del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.**
8	Si se pone en marcha el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información., el coordinador debe identificar el área o áreas afectadas con el fin de notificar al personal encargado de las mismas, para llevar a cabo las actividades del Plan.	Teléfono, WhatsApp, Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.y documento de diagnóstico de la falla.	Entre 15 y 30 minutos.	**Coordinador del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información..**
9	Localizar los recursos necesarios para dar inicio al Plan relacionado con el área afectada	Inventarios, Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información., documento de diagnóstico de la	El mínimo dependiendo de la ubicación de los recursos	**Director de la Oficina de Sistemas Coordinador Grupo Línea de atención a**
		Falla, último backup, manuales de usuario y técnico de la	Necesarios. Máximo 1 hora.	**Usuarios de la empresa desarrolladora, al igual que Ingeniero designado por está**

PASO	ACCION	RECURSO NECESARIO	DURACIÓN	RESPONSABLE
		aplicación afectada. Medios magnéticos necesarios.		**para soporte al desarrollo. Y Técnico de Soporte de la Alcaldía**
10	Implementar la solución y ejecutar las actividades establecidas en el Plan para mantener la continuidad del proceso afectado.	Recursos necesarios localizados en la actividad 9.	El mínimo dependiendo de la complejidad de la solución. No debe ser mayor a 5 horas.	**Director de la Oficina de Sistemas Coordinador Grupo Línea de atención a Usuarios de la empresa desarrolladora, al igual que Ingeniero designado por está para soporte al desarrollo. Y Técnico de Soporte de la Alcaldía**
11	Reportar al Coordinador del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, la conclusión de las actividades previstas y la puesta en marcha de la solución.	Reporte de las actividades realizadas, debidamente firmada por el usuario, como recibo a satisfacción.	Entre 15 y 30 minutos.	
12	Monitorear el correcto funcionamiento de la solución implementada, con el fin de avisar cualquier anomalía a la Oficina de Sistemas.	Documentación del proceso afectado.	Observación permanente, mientras dure la contingencia	**Funcionario delegado en la dependencia encargado de la vigilancia y soporte de la aplicación reportada en emergencia**
13	**Iniciar las acciones pertinentes para el restablecimiento del proceso normal (ubicar al proveedor, hacer efectivas pólizas, hacer soporte correctivo, contratar nuevas soluciones, etc., según convenga o este planeado).**	**Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.. Documentación soporte del proceso.**	**No mayor a un (1) mes dependiendo del nivel de criticidad del proceso afectado.**	**Director de la Oficina de Sistemas Coordinador Grupo Línea de atención a Usuarios de la empresa desarrolladora, al igual que Ingeniero designado por está para soporte al desarrollo. Y Técnico de Soporte de la Alcaldía**

9.1.1.1.5 Software Ofimático

Estado Actual: La entidad en la actualidad cuenta a nivel de software con:

Software Ofimático: Microsoft Office 2007, Microsoft Office 210 Microsoft Office 2013 y Microsoft Office 2016

Software Operativo: Windows X P , Windows 7, Windows 8, Windows 8.1, Windows 10, Linux, Windows NT

Proveedor: Distribuidores autorizados MICROSOFT.

Usuario: Todas las dependencias de la Entidad

Riesgos Asociados: Mal funcionamiento de las aplicaciones críticas o de los Equipos en donde están instaladas, Posible pérdida de información, Posible falla de equipos electrónicos y Hardware fuera de inventario.

Soluciones en contingencia: Ante la posible materialización de los riesgos se plantea la utilización de los medios originales del software existente para realizar las respectivas reinstalaciones.

En el momento en que se presente la emergencia, el usuario debe seguir el procedimiento Atención a Usuarios que a continuación se describe

PROCEDIMIENTO DE ATENCIÓN A USUARIOS

No.	EJECUTOR	ACTIVIDAD	REGISTRO	OBSERVACIONES
1	Jefes de dependencia, Auxiliares, Contratistas	Informan a la Oficina de Sistemas los problemas detectados en Hardware y Software.		El reporte puede ser telefónicamente, WhatsApp, personalmente o con memorando.
		Recibe la solicitud del servicio (Hardware ó Software). Se registra en la Hoja de Datos de los		Los registros deben contener como mínimo la siguiente información: ORDEN DE SERVICIO:

No.	EJECUTOR	ACTIVIDAD	REGISTRO	OBSERVACIONES
2	Profesional Universitario y/o Técnico Oficina	datos del funcionario y falla presentada. Analiza reporte y asigna funcionario del grupo SOS que atenderá el servicio reportado. Imprime orden de servicio y registra en la "Planilla de Reparto" Firma la planilla de reparto y entrega la orden de servicio generada al Técnico y/o funcionario del grupo SOS.	Planilla de Reparto Orden de Servicio	fecha de solicitud, problema detectado, nombre funcionario que solicita, teléfono, nombre funcionario grupo SOS, descripción detallada del problema. PLANILLA DE REPARTO: fecha de entrega, nombre funcionario asignado, firma de quien entrega y recibe la orden de servicio y descripción.
3	Profesional Universitario y/o Técnico Dirección	Recibe orden de servicio y firma planilla de reparto. Verifica falla y/o requerimiento del funcionario en la dependencia y elabora diagnóstico, registrando todos los campos en la orden de servicio y determina qué tipo de intervención se requiere. Si se requiere compra de repuesto se ejecuta procedimiento**.** “Instalación de elementos de Computo y/o Repuestos para		

No.	EJECUTOR	ACTIVIDAD	REGISTRO	OBSERVACIONES
		Estaciones de Trabajo e impresoras"		
4	Profesional universitario y Dirección	Si no se requiere la compra de repuestos: Subsana la falla, hace firmar al usuario la satisfacción del servicio en la Orden de Servicio. Registra en la planilla de reparto el servicio atendido, la fecha de devolución de la orden de servicio y firma.	Orden Servicio de Servicio	
5	Profesional universitario y Dirección Técnica de Informática.	Actualiza en la Hoja de Datos el cierre de la solicitud atendida. Registra en la planilla de reparto la fecha de atención de la solicitud.		

9.2 HARDWARE

9.2.1 Microcomputadores

Estado Actual: se encuentran en funcionamiento 927 equipos de cómputo, que se encuentran distribuidos en las diferentes dependencias de la entidad.

Usuario: Todas las dependencias de la Entidad

Riesgos Asociados: Mal funcionamiento de las aplicaciones críticas o de los Equipos en donde están instaladas, Posible pérdida de información, Contratación o aplicación de Soluciones Inadecuadas o Incompatibles con los Recursos Disponibles, Posible falla de equipos electrónicos y Hardware fuera de inventario.

Soluciones en contingencia: Ante la posible materialización de los riesgos, se plantea el uso del hardware existente, desarrollando un proceso de

redistribución de equipos para cubrir de manera óptima las necesidades reales y críticas de las dependencias y por ende de toda la Entidad.

En el momento en que se presente la emergencia, los usuarios deben iniciar y seguir los mismos pasos del cuadro de Procedimiento de Atención al usuario.

9.2.2 Equipos Servidores

Estado Actual: A continuación se muestra la estructura actual de la red de la Aclaldia de San Gil actualizada con la última plataforma tecnológica adquirida la cual se encuentra descrita en el item 6.4.2.2, con sus respectivos nombres de maquina y IP, descripción de su contenido.

Usuario: Centro de Computo y Usuarios de Aplicaciones implementadas en los servidores activos.

Riesgos Asociados: Mal funcionamiento de las aplicaciones críticas o de los Equipos en donde están instaladas, Posible pérdida de información, Posible incumplimiento de los contratistas, Contratación o aplicación de Soluciones Inadecuadas o Incompatibles con los Recursos Disponibles.

Soluciones en Contingencia: Se debe garantizar el mantenimiento preventivo/correctivo 7*24.

En el momento en que se presente la emergencia, los usuarios deben iniciar y seguir los mismos pasos del cuadro Atención al Usuario

9.2.3 EQUIPOS ELECTRÓNICOS

Estado Actual: Actualmente se cuenta con XX UPSs de las cuales XX de ellas está fuera de servicio y en espera de soporte.

Proveedor: Varios

Usuario: Todas las dependencias de la Entidad

Riesgos Asociados: Posibles retrasos en procesos administrativos, demoras en la efectividad de algunas comunicaciones, problemas en el control de asistencia del personal, Posible daño de equipos o pérdida de protección ante ausencia de fuente regulada y soporte en corte de energía eléctrica.

Soluciones en contingencia: se debe realizar un estudio de conveniencia y oportunidad dirigido por el área de Hacienda para que se adelante la contratación del mantenimiento correctivo y/o preventivo, que incluye el reemplazo de los bancos de baterías existentes de las UPS, compra de nuevas baterías y dar de bajas las que ya están dañadas

En el caso de no contar con fluido eléctrico regulado los equipos deben estar protegidos con reguladores de voltaje.

10. FASE DE RECUPERACION

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

Durante los primeros 5 días de interrupción prolongada del procesamiento de datos o desastre, si la interrupción del servicio va a ser por largo tiempo luego del desastre, se debe poner en ejecución la fase de recuperación del siniestro en el Centro de Cómputo alterno externo.

La estimación del tiempo en que va a durar la interrupción del servicio, se obtiene una vez se ejecute la Fase de Emergencia y una vez se halla evaluado el alcance de las fallas que se presentaron. Dicha estimación la debe obtener el Coordinador del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información., apoyado en el trabajo y resultados presentados por el grupo de desarrollo del Plan.

Si la falla es superior al 60% se deben optar por planes de uso de las otras instalaciones de la Alcaldía y adecuarlas para operaciones de las áreas afectadas.

Entonces, durante los 5 días siguientes al desastre, deberán prepararse las copias de respaldo de aplicaciones y procedimientos automatizados utilizados por las diferentes oficinas usuarias afectadas. El plan busca que las capacidades del servicio inicial del procesamiento de datos sean restauradas en el sitio alternativo en el 5º día siguiente al desastre. La reestructuración total de las capacidades del procesamiento para la red en línea está contempladas en fases durante 5 días a 28 días hábiles.

10.1 PREPARACIÓN REQUERIDA PARA RECUPERACIÓN DE DESASTRES

Los grupos de recuperación de desastre, deben estar organizados a lo largo de las líneas funcionales con la Oficina de Sistemas de la Alcaldía de San Gil y la representación de las dependencias usuarias, en la misma forma en que está organizado el grupo de desarrollo. Cada grupo es responsable del restablecimiento y mantenimiento de los procedimientos de recuperación antes del desastre. Los esfuerzos de planeación son para moderar el esfuerzo de la recuperación y maximizar el éxito de los procedimientos implementados en el evento de un desastre.

10.1.1 Grupo de oficina de Sistemas

10.1.1.1 Responsabilidades

- Mantener las especificaciones para las configuraciones de hardware que deben ser instaladas en los diferentes equipos del centro de cómputo alterno.
- 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.
- Implementar los procedimientos dados por otros grupos de recuperación para generar y/o almacenar materiales que deben estar fuera del edificio y son necesarios para la recuperación.
- 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.

10.1.1.2 Coordinador del Grupo

El Coordinador del Oficina de Sistemas de la Alcaldía, quien administra las operaciones de los sistemas.

10.1.1.3 Miembros del Grupo

- Grupo Centro de Computo
- Grupo de Atención a Usuarios.

10.1.1.4 Grupo de Atención a Usuarios

Oficina de Sistemas

10.1.1.5 Responsabilidades Predesastres

- Proveer procedimientos para crear copias legibles por los equipos, de todos los componentes del software del Sistema, librerías de software de aplicaciones, drivers y controladores de dispositivos, Software de instalación, actualización, utilitarios y antivirus.

- Ejecutar los procedimientos para mantener copias de respaldo en el centro de almacenamiento alterno con la información de las aplicaciones críticas, de los directorios de trabajo de cada una de las dependencias de la Alcaldía de San Gil y el recurso de software necesario para las mismas.

- Evaluar y Verificar el software de recuperación de desastres en la forma usual, en cooperación con el grupo de operaciones y el sistema de aplicaciones.

- Documentar cada evaluación de recuperación desde la perspectiva de las actividades del grupo de soporte técnico.

10.1.1.6 Coordinador del Grupo

- Coordinador del grupo de Atención a Usuarios.

10.1.1.7 Miembros del Grupo

- Grupo de Soporte de Atención a Usuarios
- Responsable de la operación de programas y comunicaciones.

10.1.1.8 Grupo de Análisis y Desarrollo

- Profesional universitario de la Oficina de Sistemas

10.1.1.9 Responsabilidades Predesastre

- Establecer procedimientos que permitan las revisiones de todo el software de aplicaciones en producción, para que sea almacenado y copiado rutinariamente en un sitio externo como parte de los procedimientos de backup de la operación del computador.
- Coordinar con los grupos de usuarios para asegurar que sus planes de acción en caso de desastre sean seguros, viables y actualizados con el fin de reflejar las operaciones actuales.

- Mantener una estrategia general, un plan y documentación para la evaluación de las aplicaciones luego de que la recuperación en el centro alterno se haya terminado por parte de los grupos de soporte técnico y de operaciones, pero antes de que los sistemas se coloquen de nuevo en producción.
- Coordinar con el grupo de operaciones el mantenimiento de los proyectos de las aplicaciones y la documentación en el lugar de respaldo.

10.1.1.10 Coordinador del Grupo

- Coordinador del Grupo de Análisis y Desarrollo

10.1.1.11 Miembros del Grupo

- Ingenieros programadores y analistas responsables de la aplicaciones contratadas.
- Usuario final, responsable de la operación del programa.
- Funcionario Delegado de cada dependencia encargado de la supervisión de la aplicación.

10.2 RECUPERACIÓN DEL DESASTRE: PLAN DE ACCION

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

10.2.1 PRIMERA FASE: Procedimientos Iniciales de Respuesta/Notificación

Los siguientes deben ser los procedimientos a ser implantados en el momento del desastre, 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 previa notificación a uno de sus integrantes.

10.2.1.1 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 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 sus delegados).
Si hay tiempo para apagar, se deben realizar las siguientes actividades, en el orden especificado:

a) Inicializar procedimientos de emergencia organizacional estándar (los establecidos por el Grupo de Salud Ocupacional).
b) Ejecutar procedimientos de apagado para los servidores y demás dispositivos del centro de cómputo.
c) Apagar extractores
d) Apagar luces y bajar tacos en las cajas de distribución
e) Notificar al grupo de Administración de Emergencia

10.2.1.2 Grupo de Administración de Emergencia de la Oficina de Sistemas

Coordinador Grupo de Análisis y Desarrollo
Oficina de Sistemas

10.2.1.3 ARBOL TELEFONICO DE EMERGENCIA

El grupo de emergencia, o su designado, llamará a los líderes de grupo de recuperación de desastre con información actualizada de la situación del desastre, junto con la localización y hora de reunión del Grupo de Administración de Emergencia.

10.2.1.4 Líderes de Grupo

Coordinador del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.
Grupo de Administración de la Emergencia
Coordinador de la Oficina de Sistemas

Estos líderes de grupo tendrán copias del Plan para el grupo, con la lista de las personas que lo conforman. El líder iniciará un árbol telefónico para contactar todos los miembros del grupo.

El Administrador asumirá la responsabilidad total del grupo de administración de emergencia. El Grupo de Administración de Emergencia hará una apreciación inicial de la extensión del desastre tan rápido como sea posible.

Será decisión del Grupo de Administración de Emergencia, si se inicializa el resto del Plan o no (Si se activa el Centro Alterno o no). Se espera que esto ocurra en un lapso de 4 horas después del desastre.

10.2.2 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 Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

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.

10.2.2.1 Acciones

Dentro de las 6 horas siguientes al desastre se debe:

- Notificar a los usuarios la interrupción del servicio.
- Notificar al Director de la Sede Alterna, Jefes de Dependencia Contratistas
- Activar el procesamiento manual de las aplicaciones (si es necesario)
- Efectuar una evaluación de daños e identificar el equipo reusable para transferirlo al Centro Alterno.
- Notificar al Proveedor las configuraciones de Hardware y alistar los requerimientos.
- Notificar a todos los funcionarios de la Dirección de Informática, que están involucrados en el Plan.
- Seleccionar y catalogar las oficinas de servicio para el procesamiento de los reportes de respaldo.
- Inicializar las preparaciones ambientales en la Oficina de Sistemas o Centro de Respaldo. (Eléctrica, protección contra incendio, extractores).
- Ordenar los circuitos para comunicación de datos en el Centro Alterno, si es necesario.

Dentro de las 24 horas siguientes al desastre debe:

- Contactar con el proveedor y ordenar el soporte tanto de hardware como de software
- Iniciar y coordinar los procedimientos de preparación del lugar para el Centro Alterno.
- Iniciar el ensamblaje de la documentación y medios magnéticos en el lugar de almacenamiento externo.

- Confirmar el soporte dado por el proveedor.
- Complementar el procesamiento de los reportes seleccionados en el Centro Alterno.

Dentro de los 2 días siguientes al desastre debe:

- Catalogar el despacho de suministros
- Trasladar el personal necesario y/o requerimientos al Centro Alterno
- Completar el ensamblaje de la documentación y los medios magnéticos en el Centro Alterno, coordinando la prestación de los servicios desde el Centro Alterno.

Dentro de los 3 días siguientes al desastre:

- El Centro Alterno 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 Centro Alterno suficientes suministros, muebles y equipo relacionado.
- Determinar el punto inicial de aplicaciones críticas.
- Establecer un catálogo de procesamiento de las aplicaciones críticas.
- Evaluar las líneas de comunicación de datos catalogados para una restauración inicial.

Dentro de los 4 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 Centro Alterno.
- Asegurar el ambiente físico en el Centro Alterno y establecer la seguridad de los datos.
- Restablecer los backups de datos de producción de las cintas de backups.
- Evaluar los sistemas en línea, para verificar la operación y validez de los datos restaurados.
- Evaluar los sistemas operacionales
- Notificar a los usuarios el estado de la recuperación

Dentro de los cinco 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 28 días siguientes al desastre:

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

10.2.3 TERCERA FASE: Procesamiento en el Centro de Cómputo Alterno

Las actividades paralelas listadas abajo caracterizan las acciones a tomar durante esta fase. Empiezan cuando los sistemas críticos y las redes de computación son operativas y no se ha podido completar la restauración de los datos del sistema. Esta fase continúa hasta que los servicios de procesamiento de datos son restaurados en el lugar u otro sitio permanente.

En este momento es cuando se debe informar al personal de las actividades que han sucedido y la operabilidad del plan. Los logs de recuperación del desastre se deben recolectar y analizar por parte del Grupo de Administración de Emergencia de la Dirección de Informática. Deben realizarse preparaciones en la marcha para regresar al sitio original o alternativo.

10.2.3.1 Actividades de esta Fase

- Asegurar un medio ambiente físico y restablecer la seguridad en los datos
- Comenzar el procesamiento de transacciones críticas
- Tener todos los recursos en su lugar en el Centro de Cómputo Alterno
- Localizar los procedimientos de backup y almacenamiento
- Obtener una recuperación total
- Distribución del grupo de personal y reportar a la administración

10.2.4 CUARTA FASE: Recuperación en el sitio original o alterno

Mientras que las operaciones se estén ejecutando en el Centro 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. Esta fase es muy similar a la descrita en la fase 3 pero en una localización permanente.

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

- Convertir a procesamientos en producción
- Realizar auditoría post-desastre
- Preparar reclamación de los seguros
- Reportar a la administración

10.2.5 QUINTA 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 es además críticamente importante. El Plan será auditado para ver que estos detalles sean actualizados rutinariamente en el Plan y en todas sus copias.

11 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 cada dependencia, software específico y operativo.
- Recuperación de errores y fallas del sistema
- Seguridad física y lógica
- Mantenimiento preventivo y correctivo de equipos
- 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 de la Oficina de Sistemas. Seguido, debe ser probado y realizar al menos una simulación.

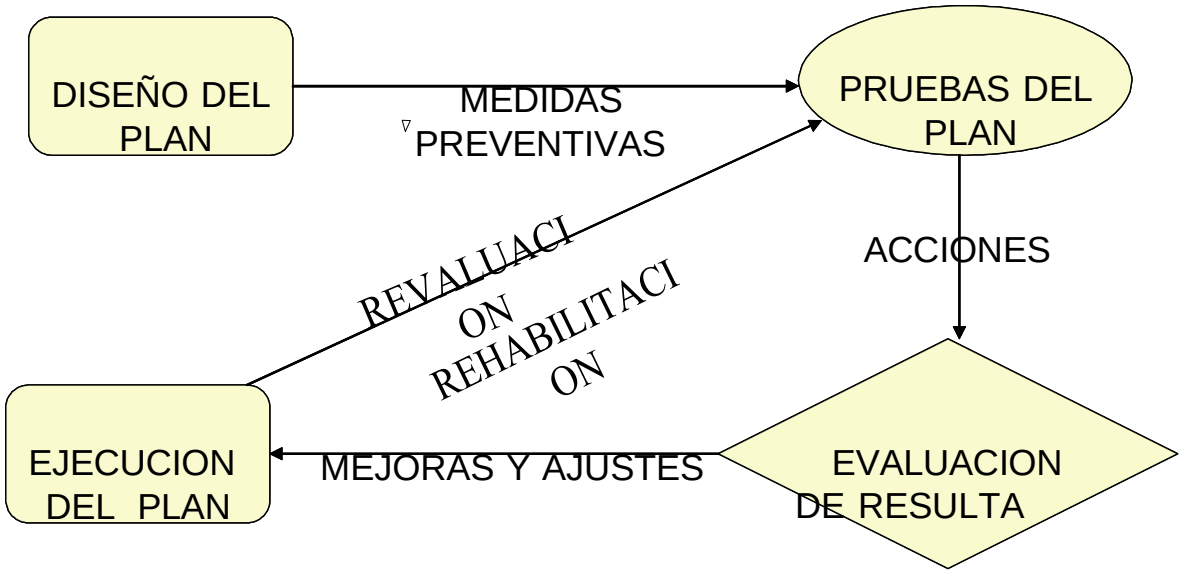
En segunda instancia, desarrollar un programa de entrenamiento a los sujetos y áreas directamente involucradas, aquellas que asumen responsabilidades y funciones dentro del plan.

Finalmente, debe adoptarse a nivel institucional mediante Acto Administrativo, es decir, reglamentado por Resolución emanada del despacho del Alcalde.

Posteriormente, se debe recopilar bimensualmente las modificaciones al plan y realizar actualizaciones periódicas al mismo.

12 PLAN EXPERIMENTAL DE PRUEBAS

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información. comprende, finalmente, el desarrollo de un plan experimental de pruebas en el cual se incluye la simulación de los diferentes siniestros para comprobar que el plan diseñado es eficaz o, en caso contrario, se le deben efectuar ajustes para su funcionalidad.



El mayor énfasis será ejercido sobre las pruebas o simulacros, y sobre los eventos posteriores a la emergencia relacionados con el reinicio de las operaciones normales de la Alcaldía de San Gil

Los siguientes son los objetivos de control y auditoria de las pruebas del plan:

- Validar la habilidad de los funcionarios y la consistencia de los procedimientos en eventos de recuperación de siniestros.
- Probar la factibilidad y compatibilidad de las instalaciones de respaldo y de los procedimientos relacionados.
- Identificar y corregir fallas en el plan.
- Facilitar la divulgación y el entrenamiento en los procedimientos y guías de recuperación
- Fomentar el respeto por el plan y la seguridad en su efectiva aplicación en caso de presentarse emergencias
- Estar preparado para evaluar las necesidades de seguros y reducir al máximo los costos en primas de aseguramiento
- Motivar a los funcionarios involucrados en el diseño y desarrollo del plan a mantener actualizados los procedimientos inherentes

La Oficina de Control Interno evaluará que sean definidas las responsabilidades de las pruebas del plan, tales como:

Personal de administración: Grado de participación y compromiso, Niveles jerárquicos de aprobación y Asignación de recursos, capital y tiempo.

Personal del área de informática: Programación, operación y soporte técnico

Grupo de usuarios por segmento operativo

Personal externo: Proveedores, grupos de apoyo internos o externos y centros de recuperación contratados o comprometidos.

La Oficina de Control Interno conocerá la frecuencia de las pruebas y la periodicidad de cambios en el ambiente informático o cualquier ajuste en el mismo.

La Dirección de Informática y la Oficina de Control Interno, identificarán y documentarán los diferentes niveles de prueba del plan. Estos pueden ser por segmentos, por áreas relacionadas o a gran escala; éste último, como prueba global del plan, según los lineamientos que establezca el comité directivo. Como métodos de prueba, se sugieren: en papel, real o a gran escala probado por segmento mediante simulacro a criterio del comité directivo con apoyo del grupo de desarrollo; la Oficina de Control Interno conocerá los períodos de prueba.

12.1 PASOS PARA CONDUCIR LA PRUEBA

El grupo de desarrollo del plan indicará a la Oficina de Control Interno el esquema ordenado de las pruebas, teniendo en cuenta:

1) Selección del sujeto de la prueba para identificar los aspectos o capítulos del plan que están siendo evaluados
2) Descripción de los objetivos de la prueba y mecanismos de medición del alcance exitoso de los objetivos.
3) Reunión con el comité directivo para explicar la prueba y sus objetivos, y obtener como resultado su acuerdo y soporte
4) Comunicación formal de una prueba anunciada, los factores críticos a considerar y el tiempo estimado de la prueba.
5) Consolidación de los resultados de la prueba al final de ésta.
6) Evaluación de resultados: progresos, inconvenientes y logros.
7) Determinación de las implicaciones de los resultados de la prueba. Se debe analizar si el resultado de un caso simple (segmento) puede tomarse como referencia para la realización satisfactoria de todos los capítulos del Plan (a gran escala)
8) Generación de recomendaciones para cambios o ajustes, definición de la fecha límite para respuesta y gestión
9) Notificación de los resultados de las pruebas al Alcalde , Junta de Gobierno y Oficina de Sistemas
10) Cambios en documentación o manuales, si es aplicable.

12.2 AREAS O PARTES A PROBAR

- Recuperación del sistema aplicativo individual utilizando archivos y documentación almacenada en el sitio externo
- Habilidad para procesar en modo “degradado” o limitado
- Recarga de los discos del sistema y de los procedimientos de carga y arranque utilizando archivos y documentación almacenada en el sitio externo
- En sitios de procesamiento alterno, solución de diferencias en configuración de equipos
- Disponibilidad de equipos periféricos y de procesamiento
- Disponibilidad de equipos de soporte: aire acondicionado, unidades de potencia no interrumpida de corriente eléctrica
- Disponibilidad de soporte logístico: provisiones, transporte y comunicaciones.
- Evacuación del equipo desde el centro de cómputo de la Entidad, en respuesta a eventos tales como inundación o terrorismo.
- Habilidad de la administración y del comité directivo para determinar la prioridad de sistemas cuando se procesa con recursos computacionales limitados.
- Habilidad para recuperar y procesar en forma satisfactoria sin personal clave, asumiendo la pérdida del personal o turnos primarios.
- Habilidad para adaptar el plan a desastres menores

- Efectividad de alternativas manuales para aquellos sistemas que confían en esa opción.
- Habilidad de entrada de datos para alimentar sistemas críticos utilizando las instalaciones del área de soporte externo.
- Habilidad de los usuarios para continuar con las operaciones normales de la entidad para los sistemas clasificados como no críticos.
- Habilidad para establecer contacto en un período definido por emergencia y de manera organizada, con el personal clave o sus designados alternos.
- Nivel de cumplimiento de los estándares normativos aprobados por la entidad.
- Identificación de los recursos utilizados durante la emergencia que son cubiertos por la póliza de seguros.
- Distribución correcta y oportuna de listados, transmisión de datos vía telefónica conmutada, servicios de correo.
- Disponibilidad de formas y cantidad mínima de papelería. Control de formas numeradas o asimilables a títulos valores.
- Adherencia nula, parcial o total a medidas de seguridad durante el período de emergencia.
- Habilidad para ejecutar tareas de evacuación y tratamiento de primeros auxilios.
- Mecanismos para recuperación de información perdida en caso de sistemas en línea.
- Análisis de tiempos y movimientos durante las pruebas.

12.3 PROCESO GENERAL PARA PRUEBA ANUNCIADA

1) Presentación a consideración del comité directivo
2) Procedimiento de comunicación formal
3) Desarrollo de la prueba

12.4 PROCESO GENERAL PARA SIMULACRO

1) Presentación a consideración del comité directivo
2) Desarrollo del simulacro

13. POLÍTICAS DE SEGURIDAD

Las políticas de seguridad de información son la piedra angular de la eficacia de la seguridad de la información, sin una política sobre la cual basar los estándares y procedimientos, las decisiones tomadas serán probablemente inconsistentes y los agujeros de seguridad estarán presentes listos para ser explotados por personas internas y externas a la organización.

Esta es una primera fase en la implementación de políticas, para evaluar su aceptación y cumplimiento en la organización.

13.1 REINICIALIZAR O RESTAURAR SU SISTEMA

Los propietarios de los sistemas de información deben asegurarse de la existencia de un backup completo y que los procedimientos de recuperación de sistemas están en su sitio.

Descripción
Facilita las instalaciones para asegurar que su equipo reinicie exitosamente después de una interrupción voluntaria o involuntaria.

- No tener disponible el sistema después de una interrupción en el proceso normal puede impactar la eficiencia en las operaciones de la entidad.
- Pérdida de información después de una interrupción en el proceso normal, puede interrumpir las operaciones y retrasar los procesos de la entidad.

13.1.1 PANTALLA SIN INFORMACIÓN VISIBLE

Los usuarios de los computadores de la Alcaldia de San Gil deben asegurarse que su monitor o pantalla se encuentre en blanco, cuando el usuario no la este utilizando.

- Si la pantalla es legible cuando el usuario se encuentra ausente de su escritorio o de su lugar de trabajo, esto podría dar como resultado que la información confidencial (sensible) pueda ser leída por personal no autorizado.

- Cuando el personal puede ver como un sistema confidencial es accesado, esto puede facilitar su premeditación a intentos oportunos para leer y copiar los datos cuando el computador es abandonado aunque sea por un corto periodo.

13.2 MANEJO DE BACKUPS Y PROCEDIMIENTOS DE RECUPERACION

El backup de los archivos de información de la organización y la habilidad para recuperar información es una prioridad alta. La administración es responsable por asegurar que la frecuencia de cada operación de backup y los procedimientos de recuperación se ajusten a las necesidades de la organización.

Los procedimientos usados para iniciar una recuperación deben ser claramente documentados y probados. Si los procedimientos de restauración no han sido probados, una restauración parcial o incompleta puede corromper la integridad del sistema.

Descripción

- Cuando los procedimientos de backups son inadecuados o débiles, la información puede perderse o no estar disponible, lo que compromete la confiabilidad de los procesos de la organización.

- Modificaciones maliciosas, de los resultados de la secuencia diaria del backup dentro de una falla para proteger todos los datos requeridos.

13.3 ARCHIVAR INFORMACIÓN

Los medios de almacenamiento usados para archivar la información deben ser apropiados de acuerdo a las expectativas de vida de la información. El formato en el cual es almacenada la información debe ser cuidadosamente considerado, especialmente cuando los formatos propios están implicados.

Se hace referencia a la información la cual no es requerida en el día a día, pero la cual necesita ser guardada por un cierto periodo y también información la cual debe ser guardada perpetuamente. Los datos que son removidos del procesamiento cotidiano, reducen los niveles de almacenamiento y de recursos de procesamiento.

Las recomendaciones que deben ser consideradas cuando se implemente esta política incluyen lo siguiente:

Las debilidades en la longevidad de los medios usados para archivar, pueden causar fallas en la restauración de los datos cuando eventualmente sean requeridos.

Los datos archivados pueden ser conservados a menudo en un formato del usuario que sea apoyado solamente por los sistemas actuales, asi intentos frustrados

de acceso.

13.4 ENVIO DE CORREO ELECTRONICO

El e-mail se debe utilizar solamente para los propósitos institucionales, usándolo en términos que sean consistentes con otras formas de comunicación de la Entidad. Los archivos adjuntos a un e-mail se pueden adjuntar solamente después de confirmar la clasificación de la información que es enviada y después de explorar y verificar que el archivo no posee virus o código malévolo.

Descripción

- El uso de e-mail se ha hecho tan popular hasta el punto donde es obligatorio para todas las compañías ser accesadas a través de este medio. La carencia inherente de seguridad para enviar mensajes, información, archivos o instrucciones aparentemente es ignorado por muchos usuarios que utilizan este servicio.

- Enviar e-mail usando firmas digitales (opcionalmente encriptado) es una forma de asegurar su validez e integridad. El contenido de e-mail recibidos sin autenticación podría ser considerado poco fiable.

    1. La transmisión de un virus puede no solamente causar daño en los equipos sino que puede dañar permanente la reputación de la organización.
    2. Enviar un e-mail vía líneas publicas (por ejemplo internet) puede comprometer la confidencialidad e integridad de la información que está siendo transmitida. Esto es similar a una carta postal porque cualquiera que la pueda abrir, la puede leer.
    3. Archivos confidenciales podrían ser transmitidos por e-mail como adjuntos, rompiendo así la confidencialidad y potencialmente ocasionando pérdidas financieras.
    4. Enviar una copia de archivos a los colegas dentro de la red interna, crea duplicados innecesarios y también compromete la integridad del documento o archivo original.

14. CONCLUSIONES

- En el presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se describen los métodos y procedimientos a seguir en la Acadia de San Gil en caso de presentarse desastres que destruyan, modifiquen o alteren la información y los equipos de computo que la procesan, con el propósito de proteger la información y asegurar la continuidad del procesamiento de la información necesaria para el adecuado cumplimiento de sus Objetivos Institucionales.

- Lograr integración interinstitucional, a través de convenios entre las entidades públicas de tal forma que se ofrezca apoyo en sus centros de cómputo principales y alternos con la implementación de aplicaciones de propósito común, compatibles entre sí, garantizando el desempeño y continuidad en cada una de sus funciones.

- Concientizar a los funcionarios de la Entidad acerca de la seguridad de la información, labor que no es sólo de la dirección de Informática, sino que debe comprometer a toda la organización.

- Con el desarrollo de este trabajo en la Contraloría se establecen los perfiles acerca de las labores que ha de cumplir el grupo encargado del seguimiento del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

ALCALDÍA MUNICIPAL DE SAN GIL

CONTROL DEL DOCUMENTO

	Nombre	Cargo	Dependencia	Fecha
Autor	Manuel Fernando Lizarazo Ballesteros Marcos Fernando Reyes Álvarez	Profesional Universitario Profesional Universitario	Dirección administrativa Secretaría de desarrollo económico	28-01-19
Revisó	Rafael Norberto Acosta Wandurraga	Secretario de desarrollo económico	Secretaría de desarrollo económico	29-01-19
Aprobó	Hermes Ortiz Rodríguez	Alcalde	Despacho	30-01-19

CONTROL DE LOS CAMBIOS

IDENTIFICACION DEL CAMBIO	DETALLES DEL CAMBIO	FECHA DEL CAMBIO	VERSION
Creación	Creación del Documento y adoptado mediante Resolución N° 100-33-082-2019	30-01-2019	0.0
Modificación	Modificación para la vigencia 2020 y adoptado mediante Resolución N° 100-33-028-2020	30-01-2020	0.1