REGISTRO NACIONAL
DE LAS PERSONAS NATURALES

PLAN DE CONTINGENCIA DE LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES.

Registro Nacional de las Personas Naturales

Dirección de Informática

DOCUMENTO ELABORADO POR:

Nombre y Apellido: Ing. Nelson Atilio Cornejo
Cargo: Director de Informática

Firma:
Fecha: 31 de julio 2015.

DOCUMENTO REVISADO POR:

Nombre y Apellido: Lic. Otto Rolando Olivares Salazar
Cargo: Director Ejecutivo

Firma:
Fecha: 11 de agosto 2015.

DOCUMENTO REVISADO POR DIRECCION DE ASEGURAMIENTO DE CALIDAD:

Nombre y Apellido: Ing. José Ricardo Avendaño Castañeda
Cargo: Director de Aseguramiento de Calidad – Ad honorem

Firma:
Fecha: 11 de agosto 2015.

DOCUMENTO APROBADO POR:

Nombre y Apellido: Licda. María Margarita Velado Puentes
Cargo: Presidenta Registradora Nacional
2015

Firma:
Fecha: 03 de septiembre

CONTENIDO DEL DOCUMENTO:

APROBACIÓN DE JUNTA DIRECTIVA
ACTA No. ____ PUNTO No. ____ FECHA _____

REGISTRO NACIONAL DE PERSONAS NATURALES - RNPN
COPIA CONTROLADA No. _____ FECHA _____

1) INTRODUCCIÓN.

La preservación de la integridad de los datos y el aseguramiento de la continuidad de los procesos, es el eje transversal de la tecnología informática para una organización, en este sentido se auxilia de diversos recursos tales como equipos electrónicos, programas de computadoras, documentación técnica, talento humano especializado, protocolos de comunicación, normativas e instructivos, así como la debida planeación de la gestión de sus procedimientos.

Por lo que se hace necesario la estructuración del Plan de Contingencia Informática del RNPN, que incluye la prevención y medidas alternas a ejecutar, que permitan recuperar el estado normal de funcionamiento de los sistemas de aplicaciones, y comunicaciones en caso se sufra algún incidente imprevisto que repercuta en una amenaza a la continuidad de los procesos oficiosos de la institución, teniendo en consideración los diferentes riesgos.

Las medidas de seguridad están basadas en la especificación de controles físicos y lógicos, funciones, procedimientos y programas, que propicien la protección y medidas de contingencia para la integridad de los datos, seguridad física a los equipos, entorno de trabajo, talento humano y todo otro proceso que sea importante para la continuidad de los procesos del RNPN.

El Plan de Contingencias implica un análisis de los posibles riesgos de tecnología de información y comunicaciones (TIC), a los que se están expuestos, así como establecer los respectivos objetivos, alcance y metodología a desarrollar en este.

Pese a todas las medidas de seguridad a implementar, puede ocurrir un desastre, por tanto es necesario que el Plan de Contingencias incluya un Plan de Recuperación de Desastres, el cual tendrá como objetivo, restaurar el Servicio en forma rápida, eficiente y con el menor costo y pérdidas posibles.

Si bien es cierto que se pueden presentar diferentes niveles de daños, también se hace necesario presuponer que el daño ha sido total, con la finalidad de tener un Plan de Contingencias lo más completo posible.

2) OBJETIVOS.

2.1. General.

Contar con los lineamientos precisos, que garanticen la continuidad de los servicios del área de Tecnología de la Información que apoyan los procesos administrativos y operativos de la institución, mediante la ejecución de medidas alternas que permitan una solución en el menor tiempo posible, y así los servicios no sean interrumpidos.

2.2. Específicos.

A. Definir las acciones a ejecutar, en caso de incidentes en el entorno y la plataforma tecnológica del RNPN.
B. Contar con un marco de acción que permita la reacción inmediata y la disminución de los tiempos de recuperación o respuesta, en apoyo a los procesos del RNPN.
C. Disminuir las posibilidades de pérdida o daño de los recursos informáticos, al servicio de las diferentes direcciones y unidades del RNPN.
D. Identificar y evaluar los riesgos, estableciendo el punto de origen y concurrencia, la causa, la magnitud, las consecuencias, las acciones a seguir y el apoyo necesario para el control.

3) ALCANCES Y COBERTURA.

El plan de contingencia informático estima las acciones preventivas y correctivas para asegurar la continuidad de los servicios de apoyo que presta la Dirección de Informática, cuyo propósito es proteger los activos de información y demás recursos informáticos de la institución.

Debido al acelerado desarrollo de la tecnología, el presente plan deberá actualizarse al menos cada 3 años.

4) PLANIFICACIÓN Y TIPO DE FALLAS.

4.1. Planificación de la contingencia.

El Plan está orientado a establecer, junto con otros trabajos de seguridad, un adecuado sistema de seguridad física y lógica en previsión de desastres.

Se define la **Seguridad de Datos** como un conjunto de medidas destinadas a salvaguardar la información contra los daños producidos por hechos naturales o por el hombre. Se ha considerado que para la

compañía, la seguridad es un elemento básico para garantizar su supervivencia y entregar el mejor Servicio a sus usuarios, y por lo tanto, considera la Información como uno de los activos más importantes en la Organización, lo cual hace que la protección de esta sea el fundamento más importante de este Plan de Contingencia.

El Plan de Contingencias abarcará los siguientes aspectos:

a) Plan de Reducción de Riesgos (Plan de Seguridad).

b) Plan de Recuperación de Desastres.

b.1. Actividades Previas al Desastre.

b.2. Establecimiento del Plan de Acción.

c) Actividades durante el Desastre.

d) Plan de Emergencias.

e) Actividades después del Desastre.

f) Evaluación de Daños.

g) Ejecución de Actividades

h) Evaluación de Resultados.

i) Retroalimentación del Plan de Acción.

4.2. Tipos de fallas a considerar:

a) Red eléctrica.

b) Red de datos.

c) Acceso a sistemas internos.

d) Integridad del software y la información.

e) Problemas con servidores.

f) Estaciones y periféricos.

g) Servicio de Internet.

h) Seguridad Física y ambiental.

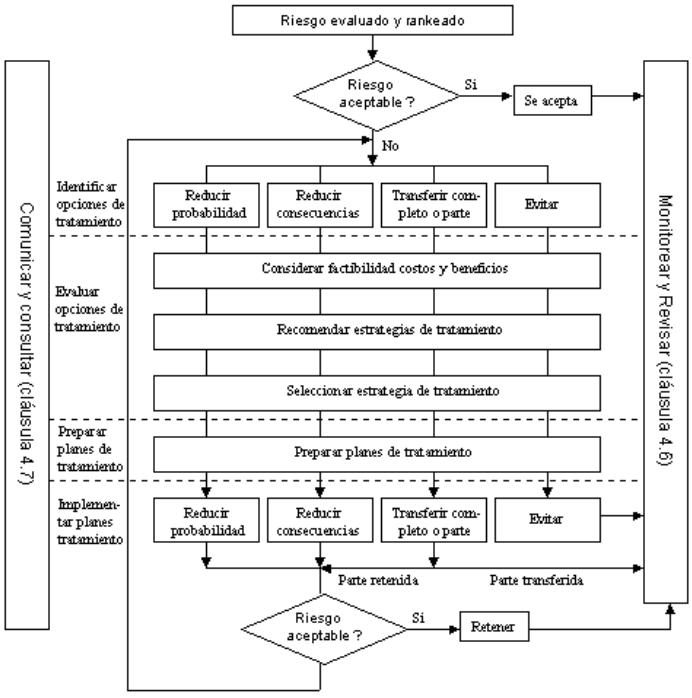
i) Sistemas de enfriamiento de ambientes.

5) ANALISIS E IDENTIFICACIÓN DE RIESGOS.

Los objetivos de análisis son separar los riesgos menores aceptables de los riesgos mayores, y proveer datos para asistir en la evaluación y tratamiento de los riesgos. El análisis de riesgos involucra prestar consideración a las fuentes de riesgos, sus consecuencias y las probabilidades de que puedan ocurrir esas consecuencias. Pueden identificarse los factores que afectan a las consecuencias y probabilidades. Se analiza el riesgo combinando estimaciones de consecuencias y probabilidades en el contexto de las medidas de control existentes.

Se puede llevar a cabo un análisis preliminar para excluir del estudio detallado los riesgos similares o de bajo impacto. De ser posible los riesgos excluidos deberían listarse para demostrar que se realizó un análisis de riesgos completo.

Se ha de tener en cuenta la probabilidad de que sucedan cada uno de los problemas posibles. De esta forma se pueden priorizar los problemas y su coste potencial desarrollando un plan de acción adecuado.



Para cada riesgo, se debe determinar la probabilidad del factor de riesgo. Como ejemplo se mencionan algunos factores de riesgo:

a) Factor de riesgo bajo.
b) Factor de riesgo muy bajo.
c) Factor de riesgo medio.
d) Factor de riesgo alto.
e) Factor de riesgo muy alto.

5.1. Bienes susceptibles a daños.

Entre estos podemos identificar los siguientes bienes afectos a riesgos:

5.1.1. Instalaciones.

a) Robo.

Entrar a las instalaciones de la Dirección de informática, de parte de agentes externos con intenciones de robar recursos informáticos en forma parcial o total.

b) Incendio.

Incendio en el área del Data Center, UPS Y demás áreas del departamento de Informática.

c) Humo.

Expansión de humo de cualquier tipo.

d) Sismos o Terremoto.

Al producirse el sismo ocasiona daño en las instalaciones**.**

e) Interferencia en el suministro de energía.

Falta del suministro de energía eléctrica.

f) Inundación.

Inundación en la Dirección de Tecnología o áreas críticas de las instalaciones.

5.1.2. Personal.

a) Salud.

Enfermedad común o profesional imprevista en el personal.

b) Administración.

i. Ausencia del personal a sus labores.

ii. Traslado del personal.

iii. Renuncia de personal.

5.1.3. Hardware.

a) Fallos de Infraestructura.

i. Falla del servidor de base de datos.

ii. Falla del servidor de aplicaciones.

iii. Falla de los equipos de comunicación en la red.

iv. Falla de UPS central.

v. Falla del Servidor de Correo Electrónico.

vi. Falla en el servicio de internet.

vii. Falla en los equipos de seguridad (Firewall).

b) Fallas y Robo de Equipo.

i. Hurto o robo de equipos portátiles.

ii. Falla en equipo informático asignado.

5.1.4. Software.

Virus Informáticos.

i. Infección de virus en computadoras portátiles y desktops.

ii. Infección de virus en servidores de bases de datos, producción, de aplicaciones y otros servicios.

5.1.5. Datos e información.

a) Atentados.

i. Irrupción de usuarios extraños a la base de datos y/o aplicaciones.

ii. Divulgación de Información.

b) Pérdida de datos.

Pérdida o corrupción de la información.

5.1.6. Documentación.

Falta de documentación de los sistemas desarrollados, procesos y manuales de uso, y su documentación técnica necesaria.

5.1.7. Servicios.

a) Capacidad Instalada.

La demanda de atención a usuarios supera nuestra capacidad instalada**.**

b) Suministro de energía eléctrica.

c) Sistema de redes y comunicación.

La capacidad en ancho de banda no es suficiente, ni la topología de red cumple con las necesidades actuales.

d) Sistema aire acondicionado.

Falla en los sistemas de enfriamiento ambiental.

5.2. Cuadro de riesgos.

5.2.1. Instalaciones.

a) Robo.

Riesgo Identificado	Entrar a las instalaciones de la Dirección de informática, de parte de agentes externos con intenciones de robar recursos informáticos en forma parcial o total
Factores que originan el riesgo.	Fallas en la vigilancia y control de entrada y circulación en el edificio.
Descripción del Riesgo	Extracción de equipo, software o información propiedad del RNPN.
Posibles Consecuencias:	Retraso o interrupción en las funciones de las diferentes áreas del RNPN.
Nivel de impacto:	GRAVE
Probabilidad.	Poco Frecuente.
Factor de riesgo	Medio.

Acciones a ejecutar:

ACCION PREVENTIVA	RESPONSABLE	ACCION CORRECTIVA	RESPONSABLE	RECURSOS
Tener comunicación directa con las áreas de vigilancia del RNPN.	Personal de Seguridad	Contactar vía teléfono o personalmente , para el auxilio correspondiente	Director de la DAF, en ausencia de un jefe de seguridad	Teléfono. …..
Instalación de cámaras de vigilancia	DAF	Monitoreo del movimiento dentro de las instalaciones del RNPN.	Personal de seguridad	Cámaras. Monitoreo de las mismas.
TIEMPO FUERA (DOWNTIME) Expresado min, hrs, días:0 MINUTOS				

b) Incendio.

Riesgo Identificado	Incendio en el área del Data Center, UPS Y demás áreas del departamento de Informática
Factores que originan el riesgo.	Generalmente provocado por corto circuito
Descripción del Riesgo	Daños severos en los componentes tecnológicos de la plataforma instalada.
Posibles Consecuencias:	Retraso o interrupción en las funciones de las diferentes áreas del RNPN.
Nivel de impacto:	GRAVE
Probabilidad.	Poco Frecuente.
Factor de riesgo	Medio.

Acciones a ejecutar:

ACCION PREVENTIVA	RESPONSABLE	ACCION CORRECTIVA	RESPONSABLE	RECURSOS
Tener sensores de humo y sistemas contra incendios	Personal de soporte del Data Center, o en ausencia Director de TI	Contactar vía teléfono o personalmente , para el auxilio correspondiente	Director de la DAF, en ausencia de un jefe de seguridad	Teléfono. …..
Mantener contrato de soporte para los equipos de monitoreo	DAF	Monitoreo del movimiento dentro de las instalaciones del RNPN.	Personal de seguridad	
TIEMPO FUERA (DOWNTIME) Expresado min, hrs, días: 2 horas				

c) Humo.

Riesgo Identificado	Expansión de humo de cualquier tipo
Factores que originan el riesgo.	Escape de gas del sistema de enfriamiento, corto circuito en la red eléctrica o en componentes de TI
Descripción del Riesgo	Daños en la salud humana y en los equipos de TI.
Posibles Consecuencias:	Retraso o interrupción en las funciones de las diferentes áreas del RNPN.
Nivel de impacto:	MUY GRAVE
Probabilidad.	Frecuente.
Factor de riesgo	Alto.

Acciones a ejecutar:

ACCION PREVENTIVA	RESPONSABLE	ACCION CORRECTIVA	RESPONSABLE	RECURSOS
Tener definidas las rutas de escape. Contar con sitio de contingencia	Todo el personal de TI	Poner en operación Plan de contingencia	La Administración del RNPN y todo el personal técnico	
Mantener visible las recomendaciones en caso de terremoto	DAF	Seguir los planes estipulados para este evento	La Administración del RNPN y todo el personal técnico	
TIEMPO FUERA (DOWNTIME) Expresado min, hrs, días: 8 horas				

d) Sismos o Terremoto.

Riesgo Identificado	Desastre natural que daña edificaciones y puede hasta dejar inhabilitado un inmueble
Factores que originan el riesgo.	Desplazamiento de placas tectónicas
Descripción del Riesgo	Daños en la infraestructura de la obra civil.
Posibles Consecuencias:	Retraso o interrupción en las funciones de las diferentes áreas del RNPN.
Nivel de impacto:	GRAVE
Probabilidad.	Poco Frecuente.
Factor de riesgo	Medio.

Acciones a ejecutar:

ACCION PREVENTIVA	RESPONSABLE	ACCION CORRECTIVA	RESPONSABLE	RECURSOS
Tener sensores de humo. Contar con mascarillas anti-gas	Personal de soporte del Data Center, o en ausencia Director de TI	Contactar via teléfono o personalmente , para el auxilio correspondiente	Director de la DAF, en ausencia de un jefe de seguridad	Teléfono. …..
Mantener contrato de soporte para los equipos de monitoreo	DAF	Monitoreo de los sensores de humo dentro de las instalaciones del RNPN.	Personal de soporte del Data Center	
TIEMPO FUERA (DOWNTIME) Expresado min, hrs, días: 2 horas				

e) Interferencia en el suministro de energía.

Riesgo Identificado	Falta del suministro de energía eléctrica
Factores que originan el riesgo.	Corte del servicio por parte de compañía proveedora
Descripción del Riesgo	Daños en los sistemas informáticos.
Posibles Consecuencias:	Retraso o interrupción en las funciones de las diferentes áreas del RNPN.
Nivel de impacto:	MUY GRAVE
Probabilidad.	Frecuente.
Factor de riesgo	Alto.

Acciones a ejecutar:

ACCION PREVENTIVA	RESPONSABLE	ACCION CORRECTIVA	RESPONSABLE	RECURSOS
Tener sistema de alimentación eléctrica de emergencia (planta generadora y ups)	Personal de soporte del data Center o Director de TI	Poner en operación Plan de contingencia	La Administración del RNPN y todo el personal técnico	Planta generadora diesel y Ups's
Mantener contrato de planta generadora y Ups's	DAF	Seguir los planes estipulados para este evento	La Administración del RNPN y todo el personal técnico	
TIEMPO FUERA (DOWNTIME) Expresado min, hrs, días: 1-3 horas				

f) Inundación.

Riesgo Identificado	Inundación en la Dirección de Tecnología o áreas críticas de las instalaciones.
Factores que originan el riesgo.	Rotura en tuberías de aguas servidas, filtración de agua por el techo, obstrucción en el sistema de desagüe.
Descripción del Riesgo	Daños en los sistemas informáticos.
Posibles Consecuencias:	Retraso o interrupción en las funciones de las diferentes áreas del RNPN.
Nivel de impacto:	MUY GRAVE
Probabilidad.	Poco Frecuente.
Factor de riesgo	Alto.

Acciones a ejecutar:

ACCION PREVENTIVA	RESPONSABLE	ACCION CORRECTIVA	RESPONSABLE	RECURSOS
Dar mantenimiento a los servicios de agua servida y sistemas de desagüe	Personal de mantenimiento del RNPN	Reparación de las averías en ductería o techos	DAF	Herramientas y piezas de reparación
Dar mantenimiento contra filtraciones en los techos del Data Center	DAF	Reparar filtraciones en techos	DAF	Herramientas y piezas de reparación
TIEMPO FUERA (DOWNTIME) Expresado min, hrs, días: 4 horas				

5.2.2. Personal.

a) Salud.

Riesgo Identificados	Enfermedad común o profesional imprevista en el personal
Factores que originan el riesgo.	Enfermedades comunes o producidas por actividad laboral.
Descripción del Riesgo	Daños en la salud de los técnicos operadores y en especializados.
Posibles Consecuencias:	Recarga laboral en el resto de personal y posible retraso en la respuesta a solicitudes de servicio
Nivel de impacto:	DE LEVE A GRAVE
Probabilidad.	Muy Frecuente.
Factor de riesgo	Medio.

Acciones a ejecutar:

ACCION PREVENTIVA	RESPONSABLE	ACCION CORRECTIVA	RESPONSABLE	RECURSOS
Compartir los conocimientos técnicos con los compañeros de área	Personal técnico de cada Unidad Operativa	Mantener manuales técnicos actualizados	Dirección de Informática con sus Unidades Operativas	Manuales técnicos actualizados
Mantener listados de turnos para cubrir las ausencias críticas	Dirección de Informática	Hacer del conocimiento del cuerpo técnico	Dirección de Informática	Gestión administrativa
TIEMPO FUERA (DOWNTIME) Expresado min, hrs, días: 0-8 horas				

b) Administración.

Riesgo Identificados	Ausencia del personal a sus labores., Traslado del personal o Renuncia de personal
Factores que originan el riesgo.	Motivos personales o traslados internos
Descripción del Riesgo	Ausencia de personal crítico en los procesos.
Posibles Consecuencias:	Suspensión temporal de actividades específicas que pueden afectar el servicio.
Nivel de impacto:	DE LEVE A GRAVE
Probabilidad.	Frecuente.
Factor de riesgo	Medio.

Acciones a ejecutar:

ACCION PREVENTIVA	RESPONSABLE	ACCION CORRECTIVA	RESPONSABLE	RECURSOS
Compartir los conocimientos técnicos con los compañeros de área	Personal técnico de cada Unidad Operativa	Mantener manuales técnicos actualizados	Dirección de Informática con sus Unidades Operativas	Manuales técnicos actualizados
Mantener banco de aspirantes que cumplan con los perfiles técnicos	RRHH	Contratación de personal con carácter temporal o permanente	RRHH	Gestión Administrativa
TIEMPO FUERA (DOWNTIME) Expresado min, hrs, días: 0 horas				

5.2.3. Hardware.

a) Fallos de Infraestructura.

Riesgo Identificados	Falla del servidor de base de datos, Falla del servidor de aplicaciones, Falla de los equipos de comunicación en la red, Falla de UPS central, Falla del Servidor de Correo Electrónico, Falla en el servicio de internet, Falla en los equipos de seguridad (Firewall).
Factores que originan el riesgo.	Falta de mantenimiento preventivo, fallas eléctricas, defectos de fabricación
Descripción del Riesgo	Daños en equipo informático
Posibles Consecuencias:	Retraso o interrupción en las funciones de las diferentes áreas del RNPN.
Nivel de impacto:	DE LEVE A GRAVE
Probabilidad.	Frecuente.
Factor de riesgo	Alto.

Acciones a ejecutar:

ACCION PREVENTIVA	RESPONSABLE	ACCION CORRECTIVA	RESPONSABLE	RECURSOS
Mantener contratos de mantenimiento activos	Personal técnico de cada Unidad Operativa	Asistencia de personal técnico especializado	Dirección de Informática con sus Unidades Operativas	Gestión Administrativa
Mantener banco de proveedores de tecnología.	UACI	Adquisición de servicio técnico si fuere necesario	UACI DI	Gestión Administrativa
TIEMPO FUERA (DOWNTIME) Expresado min, hrs, días: 8 horas				

b) Fallas y Robo de Equipo.

Riesgo Identificados	Hurto o robo de equipos portátiles, Falla en equipo informático asignado
Factores que originan el riesgo.	Fallas en la seguridad y custodia de equipos informáticos.
Descripción del Riesgo	Daños y pérdidas de equipo informático
Posibles Consecuencias:	Retraso o interrupción en las funciones de las diferentes áreas del RNPN.
Nivel de impacto:	DE LEVE A GRAVE
Probabilidad.	Frecuente.
Factor de riesgo	Alto.

Acciones a ejecutar:

ACCION PREVENTIVA	RESPONSABLE	ACCION CORRECTIVA	RESPONSABLE	RECURSOS
Mantener pólizas de seguro para equipos de TI	DAF	Asistencia de personal técnico especializado	Dirección de Informática con sus Unidades Operativas	Gestión Administrativa
Mantener adecuado seguridad y custodia de equipo.	Personal al que se le asigne equipo portátil	Adquisición de servicio técnico si fuere necesario	UACI DI	Gestión Administrativa
TIEMPO FUERA (DOWNTIME) Expresado min, hrs, días: 0 horas				

5.2.4. Software.

Virus Informáticos.

Riesgo Identificados	Infección de virus en computadoras portátiles y desktops, Infección de virus en servidores de bases de datos, producción, de aplicaciones y otros servicios.
Factores que originan el riesgo.	Fallas de software antivirus o de actualización de versiones.
Descripción del Riesgo	Daños y pérdidas de información
Posibles Consecuencias:	Retraso o interrupción en las funciones de las diferentes áreas del RNPN.
Nivel de impacto:	GRAVE
Probabilidad.	Muy Frecuente.
Factor de riesgo	Alto.

Acciones a ejecutar:

ACCION PREVENTIVA	RESPONSABLE	ACCION CORRECTIVA	RESPONSABLE	RECURSOS
Mantener licencias e antivirus en toda la plataforma TI	DAF	Uso de copias de respaldo si fuere necesario	Dirección de Informática con sus Unidades Operativas	Copias de respaldo
Mantener actualizada las bases de firmas y versiones de antivirus	Todo el personal que utilice equipo informático	Adquisición de servicio técnico si fuere necesario	UACI DI	Licencias de antivirus vigentes
TIEMPO FUERA (DOWNTIME) Expresado min, hrs, días: 0 horas				

5.2.5. Datos e información.

a) Atentados.

Riesgo Identificados	Irrupción de usuarios extraños a la base de datos y/o aplicaciones. Divulgación de Información
Factores que originan el riesgo.	Fallas en los sistemas de seguridad TI.
Descripción del Riesgo	Daños y pérdidas de información
Posibles Consecuencias:	Retraso o interrupción en las funciones de las diferentes áreas del RNPN.
Nivel de impacto:	GRAVE
Probabilidad.	Muy Frecuente.
Factor de riesgo	Alto.

Acciones a ejecutar:

ACCION PREVENTIVA	RESPONSABLE	ACCION CORRECTIVA	RESPONSABLE	RECURSOS
Mantener revisión y monitoreo constante de los componentes de seguridad TI	Dirección de Informática con sus Unidades Operativas	Uso de copias de respaldo si fuere necesario	Dirección de Informática con sus Unidades Operativas	Copias de respaldo
Actualización tecnológica sobre la seguridad informática	Todo el personal técnico de la Dirección TI	Adquisición de tecnología en seguridad de TI.	UACI DI	Gestión Administrativa
TIEMPO FUERA (DOWNTIME) Expresado min, hrs, días: 0 horas				

b) Pérdida de datos.

Riesgo Identificados	Pérdida o corrupción de la información
Factores que originan el riesgo.	Fallas en los sistemas de seguridad TI o en la administración de las bases de datos.
Descripción del Riesgo	Daños y pérdidas de información
Posibles Consecuencias:	Retraso o interrupción en las funciones de las diferentes áreas del RNPN.
Nivel de impacto:	GRAVE
Probabilidad.	Poco Frecuente.
Factor de riesgo	Medio.

Acciones a ejecutar:

ACCION PREVENTIVA	RESPONSABLE	ACCION CORRECTIVA	RESPONSABLE	RECURSOS
Mantener revisión y monitoreo de la integridad de la data	Dirección de Informática con sus Unidades Operativas	Uso de copias de respaldo si fuere necesario	Dirección de Informática con sus Unidades Operativas	Copias de respaldo
Revisión análisis constante de las bases de datos	Unidad de Administración de Bases de Datos	Adquisición de tecnología (sw/hw) de TI que asegure la integridad.	UACI DI	Gestión Administrativa
TIEMPO FUERA (DOWNTIME) Expresado min, hrs, días: 4 horas				

5.2.6. Documentación.

Falta de documentación.

Riesgo Identificados	Falta de documentos de los sistemas desarrollados, procesos y manuales de uso, y su documentación técnica necesaria
Factores que originan el riesgo.	Omisión del proceso de documentación de los sistemas o fallas en el resguardo de dichos documentos.
Descripción del Riesgo	Ausencia de documentación necesaria para conocimiento y posterior asistencia técnica de los sistemas
Posibles Consecuencias:	Retraso o interrupción en las funciones de las diferentes áreas del RNPN.
Nivel de impacto:	LEVE
Probabilidad.	Poco Frecuente.
Factor de riesgo	Medio.

Acciones a ejecutar:

ACCION PREVENTIVA	RESPONSABLE	ACCION CORRECTIVA	RESPONSABLE	RECURSOS
Supervisar que todos los sistemas desarrollados interna o externamente sean documentados	Dirección de Informática con sus Unidades Operativas	Reponer cualquier documento que faltare de cualquier sistema	Dirección de Informática con sus Unidades Operativas	Personal técnico
TIEMPO FUERA (DOWNTIME) Expresado min, hrs, días: 0 horas				

5.2.7. Servicios.

a) Capacidad Instalada.

Riesgo Identificados	La demanda de atención a usuarios supera nuestra capacidad instalada
Factores que originan el riesgo.	La falta de planificación basada en los recursos actuales para la firma de convenios de prestación de servicios con otras instituciones. La falta de adquisición de nuevas tecnologías. El nivel de obsolescencia en los recursos centrales.
Descripción del Riesgo	Faltar a convenios por no contar con recursos suficientes.
Posibles Consecuencias:	Dejar fuera de servicio a usuarios por falta de recursos
Nivel de impacto:	GRAVE
Probabilidad.	Frecuente.
Factor de riesgo	Medio.

Acciones a ejecutar:

ACCION PREVENTIVA	RESPONSABLE	ACCION CORRECTIVA	RESPONSABLE	RECURSOS
Todo convenio con otras instituciones debe sujetarse a una donación de tecnología al RNPN para compensar la carga de tráfico en los sistemas	Dirección de Informática y Unidades encargadas de preparar convenios	Adquirir nuevas tecnologías en Hardware y Software de plataforma central	Dirección de Informática y DAF	Gestión Administrativa
TIEMPO FUERA (DOWNTIME) Expresado min, hrs, días: 0 horas				

b) Sistema de redes y comunicación.

Riesgo Identificados	La capacidad en ancho de banda no es suficiente, ni la topología de red cumple con las necesidades actuales.
Factores que originan el riesgo.	Las necesidades de servicio crecen de forma imprevista.
Descripción del Riesgo	Mala prestación de servicios.
Posibles Consecuencias:	Dejar fuera de línea a usuarios por Insuficiente ancho de banda
Nivel de impacto:	GRAVE
Probabilidad.	Frecuente.
Factor de riesgo	Medio.

Acciones a ejecutar:

ACCION PREVENTIVA	RESPONSABLE	ACCION CORRECTIVA	RESPONSABLE	RECURSOS
Revisar constantemente los roles y uso de los usuarios de los recursos de internet	Dirección de Informática y Unidad de Administración de Redes	Mantener anualmente un crecimiento de los anchos de banda de los enlaces	Dirección de Informática y DAF	Gestión Administrativa
TIEMPO FUERA (DOWNTIME) Expresado min, hrs, días: 0 horas				

c) Sistema aire acondicionado.

Riesgo Identificados	Falla en los sistemas de enfriamiento ambiental.
Factores que originan el riesgo.	El uso permanente de los equipos
Descripción del Riesgo	Sobre calentamiento de los equipos
Posibles Consecuencias:	Retraso o interrupción en las funciones de las diferentes áreas del RNPN.
Nivel de impacto:	GRAVE
Probabilidad.	Poco Frecuente.
Factor de riesgo	Bajo.

Acciones a ejecutar:

ACCION PREVENTIVA	RESPONSABLE	ACCION CORRECTIVA	RESPONSABLE	RECURSOS
Contar con sistema de enfriamiento de contingencia	Dirección de Informática y soporte técnico de Data Center	Mantener contrato de mantenimiento preventivo de los equipos de aire acondicionado	Dirección de Informática y DAF	Gestión Administrativa
TIEMPO FUERA (DOWNTIME) Expresado min, hrs, días: 0 horas				

5.3. Daños.

Los posibles daños pueden referirse a:

a) Imposibilidad de acceso a los recursos debido a problemas físicos en las instalaciones donde se encuentran los bienes, sea por causas naturales o humanas.

b) Imposibilidad de acceso a los recursos informáticos por razones lógicas en los sistemas en utilización, sean estos por cambios involuntarios o Intencionales, llámese por ejemplo, cambios de claves de acceso, datos maestros claves, eliminación o borrado físico/lógico de información clave, proceso de información no deseado.

c) Divulgación de información a instancias fuera de la institución y que afecte su patrimonio estratégico Institucional, sea mediante Robo, hurto o Infidencia.

d) Por factores exógenos como desastres causados por un evento natural o humano, que pueden ocurrir, en cualquier parte, hora y actividad.

5.4. Riesgos.

Al referirnos a riesgos determinamos que es la posibilidad de que suceda algo que tendrá un impacto sobre los objetivos. Se lo mide en términos de consecuencias y probabilidades.
Entre esto podemos mencionar:

a) Riesgos Naturales: tales como mal tiempo, terremotos, erupción volcánica, etc.

b) Riesgos Tecnológicos: tales como incendios eléctricos, fallas de energía y accidentes de transmisión, transporte, ataque de virus, etc.

c) Riesgos Sociales: como actos terroristas y desordenes.

5.5. Prioridades.

La estimación de los daños en los bienes y su impacto, fija una prioridad en relación a la cantidad del tiempo y los recursos necesarios para la reposición de los Servicios que se pierden en el evento.

Por lo tanto, los bienes de más alta prioridad serán los primeros a considerarse en el procedimiento de recuperación ante un evento de desastre.

Considerando los sistemas prioritarios:

a) Bases de datos.
b) La red de comunicaciones.
c) Los sistemas de procesamiento.
d) Los sistemas de alimentación eléctrica.
e) Los sistemas de acondicionamiento de ambiente.

5.6. Origen de daños.

Las posibles fuentes de daño que pueden causar la no operación normal de la institución asociadas al área de tecnología son:

a) Acceso no autorizado.

Por vulneración de los sistemas de seguridad en operación (Ingreso no autorizado a las instalaciones).

b) Ruptura de las claves de acceso a los sistemas informáticos.

i. Instalación de software de comportamiento errático y/o dañino para la operación de los sistemas informáticos en uso (Virus, sabotaje).
ii. Intromisión no calificada a procesos y/o datos de los sistemas, ya sea por curiosidad o malas intenciones.

c) Desastres naturales.

i. Movimientos telúricos que afecten directa o indirectamente a las instalaciones físicas de soporte (edificios) y/o de operación (equipos informáticos).
ii. Inundaciones causadas por falla en los suministros de agua.
iii. Filtraciones de agua en los techos.

iv. Obstrucción en los sistemas de desagüe de aguas lluvias y servidas.

v. Incendios de cualquier origen.

vi. Fallas en los equipos de soporte:

a) Por fallas causadas por la agresividad del ambiente.

b) Por fallas de la red de energía eléctrica pública por diferentes razones ajenas al manejo por parte del RNPN.

c) Por fallas de los equipos de enfriamiento ambiental necesarios para una adecuada operación de los equipos computacionales más sensibles.

d) Por fallas de la comunicación.

e) Por fallas en el tendido físico de la red local.

f) Por fallas en el tendido físico de la red de alimentación eléctrica local y de emergencia.

d) Fallas de personal clave.

i. Se considera personal clave aquel que cumple una función vital en el flujo de procesamiento de datos u operación de los Sistemas de Información:

a) Personal de Informática.

b) Gerencia de la TIC.

c) Administración de Bases de Datos.

d) Administración de redes.

e) Encargados de Infraestructura

ii. Pudiendo existir los siguientes inconvenientes:

a) Enfermedad.

b) Accidentes.

c) Renuncias.

d) Abandono de sus puestos de trabajo.

e) Huelgas.

e) Fallas de hardware.

i. Falla en el Servidor de Aplicaciones y Datos, tanto en su(s) disco(s) duro(s) como en el procesador central.

ii. Falla en el hardware de Red:

a) Falla en los Switches.

b) Falla en el cableado de la Red.

iii. Falla en el Router.

iv. Falla en el FireWall.

v. Falla en los dispositivos de almacenamiento.

5.7. Revisión anual de daños.

Para evitar las pérdidas de información, se deben tomar las medidas precautorias necesarias para que el tiempo de recuperación y puesta en marcha sea menor o igual al necesario para la reposición del equipamiento que lo soporta.

5.8. Medidas preventivas.

5.8.1 Control de accesos.

a) Acceso físico de personas autorizadas y no autorizadas a las áreas definidas como restringidas

i. Personal autorizado:

Todos los accesos del personal deben ser autorizados por Presidencia o por quien delegue.

ii. Personal no autorizado:

El acceso de carácter temporal a personal no autorizado de origen interno o externo, deberá ser regido por la normativa de Protocolo de Seguridad para acceso al Centro de Datos (Anexo 1).

b) Acceso a la Red de PC's y Servidores.

c) Acceso restringido a las librerías, programas, y datos.

d) Acceso a los controles centrales del sistema eléctrico.

5.9. Previsión de desastres.

El propósito es minimizar los riesgos innecesarios dentro del Centro de Datos por medio de las siguientes acciones:

Asegurar todos los objetos susceptibles a movimientos telúricos, para evitar que una caída o destrucción genere una interrupción de los procesos informáticos.

Tener en claro los lugares de resguardo de respaldos de bases de datos y sistemas.

El lugar donde se encuentran los archivos físicos, discos duros externos, cintas magnéticas que guarden respaldos y estén aún en las instalaciones de la institución.

Tener en claro las rutas de evacuación.

En caso de incendio los extinguidores deben estar a la mano y bajo mantenimiento; debe haber personal (capacitado) encargado del uso de extinguidores y estar presente de forma inmediata.

a) Soporte de utilitarios y periféricos.

Revisión periódica de plantas eléctricas.

Revisión periódica de Ups's.

Mantenimiento preventivo de: servidores, equipos de almacenamiento, switches, Routers, Access Point, controles de acceso, cámaras, y demás periféricos de seguridad perimetral.

b) Seguridad física del personal.

Evitar derrame de líquidos sobre el piso o evacuarlo inmediatamente para evitar resbalar, lo que podría provocar serias consecuencias al personal

Se debe capacitar al personal sobre las acciones a seguir en caso de siniestros según su naturaleza.

Dentro de cada área el personal debe compartir conocimiento en lo referente a la utilización de software y elementos de soporte relevante

Las causas más representativas que originarían cada uno de los escenarios propuestos en el Plan de Contingencias y Seguridad de la Información se presentan en el siguiente cuadro.

CAUSAS	ESCENARIOS
Fallas Corte de Cable UTP Fallas Tarjeta de Red Fallas IP asignado Fallas Punto de Switch Fallas Punto Patch Panel Fallas Punto de Red	I. NO HAY COMUNICACIÓN ENTRE CLIENTE SERVIDOR EN UNO O VARIOS TERMINALES DEL RNPN.
Fallas de Componentes de Hardware del servidor. Virus. Sobrepasar el límite de almacenamiento del Disco Computador de Escritorio funciona como servidor.	II. FALLA DE UN SERVIDOR
Accidente Renuncia Intempestiva	III. AUSENCIA PARCIAL O PERMANENTE DEL PERSONAL DE LA UNIDAD DE SISTEMAS.
Corte General del Fluido eléctrico	IV. INTERRUPCIÓN DEL FLUIDO ELÉCTRICO DURANTE LA EJECUCIÓN DE LOS PROCESOS.
Falla de equipos de comunicación: SWITCH, routers, Fibra Óptica, puertos, etc. Fallas en el software de Acceso a Internet. Perdida de comunicación con proveedores de Internet	V. PERDIDA DE SERVICIOS DE INTERNET

CAUSAS	ESCENARIOS
Incendio Sabotaje Corto Circuito Terremoto Erupción Volcánica	VI. INDISPONIBILIDAD DE LA UNIDAD DE SISTEMAS (DESTRUCCIÓN DEL DATA CENTER)

6) PLAN DE RECUPERACION.

6.1. Objetivos del plan de recuperación.

Los objetivos del plan de Recuperación son:

1) Determinación de las políticas y procedimientos para respaldar las aplicaciones y datos.

2) Planificar la reactivación dentro de las 08 horas de producido un desastre, todo el sistema de procesamiento y sus funciones asociadas.

3) Permanente mantenimiento y supervisión de los sistemas y aplicaciones.

4) Establecimiento de una disciplina de acciones a realizar para garantizar una rápida y oportuna respuesta frente a un desastre.

Cuando ocurra una contingencia, es esencial que se conozca al detalle el motivo que la originó y el daño producido, lo que permitirá recuperar en el menor tiempo posible el proceso perdido.

Los procedimientos deberán ser de ejecución obligatoria y bajo la responsabilidad de los encargados de la realización de los mismos, debiendo haber procesos de verificación de su cumplimiento. En estos procedimientos estarán involucrados específicamente los técnicos y especialistas del área.

Las actividades a realizar en un Plan de Recuperación se pueden clasificar en tres etapas:

- Actividades Previas a la falla o desastre.
- Actividades Durante la falla o Desastre.
- Actividades Después de la falla o Desastre.

6.2. Actividades previas al desastre.

Son todas las actividades de planeación, preparación, entrenamiento y ejecución de las actividades de resguardo de los activos de la Dirección de Informática, que nos aseguren un proceso de recuperación con el menor costo posible para el RNPN.

6.3. Actividades durante el desastre.

Una vez presentada la Contingencia, Falla o Siniestro, se deberá ejecutar las siguientes actividades, planificadas previamente:

- Plan de Emergencias.
- Entrenamiento.

6.3.1. Plan de emergencias.

En este plan se establecen las acciones se deben realizar cuando se presente un Siniestro, así como la difusión de las mismas.

Es conveniente prever los posibles escenarios de ocurrencia del Siniestro:

- Durante el día.
- Durante la Noche o madrugada.

6.3.2. Entrenamiento.

Establecer un programa de prácticas periódicas de todo el personal en la lucha contra los diferentes tipos de siniestros, de acuerdo a los roles que se le hayan asignado a cada técnico o especialista.

La responsabilidad sobre el Plan de Recuperación es de la Administración, la cual debe considerar la combinación de todo su personal, equipos, datos, sistemas, comunicaciones y suministro.

6.3.4. Actividad después del desastre o falla.

Después de ocurrido la contingencia, falla, Siniestro o Desastre es necesario realizar las actividades que se detallan, las cuales deben estar especificadas en el Plan de Acción:

- Evaluación de Daños.
- Ejecución de Actividades.
- Evaluación de Resultados.
- Retroalimentación del Plan de Acción.

a) Evaluación de daños.

Inmediatamente después que la contingencia, falla, siniestro o desastre ha concluido, se deberá evaluar la magnitud del daño que se ha producido, que equipos han quedado no operativos, cuales se pueden recuperar, y en cuanto tiempo, etc.

b) Ejecución de actividades.

Los trabajos de recuperación tendrán dos etapas, la primera la restauración del servicio usando los recursos de la Institución o local de respaldo, y la segunda etapa es con el apoyo de la proveedores de servicios de conectividad, en el caso de fallas del servicio de Internet y otros.

c) Evaluación de resultados.

Una vez concluidas las labores de Recuperación del equipo que fue afectado, se debe de evaluar objetivamente, todas las actividades realizadas, que tan bien se hicieron, que tiempo tomaron, que circunstancias modificaron (aceleraron o entorpecieron) las actividades del plan de acción, como se comportaron los equipos de trabajo, etc.

De la evaluación de resultados, se debe realizar dos tipos de recomendaciones, una que es la retroalimentación del plan de Contingencias y otra una lista de recomendaciones para minimizar los riesgos y pérdida que ocasionaron el siniestro o la falla.

7. PLANES.

	EMERGENCIA	RESTAURACION	RECUPERACION
OBJETIVO	Limitar el daño	Continuar Procesos Vitales	Recuperar proceso total
ACTUACION	Inmediata	A corto plazo	A medio plazo
CONTENIDO	1 Evacuación 2 Valoración de daños 3 Arranque de acciones	Alternativas para los procesos vitales	Estrategias para la recuperación de todos los recursos
RESPONSABILIDAD PRINCIPAL	Institución	Usuarios	Unidad de Sistemas

7.1. Elementos esenciales de los planes.

Documentación.

- Recursos.
- Pruebas.
- Seguros.

a) Recursos.

i. Contar con lugar alternativo de trabajo.
ii. Ordenadores con "hardware" y "software" apropiados.
iii. Computadoras de escritorio y portátiles.
iv. Copias de seguridad actualizadas.

b) Pruebas.

i. Validez de las copias de seguridad.
ii. Formación y reciclaje del personal.

c) Seguros.

Asegurar con póliza de seguro los equipos informáticos.

7.2. Objetivos.

1. Definir las actividades de planeamiento, preparación, entrenamiento y ejecución de tareas destinadas a proteger la información contra los daños y perjuicios producidos por corte de servicios, fenómenos naturales o humanos.
2. Establecer un plan de recuperación, formación de equipos y entrenamiento para restablecer la operatividad del sistema en el menor tiempo posible.
3. Establecer actividades que permitan evaluar los resultados y retroalimentación del plan general.

7.3. Plan de Respaldos.

Los respaldos de las bases de datos del sistema DUI se generan de la siguiente forma:

Un respaldo completo al cierre de producción del último día de labor semanal por medio de cintas magnéticas para LTO 5. El día lunes estas cintas se depositan en caja de seguridad en Banco.

Se genera un respaldo incremental de la producción diaria al final del cierre de producción.

Generar imágenes de los sistemas y resguardarlos en discos extraíbles. Se deben generar estas imágenes cada vez que los sistemas tengas modificaciones e identificarlas por versiones.

Recursos del plan de respaldo.

1 unidad de LTO 5.

3 Discos Sata o Sas extraíbles de 3 Tb c/u.

1 Data Protection recovery.

Plan de Contingencia: Son procedimientos que definen cómo una Institución continuará o recuperará sus funciones críticas en caso de una interrupción no planeada.

Los sistemas de TI son vulnerables a diversas interrupciones.

a) **Leves**: Caídas de energía de corta duración, fallas en disco duro, etc.

b) **Severa**: Destrucción de equipos, incendios, etc.

Asegura que se dé una interrupción mínima a los procesos de atención al usuario en caso de una interrupción significativa de los servicios que normalmente soportan esos procesos.

8) DISEÑO DE ESTRATEGIA DE CONTINUIDAD DE LOS PROCESOS Y SERVICIOS QUE BRINDA EL RNPN.

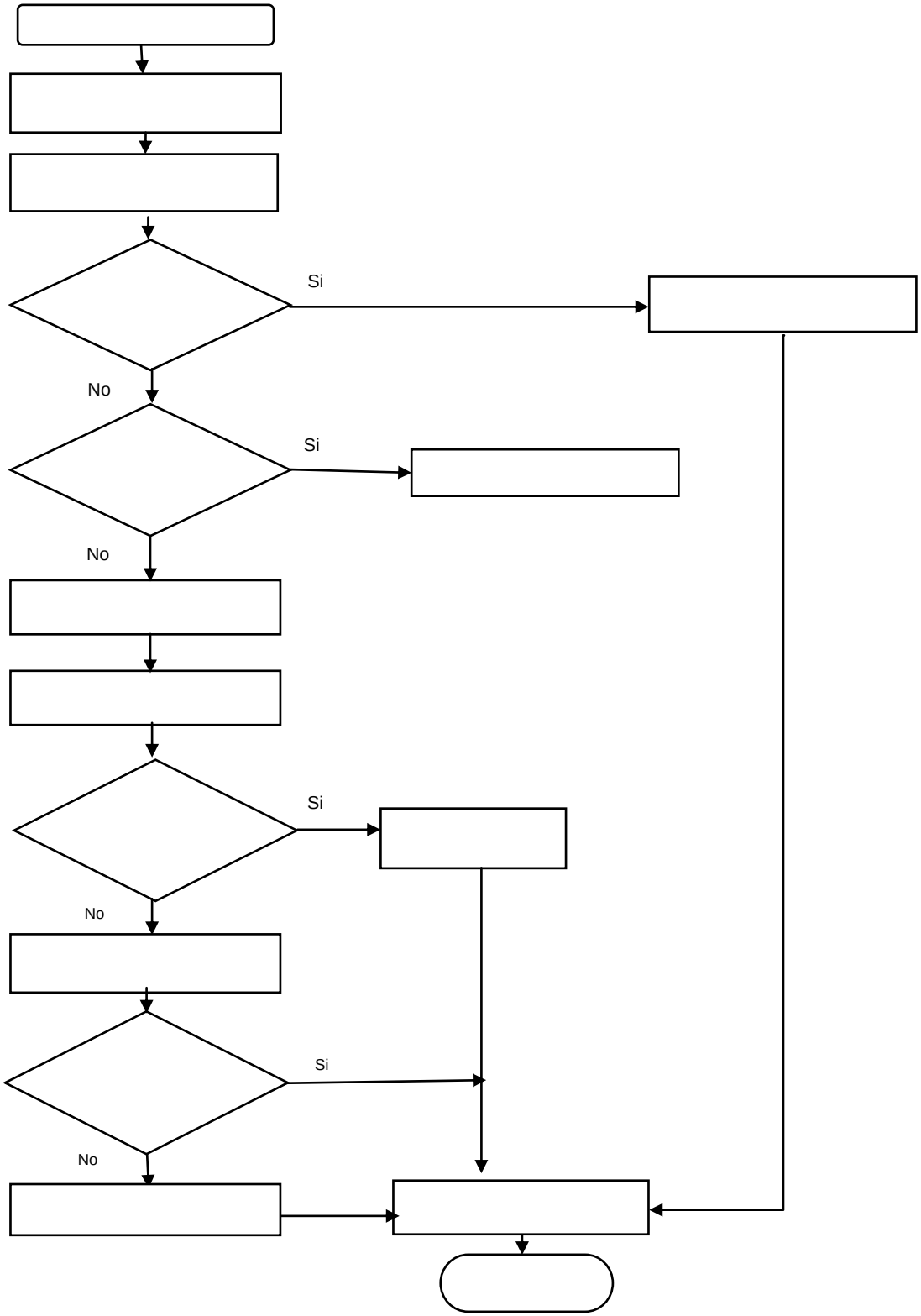
Escenario I. No hay comunicación entre los sistemas (servidores del RNPN) y usuarios.

Impacto.

Impacto Área Afectada	
No se puede trabajar con los recursos de la red del RNPN (Información).	Área en que labora
Interrupción de sus actividades	Área en que labora
Recurso	**Prioridad de recuperación**
Sistemas: Registro, emisión y Entrega del DUI Sistemas de Procesamiento de Partidas. Sistemas de Consulta de DUI y partidas	**ALTO**
Servidores: Controlador de Dominio Primarios Base de Datos Web Aplicaciones	**ALTO**
Servidor correo y sistema documental	**ALTO**
Servidor Internet	**ALTO**

Recursos de la Contingencia y Componentes de Reemplazo: Tarjeta de Red, Conector RJ-45, Jack RJ-45, cable utp, etc. Testers de continuidad comunicación de red y de electricidad, Kit de herramientas de Cableado estructurado, kit de limpieza de equipos, etc.

Procedimiento: No hay comunicación entre los sistemas (servidores del RNPN) y usuarios.



Escenario II. Falla de un servidor.

Impacto.

Impacto Área Afectada	
Suspensión de los sistemas o aplicaciones que se encuentran en los servidores que presentan fallas	Todas las Áreas
Posible Pérdida de Hardware y software	Unidad de Sistemas
Perdida del proceso automático de respaldo y recuperación	Unidad de Sistemas
Recurso	**Prioridad de recuperación**
Servidores: Controlador de Dominio Primarios Base de Datos Web Aplicaciones	**ALTO**
Servidor sistema documental, y de correo	**ALTO**
Servidor de internet	**ALTO**

Detalle de algunas de las causas de la Falla del Servidor.

CASO A: Error Físico de Disco de un Servidor (Sin RAID). Dado el caso crítico de que el disco presenta fallas, tales que no pueden ser reparadas, se debe tomar las acciones siguientes:

1. Ubicar el disco que esté dando falla.

2. Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a jefes de área.

3. Deshabilitar la entrada al sistema para que el usuario no reintente su ingreso.

4. Bajar el sistema y apagar el equipo.

5. Retirar el disco malo y reponerlo con otro del mismo tipo, formatearlo y darle partición. 6. Restaurar el último backup en el disco, seguidamente restaurar las modificaciones efectuadas desde esa fecha a la actualidad.

7. Revisar los sistemas que se encuentran en dicho disco y verificar su buen estado.

8. Habilitar las entradas al sistema para los usuarios.

CASO B: Error de Memoria RAM.

En este caso se pueden dar los siguientes síntomas:

1. El servidor no responde correctamente, por lentitud de proceso o por no rendir ante el ingreso masivo de usuarios.

2. Ante procesos mayores se congela el proceso.

3. Arroja errores con mapas de direcciones hexadecimales.

4. Es recomendable que el servidor cuente con ECC (error correctchecking), por lo tanto si hubiese un error de paridad, el servidor se autocorregirá. Todo cambio interno a realizarse en el servidor será fuera de horario de trabajo fijado por la Institución, a menos que la dificultad apremie, cambiarlo inmediatamente.

Se debe tomar en cuenta que ningún proceso debe quedar cortado, y se deben tomar las acciones siguientes:

a) Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a jefes de área.

b) El servidor debe estar apagado, dando un correcto apagado del sistema.

c) Ubicar las memorias malogradas.

d) Retirar las memorias malogradas y reemplazarlas por otras iguales o similares.

e) Realizar pruebas locales, deshabilitar las entradas, luego conectar el cable, habilitar entradas para estaciones en las cuales se realizarán las pruebas.

f) Probar los sistemas que están en red en diferentes estaciones.

g) Finalmente luego de los resultados, habilitar las entradas al sistema para los usuarios.

CASO C: Error de Tarjeta(s) Controladora(s) de Disco.

Se debe tomar en cuenta que ningún proceso debe quedar cortado, debiéndose ejecutar las siguientes acciones:

1. Avisar a los usuarios que deben salir del sistema, utilizar mensajes por red y teléfono a jefes de área.

2. El servidor debe estar apagado, dando un correcto apagado del sistema.

3. Ubicar la posición de la tarjeta controladora.

4. Retirar la tarjeta con sospecha de deterioro y tener a la mano otra igual o similar.

5. Retirar la conexión del servidor con el concentrador, ésta se ubica detrás del servidor, ello evitará que al encender el sistema, los usuarios ingresen.

6. Realizar pruebas locales, deshabilitar las entradas, luego conectar el cable hacia el concentrador, habilitar entradas para estaciones en las cuales se realizarán las pruebas.

7. Al final de las pruebas, luego de los resultados de una buena lectura de información, habilitar las entradas al sistema para los usuarios.

CASO D: Error Lógico de Datos.

La ocurrencia de errores en los sectores del disco duro del servidor puede deberse a una de las siguientes causas:

• Caída del servidor de archivos por falla de software de red.

• Falla en el suministro de energía eléctrica por mal funcionamiento del UPS.

• Bajar incorrectamente el servidor de archivos.

• Fallas causadas usualmente por un error de chequeo de inconsistencia física.

En caso de producirse alguna de las situaciones descritas anteriormente; se deben realizar las siguientes acciones:

1. Verificar el suministro de energía eléctrica. En caso de estar conforme, proceder con el encendido del servidor de archivos.

2. Deshabilitar el ingreso de usuarios al sistema.

3. Descargar todos los volúmenes del servidor, a excepción del volumen raíz. De encontrarse este volumen con problemas, se deberá descargarlo también.

4. Cargar un utilitario que nos permita verificar en forma global el contenido del(os) disco(s) duro(s) del servidor.

5. Al término de la operación de reparación se procederá a habilitar entradas a estaciones para manejo de soporte técnico, se procederá a revisar que las bases de datos índices estén correctas, para ello se debe empezar a correr los sistemas y así poder determinar si el usuario puede hacer uso de ellos inmediatamente.

Si se presenta el caso de una o varias bases de datos no reconocidas como tal, se debe recuperar con utilitarios.

CASO E: Caso de Virus.

Dado el caso crítico de que se presente virus en las computadoras se procederá a lo siguiente:

1. Se contará con antivirus para el sistema que aíslan el virus que ingresa al sistema llevándolo a un directorio para su futura investigación.

2. El antivirus muestra el nombre del archivo infectado y quién lo usó.

3. Estos archivos (exe, com, etc.) serán reemplazados del CD/DVD original de instalación o del backup.

4. Si los archivos infectados son aislados y aún persiste el mensaje de que existe virus en el sistema, lo más probable es que una de las estaciones es la que causó la infección, debiendo retirarla del ingreso al sistema y proceder a su revisión y desinfección.

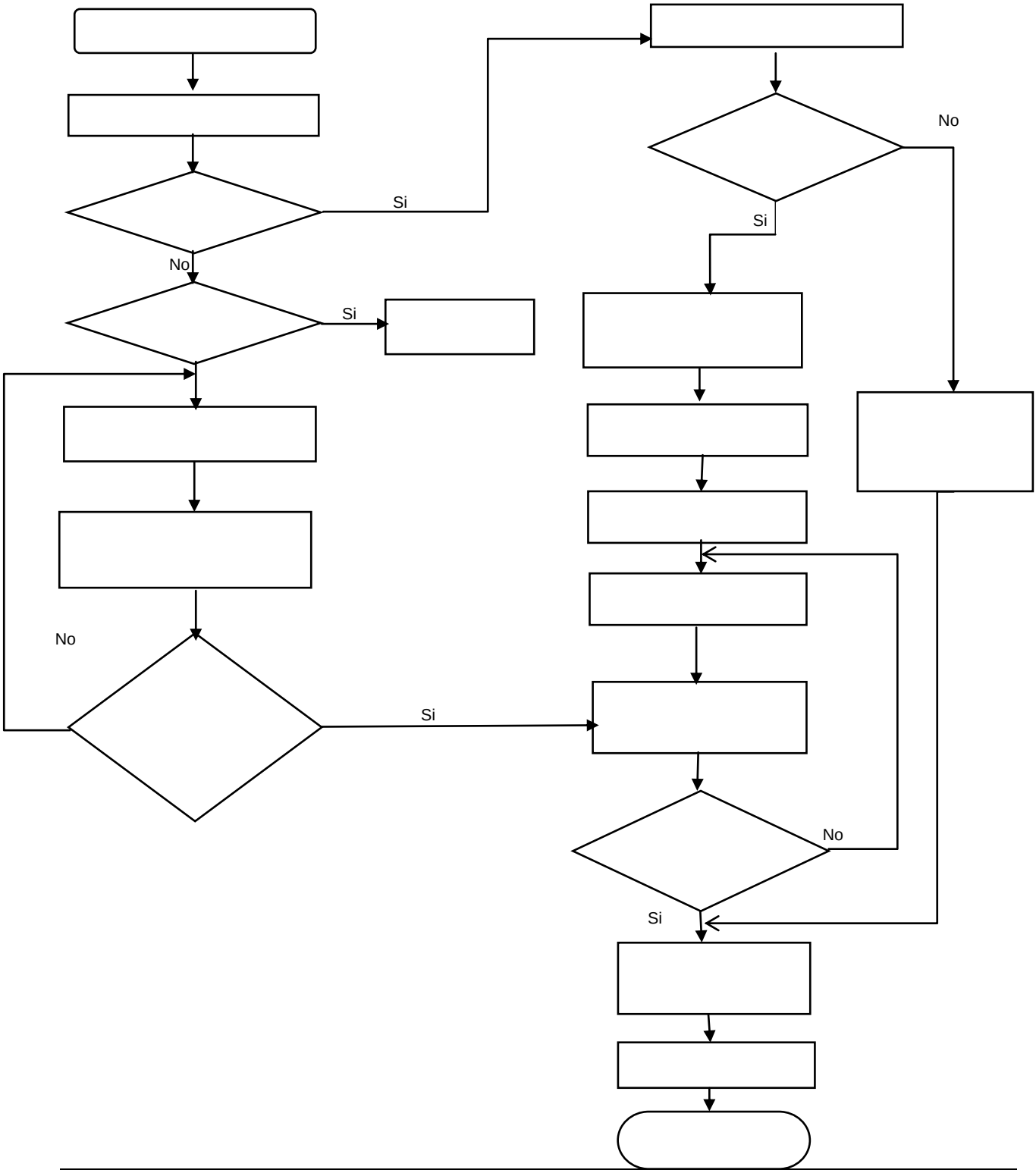
Recursos de Contingencia.

Componente de Remplazo (Memoria, Disco Duro, etc.).

Backup diario de Ia Información de los servidores, para recuperarla en otro equipo.

Procedimiento:

Falla de un servidor crítico



Escenario III. Ausencia parcial o permanente del personal de la Unidad de Sistemas.

Impacto.

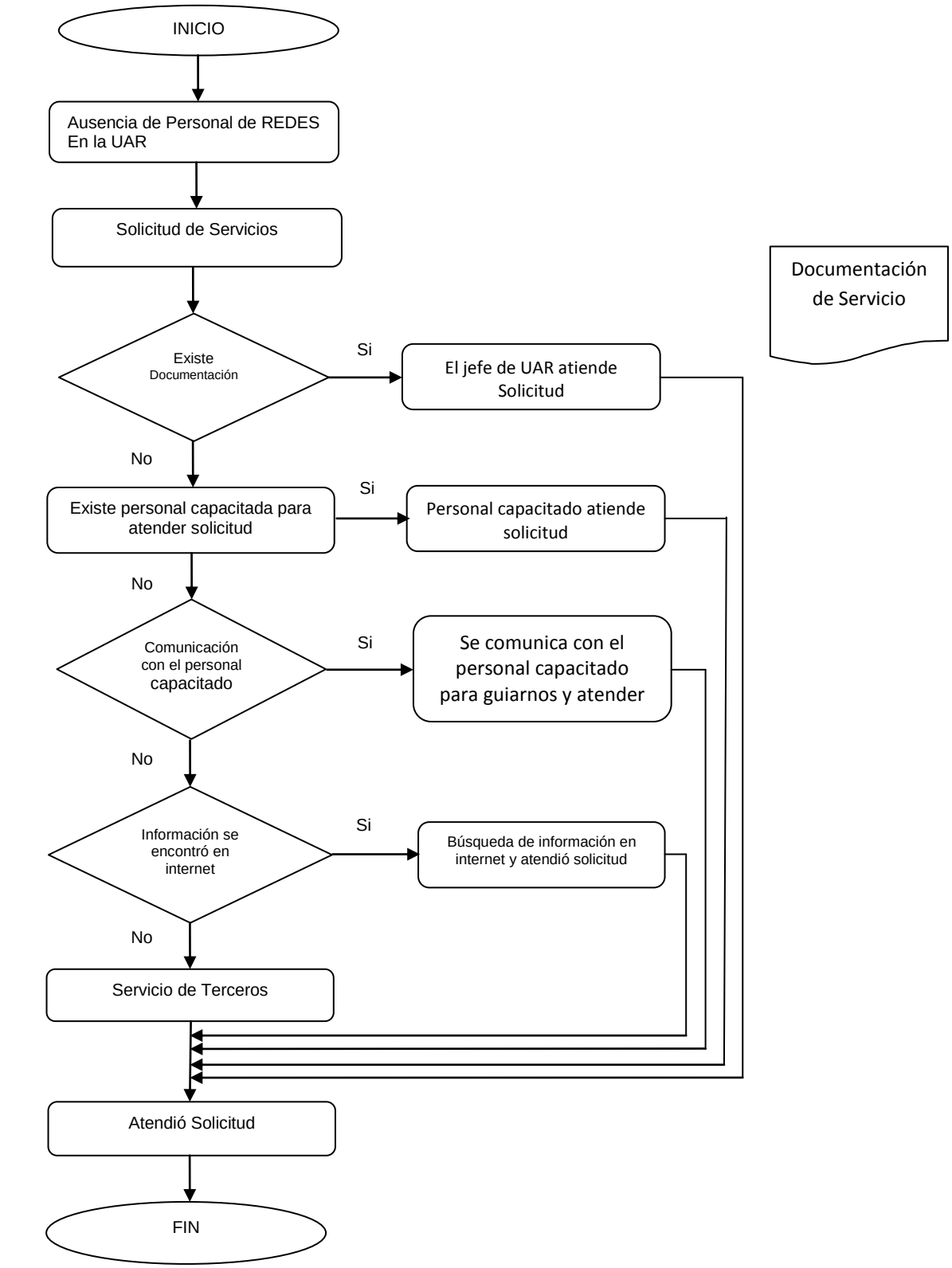
Impacto Área Afectada	
Interrupción de funciones de la persona ausente	Todas las Áreas
Administración de bases de datos Control y monitoreo de servidores. Soporte a los usuarios. Ajustes a programas críticos en producción	Todas las Áreas

Recursos de Contingencia.

Los perfiles de los técnicos de cada área.

Procedimiento.

Ausencia parcial o permanente del personal de la Unidad de Sistemas.



Escenario IV. Interrupción del fluido eléctrico durante la ejecución de los procesos.

Impacto.

Impacto Área Afectada	
Cierre inapropiado de las Bases de Datos	Todas las áreas
Finalización incompleta de los Backup T	Todas las áreas
Falla de un componente de equipo servidor	Todas las áreas
Pérdida total o parcial de la operatividad de los sistemas	Todas las áreas

Normalmente, ante una suspensión del servicio de alimentación eléctrica, los Ups's sostienen la alimentación eléctrica a los sistemas de forma emergente, si el corte dura más de 1 minuto, entra en operación la planta generadora de emergencia con un tolerancia de 19 horas continuas, pero ante una falla de la planta eléctrica se puede dar lo siguiente:

1. Si fuera corto circuito o una interrupción de hasta 20 minutos, el UPS mantendrá activo los servidores, mientras se evalúa y repara la avería eléctrica.
2. Para el caso de apagón se mantendrá la autonomía de corriente que el UPS nos brinda (corriente de emergencia), hasta que los usuarios completen sus operaciones (para que no corten bruscamente el proceso que tienen en el momento del apagón); posteriormente se apagará manualmente los servidores y UPS.
3. Cuando el fluido eléctrico de servicio se ha restablecido se procederá a encender de forma manual el UPS y servidores.

Llámese corriente de emergencia a la brindada por planta generadora y UPS.

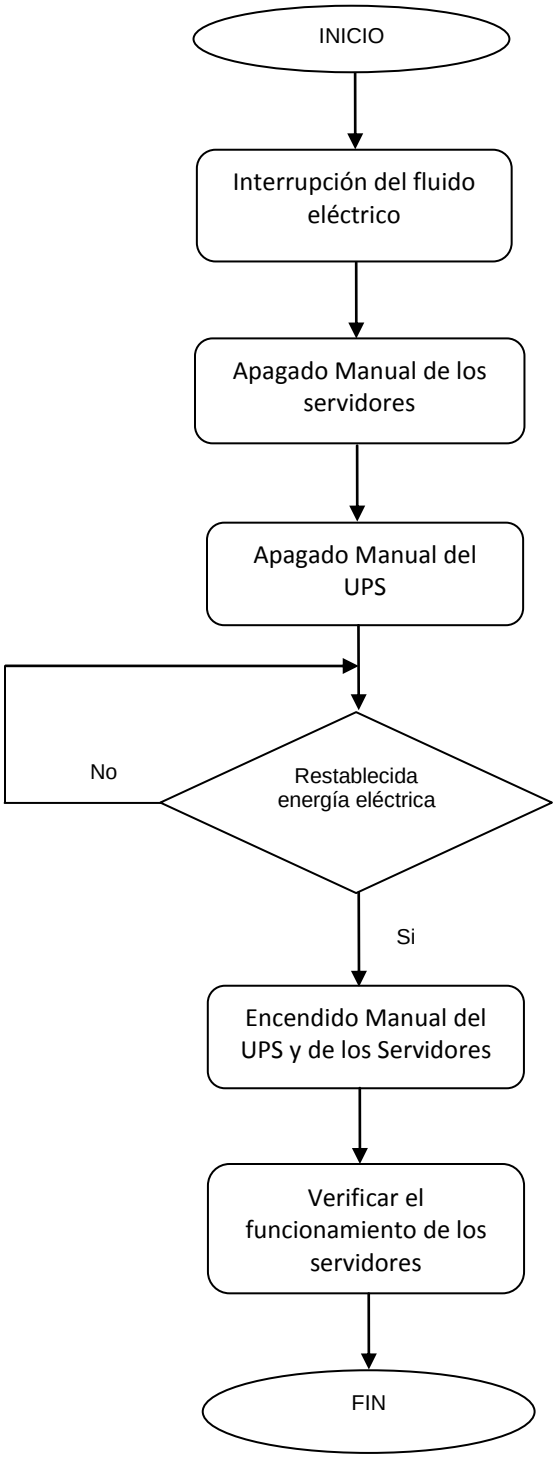
Llámese corriente normal a la brindada por la compañía eléctrica.

Recursos de Contingencia.

Si se produjera en horas no laborables una interrupción del fluido eléctrico, se podrían paralizar los procesos de cierre y backup de los servidores con motores de base de datos, por tal motivo es necesario revisar continuamente el estado de las baterías del UPS y planta generadora de emergencia; el personal de seguridad del RNPN avisar al personal de Informática que se ha producido un corte de energía. El UPS se caracteriza por emitir una alarma fácil de identificar.

Procedimiento.

Interrupción de fluido eléctrico.



Escenario V. Pérdida de servicios de internet.

Impacto.

Impacto	**Área Afectada**
Interrupción de la recepción y envío de información, mensajes y datos a nivel nacional e internacional.	Todas las áreas

Recursos de Contingencia.

Hardware.

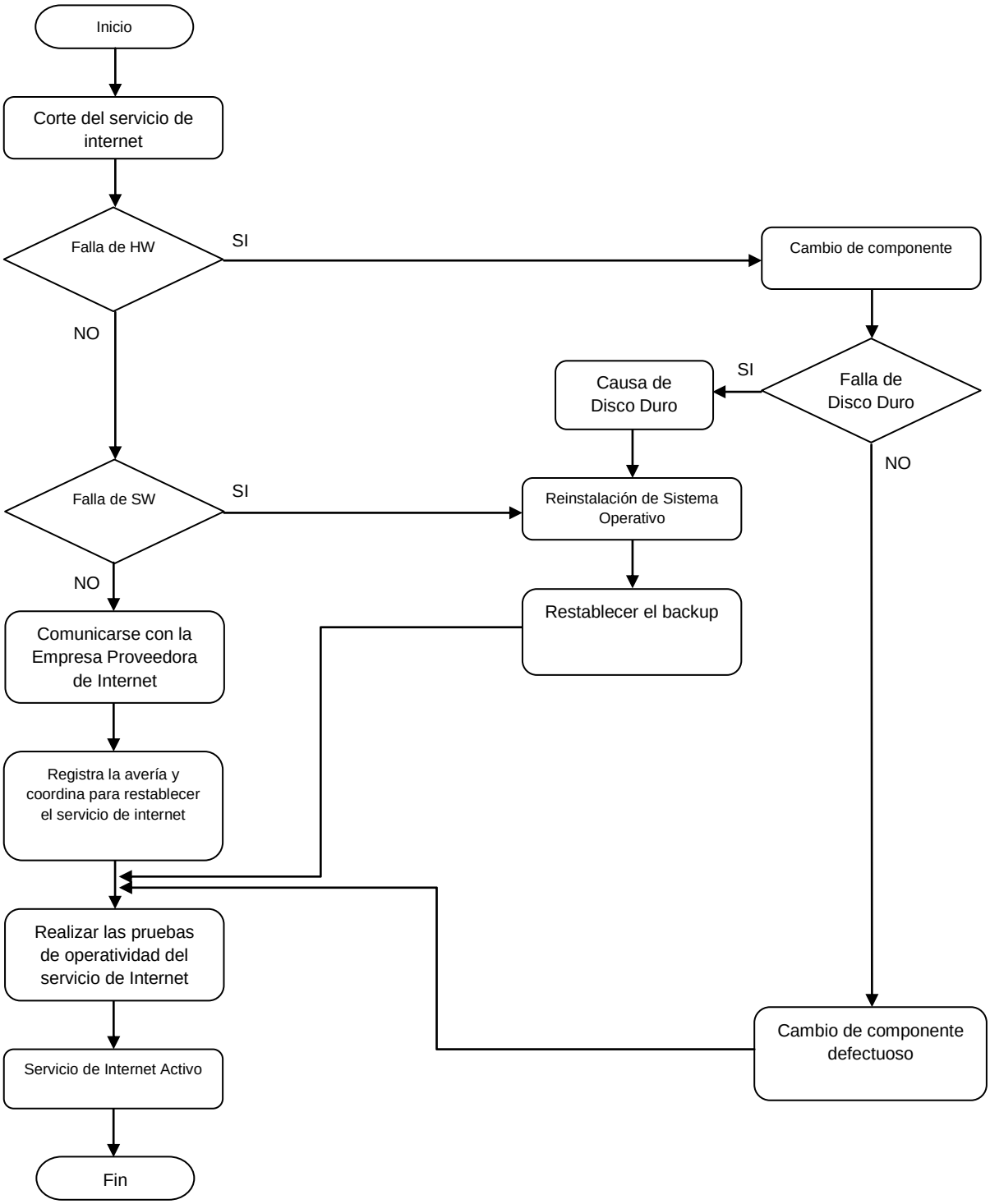
1 entrada LAN.

Software Herramientas de Internet.

Backup de las reglas del servidor Firewall.

Procedimiento:

Perdida de servicios de internet.



Escenario VI. Indisponibilidad de la Unidad de Sistemas (destrucción del área de servidores).

Impacto.

Impacto Área Afectada	
Caída de la Red LAN: Servidores Windows y Linux, equipos de comunicación	Todas las Áreas
Interrupción de las comunicaciones Internas y Externas	Todas las Áreas
Paralización de los equipos que soportan los sistemas de la Institución	Todas las Áreas
Paralización de operaciones de Informática	Todas las Áreas
Perdida de Hardware y Software	Tecnología de la Información

IDENTIFICAR IMPACTO DE LA CAIDA Y TIEMPOS ACEPTABLES DE CAIDA		
RECURSO	IMPACTO	TIEMPO DE CAÍDA ACEPTABLE
1. Servidores Base de Datos y Aplicaciones	No se emiten DUIs No se entregan certificaciones No se da servicio de consulta No hay actualización de partidas No hay envíos al TSE No hay sistemas de gestión	3 Horas
2. Servidores Sistemas web	No hay servicios en línea	8 Horas
3. Servidor de Controlador de Dominio Primario	No existiría seguridad Centralizada en el acceso a la red del RNPN No se administra Perfiles, accesos a	3 Horas

IDENTIFICAR IMPACTO DE LA CAIDA Y TIEMPOS ACEPTABLES DE CAIDA		
RECURSO	IMPACTO	TIEMPO DE CAÍDA ACEPTABLE
	los sistemas	
4. Servidor de Correo	No existiría comunicación electrónica Interna y Externa (Proveedores, Instituciones Gubernamentales, etc.)	3 Horas

Recursos de Contingencia Generales.

Router (Proveído por el proveedor de Internet).

Servidores y Equipos de Comunicación (Switchs, Antenas, Fibra, etc.).

Gabinete de Comunicaciones y Servidores.

Materiales Y herramientas para cableado estructurado cat 6.

UPS Backup de los Sistemas.

Instaladores de las aplicaciones, de Software Base, Sistema Operativo, Utilitarios, etc.

Recursos de Contingencia Específicos.

a. Hardware:

10 servidores tipo Xeon mínimo con las siguientes características:

2 Procesadores de 4 núcleos.

2 discos de 600 GB.

16 GB de RAM. El equipo deberá contar con unidad para DVD.

1 Unidad de almacenamiento SAN de 25 Tb.

Un SWITCH de 24 puertos 10/1000.

1 bobina de cable UTP cat 6.

50 conectores RJ45.

1 Router para la conexión a internet (CNT).

1 UPS de 20 Kva.

b. Software y data:

Windows Server 2013 Estándar Edition.

Oracle Data Base, 11g.

Backup de las Bases de Datos.

Backup de las imágenes de los servidores.

Sitio de recuperación o de Contingencia.

El RNPN cuenta con las instalaciones del Data Center en que funcionó anteriormente la plataforma de producción del DUI, la cual aunque algunas de sus características ya son obsoletas, todavía cumple con muchas características propias de un Data Center como piso elevado, seguridad periférica, área de Ups's, área de planta generadora de emergencia, área de servidores, área de comunicación y área para oficinas de técnicos lo cual hace que la inversión para implementar un Data Center sea de menor costo que levantar de cero.

Para implementar un Sitio de Recuperación de los sistemas lo más recomendable es clonar todos los componentes de las plataformas tecnológicas de los sistemas a recuperar, no basta con replicar las bases de datos, se debe también incluir todos los nodos de los sistemas.

Opción 1:

Reacondicionar el antiguo Data Center del RNPN en la Col. Escalón y adquirir hardware y software para clonar los sistemas a recuperar:

Sistema DUI.
Sistema de actualización de partidas de nacimiento y defunción.
Sistemas de consulta de registros (DocTo, Sinfo, etc.).
OS Ticket.
Sitio Web.

Opción 2:

Contratación de hosting de servidores dentro del territorio nacional o fuera del país.

Recursos de Sitio de Recuperación.

Hardware.

20 servidores con características mínimas:

2 procesadores con 6 cores.

32 RAM.

Disco duro de 1 Tb.

4 puertos de red.

2 puertos fiber cannel.

4 Racks de 42 unidades.

3 monitores con KVM de 8 canales.

Teclado español latino.

2 UPS's de 20 KVA.

Software.

Oracle Data Base 11g.

Web Logic de Oracle.

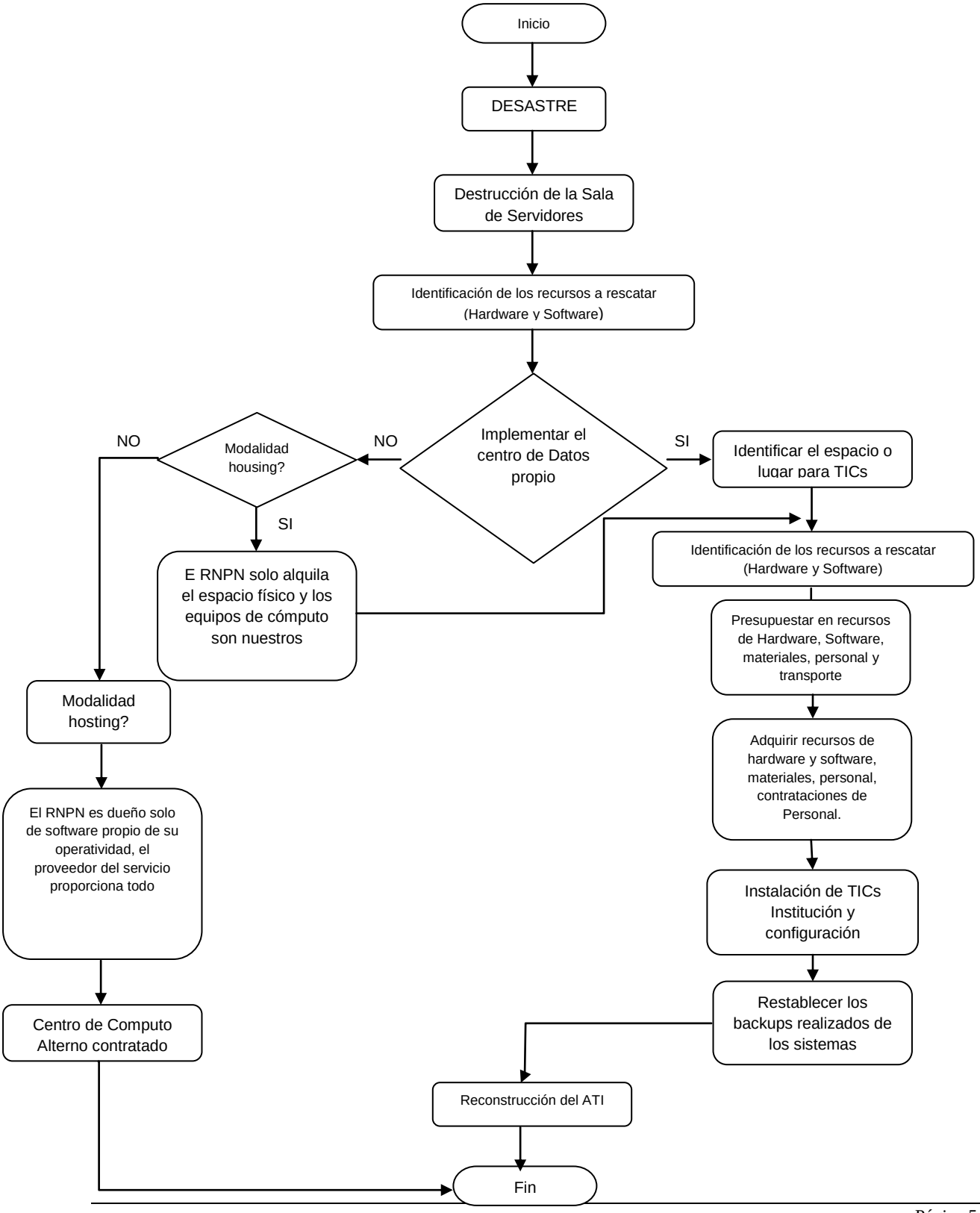
My SQL.

Microsoft SQL server.

SQL Navigator, Toad.

Procedimiento.

Indisponibilidad de la Unidad de Sistemas (destrucción del área de servidores).



9) PLAN DE VERIFICACION Y PLAN DE PRUEBAS.

Tres medidas para minimizar los riesgos de la tecnología son:

- Verificación.
- Prueba.
- Mantenimiento de los sistemas.

Cada componente de un sistema de cómputo, equipo, comunicaciones y programas debe ser verificado y probado rigurosamente antes de utilizarlo para un evento.

Plan de Verificación.

Para el Plan de Contingencia es muy importante y es conveniente que una autoridad independiente aplique las pruebas de verificación. Para sistemas de menor importancia, la verificación puede realizarse internamente.

Las pruebas de verificación (también conocidas como pruebas de calidad) pueden incluir:

- Probar los equipos bajo condiciones que simulen las de operación real.
- Probar los programas para asegurar que se siguen los estándares apropiados y que desempeñan las funciones esperadas.
- Asegurar que la documentación sea la adecuada y esté completa.
- Asegurar que los sistemas de comunicación se ciñan a los estándares establecidos y funcionen de manera efectiva.
- Verificar que los sistemas sean capaces de operar bajo condiciones normales, pero también bajo potenciales condiciones inesperadas.
- Asegurar que se cuente con las debidas medidas de seguridad.

10) GLOSARIO TÉCNICO.

A

Amenaza.

Posibilidad de riesgo que pueda interferir con el funcionamiento adecuado de la infraestructura tecnológica, ejemplo de estos: fallas de suministro eléctrico, incidencia de virus, saturación del ancho de banda de red.

Ataque.

Cualquier acción o evento con el que se intente interferir nocivamente con el funcionamiento adecuado de un sistema informático o con la integridad de sus datos y/o recursos.

B

Base de Datos.

Conjunto de datos informativos organizados y almacenados en un mismo contexto para su uso y vinculación por medio de sistemas informáticos.

C

Contingencia.

Interrupción, no planificada, de la disponibilidad de recursos informáticos.

D

Dato.

En este caso los datos es la representación simbólica (numérica, alfabética, algorítmica, espacial, etc.) de un atributo o variable cuantitativa o cualitativa. Los datos describen hechos empíricos, sucesos y entidades, de los cuales se genera información y soluciones.

I

Impacto.

El impacto de una actividad crítica se encuentra clasificado, dependiendo de la importancia dentro de los procesos TIC:

Impacto Alto: se considera que una actividad crítica tiene impacto alto sobre las operaciones del RNPN, cuando ante una eventualidad en ésta se encuentran imposibilitadas para realizar sus funciones normalmente.

Impacto Medio: se considera que una actividad crítica tiene un impacto medio cuando la falla de esta, ocasiona una interrupción en las operaciones del RNPN por un tiempo mínimo de tolerancia.

Impacto Bajo: se considera que una actividad crítica tiene un impacto bajo, cuando la falla de ésta, no tiene un impacto en la continuidad de las operaciones de la Institución.

Incidente.

Circunstancia o evento que sucede de manera inesperada y que puede afectar al desarrollo de un asunto o negocio, aunque no forme parte de él.

Infraestructura.

Conjunto de medios técnicos, servicios e instalaciones necesarios para el desarrollo de una actividad o para que un lugar pueda ser utilizado.

Integridad referencial.

La integridad referencial es un sistema de reglas que utilizan la mayoría de las bases de datos relacionales para asegurarse que los registros de tablas relacionadas son válidos y que no se borren o cambien datos relacionados de forma accidental produciendo errores de integridad.

P

Proceso crítico.

Proceso considerado indispensable para la continuidad de las operaciones y servicios de la Institución, y cuya falta o ejecución deficiente puede tener un impacto negativo para la Institución y por ende para la ciudadanía.

S

Seguridad Física.

La seguridad física consiste en la aplicación de barreras físicas, y procedimientos de control como medidas de prevención y contra medidas ante amenazas a los recursos y la información confidencial.

Seguridad Lógica.

Es la aplicación de mecanismos y barreras para mantener el resguardo y la integridad de la información dentro de un sistema informático.

U

UPS.

Sistema de alimentación ininterrumpida (SAI), en inglés uninterruptible power supply (UPS), es un dispositivo que gracias a sus baterías u otros elementos almacenadores de energía, puede proporcionar energía eléctrica por un tiempo limitado y durante un apagón eléctrico a todos los dispositivos que tenga conectados.

11) MODIFICACIONES DEL DOCUMENTO:

Revisión nro.	Modificaciones	FUR