PLAN DE CONTINGENCIA

GESTION INFORMATICA

“Los desastres pueden ocurrir a cualquier hora y por diversas razones. Un plan de contingencia bien elaborado debe ayudarnos a reducir los efectos de un desastre**”**

Neiva, Febrero de 2018

Carrera 1 No. 60 – 79. Barrio Las Mercedes
Neiva – Huila (Colombia).
Tel. (57 8) 8765017 - (57 8) 8765344
Correo: camhuila@cam.gov.co
www.cam.gov.co

INTRODUCCION

A partir del modelo de seguridad de la información adoptado por la Corporación Autónoma Regional del Alto Magdalena, se ha elaborado el presente plan de contingencia de Gestión Informática, con el fin de contar con un plan debidamente diseñado y socializado que permita afrontar en debida forma un incidente a efectos de asegurar la disponibilidad y seguridad de los datos y aplicaciones críticas de la entidad.

OBJETIVOS

1. Asegurar la disponibilidad, confiabilidad y seguridad de los datos y aplicaciones críticas de la CAM, ante eventos que pongan en peligro su existencia.

2. Proteger y conservar los activos de la CAM, de riesgos, desastres naturales o actos mal intencionados.

3. Reducir la probabilidad de las pérdidas, a un mínimo de nivel aceptable, a un costo razonable y asegurar la adecuada recuperación.

4. Asegurar que existan controles adecuados para reducir el riesgo por fallas o mal funcionamiento tanto del equipo, como del software, de los datos, y de los medios de almacenamiento.

Para tal efecto, se debe comunicar a todo el personal activo de la CAM, cuáles son los pasos a seguir en caso de ocurrencia de cualquier riesgo previamente identificado.

La vigencia de este plan esta sujeto a cambios tecnológicos, de equipamiento y de los sistemas informáticos relacionados con la CAM.

DATOS DE LA EMPRESA

Corporación Autónoma Regional del Alto Magdalena – CAM

- Datos territoriales
  - Centro: Carrera 4A No. 4-46 Garzón
  - Occidente: Carrera 6 No. 5-46 La Plata
  - Sur: Finca Marengo kilómetro 4 vía Pitalito - San Agustín

- Datos sede principal
  - Dirección: Carrera 1 No. 60-79 – Neiva
  - Servidores

Nombre	IP	Sistema Operativo	DD (Gb)	Espacio Libre (Gb)	Función	Base de datos
Servidor6 (Aplicaciones)	Confidencial	Windows Server 2003	136	27,88	Servidor de aplicaciones web.	Confidencial
			68,3	9,84		
Servidor base de datos	Confidencial	Windows Server 2012	3.686,4	3171,81	Servidor de base de datos	Confidencial
Servidor11 VMWare esxi 5.5.0 vSphere Client (Virtualizador) Creación de DataStorage para virtualización de 3,27 TB.	Confidencial	Windows Server 2012	79,66	62,06	AD DS (Active Directory Domain Services), DHCP DNS	Confidencial
	Confidencial	Windows Server 2012	119,66	60,15	Servidor de Aplicaciones Manager de AP Consola de administración Antivirus	Confidencial
	Confidencial	Windows Server 2012	60	34,80	Servidor de Aplicaciones Sistema Administrativo y Financiero	Confidencial
			260	132,64		
	Confidencial	Ubuntu Server	1044,48	783,31	Servidor de Gestión Documental	Confidencial

Servidor Estaciones Metereológicas.	Confidencial	Windows 7	X	X	Servidor de las estaciones metereológicas.	Confidencial

- Dispositivo firewall

MARCA	MODELO	SERIAL	LICENCIA
Fortinet	Fortigate 100-E	x	x

- 82 equipos, incluidos computadores de escritorio y portátiles conectados en red en la sede Neiva.

TIPO DE EQUIPO	PC´S
Servidores	5
Equipos de escritorio en uso	48
Portátiles en uso	30

- 26 equipos, incluidos computadores de escritorio y portátiles de las direcciones territoriales centro, sur y occidente, distribuidos así:

DIRECCIÓN TERRITORIAL	PC´S	PORTÁTILES
Centro	7	2
Sur	8	2
Occidente	5	2

Red inalámbrica identificada como WCAM, con 10 access point administrables, distribuidos así:

Dependencia	Ubicación
Secretaría General	Entrada bloque 1

Dirección Territorial Norte	Entrada bloque 2
Regulación y Calidad Ambiental	Entrada bloque 3
Planeación	Bloque 3
Dirección General	Entrada bloque 4
N.A.	Auditorio
CAV	CAV
N.A.	Centro de Atención al Usuario
N.A.	Centro de Documentación
N.A.	Proyecto Ceibas

Comunicación entre la sede principal y las direcciones territoriales: canal de datos

UBICACION	**ANCHO DE BANDA**
Principal	21 Mbps
Dirección Territorial Centro	7 Mbps
Dirección Territorial Sur	7 Mbps
Dirección Territorial Occidente	7 Mbps

El servicio de internet es dedicado, está instalado en la sede principal con un ancho de banda de 50 Mbps.

INFORMACION DE LA SEDE PRINCIPAL Y TERRITORIALES

El edificio de la Sede Neiva se encuentra aislado de los edificios aledaños, con vigilancia las 24 horas del día y sistemas de alarmas, mientras que las direcciones territoriales no cuentan con vigilancia ni sistema de alarmas.

Con respecto a la disposición física de los servidores de Sede Neiva se encuentran ubicados en el primer piso del edificio, en lugar acondicionado para tal fin, con techos y piso falso, control de temperatura, extintores, sistema de detección de humo y acceso biométrico.

Las instalaciones de la Sede Neiva y sucursales, cuentan con salidas de emergencia. También cuentan con extinguidores de tipo Solkaflam 123, las Direcciones Territoriales NO cuentan con sistemas de detección de humo e irrigación.

La CAM ha contratado por el sistema de outsourcing el soporte y mantenimiento de los sistemas de cómputo y redes de datos. El outsourcing provee a un ingeniero de sistemas para la administración del sistema y dos técnicos para el soporte de hardware, redes y comunicaciones.

Para el control de ingreso y salida a las instalaciones, cada persona es registrada manualmente. Todos los automóviles son registrados tanto a la entrada como a la salida de la Corporación en la sede principal.

PLAN DE CONTINGENCIA

Se tendrá en cuenta:

1) Alcance
2) Análisis de Riegos.
3) Evaluación del riesgo (en cada sucursal).
4) Asignación de prioridades.
5) Tratamiento del riesgo.
6) Mantenimiento del plan de contingencia.
7) Implementación del plan (acciones correctivas y preventivas).
8) Distribución y mantenimiento del plan.

1) <u>Alcance</u>

Este plan de contingencia cubrirá los procesos soportados por el área de Sistemas de la Corporación Autónoma Regional del Alto Magdalena – CAM, en lo que se refiere a:

- Infraestructura tecnológica: centro de cómputo
- Administración de bases de datos
- Sistemas de información que soportan los procesos realizados en la Entidad
- Red de datos

2) Análisis de Riesgos:

Se tienen en cuenta dos factores:

- Los que afectan a la seguridad del edificio.
- Los que afectan la integridad de los datos.

Los que afectan la seguridad del edificio:

- **Inundación:** poco probable, debido a que tanto la Sede Neiva como las sucursales, se encuentran ubicadas en lugares que no son propensos a inundaciones.
- **Incendio:** poco probable, porque no se manipulan materiales altamente volátiles, de igual forma se cuenta con redes eléctricas y redes de datos que cumplen con las nomas técnicas de calidad de la IEEE. Así mismo, se cuenta con extintores multipropósito.
- **Corte de energía eléctrica:** probables, se cuenta con dos UPS, una para servidores y otra para las estaciones de trabajo. **Cortes prolongados** (más de 1 hora): poco probables, la Corporación tiene una planta eléctrica.
- **Robo:** poco probable, en la sede Neiva se cuenta con vigilancia las 24 horas del día, mientras que en las direcciones territoriales no hay vigilancia ni sistema de alarmas.

Los que afectan la integridad de los datos:

- **Problemas de comunicación del cliente con los servidores:** probable.
- **Problemas en el cableado eléctrico de las estaciones de trabajo:** poco probable.
- **Problemas con los recursos compartidos de la red:** poco probable.
- **Caída de la base de datos:** poco probable.
- **Caída temporal del o los servidor/es por falla mecánica:** poco probable.
- **Pérdida total de un servidor:** poco probable.
- **Falla total o parcial del cableado:** poco probable.
- **Pérdida total o parcial de las estaciones de trabajo:** probable.
- **Virus informáticos:** probable, se cuenta con firewalls, antivirus, control de los equipos de la sede Neiva.
- **Ataques internos:** poco probables, se cuenta con restricciones de acceso a los servidores.

3) Evaluación del riesgo:

IMPACTO	PROBABILIDAD OCURRENCIA	NIVEL IMPACTO
BAJO	*BAJO*	BAJO
MEDIO	*MEDIO O BAJO*	MEDIO
ALTO	*MEDIO O BAJO*	ALTO
BAJO O MEDIO	*ALTO*	ALTO
ALTO	*ALTO*	ALTO

Los que afectan la seguridad del edificio

- **Inundación:** ocasionaría pérdidas totales o parciales por lo tanto, actividades interrumpidas hasta solucionar el problema. El costo promedio de los equipos se calcula de acuerdo a la TRM del dólar ($2.900).

TIPO DE EQUIPO	VR. EN DÓLARES	VR. EN PESOS
Servidor	5.103,45	$14.800.000
Pc o portátil	2.241,38	$6.500.000

  - Costo total de Hardware en sucursales: $ 130.000.000
  - Costo total de Hardware en Sede Neiva: $ 509.500.000
  - Costo de Instalación en Sede Neiva: $ 30.000.000

- **Incendio:** ocasionaría pérdidas totales o parciales. Si la pérdida es total, los costos serían los mencionados en el punto anterior.
- **Corte de energía eléctrica:** discontinuidad en el trabajo; costo mínimos, en épocas no pico; en épocas pico, la CAM no podría realizar los procesos críticos del negocio, tales como: facturación, recaudos, generación de informes, cobros coactivos, acuerdos de pago, expedición de CDP`s, lo que ocasionaría pérdidas que irían en proporción directa a la demanda de los servicios no prestados. En Sede Neiva, también generaría caída total de los sistemas de la compañía, caída total de los servidores, y por tal motivo inactividad total en territoriales.
- **Robo:** perdidas totales o parciales, según la gravedad de los hechos. Costos de Hardware: antes mencionados.

Los que afectan la integridad de los datos:

- **Los problemas de comunicación del cliente con los servidores, los problemas en el cableado eléctrico de las estaciones de trabajo, los problemas con los recursos compartidos de la red y la caída de la base de datos:** ocasionarían pérdidas totales o parciales, por lo tanto, se produce una interrupción en las actividades, hasta solucionar el problema. Costo: en épocas no pico, costos mínimos; pero en épocas pico, la CAM no podría realizar los procesos críticos del negocio, tales como: facturación, recaudos, generación de informes, cobros coactivos, acuerdos de pago, expedición de CDP`s, lo que ocasionaría pérdidas que irían en proporción directa a la demanda de los servicios no prestados. En Sede Neiva, también generaría caída total de los sistemas de la Corporación, caída total de los servidores, y por tal motivo inactividad total en territoriales.

- **Caída temporal del o los servidor/es por falla física:** ocasionarían pérdidas totales o parciales, por lo tanto, se produce una interrupción en las actividades, hasta solucionar el problema. Evaluar costo de reparación del desperfecto físico.
- **Perdida total de un servidor:** ocasionaría pérdidas totales o parciales, por lo tanto, hay una interrupción en las actividades, hasta solucionar el problema, además evaluar costo de reparación o de reposición.
- **Falla total o parcial del cableado:** ocasionaría pérdidas totales o parciales, por lo tanto, las actividades se encuentran interrumpidas hasta solucionar el problema.
- **Pérdida total o parcial de las estaciones de trabajo:** ocasionaría perdidas totales o parciales, por lo tanto, las actividades se encuentran interrumpidas hasta solucionar el problema, en caso de pérdida total, evaluar costos.
- **Virus informáticos:** generaría molestias en el sistema, ya que lo degradan y lo hacen más lento. Habría pérdidas totales o parciales, de la información almacenada.
- **Ataques internos:** generaría pérdidas totales o parciales, así como también, vulnerabilidad del sistema.

Item	Tipo de Riesgos	Impacto	Probabilidad Ocurrencia	Nivel de Impacto
Los que afectan la seguridad del edificio				
R1	Inundación	MEDIO-ALTO	BAJO	MEDIO-ALTO
R2	Incendio	MEDIO-ALTO	BAJO	MEDIO-ALTO
R3	Corte de energía eléctrica prolongado	MEDIO-ALTO	MEDIO	MEDIO-ALTO
R4	Robo	MEDIO-ALTO	BAJO	MEDIO-ALTO
Los que afectan la integridad de los datos				
R5	Problemas de comunicación del cliente con los servidores	MEDIO-ALTO	MEDIO	MEDIO-ALTO
R6	*Problemas en el cableado eléctrico de las estaciones de trabajo*	MEDIO-ALTO	BAJO	MEDIO-ALTO

R7	Problemas con los recursos compartidos de la red	MEDIO-ALTO	BAJO	MEDIO-ALTO
R8	Caída de la base de datos	MEDIO-ALTO	BAJO	MEDIO-ALTO
R9	Caída temporal del o los servidor/es por falla mecánica	MEDIO	BAJO	MEDIO-ALTO
R10	Perdida total de un servidor	ALTO	BAJO	ALTO
R11	Falla total o parcial del cableado	MEDIO-ALTO	BAJO	MEDIO-ALTO
R12	Perdida total o parcial de las estaciones de trabajo	MEDIO	MEDIO	MEDIO
R13	Virus informáticos	MEDIO	MEDIO	MEDIO
R14	Ataques internos	BAJO-MEDIO	BAJO	BAJO-MEDIO

4) Asignación de prioridades

Después de que acontezcan el o los incidentes antes mencionados, se debe establecer un orden de prioridades, para poder reestablecer los sistemas y así, poder comenzar a operar normalmente, teniendo en cuenta que la CAM tiene que realizar los procesos propios del negocio, sin descuidar la atención al público.

Las prioridades, según el riesgo que se presente pueden variar. El orden de importancia para restablecer los sistemas son:

- Sistema operativo de los servidores
- Controlador de dominio
- Servidor DHCP y DNS
- Proxy y firewall
- Motor de base de datos
- Servidores de aplicaciones web

5) Tratamiento del Riesgo

ACCIONES PREVENTIVAS

Riesgos que afectan la seguridad del edificio

Inundación:

Realizar mantenimiento periódico a los sistemas de aguas lluvias.

Incendio:

Mantener recargados los extintores y ubicarlos en sitios estratégicos. Realizar simulacros de incendio, capacitando al personal en el uso de los extintores.

Corte de energía prolongado:

Mantener la planta eléctrica de la sede Neiva, con combustible y en óptimas condiciones con el fin de que no muestre alarmas al entrar en funcionamiento.

Robo

Contratación de vigilancia privada

Riesgos que afectan la integridad de los datos

Las acciones preventivas a realizar para mitigar los riesgos relacionados con la integridad de los datos se describen a continuación:

Copias de seguridad: se realizarán de la siguiente manera:

Al final de cada semana se ejecuta el plan de backups, copiando los archivos al disco duro externo, esto permite salvar la información en caso de ruptura parcial o total de uno o más servidores, o de la propia base de datos. Al final de cada mes se copian los archivos en DVD´s para archivar definitivamente, enviándolas a dos sitios diferentes a la sede Neiva, con el fin de asegurar de que en caso de robo en las instalaciones de la Corporación, se cuente con otra copia de la información.

Adicionalmente se contrató el servicio de backup en la nube para mantener copias de los servidores, de tal manera que sea posible ejecutar un plan de recuperación en caso de presentarse pérdida total o parcial de los equipos servidores.

Red inalámbrica

Para mitigar los riesgos sobre el cableado estructurado es importante contar con tarjetas inalámbricas para los equipos que se conectan físicamente y que en el momento del incidente se requiera realizar tareas críticas en ellos.

Mantenimiento servidores

Dos veces al año debe realizarse mantenimiento preventivo a los servidores, el cual debe incluir limpieza lógica y limpieza física, ésta última puede realizarse anualmente.

Actualización PATCH de seguridad

Es importante ejecutar los patch de seguridad del sistema operativo para garantizar la disponibilidad de los servidores.

Actualización antivirus

Actualmente uno de los problemas que comúnmente se presentan en las redes es el ataque de virus, para mitigar este riesgo es recomendable contar con un software antivirus que tenga opciones de actualización diaria.

Vacunar las memorias USB antes de acceder a cualquier información contenida en ellas.

Activar las opciones de autoprotección del antivirus instalado, para que en un determinado momento nos indique a través de un mensaje que se ha detectado un virus.

Mantenimientos preventivos de los equipos

Una de las acciones para prevenir los riesgos que tienen que ver la integridad de los datos es la de realizar mantenimientos preventivos a las estaciones de

trabajo que se conectan a la red de datos, deben ejecutarse con una frecuencia semestral

Inventario de equipos

Mantener el inventario de equipos actualizado contribuye a tener conocimiento sobre el tiempo de vida útil de cada equipo y por ende a determinar cuáles estaciones de trabajo deben reponerse anualmente.

ACCIONES DE CONTINGENCIA

Falla en los servidores

- Ejecutar las herramientas de diagnóstico del fabricante del servidor para descartar daños físicos.
- Desconectar discos externos
- Ingresar en modo a prueba de errores con el fin de revisar dispositivos que pueden estar en conflicto.
- Deshabilitar servicios ajenos al inicio normal del sistema operativo.
- Una vez sea posible ingresar al servidor, es necesario revisar visor de sucesos, y que todos los servicios configurados en él estén disponibles.
- Si no es posible acceder al servidor, se requiere ubicar un equipo alterno para habilitar la copia de seguridad almacenada en la nube.

Cableado estructurado

Es importante disponer de patch cord para reemplazar aquellos que estén dañados y no permiten la conexión entre el cliente y el servidor.

Igualmente se debe mantener un switch de respaldo para habilitar los servicios de red.

Es importante realizar mantenimiento a la canaleta del cableado estructurado para evitar daños en los cables por roedores

Bases de datos

Actualmente el motor de base de datos, que en el evento de no estar diponibles, para asegurar el acceso a la información es indispensable:

- Encender la máquina virtual que está configurada como servidor de base de datos de contingencia, con el fin de restaurar allí los backups de las bases de datos
- Mantener copia con la configuración de la conexión a la base de datos alterna.
- Configurar en el regedit de los equipos cliente del Sistema Administrativo y Financiero la clave local con con el SID de la base de datos de contingencia
- Modificar el archivo que contiene los datos de conexión a la base de datos con los de la conexión alterna.
- Cuando se restablezcan todos los servicios se informa a los usuarios que suspendan el registro de datos en la base de datos de contingencia.
- Realizar backup de la base de datos de contingencia.
- Restaurar el backup en la ubicación de la base de datos de producción.
- Informar a los usuarios sobre la habilitación de los servicios para que continúen trabajando como lo hacen normalmente.

Instaladores (medios magnéticos)

Es necesario crear copias de los CD´s instaladores de los programas instalados en los servidores y conservarlos en un sitio diferente a la Sede Principal.

Falla en las estaciones de trabajo

Una vez se presentan fallas en las estaciones de trabajo se deben ejecutar las actividades definidas en el procedimiento *P-CAM-032 Mantenimiento correctivo de equipos*.

Para evitar que se presenten fallas irreparables en las estaciones de trabajo se debe definir la reposición de equipos para aquellos que cumplen con su ciclo de vida de cinco años.

Con el fin de dar continuidad en las actividades de los funcionarios a quienes sus estaciones de trabajo presentan fallas y no se pueden reparar inmediatamente, es necesario contar con al menos un equipo de contingencia que se pueda asignar mientras el daño se corrige.

Ataque de virus

Ante un ataque de virus se debe buscar la utilidad o herramienta para eliminarlo y copiarla en la carpeta compartida del servidor SRV_APP01 denominada *Instaladores* con el fin de distribuir la solución a los equipos de la red.

Falla en la intranet

- Instalar y configurar la intranet secundaria en el servidor de aplicaciones.
- Informar a los usuarios la URL para que puedan acceder a la intranet secundaria.
- Revisar y actualizar los documentos del Sistema Integral de Gestión en la intranet secundaria, con una periodicidad de dos meses.
- Revisar los archivos log y visor de sucesos del servidor para identificar la posible causa que dejó fuera de línea la intranet principal.
- Realizar los ajustes respectivos para restaurar la intranet principal.
- Una vez sea posible acceder nuevamente a la intranet principal, informar a los usuarios
- Dejar fuera de línea la intranet secundaria.

Aclaración: Las áreas encargadas de coordinar las contingencias son:

- Director General: responsable del edificio Sede Neiva.
- Director Territorial: responsable de la Dirección Territorial.
- Mantenimiento: encargado de solucionar problemas edificios, ya sea inundación, humedad, generador eléctrico, o cualquier otro problema relacionado.
- Departamento de Sistemas (OUTSOURCING): encargado de solucionar todo lo relacionado con redes, sistemas, servidores, hardware, software, cableados de red, entre otros.
- Encargado de Seguridad: su función es custodiar las instalaciones del edificio, y avisar al área correspondiente, en caso de incendio o robo.

5) Mantenimiento del plan de contingencia:

Semestralmente se deberá realizar un informe sobre el plan de contingencia, teniendo en cuenta las posibles modificaciones que se pudieran hacer.

Con el fin de mantener actualizado el plan de contingencia es necesario:

a) Llamar con una frecuencia semestral a los teléfonos de los colaboradores incluidos en la lista del plan de contingencia.

6) Distribución y mantenimiento del plan

Distribuir el plan de contingencia a todos los empleados de la Corporación, tanto en la Sede Neiva, como en cada una de las territoriales. Además, realizar una lista con los nombres, teléfonos y direcciones, de las personas encargadas de llevar adelante dicho plan.

Aclaración: en caso de modificarse el plan de contingencia, actualizar la versión en la intranet de la Corporación.

Elaboró: NIDIA ANDREA RATIVA GARCIA – Outsourcing sistemas

Administradora del sistema

Vo.Bo. EDISNEY SILVA ARGOTE

Jefe Oficina de Planeación

Aprobó. CARLOS ALBERTO CUELLAR MEDINA

Director General.