GOBIERNO DE EL SALVADOR

CENTRO NACIONAL DE REGISTROS

DOCUMENTO EN VERSIÓN PÚBLICA

De conformidad a los Artículos:

24 letra “c” y 30 de la LAIP.

Se han eliminado los datos personales

Respuesta a su solicitud de información sobre auditoria informática CNR-2020-58

Pregunta	Si	No	Explicación
1. ¿Aplican normas, estándares, técnicas y buenas prácticas de auditoria? ¿Cuáles serían?	Sí		Las Normas de Auditoría Interna del Sector Gubernamental, emitidas por la Corte de Cuentas de la República.
2. ¿Poseen informes de auditoría de sistemas? ¿Cuáles podrían darnos?	Sí		Las Unidades de Auditoría Interna, no están facultado legalmente para entregar informes según Ley de la Corte de Cuentas.
3. ¿si poseen auditoria de sistemas externa o interna? ¿si es externa, que empresa se las realiza?		No	
4. ¿Qué herramientas han utilizado para realizar auditoria de sistemas?			Las Normas de Auditorias citadas y software IDEA.
5. ¿a qué áreas de la empresa se le aplica la auditoria de sistemas?			A toda la organización, controles generales y de aplicación.
6. ¿Qué planes de contingencia posee la empresa?			Pendiente Dirección de Tecnología de Información de brindar respuesta.
7. ¿cada cuánto tiempo realizan auditoria de sistemas en la empresa?			Anualmente.
8. ¿si tienen auditoria interna, que certificaciones poseen las personas que realizan dicha auditoria? """"			Todos tienen grados académicos y autorizados por el Consejo de la Vigilancia de la Contaduría Pública y Auditoría y otras competencias técnicas.

Centro Nacional de Registros (CNR)

EL SALVADOR
GOBIERNO DE
UNIR. CRECER. INCLUIR

CENTRO NACIONAL DE REGISTROS

PLAN DE CONTINGENCIA PARA LA CONTINUIDAD DE SERVICIOS INFORMÁTICOS DEL CNR

VERSION 1.0

DIRECCIÓN DE TECNOLOGÍA DE LA INFORMACIÓN (DTI)

DTI

INDICE

1. INTRODUCCIÓN

Las Tecnologías de la Información y Telecomunicaciones, así como los sistemas de información, son elementos vitales en la mayoría de procesos de negocios. Debido a esto, los servicios informáticos se convierten en críticos para la operación efectiva de los procesos de negocio.

El CNR, consciente de la importancia que representan los servicios informáticos en las operaciones de la institución, incluye dentro de la Política de Tecnologías de información y Telecomunicación aprobada por Consejo Directivo el 14 de junio de 2005, el literal 7 que dice:

> "Siendo la información de los Registros de Propiedad Inmobiliaria, Comercio, Propiedad Intelectual e IGCN de carácter público; el CNR tiene la Obligación de garantizar la disponibilidad, integridad y confiabilidad de dicho activo.
>
> Debido a su importancia a nivel nacional, se debe asegurar que la información tenga resguardos apropiados y planes de contingencia que garanticen la continuidad de las operaciones en caso de siniestros o daños a la misma. Por lo anterior, se debe proveer, gestionar y controlar los recursos necesarios para cumplir con esta responsabilidad institucional."

El cumplimiento de esta responsabilidad institucional reflejada en la Política de Tecnologías de información y Telecomunicación, implica la creación del presente Plan de Contingencia para la Continuidad de Servicios Informáticos del CNR.

1. 1. Propósito

El presente documento establece procedimientos para dar continuidad a la prestación de los servicios críticos que la DTI proporciona al CNR luego de una interrupción ocasionada por la ocurrencia de siniestros o daños en la información o en su infraestructura de soporte.

Se han establecidos los siguientes objetivos para este plan:

- Definir la Política de planeamiento de la continuidad para los servicios informáticos del CNR.
- Establecer los alcances del plan de contingencia.
- Identificar los servicios críticos que la DTI proporciona al CNR.
- Identificar las medidas de mitigación preventivas del plan de contingencia.
- Maximizar la efectividad de las operaciones de contingencia a través de un plan establecido y que considere las siguientes fases:

  1. **Fase de activación y notificación.**

     Para detectar, evaluar el daño y activar el plan.

  2. **Fase de recuperación.**

     Para restablecer temporalmente las operaciones de TI y recuperar el daño hecho al sistema original.

  3. **Fase de retorno a las operaciones normales.**

     Para restablecer las capacidades de los sistemas de procesamiento a la operación normal.

- Identificar los recursos, actividades y procedimientos necesarios para soportar los servicios informáticos críticos durante una interrupción prolongada a las operaciones normales.
- Asignar responsabilidades al personal de la DTI para una efectiva recuperación de los servicios informáticos críticos durante períodos prolongados de interrupción a las operaciones normales.
- Asegurar la coordinación con otros miembros del staff del CNR quienes participan en las estrategias del plan de contingencia.

Asegurar la coordinación con puntos de contacto externo y proveedores que podrían participar en las estrategias de planeación de la contingencia.

- Cumplimiento con requisitos propios de la institución y de gobierno.

1. 2. Aplicabilidad

Existen varios tipos de Planes de Contingencia que se diferencian entre ellos por su propósito y alcance (Ver anexo I). El presente plan de Contingencia está basado en el *Plan de soporte a la Continuidad/ Plan de Contingencia de TI (Continuity of Support Plan / IT contingency Plan).* Dicho plan se basa en el desarrollo y mantenimiento de un plan de soporte general a los sistemas y aplicaciones informáticas.

1. 3. Alcance

El Plan de Contingencia descrito en el presente documento considera los servicios informáticos críticos que proporciona la DTI al CNR y su ámbito de acción comprende las oficinas regístrales a nivel nacional.

1. 4. Base legal

El presente documento se emite de conformidad a lo requerido en:

- Política de Tecnologías de información y Telecomunicación del CNR.
- Normas Técnicas de Control Interno específicas del CNR.

2. POLÌTICA DE CONTINUIDAD DE LOS SERVICIOS INFORMATÌCOS.

Se define la siguiente política de continuidad de los servicios informáticos del CNR:

"La Dirección de Tecnología de la Información del Centro Nacional de Registros, desarrollará un Plan de Contingencia para el Soporte General de Sistemas de Tecnologías de la Información para resolver las necesidades de las operaciones críticas de Tecnologías de la información ante eventos de disrupción que se extiendan por más de 72 horas.

Los procedimientos para la ejecución de dicha capacidad deben ser documentados en un Plan de Contingencia formal, ser revisados anualmente y actualizados cuando sea necesario por el Coordinador del Plan de Contingencia.

Se deben definir procedimientos de respaldo de datos completos para ser enviados a un lugar designado fuera del sitio de operación normal. El Plan debe asignar responsabilidades específicas a personal designado para facilitar la recuperación y/o continuidad de las funciones esenciales de Tecnologías de Información.

Deben ser adquiridos y mantenidos los recursos necesarios para asegurar la viabilidad de los Procedimientos de Contingencia. El Personal responsable debe ser entrenado en la ejecución de dichos Procedimientos de Contingencia. El plan, la capacidad de recuperación y el personal deben ser probados anualmente para identificar debilidades en la ejecución del Plan de Contingencia".

3. ANÁLISIS DE IMPACTO EN EL NEGOCIO.

3.1. Identificación de servicios críticos

La DTI proporciona servicios de soporte a los procesos de negocio del CNR. El anexo II contiene un listado completo de dichos servicios.

Dentro de este universo de servicios, existen algunos considerados críticos por su impacto en las operaciones de la organización. Estos son:

6.5.1 Recuperación, respaldo y verificación de datos.

6.5.2 Administración de Servidores

6.5.4 Administración de base de Datos

6.5.5 Enlaces de telecomunicaciones

3.2. Análisis de riesgo de los servicios críticos

Como soporte a la definición del presente plan, se realizaron los siguientes Análisis de Riesgo:

- **Análisis de Riesgo de la Recuperación, respaldo y verificación de datos.**
- **Análisis de Riesgo de la Administración base de Datos**
- **Análisis de Riesgo de la Administración de Enlaces y Telecomunicaciones**

Nota. Es importante especificar que de la Administración de Servidores no se realizó un análisis de riesgo por ser parte integral de los otros servicios críticos considerados.

Del resultado del análisis y evaluación de riesgos de los servicios críticos que la DTI provee a la institución, surge la necesidad de:

Desarrollar e implementar un plan de contingencia adecuado que permita la continuidad de los servicios críticos que la DTI proporciona al CNR, ante desastres que puedan afectar las operaciones normales de los registros en todo el país.

4. MEDIDAS DE MITIGACIÓN PREVENTIVAS DEL PLAN DE CONTINGENCIA

Como una medida inmediata para mitigar el riesgo de una falla en la continuidad mayor, es necesario contar con medidas preventivas claramente identificadas. Dichas medidas se listan a continuación.

4.1. Medidas de protección de Datos y Sistemas Informáticos

a. Respaldo (Backup) de Datos

Se dispone de un procedimiento para la realización de los respaldos de datos, el cual se encuentra actualmente en operación. (ver anexo V)

b. Verificación de Respaldo (Backup) de Datos

El procedimiento descrito en el anexo V, incluye los pasos a seguir para efectuar la verificación de los respaldos, con el fin de comprobar la disponibilidad, integridad y confiabilidad de la data respaldada tanto en las oficinas centrales del CNR como en las oficinas departamentales.

4.2. Medidas de protección a los elementos físicos

a. Prevención de incendios

En cada cuarto de servidores institucionales se cuenta con alarmas para la detección de humo, así como también extintores manuales. En el cuarto de servidores central, ubicado en la DTI, se dispone adicionalmente de un sistema automático, de gas inerte, para extinción de fuegos.

b. Sistema Ininterrumpido de Poder (UPS)

Todos los equipos informáticos, incluyendo servidores, están conectados a fuentes ininterrumpibles de poder (UPS).

c. Plantas Eléctricas

En caso de presentarse cortes prolongados de energía eléctrica, todas las oficinas del CNR a nivel nacional, cuentan con plantas generadoras de electricidad como medida de contingencia.

d. Cajas de Seguridad Internas

A fin de proteger los medios magnéticos que contienen los datos respaldados, se cuenta con cajas de seguridad internas, en todas las oficinas departamentales y en las oficinas centrales, .

e. Cajas de Seguridad Externas

Se cuenta con un procedimiento para el resguardo de cintas en cajas de bancos, fuera de las oficinas del CNR. (anexo VI)

4.3. Medidas de protección a las Telecomunicaciones

A fin de asegurar las comunicaciones entre las oficinas departamentales e instalaciones centrales del CNR, se cuenta con enlaces redundantes, a través de backbones diferentes.

4.4. Medidas de protección a nivel de servidores

a. Falla de Servidores

Se dispone de un procedimiento para atender contingencias en caso de falla en hardware o software de los servidores institucionales incluidos en el anexo IV.

b. Servidores Secundarios para Autenticación de Usuarios de Dominio (Backup Domain)

c. Arreglos de Discos

Con el fin de disponer de un mecanismo para la prevención de pérdida de datos como consecuencia del fallo de un disco duro, los servidores poseen arreglos de discos redundantes, lo que provee tolerancia a fallas y pérdida de datos.

d. Fuentes redundantes.

La mayoría de servidores cuentan con fuentes de poder redundantes, que les permiten continuar operando en caso de fallar la fuente primaria.

4.5. Medidas de protección a nivel humano

a. Soporte Local

En todas las dependencias del CNR, se dispone de al menos un soporte informático en cada sitio.

b. Soporte Regional

Dentro del grupo de soportes informáticos locales que operan en la región paracentral y oriental, se ha designado un soporte, con mayor experiencia, que funciona como soporte regional, para dar apoyo en caso de necesidad a Registros vecinos. Adicionalmente, se cuenta con un Coordinador de Soportes Informáticos cuya función es apoyar los Registros a nivel nacional.

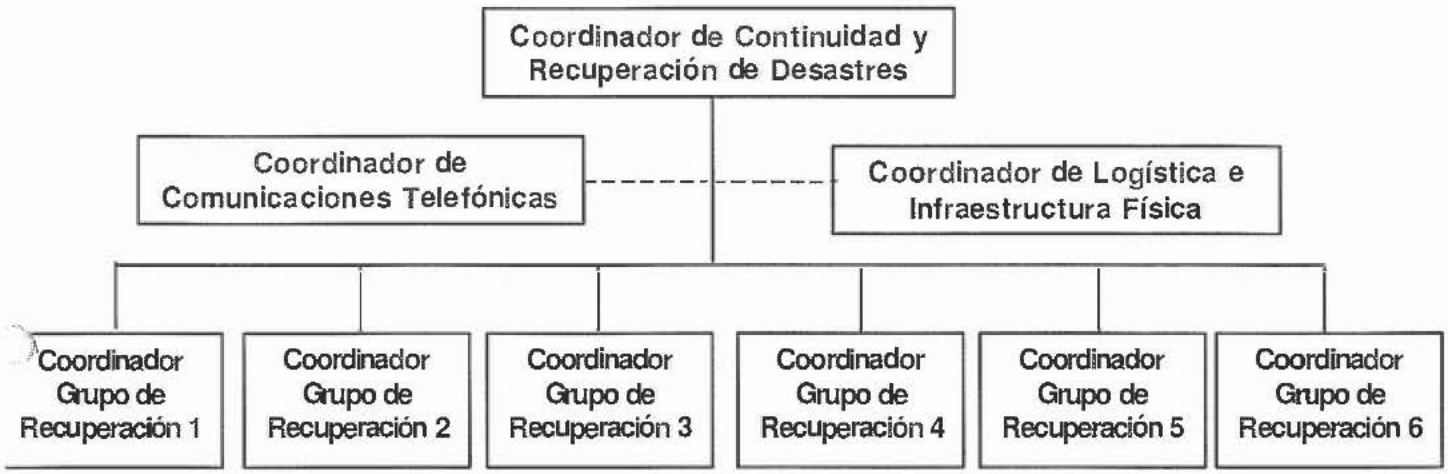
4.6. Repositorio centralizado de Datos .

Se dispone de un esquema de base de datos que permite replicar, a un servidor centralizado, la información de las bases de datos de todas las oficinas departamentales del Registro de Propiedad Raíz e Hipotecas.

Las medidas anteriores son soportadas por una serie de procedimientos para solventar fallas consideradas menores. (Ver anexo IV)

5. ESTRUCTURA ORGANIZACIONAL

5.1. Organigrama del equipo de soporte al plan de contingencia



PUESTO FUNCIONAL	RESPONSABLE
Coordinador de Continuidad y Recuperación de Desastres	Director de Tecnología de la Información
Coordinador de Comunicaciones Telefónicas	Coordinador de Servicios de Telefonía DTI
Coordinador de Logística e Infraestructura Física	Jefe Administrativo de la DTI
Coordinador de Grupo de Recuperación 1	Gerente de Infraestructura Informática
Coordinador de Grupo de Recuperación 2	Gerente de Soporte Técnico
Coordinador de Grupo de Recuperación 3	Coordinador de Base de Datos
Coordinadores de Grupos de Recuperación 4 (Recuperación de Sistemas)	Gerentes de Sistemas Registrales, Gerente de Sistemas Catastrales y Geográficos, y Gerente de Sistemas Administrativos y Financieros
Coordinador de Grupo de Recuperación 5	Administrador de Servidores de Aplicaciones
Coordinador de Grupo de Recuperación 6	Jefe de Atención al Cliente de la DTI

5.2. Funciones y responsabilidades

• **Coordinador de Continuidad y Recuperación de Desastres**

- ✓ Provee enlace con los Titulares, Directores y encargados de los sitios alternos de operación internos y externos, para reportar las actividades relacionadas con la activación y estatus de la operación del Plan de Contingencia, entrenamiento y pruebas.
- ✓ Asegura que el grupo de Contingencia suministre y evalúe el adiestramiento necesario a los miembros del grupo de Contingencia y otras partes involucradas.
- ✓ Asegura que el grupo de Contingencia evalúa los planes y reevalúa la criticidad de los servicios de forma periódica.
- ✓ Activa el Inicio del Plan de Contingencia.
- ✓ Coordina las actividades de Procesamiento de datos, Telecomunicaciones, Recuperación y Reconstitución de Sistemas, es decir, la restauración operacional de las instalaciones y operaciones del sitio alterno determinado así como del retorno a las operaciones normales del sitio original.

• **Coordinador de Comunicaciones Telefónicas**

- ✓ Evaluación de daños en infraestructura de equipos del Centro Nacional de Registros, como también de los diferentes operadores de telecomunicaciones en las áreas de telefonía fija, móvil, enlaces de datos, internet.
- ✓ Elaborar informe de daños causados con las áreas de afectación de ubicación y servicios críticos a restablecer, que incluya equipos propios y ajenos y servicios de operadores.
- ✓ Presupuesto del restablecimiento de los equipos y servicios dañados o afectados.

- ✓ Plan de restablecimiento de equipos y servicios, apoyado con áreas internas, proveedores de servicios externos y proveedores de servicios de telefonía y datos.
- ✓ Protocolo de pruebas y puesta en servicio de los equipos.

• Coordinador de Logística e Infraestructura Física

- ✓ Evaluación y diagnostico de daños.
- ✓ Mantener vehículos con gasolina y disponibilidad de motoristas.
- ✓ Coordinar con jefes administrativos de las oficinas centrales y departamentales para apoyo informático.
- ✓ Coordinar con la Gerencia de Infraestructura y Mantenimiento reparación de daños físicos en las instalaciones del Centro de Computo de la Oficina de San Salvador
- ✓ Coordinar con Transporte el traslado de equipo
- ✓ Compra de alimentos para personal que realice turnos de trabajo.

• Coordinador de Grupo de Recuperación 1 (Infraestructura Informática)

- ✓ Inspecciona todos los equipos computacionales que pueden ser afectados en caso de desastre y evalúa los daños, para emitir informe al Coordinador de Continuidad . Estos equipos incluyen: Servidores, Equipos de Telecomunicaciones, Libreras de Datos, UPS, Equipos de Aire, Plantas Eléctricas de Emergencia, Sistemas Detección Incendios, etc.
- ✓ Coordina la restauración de Sistemas Operativos con los grupos de recuperación bajo su cargo.

- En caso de necesitarse restauraciones de las Bases de Datos y/o archivos de datos institucionales, coordina con los grupos de recuperación bajo su cargo, la obtención de los medios magnéticos (cintas) que contienen dichos datos, desde las bóvedas de seguridad del proveedor externo.
- Supervisa las restauraciones de las bases de datos institucionales, junto al personal técnico de la Unidad de Base de Datos de la DTI.
- En caso de necesitarse restauraciones de las configuraciones de los equipos de telecomunicaciones (switches, routers), coordina con los grupos de recuperación bajo su cargo, la obtención de los medios

- Evalúa rutas alternas para el ingreso de cableado de datos con proveedores externos, en el caso la ruta principal se encuentre dañada, con los grupos de recuperación bajo su cargo .
- Se comunica con los proveedores involucrados en las tareas de recuperación .
- Gestiona con los proveedores de servicio para asegurar que el reemplazo de equipos y accesorios se encuentre disponible e instalado oportunamente .
- Supervisa el trabajo de los proveedores de servicio para Servidores, Sistemas de Almacenamiento , Equipos de Telecomunicaciones, Bases de Datos, Enlaces de Datos Primarios y Secundarios .
- Monitorea y reporta el avance de las actividades de los grupos de recuperación y les asiste, si es necesario, en los esfuerzos de recuperación .
- Coordina con la Gerencia de Infraestructura y Mantenimiento la habilitación de sistemas alternos de energía eléctrica y aire acondicionado en el caso que los sistemas principales se encuentren dañados Informa oportunamente el estado de los avances de recuperación al
- Coordinador de Continuidad.

- **Coordinador de Grupo de Recuperación 2 (Soporte Técnico)**

- ✓ Inspecciona equipos computacionales en presencia de catástrofe y evalúa los daños, para emitir reporte al Coordinador de Continuidad. Estos equipos incluyen : computadoras personales, impresores, scanners, plotters, plantas eléctricas, UPS, cableado estructurado, etc.
- ✓ Se verifican los inventarios de equipos y se emite reporte al Coordinador de Continuidad, para movilizarlos si fueren necesarios.
- ✓ Coordinar los traslados y las instalaciones de los equipos a sustituir en las oficinas afectadas, departamentales u oficinas centrales.
- ✓ Coordinar el funcionamiento de los aplicativos a nivel de estaciones de trabajo y periféricos.
- ✓ Coordinar con la Gerencia de Infraestructura y Mantenimiento el funcionamiento de aires acondicionados y el suministro de energía eléctrica, así como plantas de emergencias.
- ✓ Coordinar la asignación de personal de refuerzo para la recuperación del funcionamiento de las oficinas departamentales o centrales.
- ✓ Monitorea y reporta el avance de las actividades de los grupos de recuperación y les asiste, si es necesario, en los esfuerzos de recuperación.

- **Coordinador de Grupo de Recuperación 3 (Base de Datos)**

- ✓ Inspecciona los activos en presencia de catástrofe y evalúa los daños, para emitir reporte al Coordinador de Continuidad.
- ✓ Coordina la restauración de Aplicaciones y Base de Datos a través de los grupos de recuperación bajo su cargo.
- ✓ Monitorea y reporta el avance de las actividades de los grupos de recuperación y les asiste, si es necesario, en los esfuerzos de recuperación.

- ✓ Consulta a los contratistas externos y proveedores de servicio para asegurar que el reemplazo de equipo y materiales esté disponible e instalado oportunamente.
- ✓ Se comunica con los proveedores involucrados en las tareas de recuperación.

- **Coordinador de Grupo de Recuperación 4 (Sistemas)**

- ✓ Evaluar los daños y funcionalidad de los sistemas institucionales
- ✓ Diagnosticar el daño al interior del CNR para emitir un reporte al Coordinador de Continuidad
- ✓ Solicitar al Coordinador de Comunicaciones Telefónicas la disponibilidad del personal del presente grupo de recuperación
- ✓ Coordinar la restauración de las aplicaciones
- ✓ Coordinar con los grupos de recuperación 1, 3 y 5 los recursos disponibles para la puesta en funcionamiento de las aplicaciones
- ✓ Coordinar con el grupo de recuperación 2 la implementación de los nuevos accesos a las aplicaciones para los usuarios internos
- ✓ Coordinar con el grupo de recuperación 6 el acceso a las aplicaciones para los clientes externos
- ✓ Elaborar un informe del estado general de las aplicaciones para el Coordinador de Continuidad

- **Coordinador de Grupo de Recuperación 5 (Administrador de Servidores de Aplicaciones)**

- ✓ Inspección y evaluación de daños de servidores de aplicaciones y servicios.
- ✓ Preparar informe de servicios activos e interrumpidos, anexando un detalle de las causas observadas como originadoras de la interrupción.

- ✓ Entregar informe de servicios activos e interrumpidos al "Coordinador de Continuidad y Recuperación de Desastres" y a las coordinaciones que dependen de él.
- ✓ Definir el plan de reactivación de servicios en conformidad con el informe de servicios interrumpidos.
- ✓ Gestionar los recursos necesarios para la reactivación de servicios
- ✓ Implementar el plan de reactivación de servicios
- ✓ Mantener comunicación con Unidad de Telecomunicaciones para restablecer la ínter-conectividad de servicios con recursos externos enlazados por la red.
- ✓ Mantener comunicación con Unidad de Base de Datos para restablecer la ínter-conectividad y buen funcionamiento de servicios de aplicaciones que dependen de base de datos.
- ✓ Mantener comunicación con Unidad de Atención al Cliente y Gerencias de Sistemas para informarles sobre los servicios restablecidos y confirmar el buen funcionamiento de los mismos.

•Coordinador de Grupo de Recuperación 6 (Atención al Cliente)

- ✓ Contactar por cualquier medio (teléfono, correo, radio o mensajería) al personal técnico de la DTI y a los proveedores de equipos y servicios informáticos.
- ✓ Evaluar e identificar los servidores de base de datos, aplicaciones y equipo de telecomunicaciones afectados a fin de identificar que sistemas y servicios se encontraban alojados en dichos servidores.
- ✓ Elaborar un inventario de los sistemas y servicios afectados para llevar el control del tiempo fuera de servicio y su impacto en cada oficina departamental.
- ✓ Control y seguimiento de sistemas y servicios afectados a fin de informar a los usuarios y unidades afectadas hasta la puesta en marcha.

5.3. Listado de personal responsable

En el anexo III se especifica la información relevante de las personas responsables del Plan de Contingencia, así como las personas suplentes que puedan asumir el rol del titular en caso de que este último no esté disponible.

6. ESTRATEGIA DE RECUPERACIÓN

Para seleccionar la estrategia de recuperación, debemos considerar los métodos de recuperación existentes. Dichos métodos de recuperación se clasifican en:

- Sitios en Frío (cold site)
- Sitios Cálidos (warm site)
- Sitios en Caliente (hot site)
- Sitios Móviles (Mobil site)
- Sitos Replicado (mirrored site)

Obviamente hay una diferencia de costo y disponibilidad entre las cinco opciones. Los sitios replicados son la selección más costosa, pero esta asegura un 100% de disponibilidad. Los sitios en frío son más baratos de mantener; sin embargo, puede requerir de un tiempo sustancial adquirir e instalar en equipo necesario. Los equipos parcialmente equipados, tales como los sitios cálidos caen en medio del espectro. En muchos casos, los equipos móviles pueden ser enviados a una ubicación deseada en un término de 24 horas. Sin embargo, el tiempo necesario para instalación puede incrementar el tiempo de respuesta.

.

6.1. Procedimientos de soporte.

Para soportar dicha estrategia, se tienen implementados los procedimientos:

- Anexo V - P625. Recuperación, respaldo y verificación de información

- Anexo VI - DTI-PRO-009 Procedimiento de resguardo de cintas fuera de oficinas del CNR

6.2. Factores claves del éxito.

Como factores claves para el éxito de la estrategia de recuperación se tienen:

- Disponibilidad de recursos humanos, hardware e infraestructura de soporte.
- La realización eficiente de los procedimientos de soporte a la estrategia.
- La realización de pruebas para validar la efectividad del plan.

7. FASES DEL PLAN DE CONTINGENCIA

7.1. Procedimiento de activación del plan de contingencia

No.	EVENTO/ ACTIVIDAD	Responsable
1	Gestionar autorización para tener acceso a las instalaciones que han sufrido daño, o a diferentes áreas geográficas	Coordinador de Continuidad
2	Evaluar con los Grupos de Recuperación y proveedores, la severidad de los daños a los activos involucrados de hardware y Software e informar al Coordinador de Continuidad el tiempo estimado de restauración. Adicionalmente los Grupos de Recuperación continúan las actividades de restablecimiento del servicio.	Coordinadores de Logística e Infraestructura Física, de Comunicaciones Telefónicas, y de Grupos de Recuperación 1, 2,3,4,5,6
3	Proceder a la activación del Plan de Contingencia, con base en el reporte del (los) Coordinador(es) de Recuperación o reportes por parte de los usuarios debido a la no disponibilidad del servicio.	Coordinador de Continuidad
4	Contactar a coordinadores de recuperación, informándoles la necesidad de activar el plan de Contingencia. A efectos de comenzar las actividades de logística o apoyo correspondientes.	Coordinador de Continuidad
5	Comunicar a Titulares, Directores y Gerentes encargados de sitios alternos de operación, la activación del plan, con la finalidad que éstos emitan las autorizaciones, resoluciones o lineamientos correspondientes para que cada Dirección, así como las instituciones usuarias, ejecuten sus tareas de Contingencia. Informar a Directores, Gerentes y Jefes de Unidad el tiempo estimado de no disponibilidad del servicio.	Coordinador de Continuidad
6	Informar a usuarios el tiempo estimado de no disponibilidad del servicio	Coordinador de Grupo de Recuperación 6

7.2. Procedimiento para recuperación de los servicios críticos

No.	EVENTO / ACTIVIDAD	Responsable
1	Comunicar a los coordinadores de recuperación sobre el Sitio que ha sido designado para el restablecimiento de los servicios de la DTI	Coordinador de Continuidad
2	Notificar al Gerente / encargado del sitio de reactivación designado, sobre la activación del plan y la necesidad de reactivar los sistemas en el sitio bajo su responsabilidad.	Coordinador de Continuidad
3	Obtener los suministros y espacio de oficina necesarios.	Coordinador de Continuidad
4	Comunicar al Coordinador del Grupo de Recuperación 1 de la necesidad de reactivar los sistemas críticos en el sitio designado	Coordinador de Continuidad
5	Obtener e instalar los componentes de hardware necesarios.	Coordinador de Grupo de Recuperación 1, 2
6	Obtener respaldos de datos a utilizar	Coordinador de Grupo de Recuperación 1
7	Recuperar sistemas operativos críticos y aplicaciones de software.	Coordinador de Grupo de Recuperación 1
8	Recuperar datos de los sistemas	Coordinador de Grupo de Recuperación 1
9	Hacer pruebas de funcionalidad de los sistemas, incluidos los controles de seguridad y de telecomunicaciones.	Coordinador de Grupo de Recuperación 1,2,3,4,5
10	Habilitar los sistemas en la red.	Coordinador de Grupo de Recuperación 1
11	Verificar la operación exitosa del equipo y los sistemas en el sitio alterno.	Coordinador de Grupo de Recuperación 1,2,3,4,5
12	Informar al Coordinador de continuidad de la finalización exitosa de las labores de reactivación de los sistemas críticos.	Coordinador de Grupo de Recuperación 1,2,3,4,5
13	Comunicar a Titulares, Directores y Gerentes encargados de sitios alternos de operación, la activación del plan, con la finalidad que éstos emitan las autorizaciones, resoluciones o lineamientos correspondientes para que cada Dirección, así como las instituciones usuarias, ejecuten sus tareas de Contingencia.	Coordinador de Continuidad
14	Comunicar a usuarios la activación del Plan	Coordinador de Grupo de Recuperación 6

7.3. Procedimiento de retorno a las operaciones normales

No.	EVENTO/ ACTIVIDAD	RESPONSABLE
1	Verificar el restablecimiento adecuado de los servicios de soporte, tales como: Energía eléctrica, agua, telecomunicaciones, seguridad, control ambiental, equipamiento y suministro y equipamiento de oficinas.	Coordinador de Continuidad Coordinador de Logística e Infraestructura Física, Coordinador de Telefonía
2	Notificar a los Coordinador de Grupos de Recuperación (1,2,3,4,5,6) acerca de la necesidad iniciar el proceso de restauración de las operaciones en el sitio original	Coordinador de Continuidad
3	De ser necesario coordinar la reinstalación del hardware, software.	Coordinador de Recuperación 1, 2
4	Establecer conectividad e interface con componentes del sistema y redes externas.	Coordinador de Recuperación 1, 2
5	Probar las operaciones del sistema y asegurar su completo funcionamiento.	Coordinador de Recuperación 1,2,3,4,5
6	Organizar y coordinar las labores de respaldo de datos procesados por el equipo de provisional durante la contingencia y se trasladan al sistema recuperado.	Coordinador de Recuperación 1
7	Proceder a efectuar las actividades de recuperación de datos la contingencia.	Coordinador de Recuperación 1
8	Informar al Coordinador de Continuidad de la disponibilidad de la infraestructura tecnológica del sitio original o del nuevo sitio designado y del traslado exitoso de los datos procesados durante la contingencia.	Coordinador de Recuperación 1,2
9	Comunicar a Titulares, Directores y Gerentes encargados de sitios alternos de operación, sobre la disponibilidad del sitio original o del nuevo sitio y la inminente desactivación del Plan de Contingencia, con la finalidad que éstos emitan las autorizaciones, resoluciones o lineamientos correspondientes para reanudar las actividades en forma normal.	Coordinador de Continuidad
10	Notificar al Coordinadores de Grupos de Recuperación (1,2,3,5) acerca de la necesidad iniciar el proceso de eliminación de datos de los equipos utilizados durante la contingencia y la deshabilitación de los mismos.	Coordinador de Continuidad
11	Dar instrucciones para que el personal de recuperación proceda a remover datos del equipo utilizado durante la contingencia, así como remover o reubicar materiales sensitivos o confidenciales del sitio de contingencia.	Coordinador de Recuperación 1,2,3,5
12	Desconectar el sistema de contingencia y proteger los equipos adecuadamente.	Coordinador de Recuperación 1,2,3,5
13	Organizar el retorno del personal de recuperación a las instalaciones nuevas o a las originales.	Coordinador de Logística, Coordinadores de Grupos 1,2,3,4,5,6

14	Informar al Coordinador de Continuidad de la finalización de la fase de limpieza de datos y materiales sensitivos.	Coordinador de Recuperación 1,2,3,5
15	Dar por concluida la fase de contingencia.	Coordinador de Continuidad
16	Comunicar a Titulares, Directores y Gerentes encargados de sitios alternos de operación, sobre la desactivación definitiva del sitio alterno y del Plan de contingencia.	Coordinador de Continuidad
17	Informar a los usuarios el tiempo estimado de no disponibilidad del servicio.	Coordinador de Recuperación 6

8. MANTENIMIENTO Y REVISIÓN DEL PLAN

La Unidad de Seguridad en Tecnología de la Información es responsable de que el Plan de Contingencia para la Continuidad de los Servicios Informáticos del CNR se mantenga al día por medio de revisiones y actualizaciones periódicas para garantizar su eficacia.

9. PRUEBA Y VALIDACIÓN DEL PLAN

El Coordinador de Continuidad debe velar porque, por lo menos una vez al año, el Plan de Contingencia para la continuidad de los servicios informáticos del CNR sea probado a efecto de garantizar su efectividad, tomando en consideración lo siguiente:

- Pruebas con varios escenarios;
- Simulaciones;
- Pruebas de recuperación técnica;
- Pruebas de recuperación en sitios alternos;
- Pruebas de las instalaciones y servicios de proveedores; y
- Ensayos completos que confirmen que el personal, equipo, instalaciones y procesos pueden afrontar las interrupciones.

Para todas las pruebas es necesario que todo el equipo de Contingencia esté presente para dar soporte y apoyo a las necesidades que se presentan.

Es necesario que los Coordinadores de Contingencia se reúnan al menos una vez cada para dictar nuevos cambios que pueden surgir como resultado de la adquisición de nuevo equipo, nuevos contratos, nuevos proveedores y nuevo personal que se involucrará con el Plan de Contingencia para la Continuidad de los Servicios Informáticos del CNR.

10.CONTROL DE CAMBIOS

Las modificaciones hechas al plan desde su aprobación:

Registro de cambios

Página No.	Comentario del Cambio	Fecha del Cambio	Firma

DIRECCION DE TECNOLOGIA DE LA INFORMACION
CENTRO NACIONAL DE REGISTROS

ANEXO I

Tipos de Contingencia - Planes Relacionados

Plan	Propósito	Alcance
Plan de Continuidad del Negocios	Proveer procedimientos para el sostenimiento de las operaciones esenciales del negocio mientras se recupera de una interrupción significativa	Orientar los Procesos de Negocio; enfocado a TI solamente como soporte para los procesos del negocio.
Plan de Recuperación (o Reanudación) del Negocio	Proveer procedimientos para recuperación de las operaciones del negocio después de un desastre.	Orienta a los Procesos de Negocio; No enfocado en TI - TI orientado a TI solamente como soporte para los procesos del negocio.
Continuidad del Plan de Operaciones (COOP)	Provee procedimientos y capacidades para sostener las funciones estratégicas y esenciales de una organización, en un sitio alterno hasta por 30 días.	Se orienta el sub conjunto de una misión crítica de la organización; generalmente escrito a nivel de sedes. No esta enfocado a TI
Continuidad de Plan de Soporte / Plan de Contingencia de TI	Provee procedimientos y capacidades para la recuperación de una aplicación mayor o un sistema de soporte en general.	Al igual que el Plan de Contingencia; orienta las interrupciones del sistema de TI. No está enfocado al procesos de Negocios.
Plan de Comunicaciones Críticas	Provee procedimientos para divulgación de reportes de status al personal y al público.	Orienta la comunicación con el personal y con el público. No esta enfocado a TI.
Plan de respuesta a Incidentes Cibernéticos	Provee estrategias para detectar, responder a, y limitar las consecuencias de incidentes cibernéticos maliciosos	Se enfoca en las respuestas a la seguridad de la información para los incidentes que afecten los sistemas y/o la red.
Plan de Recuperación de Desastres (DRP)	Provee procedimientos detallados para facilitar la recuperación de capacidades en un sitio alterno.	A menudo enfocado en TI; limitado para interrupciones mayores con efectos de largo plazo.
Plan de Emergencia para Ocupantes (OEP)	Provee procedimientos coordinados para minimizar las pérdidas de vidas o daños, protegiendo daños a la propiedad en respuesta a una amenaza físicas.	Se enfoca al personal y a la propiedad de unas instalaciones específicas; no basado en los proceso del negocios o sistema funcionales de TI .

ANEXO II

SERVICIOS PROPORCIONADOS POR LA DTI

a) Soporte Primario

6.3.1 Asistencia Básica al Usuario

6.3.2 Asistencia Básica al Usuario de Software

6.3.3 Asistencia de actualización de Registros de la Base de Datos

b) Mantenimiento de Equipos

6.4.1 Mantenimiento e Instalaciones de PC

6.4.2 Mantenimiento e Instalación de Servidores

6.4.3 Mantenimiento e Instalación de equipos de Comunicación

c) Procesamiento y Administración de Datos

6.5.1 Recuperación, respaldo y verificación

6.5.2 Administración de Servidores

6.5.3 Desarrollo y mantenimiento de Sistemas

6.5.4 Administración de base de Datos

6.5.5 Enlaces de telecomunicaciones

ANEXO III

LISTADO DE PERSONAS RESPONSABLES
COORDINADORES y SUPLENTES PLAN DE CONTINGENCIA

COORDINADOR DE CONTINUIDAD Y RECUPERACION DE DESASTRES					
CONTACTO	TELEFONOS			EMAIL	
	OFICINA	CASA	CELULAR		

COORDINADOR DE COMUNICACIONES TELEFONICAS		
CONTACTO	TELEFONOS	EMAIL

COORDINADOR DE LOGISTICA E INFRAESTRUCTURA FÍSICA					
CONTACTO	TELEFONOS			EMAIL	
	OFICINA	CASA	CELULAR		

COORDINADOR DE GRUPO DE RECUPERACION 1 (INFRAESTRUCTURA INFORMATICA)					
CONTACTO	TELEFONOS			EMAIL	
	OFICINA	CASA	CELULAR		

COORDINADOR DE GRUPO DE RECUPERACION 2 (SOPORTE TECNICO)					
CONTACTO	TELEFONOS			EMAIL	
	OFICINA	CASA	CELULAR		
SUPLENTE:					

COORDINADOR DE GRUPO DE RECUPERACION 3 (BASE DE DATOS)					
CONTACTO	TELEFONOS			EMAIL	
	OFICINA	CASA	CELULAR		

COORDINADOR DE GRUPO DE RECUPERACION 4 (SISTEMAS)					
CONTACTO	TELEFONOS			EMAIL	
	OFICINA	CASA	CELULAR		

COORDINADOR DE GRUPO DE RECUPERACION 5 (ADMINISTRACION DE SERVIDORES DE APLICACIÓN)					
CONTACTO	TELEFONOS			EMAIL	
	OFICINA	CASA	CELULAR		

COORDINADOR DE GRUPO DE RECUPERACIÓN 6 (ATENCIÓN AL CLIENTE)					
CONTACTO	TELEFONOS			EMAIL	
	OFICINA	CASA	CELULAR		

CONTACTOS PARA PLAN DE CONTINGENCIA POR GRUPOS DE RECUPERACIÓN

DIRECTORIO DTI-SEGÚN ORGANIGRAMA					
FECHA DE ACTUALIZACION: 03 DE ABRIL DE 2014					
Carnet	Nombre	Ext	Tel. casa	Celular	Correo personal
COORDINADOR DE SERVIDORES DE TELEFONIA					
UNIDAD ADMINISTRATIVA					
GERENCIA DE INFRAESTRUCTURA INFORMATICA					

GERENCIA DE SOPORTE TECNICO				

BASE DE DATOS

GERENTE DE SISTEMAS REGISTRALES

GERENTE DE SISTEMAS CATASTRALES Y GEOGRAFICOS

GERENTE DE SISTEMAS ADMINISTRATIVOS Y FINANCIEROS

ADMINISTRADOR DE SERVICIOS DE APLICACIÓN					
JEFE DE ATENCIÓN AL CLIENTE DE LA DTI					
JEFE UNIDAD DE GESTIÓN DE LA CALIDAD					

CENTRO NACIONAL DE REGISTROS

ANEXO IV

PROCESOS PARA SOLVENTAR FALLAS MENORES
DIRECCIÓN DE TECNOLOGÍA DE LA INFORMACIÓN
(DTI)
VERSION 1.0

CONTENIDO

CÓDIGO DTI-PP-AS-01

Nombre del procedimiento: Puesta en operación de servidor ante falla de hardware.

Responsable del procedimiento: Administrador de Servidor/Soporte Local/ Gerencia de Infraestructura Informática (GII).

Tiempo estimado: 8 Hrs.

No.	EVENTO / ACTIVIDAD	Responsable
1	Determinar el tipo de falla de hardware.	Soporte Primario
2	Si al soporte primario le resulta imposible resolver la falla, procede de la forma siguiente:	Soporte Primario
	2.1 Reporta a la Unidad de Atención al Cliente Interno de la DTI, a través del SISSOR y/o telefónicamente.	Soporte Primario
	2.2. Si el Técnico en Servidores no logra dar soporte vía escritorio remoto o telefónicamente, se transporta al lugar donde se encuentra el servidor.	Técnico en Servidores
	2.3 El Técnico de Servidores verifica el visor de sucesos para determinar posibles causas de la falla y luego con base a estos logs se procede a solucionarla.	Técnico en Servidores
	2.4. Si con base al diagnóstico del técnico se determina que la falla de hardware puede ser reparada internamente *(Discos, memoria, tarjetas de red, tarjeta controladora de arreglo de disco, fuente de poder, CPU, Mother Board)*, se procede en la forma siguiente:	Técnico en Servidores
	2.4.1 Si la falla es de disco se procede de la forma siguiente:	
	2.4.1.1 Si falla un disco duro, este se sustituye en caliente por otro de iguales características. Esto no afecta la operación debido a que se cuenta con arreglos de disco en Mirror (RAID1) y RAID 5. Ir al paso 5	Técnico en Servidores
	2.4.2. Si fallan dos discos en raid 5, se procede en la forma siguiente:	
	2.4.2.1 Se pierde el arreglo por lo cual se procede a restaurar un backup.	Técnico en Resguardo de Datos o Soporte Informático
	2.4.2.2 Se crea nuevamente el arreglo de discos y se baja el backup. Se va al paso 5.	Técnico en Resguardo de Datos o Soporte Informático

Elaboró

	2.5 Si la falla es de tarjeta controladora del arreglo de discos, esta se reemplaza por una de iguales características para mantener el arreglo. Si no se cuenta con el repuesto adecuado, se procede a sustituir el servidor. Se va al paso 5	Técnico en Servidores
	2.6 Si se trata de daño en la fuente de poder se cuenta con redundancia, por lo que no se ve afectada la operación, pues únicamente se sustituye la unidad dañada. Se va al paso 5	Técnico en Servidores
3	Si la falla de hardware es grave(CPU, Motherboard) y no se puede solventar internamente se va al paso 4; de lo contrario se procede de la forma siguiente:	Técnico en Servidores
	3.1 Si la falla es de CPU se va al paso 3.2; si es de PPM se va al paso 3.3	Técnico en Servidores
	3.2 Cambiar CPU, hacer pruebas. Se va al paso 5	Técnico en Servidores
	3.3 Cambiar el módulo PPM(Power Process Module), hacer pruebas. Se va al paso 5	Técnico en Servidores.
4	**Reemplazo del servidor**. Si se dispone de un servidor de reemplazo que pueda ser utilizado, se realiza lo siguiente:	
	4.1 Se verifica que el servidor de respaldo cumpla con las mismas características de hardware y controladora de discos para conservar el arreglo y no exista pérdida de datos.	Técnico en Servidores
	4.2. Se bajan los respaldos de datos y de software instalado	Técnico en Resguardo de Datos o Soporte Informático
	4.3. Prueba y puesta en operación del servidor de producción	Técnico en Resguardo de Datos y Soporte Informático
	4.4. Se hacen los trámites de envío del servidor para su reparación, de acuerdo con el numeral 4.5.2.	Técnico en Resguardo de Datos o Soporte Informático
	4.5. Si el servidor esta bajo garantía, se realiza lo siguiente:	
	4.5.1. Se comunica inmediatamente con el proveedor del servidor, para hacer efectiva la garantía.	Técnico en Servidores
	4.5.2. Se hacen trámites para su reparación o para adquirir uno nuevo.	Técnico en Servidores /Gerencia de

	4.6.Si no se dispone de un servidor de reemplazo, se negocia con el proveedor el suministro de un Servidor en calidad de préstamo, vía contrato servicio de soporte técnico.	Técnico en Servidores
5	Retornar el servidor a producción normal	Técnico en Servidores

CÓDIGO DTI-PP-AS-**02**

Nombre del procedimiento: Puesta en operación de servidor ante falla de software.

Responsable del procedimiento: Administrador de Servidor/Soporte Local/ Gerencia de Infraestructura Informática (Gii).

Tiempo estimado: 8 Hrs.

No.	EVENTO/ ACTIVIDAD	Responsable
1	Si analiza la falla (Sistema Operativo, utilitarios, configuraciones, etc.) y en caso que no se pueda solventar internamente se va al paso 2; de los contrario, se realiza lo siguiente:	Técnico en Servidores o Soporte Informático
	1.1 Se verifica el visor de sucesos para determinar las posibles causas de error y las posibles soluciones.	Técnico en Servidores o Soporte Informático
	1.2 Si la falla es de Sistema Operativo entonces	Técnico en Servidores
	1.2.1 Si el Sistema Operativo se encuentre instalado en una partición independiente y luego procede a reinstalarlo sin haber pérdida de datos y se va al paso 1.2.3 De lo contrario se va al paso 1.2.2	Técnico en Servidores
	1.2.2 Se verifica la configuración del servidor para la carga de los respaldos de los datos y del software de aplicación.	Técnico en Servidores o Soporte Informático
	1.2.3. Prueba y puesta en operación del servidor de producción.	Técnico en Servidores Y Soporte Informático
2	Si la falla de software no se puede solventar internamente, se realiza lo siguiente:	
	2.1. Se comunica inmediatamente con el proveedor o la empresa de soporte de software, para que proporcione la asesoría adecuada para resolver el problema, sobre la base del contrato con el proveedor del software.	Técnico en Servidores
	2.2. Se preparan los respaldos de datos y del software instalado, para su reinstalación	Técnico en Resguardo de Datos
	2.3. Se realizan las acciones pertinentes de acuerdo con la asesoría proporcionada por el proveedor o la empresa de soporte de software.	Técnico en Servidores
	2.4. En caso de ser necesario se bajan los respaldos de datos y del software instalado en el servidor.	Técnico en Resguardo de Datos o Soporte Infprmático
	2.5. Prueba y puesta en operación de la aplicación en el servidor de producción.	Técnico en Servidores

CÓDIGO DTI-PP-AS-03

Nombre del procedimiento: Puesta en operación de servidor DNS/WINS.

Responsable del procedimiento: Administrador de Servidor/Soporte Local/ Gerencia de Infraestructura Informática (Gli).

Tiempo estimado: 4-8 Hrs.

No.	EVENTO / ACTIVIDAD	Responsable
1	Diagnóstico de la falla.	Técnico de Servidores/ Soporte Informático
2	2.1. Si es falla de hardware del(los) servidor(es) se activa el procedimiento de contingencia DTI-PC-AS-01 – Puesta en operación de un servidor por falla de hardware.	Técnico de Servidores/ Soporte Informático
	2.2. Si es falla de software del(los) servidor(es) se activa el proceso DTI-PC-AS-02 – Puesta en operación de un servidor por falla de software.	Técnico de Servidores/ Soporte Informático
3	Si es una falla de DNS, WINS se procede de la siguiente forma:	Técnico de Servidores/ Soporte Informático
	3.1 Se verifica que el servicio esté iniciado y que este transfiriendo las zonas.	Técnico de Servidores/ Soporte Informático
	3.2 Se verifica el visor de sucesos y en base al origen y a la identificación del suceso se procede a realizar investigaciones y se determina si se trata de una falla de software.	Técnico de Servidores/ Soporte Informático
	3.3 En caso de ser necesario se desinstalan los servicios de WINS y DNS y se vuelven a reinstalar para configurarlos nuevamente.	Técnico de Servidores/ Soporte Informático
	3.4 Si en el servidor los servicios WINS y DNS fallan, se procede a iniciar estos servicios en otro servidor en donde ya existen estos servicios (Solamente que se tienen abajo) y quedan funcionando de igual forma.	Técnico de Servidores/ Soporte Informático

CÓDIGO DTI-PP-AS-04

Nombre del procedimiento: Falla de Tarjeta de Red.

Responsable del procedimiento: Administrador de Servidor/Soporte Local/ Gerencia de Infraestructura Informática (Gii).

Tiempo estimado: 2-4 Hrs.

No.	EVENTO/ ACTIVIDAD	Responsable
	Se procede a verificar la falla en la tarjeta de red, de la forma siguiente:	Técnico de Servidores / Soporte Informático
1	Se verifica el visor de sucesos para determinar el origen de la falla, ya que puede ser de la tarjeta de red o de software.	Técnico de Servidores / Soporte Informático
2	Se desinstala la tarjeta y se vuelven a cargar los controladores, se asigna la IP y se hacen las pruebas de conectividad.	Técnico de Servidores/ Soporte Informático
3	Si la falla persiste se hace el cambio de la tarjeta de red.	Técnico de Servidores / Soporte Informático
4	Si no se habilita la tarjeta de red integrada o la de backup que siempre esta en los servidores, se asigna la IP y se hacen las pruebas de conectividad,	Técnico de Servidores / Soporte Informático

CÓDIGO DTI-PP-AS-05

Nombre del procedimiento: Falla de UPS.

Responsable del procedimiento: Administrador de Servidor/Soporte Local/ Gerencia de Infraestructura Informática (Gii).

Tiempo estimado: 2 días.

No.	EVENTO/ACTIVIDAD	Responsable
1	Verificación de la Falla del Equipo (Baterías, Carga, etc.) y se reporta a los técnicos de mantenimiento.	Soporte de Informático/Administrador de Servidores/ Técnico de Unidad de Mantenimiento
2	Si la Falla del Equipo se puede solventar internamente se realiza lo siguiente:	Técnico de Unidad de Mantenimiento
	2.1 En caso de ser necesario se sustituye el UPS dañado con un UPS de respaldo mientras se realiza la reparación.	Técnico de Unidad de Mantenimiento
	2.1. Se sustituye la parte dañada con los repuestos existentes.	Técnico de Unidad de Mantenimiento
	2.2. Puesta en Operación del Equipo y desconectar el UPS de respaldo utilizado temporalmente.	Técnico de Unidad de Mantenimiento
3	Si la Falla del Hardware es grave y no se puede solventar internamente se realiza lo siguiente:	Técnico de Unidad de Mantenimiento
	3.1. Se solicita la adquisición de la pieza requerida a la UACI.	Gerente de Soporte Técnico/ Técnico de Unidad de Mantenimiento
	3.2 Recepción de repuesto, reparación y puesta en operación	Técnico de Unidad de Mantenimiento

CÓDIGO DTI-PP-ASBD-01

Nombre del procedimiento: Puesta en operación de servidor DB ante falla de hardware

Responsable del procedimiento: Administrador de Servidor/Soporte Local/ Gerencia de Infraestructura Informática.

Tiempo estimado: 2-4 días

No.	EVENTO/ ACTIVIDAD	Responsable
1	Verificación de la Falla del Hardware.	Soporte Primario/DBA
2	Si al soporte primario le resulta imposible resolver la falla, procede de la forma siguiente:	Soporte Primario/DBA
	2.1 Reporta a la Unidad de Atención al Cliente Interno de la DTI, quienes solicitan a la Gerencia de Infraestructura Informática que asigne un Técnico en Servidores para atender el requerimiento.	Soporte Primario/DBA
	2.2. Si el Técnico de Servidores no logra dar soporte telefónicamente, se transporta al lugar donde se encuentra el servidor.	Técnico en Servidores
	2.3. Si con base al diagnóstico del técnico se determina que la falla de hardware puede ser reparada internamente (Discos, memoria, tarjetas de red, tarjeta controladora de arreglo de disco, fuente de poder, CPU, Mother Board), se procede en la forma siguiente:	Técnico en Servidores
	2.3.1. Si la falla es de disco duro, este se sustituye en caliente por otro de iguales características. Esto no afecta la operación debido a que se cuenta con un arreglo de discos.	Técnico en Servidores
	2.3.3. Si la falla es de tarjeta controladora del arreglo de discos, esta se reemplaza por una de iguales características para mantener el arreglo. Si no se cuenta con el repuesto adecuado, se procede a sustituir el servidor.	Técnico en Servidores
	2.3.4 Si se trata de daño en la fuente de poder se cuenta con redundancia, no se ve afectada la operación y únicamente se sustituye la unidad dañada.	Técnico en Servidores
3	Si la falla de hardware es grave (CPU, Motherboard) y no se puede solventar internamente	Técnico en Servidores

	3.1. Reemplazo del servidor. Si se dispone de un servidor de Reemplazo que pueda ser utilizado, se realiza lo siguiente:	
	3.1.1. Se verifica que el servidor de respaldo disponga de suficiente memoria de trabajo y en disco para soportar las aplicaciones.	Técnico en Servidores
	3.1.2. En este paso se realiza lo siguiente: - Bajar los respaldos de datos y de software instalado - Instalar el Software de B.D. - Crear la B.D. - Importar el backup de B.D.	Técnico de Resguardo de Datos / DBA
	3.1.3. Prueba y puesta en operación del servidor de producción	DBA
	3.2. Si el servidor esta bajo garantía, se realiza lo siguiente: 3.2.1. Se comunica inmediatamente con el proveedor del servidor, para hacer efectiva la garantía. 3.2.2. Se hacen trámites para su reparación o para adquirir uno nuevo.	Técnico en Servidores
	3.3.Si no se dispone de un servidor de reemplazo, la Gerencia de Infraestructura Informática trata de obtener un Servidor de backup con el proveedor u otro medio. 3.3.1. Se trata de obtener un servidor en calidad de préstamo de parte del proveedor, vía contrato servicio de soporte técnico.	Técnico en Servidores

CÓDIGO DTI-PP-ASBD-**02**
Nombre del procedimiento: Puesta en operación de servidor DB ante falla de software.
Responsable del procedimiento: Administrador de Servidor/Soporte Local/ Gerencia de Sistemas.

Tiempo estimado: **2** días

No.	EVENTO / ACTIVIDAD	Responsable
1	Verificación de falla del software (Sistema operativo, servicios de base de datos, networking, configuraciones, etc.)	DBA
2	Si la falla de software se puede solventar internamente, se realiza lo siguiente:	
	2.1. Se corrige el problema de software, servicios de Base de Datos, o sistema operativo.	DBA
	2.2. En caso de ser necesario, se verifica la configuración del servidor para la carga de los respaldos de los datos y software	DBA/ Técnico en Servidores
	2.3. Prueba y puesta en operación del Servidor de Base de Datos.	DBA
3	Si la falla de software no se puede solventar internamente, se realiza lo siguiente:	
	3.1 Se verifica que el contrato de soporte técnico externo se encuentre vigente.	DBA / GSIS / GII
	3.2 Las Gerencias de Sistemas Registrales, Administrativos Financieros, Catastrales y Registrales, notifican a la Gerencia de Infraestructura Informática (GII) que se requerirá de soporte técnico externo.	GSR, GSAF, GSCR
	3.3. Se comunica inmediatamente con el proveedor o la empresa de soporte de software, para que proporcione la asesoría adecuada para resolver el problema, con base al contrato con el proveedor del software.	Técnico en Servidores
	3.4. Se preparan los respaldos de datos y del software instalado y de las Bitácoras de configuración correspondientes, para su posterior instalación.	Técnico de Resguardo de Datos
	3.5. Se realizan las acciones pertinentes de acuerdo con la asesoría proporcionada por el proveedor o la empresa de soporte de software.	DBA/ Técnico en Servidores
	3.6. En caso de ser necesario se bajan los respaldos de datos y del software instalado en el servidor.	Técnico de Resguardos
	3.7. Prueba y puesta en operación de la aplicación en el servidor de producción.	DBA

CÓDIGO DTI-PP-BK-01

Nombre del procedimiento: Falla de Equipo de Respaldo.

Responsable del procedimiento: Técnico de Resguardo de Datos/ Gerencia de Infraestructura Informática.

Tiempo estimado:

No.	EVENTO / ACTIVIDAD	Responsable
1	Verificación de la falla del dispositivo de respaldo	Técnico de Resguardo de Datos
2	Se activa el procedimiento de recuperación por falla en equipo de Respaldo.	Técnico de Resguardo de Datos/ Proveedor externo
3	En caso que la reparación vaya a demorar menos de una semana ir al paso 3.1; de lo contrario ir al paso 3.2	Técnico de Resguardo de Datos
	3.1 Si envía el respaldo al disco duro de backup que tiene cada servidor de respaldo y posteriormente se pasa a cinta.	Técnico de Resguardo de Datos
	3.2 Se verifica la existencia y disponibilidad de una unidad de backup, se prepara y se envía al lugar en donde se necesita.	Técnico de Resguardo de Datos
4	Al recibirse la unidad de respaldo reparada, se procede de la forma siguiente:	Técnico de Resguardo de Datos
	4.1 Se prueba la unidad de respaldo recibida.	Técnico de Resguardo de Datos
	4.2 Se verifica la configuración del equipo de respaldo para su funcionamiento con el software.	Técnico de Resguardo de Datos
	4.3 Se pone en operación normal el dispositivo de respaldo que fue reparado.	Técnico de Resguardo de Datos
5	En caso de necesidad se realizan temporalmente los respaldos en el disco duro del servidor, posteriormente se pasan a cinta cuando es puesta en línea la unidad que se había dañado y se devuelve a la Gerencia de Infraestructura Informática la Unidad que se encontraba en carácter de préstamo.	Técnico de Resguardo de Datos

CÓDIGO DTI-PP-BK-02

Nombre del procedimiento: Falla de Cintas de Respaldo.

Responsable del procedimiento: Técnico de Resguardo de Datos de/Gerencia de Infraestructura Informática.

Tiempo estimado:

No.	EVENTO/ ACTIVIDAD	Responsable
1	Verificación de la falla del medio de almacenamiento (Cinta) 1.1 Si la cinta es nueva, se reclama la garantía.	Técnico de Resguardo de Datos
2	Si se desea recuperar datos y la media de almacenamiento presenta falla, se procede de la forma siguiente:	Técnico de Resguardo de Datos
	2.1 Se restauran los datos con los respaldos existentes resguardados en la caja fuerte de cada registro, e en la de la oficina central (en caso que hayan sido enviadas dichas cintas), o en la bóveda de seguridad del proveedor externo mediante contrato vigente (en caso que hayan sido enviadas dichas cintas)	Técnico de Resguardo de Datos

CÓDIGO DTI-PP-TCOM-01

Nombre del procedimiento: Falla de Switch/Routers,etc.

Responsable del procedimiento: Técnico de Telecomunicaciones de la Gerencia de Infraestructura Informática (GII) /Soporte Local.

Tiempo estimado: 24 horas

No.	EVENTO / ACTIVIDAD	Responsable
1	Si la falla no es de hardware se va al paso 4; de lo contrario se procede tal como se describe a continuación:	Técnico de Telecomunicaciones
	1.1 Si no está vigente la garantía de partes o reemplazo total, ir al paso 2.	
	1.2 Contactar al proveedor para que solucione la falla.	
	1.3 Solicitar al proveedor que instale un equipo de slmllares características como reemplazo del equipo dañado, mientras se repara el equipo de la institución. Ir al paso 6.	
	1.4 Una vez recibido el equipo reparado se procede como se describe en el paso 5.	
2	SI la DTI no se tiene un equipo de respaldo con similares características al que ha fallado, ir al paso 3.	Técnico de Telecomunicaciones
	2.1 Pedir autorización al jefe inmediato para retirar el equipo de bodega.	
	2.2 Ir al paso 6.	
3	Dado que el equipo no tiene garantía con partes y la DTI no cuenta con un equipo similar, se procede de la manera siguiente	Técnico de Telecomunicaciones
	3.1 Solicitar al proveedor un equlpo de características similares.	
	3.2 Ir al paso 6.	
4	Dado que la falla es de software se procede como sigue:	Técnico de Telecomunicaciones
	4.1 SI no está vigente la garantía ir al paso 4.5.	

	4.2 Solicitar al proveedor la reinstalación del software.	
	4.3 Configurar el equipo proporcionado por el proveedor con la configuración de respaldo.	
	4.4 Ir al paso 6.	
	4.5 Dado que ya no se tiene garantía, se procede así:	
	4.5.1 Reinstalar el software o el sistema operativo del dispositivo usando los recursos de la DTI.	
	4.5.2 Se carga la configuración de respaldo.	
	Ir al paso 6.	
5	5.1 Sustituir el equipo proporcionado por el proveedor con el reparado propiedad de la institución.	Técnico de Telecomunicaciones
	5.2 Pedir autorización al jefe administrativo de la DTI para retirar el equipo propiedad del proveedor.	
6	6.1 Configurar el equipo a poner en operación con la configuración de respaldo.	Técnico de Telecomunicaciones
	6.2 Efectuar pruebas de funcionamiento.	
	6.3 Puesta en marcha del equipo.	
	6.4 Documentar el incidente de falla.	
	6.5 Archivar documentación.	

CÓDIGO DTI-PP-TCOM-02

Nombre del procedimiento: Falla de cableado

Responsable del procedimiento: Técnico de Telecomunicaciones de la Gerencia de Infraestructura Informática (Gii) /Soporte Local.

Tiempo estimado: 24 horas

No.	EVENTO/ ACTIVIDAD	Responsable
1	Si no se trata de una falla de cableado ir al paso 3.	Técnico de Telecomunicaciones
	1.1 Verificar la falla del punto de conexión (Cableado).	
	1.2 Si la falla no se puede solventar internamente ir al paso 2.	
	1.2.1 Sustituir la parte dañada con los repuestos existentes en bodega. Ir al paso 4.	
2	Contactar al proveedor externo o al área de mantenimiento del CNR para solventar la falla. Ir al paso 4.	Técnico de Telecomunicaciones
3.	En caso de tratarse de una falla con los proveedores del servicio se procede en la forma siguiente:	Técnico de Telecomunicaciones
	3.1 Se activa el servicio de contingencia utilizando el proveedor secundario.	
4	4.1 Realizar las pruebas.	Técnico de Telecomunicaciones
	4.2 Puesta en operación del punto de la red.	
	4.3 Documentación de la falla.	
	4.4 Archivar la documentación.	

CÓDIGO DTI-PP-DES-01

Nombre del procedimiento: Negación parcial de los servicios de un Registro Departamental del CNR por causas imprevistas.

Responsable del procedimiento: Jefe de Registro Departamental/ Gerencia de Soporte Técnico (GST)

Tiempo estimado: 2 días

No.	PROCESO/ACTIVIDAD	Responsable
1	Verificación de fallas en cada una de las áreas correspondientes.	Técnico de Servidores/ Soporte Informático/ Soporte de hardware del laGST
2	2.1. Si es falla de hardware del(los) servidor(es) se activa el proceso DTI-PC-AS-01 – Puesta en operación de un servidor por falla de hardware.	Técnico de Servidores/ Soporte Informático / Soporte de hardware del laGST
	2.2. Si es falla de software del(los) servidor(es) se activa el proceso DTI-PC-AS-02 – Puesta en operación de un servidor por falla de software.	Técnico de Servidores/ Soporte Informático / Soporte de hardware del laGST
3	Si mediante las acciones anteriores no se logran restablecer el servicio. Se procede a reinstalar los servicios a utilizando los servidores de un Registro vecino según se establece en el Proceso de base DTI-PC-DES-003–Negación Total del Servicio de un Sitio por causas imprevistas –Replicación en el Registro de soporte asignado.	Técnico de Servidores/ Soporte Informático/ Soporte de hardware del laGST
	3.1 Se hacen los trámites de envío del(los) servidores para su reparación, de acuerdo con el numeral 4.5.2. del proceso DTI-PC-AS-01 – Puesta en operación de un servidor por falla de hardware.	Técnico de Servidores
	3.2 Una vez restablecido el reparado el servidor que había fallado. Se efectúan los traslados correspondientes y se retorna al modo normal de operación con los activos propios del Registro.	Soporte Informático/ Soporte de hardware del laGST

CÓDIGO DTI-PP-DES-02

Nombre del procedimiento: Negación parcial del servicio de un sitio(Registro) por causas imprevistas – Alternativas: Acceso remoto.

Responsable del procedimiento: Jefe de Registro Departamental/ Dirección de Tecnología de Información (DTI)

Requisitos: - Disposición de infraestructura mínima de soporte o Equipamiento en Registro vecino.

Tiempo estimado: 2 días

No.	PROCESO/ACTIVIDAD	Responsable
1	Si existe la posibilidad de acceso remoto local, se pone en operación en la misma localidad una configuración mínima necesaria soportar los servicios.	Soporte Informático/ Soporte de hardware del la GST/Técnico de Servidores
2	Se ponen a disposición de los usuarios los servicios ofrecidos bajo esta modalidad remota.	Técnico de Servidores/ Soporte Informático/ Soporte de hardware del laGST
3	Una vez restablecido el acceso al Sitio(Registro) que se encontraba caído, Se desactiva la configuración mínima y se retorna al modo normal de operación en las instalaciones propias del Registro.	Jefe de Registro Departamental / Dirección de Tecnología de Información (DTI)/ Soporte Informático/ Soporte de hardware del laGST

CÓDIGO DTI-PP-DES-03

Nombre del procedimiento: Negación total del servicio de un sitio por causas imprevistas –Replicación en el Registro de soporte asignado.

Responsable del procedimiento: Jefe de Registro Departamental / Dirección de Tecnología de Información (DTI)

Requisitos: - Disposición de infraestructura mínima de soporte o Equipamiento de Mega Centros Regionales (San Salvador, Santa Ana y Usulután).

- Disponibilidad de Respaldos actualizados

Tiempo estimado: 2 días

No.	PROCESO/ACTIVIDAD	Responsable
1	Se verifica que el servidor de respaldo disponga de suficiente memoria de trabajo y de disco para soportar las aplicaciones, o bien se habilita una configuración mínima de hardware para soportar los servicios del sitio caído.	Técnico de Resguardos/ Soporte Informático/ Técnico de Servidores/ Soporte de hardware del laGST
2	Se preparan las Copias del Software instalado, y las Bitácoras de configuración correspondientes, para su posterior instalación	Técnico de Resguardos/ Soporte Informático
3	Se bajan los respaldos de datos y de software instalado	Técnico en Resguardo de Datos/ Soporte Informático
4	Prueba y puesta en operación del servidor de producción.	Técnico de Servidores/ Soporte Informático/ Soporte de hardware del laGST
5	Se pone en operación los servicios del Sitio caído en el Mega Registro Regional asignado para dar soporte.	Soporte Informático/ Soporte de hardware del laGST
7	Una vez restablecido el servicio en el Sitio que se encontraba fuera de línea, se traslada los datos e información trabajada durante la contingencia a los servidores propios del sitio que se encontraba fuera de línea.	Jefe de Registro Departamental / Dirección de Tecnología de Información (DTI)/ Técnico en Resguardo de Datos/ Soporte Informático/

Elaboró	Revisó	Autorizó

CÓDIGO DTI-PP-DES-04

Nombre del procedimiento: Falla generalizada de la Plataforma Tecnológica del CNR por Desastre Natural/ Denegación Total del Servicio.

Responsable del procedimiento: Jefe de Registro Departamental/ Dirección de Tecnología de Información (DTI)

Tiempo estimado: Tiempo estimado de contingencia: 2 días

No.	PROCESO/ACTIVIDAD	Responsable
1	Verificación de la Falla en cada una de las áreas correspondientes.	Todo el Personal de la Dirección de Tecnología de la Información.
2	Se Inicia la Operación de los Planes de Contingencia de cada una de las áreas que integran la DTI, de acuerdo a la ocurrencias de falla en sus procesos críticos correspondientes, afectados por Desastre natural. Esto implica que se activen una serie de Planes Contingenciales por cada área, debido al Desastre naturales, tomando en cuenta que dentro de este escenario la infraestructura física y tecnológica de la institución queda parcialmente destruida, es decir, que se dispone de recursos mínimos para llevar a cabo las operaciones de la Institución, por lo que la mayoría de los procesos de la institución se lleven en forma manual, para su posterior digitación en los sistemas computarizados una vez se encuentren habilitados los servicios.	**Gerencia de Infraestructura Informática** / **Soporte Técnico** / **Gerencia de Sistemas.**

ANEXO V

PROCEDIMIENTO DE RECUPERACION, RESPALDO Y VERIFICACIÓN DE INFORMACIÓN

1.0 Definiciones

Cliente Interno del CNR: Son todas las personas miembros de las distintas Unidades, Departamentos, Gerencias y Direcciones que conforman el CNR.

Dispositivo para realizar respaldo: Aparato electromecánico utilizado para realizar respaldos de información desde un servidor a una cinta.

Hard Drive (HD): Disco duro.

Log: Resumen de recuperación y respaldos realizados.

Soporte Primario: Subproceso perteneciente al proceso de Tecnología de la Información, responsable de proporcionar soporte primario informático a todas las áreas del CNR.

2.0 Procedimientos

Procedimiento de Recuperación de Información

6.1 Solicitar recuperación de datos. Responsable: Áreas del CNR.

6.2 Recibir solicitud de recuperación de datos. Responsable: Soporte Informático.

6.3 Recibir solicitud de recuperación de datos, distribuye y monitorea requerimiento. Responsable: Atención al Cliente Interno.

6.5.2.1 Recibir solicitud de recuperación de información, identifica cinta con información a ser recuperada almacenada en caja fuerte o dispositivo de respaldo. Responsable: Técnico en Resguardo de Datos o Soporte Informático.

6.5.2.2 Realizar recuperación de la información. Responsable: Técnico en Resguardo de Datos o Soporte Informático.

6.5.2.3 Si la recuperación de la información no tuvo éxito, se pasa a la actividad 6.5.2.4 de lo contrario continuar con la actividad 6.5.2.17. Responsable: Técnico en Resguardo de Datos o Soporte Informático.

6.5.2.4 Si la cinta está dañada, pasar a la actividad 6.5.2.16 de lo contrario continuar con actividad 6.5.2.5. Responsable: Soporte Informático.

6.5.2.5 Si existieran problemas en la recuperación de la información, se verifica si es problema de dispositivo de respaldo o de cinta, y se hacen las reparaciones necesarias y se pasa nuevamente a la actividad 6.5.2.2. Responsable: Soporte Informático.

6.5.2.17 Revisar la información recuperada. Responsable: Soporte Informático.

6.5.2.18 Si la información recuperada es la correcta, se notifica al Cliente Interno que los datos están disponibles, de lo contrario regresar a la actividad 6.5.2.1. Responsable: Soporte Informático.

Procedimiento de Respaldo de Información

6.5 2.6 Identificar cinta para hacer el respaldo de información. Responsable: Técnico Resguardo de Datos y Soporte Informático.

6 5.2.7 Realizar respaldo de información. Esta actividad se efectúa de acuerdo a una programación preestablecida. Estos respaldos de información se clasifican en incrementales, que se realizan de lunes a viernes (se hacen a diario) y completo de datos, que se realizan el fin de semana. Responsable: Técnico en Resguardo de Datos y Soporte Informático

6.5.2.8 Si el procedimiento de respaldo finalizó satisfactoriamente, se pasa a la actividad 6.5.2.10; de lo contrario se pasa a la actividad 6.5.2.9; en ambos casos queda registrado en el LOG del Software de respaldo dicha actividad (Ver anexo No.2 adjunto a este documento). Responsable: Técnico en Resguardo de Datos y Soporte Informático.

6.5.2.9 Atender fallas ocasionadas por el dispositivo de respaldo o las cintas, fallas de conexión, realizar respaldos en disco duro (HD) y notificar (Ver anexo No. 3 adjunto a este documento) vía correo electrónico a Gerente de Infraestructura Informática, Gerente de Soporte Informático y Soporte Informático donde se originó la falla, regresar a la actividad 6.5.2.7. Responsable: Técnico en Resguardo de Datos y Soporte Informático.

6.5.2.10 Codificar y Almacenar cintas en caja fuerte. Responsable: Técnico en Resguardo de Datos y Soporte Informático.

6.5.2.11 Preparar y enviar cintas completas de datos para su respectivo almacenamiento externo (ver procedimiento DTI-PRO-009). Responsable: Técnico en Resguardo de datos.

Procedimiento de Verificación de cinta

6.5.2.12 Identificar cinta a ser verificada en forma remota, esta actividad no se hace a requerimiento del Cliente Interno, sino que se hace basado en una muestra al azar. Responsable: Técnico en Resguardo de Datos.

6.5.2.13 Realizar la recuperación de información en servidor local, y verificar si la transferencia de datos escogida es correcta del último full de datos ejecutado. Responsable: Técnico en Resguardo de Datos.

6 2 1.4 Si la verificación de cinta es correcta, se pasa a la actividad 6.5 2.16; de lo contrario se pasa a la actividad 6.5.2.15. Responsable: Técnico en Resguardo de Datos.

6.5.2.15 Atender fallas ocasionadas por el equipo de respaldo o cintas y pasar a la actividad 6.5.2.16. Responsable: Técnico en Resguardo de Datos.

6.5.2.16 Elaborar reporte de las cintas verificadas (Ver anexo No 4 adjunto a este documento) y notifica al Soporte Informático. Responsable: Técnico en Resguardo de Datos.

6 5.2.19 Recibir notificación de verificación de cintas y almacena cintas buenas en caja fuerte y desecha las cintas dañadas Responsable: Soporte Informático.

3.0 Diagrama de Flujo

El diagrama correspondiente a este procedimiento se encuentra en el Anexo 1

4.0 Documentos aplicables y/o anexos

- Diagrama de Flujo.
- Anexo 2: Reporte de respaldo de datos.
- Anexo 3: Reporte de atención de fallas.
- Anexo 4: Informe de verificación de respaldos.

Lui [illegible] de Interiano Gerente de Infraestructura Informática

Miguel Alvarenga Gerente de Soporte Técnico

Ing Rafael Rovira Director del DTI

ANEXO No. 1

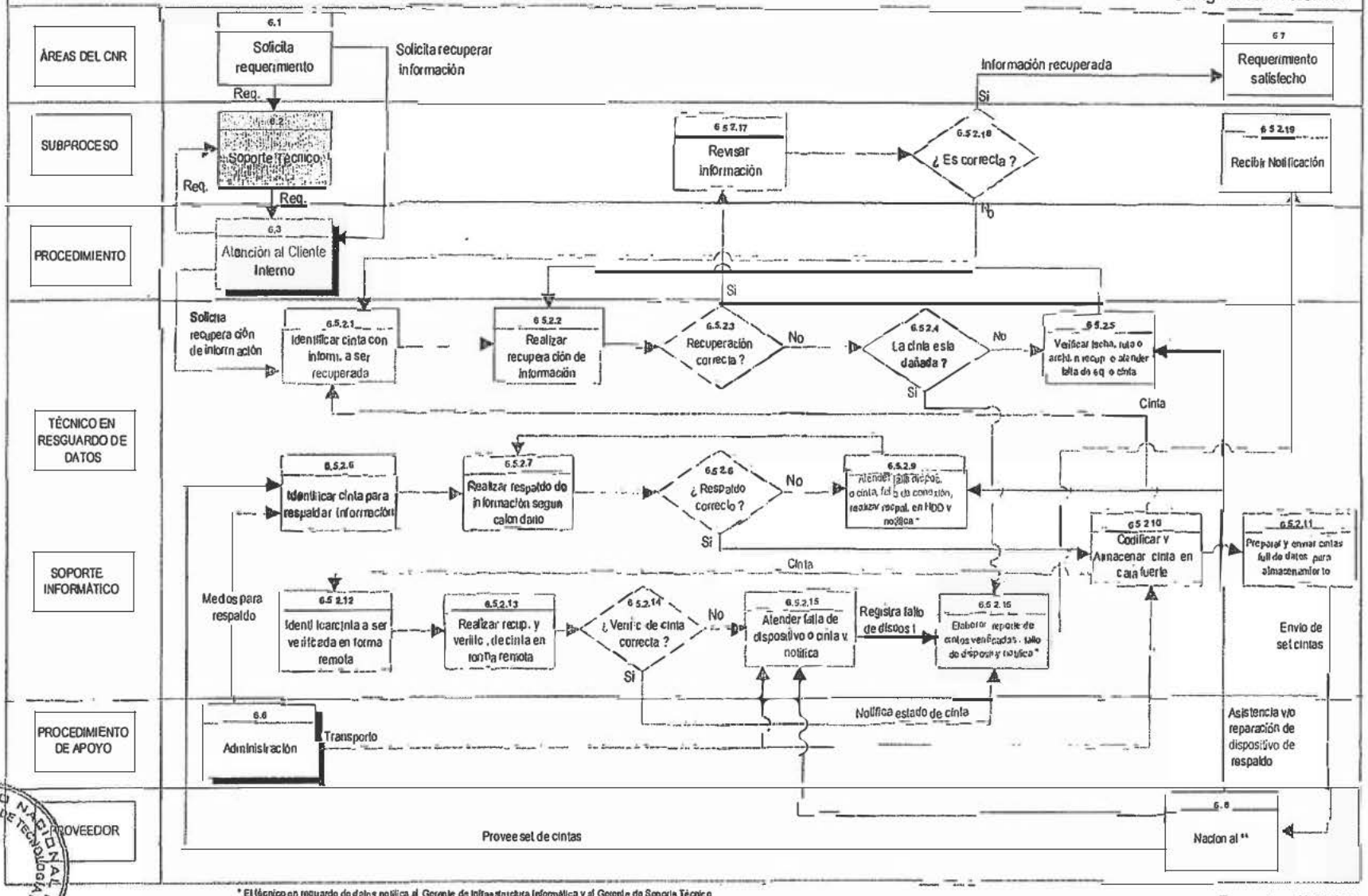
TECNOLOGÍA DE LA INFORMACIÓN

Centro Nacional de Registros (CNR)

EL SALVADOR

Código: P625 Versión: 2

MAPA DE CUARTO NIVEL: 6.5.2 RECUPERACIÓN, RESPALDO Y VERIFICACIÓN



* El técnico en resguardo de datos notifica al Gerente de Infraestructura Informática y al Gerente de Soporte Técnico.

** Los proveedores son: El de mantenimiento de equipo de respaldo y El de almacenamiento de cintas.

Formato: F0002 3

ANEXO No. 2

De:
Para:

CC:

Enviado:
Asunto:

DTI

ANEXO No. 3

CENTRO NACIONAL DE REGISTROS DIRECCIÓN DE TECNOLOGÍA DE LA INFORMACIÓN DTI

ANEXO No. 4

CENTRO NACIONAL DE REGISTROS
DIRECCIÓN DE TECNOLOGÍA DE LA INFORMACIÓN

ANEXO No.

Fecha de Vigencia: ____/____/____

HOJA DE ESPECIFICACIONES TECNICAS RESPALDOS

Horarios de Respaldos

Tipo de Servidor	Modalidad de Backup	Periodicidad	Hora Programada
		Diariamente (a	
		Diariamente a	
		Diariamente a	

Recursos asignados por Tipo de respaldos

Tipo de Respaldo	Periodicidad	Número de Cintas Estimadas

Información complementaria:

Tipo de Servidor	Ubicación	Modalidad de Backup (Periodicidad)

Elaboró	Revisó	Aprobó	Autorizó

ANEXO VI

PROCEDIMIENTO DE RESGUARDO DE CINTAS FUERA DE OFICINAS DEL CNR (DTI-PRO-009)

CENTRO NACIONAL DE REGISTROS	
Procedimiento de resguardo de cintas fuera de oficinas del CNR	
Código: DTI-PRO-009	Formato: DTI-FRM-001

1.0 Definiciones

2.0 Procedimiento

2 1 Todas las cintas que contengan los de las diferentes oficinas del CNR, deberán ser depositadas en el lugar destinado para el almacenamiento de dichas cintas
Responsable: Soporte Informático y/o Técnico en Resguardo de Datos

2.2 Previo a realizar el traslado de cintas de respaldo, se deberá llenar el formato de control, en donde se pondrá información específica de las cintas y quienes son las personas que entregan y reciben Se dará una copia ubicado en la puerta de salida de la oficina respectiva **(Ver anexo No . 1)**. Responsable: Soporte Informático y/o Técnico en Resguardo de Datos

2. 3 el técnico de resguardo de datos de la DTI irá a traer las cintas de respaldo completo de datos al lugar donde han sido almacenadas y hará un recorrido por todas las oficinas de occidente entregando dichas cintas; recibiendo a cambio, por parte del Soporte Informático, las cintas de respaldo de datos de la semana anterior, llenando el Soporte Informático el formato de control correspondiente. Dichas cintas serán transportadas por al lugar designado para su respectivo resguardo
- Para el se realizará el mismo procedimiento, con la diferencia que se ejecutará para la , y de . Responsable: Soporte Informático y/o Técnico en Resguardo de datos

2.4 Las cintas que alcancen su máximo nivel de capacidad, (respaldo completo e incrementales) , deberán ser enviadas y Responsable: Soporte Informático y/o Técnico en Resguardo de Datos

2 5 Todas las cintas a ser trasladadas, deberán ser debidamente identificadas con su código de barra y una viñeta grande, la cual tiene que contener la información abajo detallada. Responsable: Soporte Informático y/o Técnico en Resguardo de Datos

La viñeta debe contener: .

2 6 Las cintas que lleguen a su máxima capacidad, al mes actual en curso (respaldo completo), se enviarán al lugar destinado para su respectivo almacenamiento. Responsable: Soporte Informático y/o Técnico en Resguardo de Datos

2 7 Las cintas incrementales se resguardarán en l
Responsable: Soporte Informático y/o Técnico en Resguardo de Datos

Nota:

En el caso de la zona oriental, occidental, central y paracentral, el responsable de la logística de trasladar las cintas de respaldos full e incrementales, ya sea al lugar destinado para el almacenamiento o a la DTI, será el motorista designado por la DTI

3.0 Diagrama de Flujo

3 1 El diagrama correspondiente a este procedimiento se encuentra en el Anexo No 2.

Elaboró: Revisó:

Aprobó:

Ing Miguel Alvarenga (Gerente de Soporte Técnico)

Ing. Luis Interiano (Gerente de Infraestructura Informática)

Autorizó:

Ing Rafael Rovira (Director del DTI)

CENTRO NACIONAL DE REGISTROS DIRECCIÓN DE TECNOLOGÍA DE LA INFORMACIÓN DTI

Centro Nacional de Registros (CNR)

EL SALVADOR

CENTRO NACIONAL DE REGISTROS
DIRECCION DE TECNOLOGIA DE LA INFORMACION
CONTROL DE TRASLADO DE CINTAS DE RESPALDO

Anexo No. 1

No.	Nombre de Cinta	ID ArcServer	Código de Barra	Tipo de Backup	Contenido	Observaciones
1						
2						
3						
4						
5						
6						
7						
8 9						
10						
11						
12						
13						
14						
15						
16						
17						
18						

Entregó / Trasladó :	
Nombre:	
Ubicación: (Origen)	
Fecha:	
Firma:	

Recibió:	
Nombre:	
Ubicación (Destino)	
Fecha:	
Firma:	

CENTRO NACIONAL DE REGISTROS
DIRECCIÓN DE TECNOLOGÍA DE LA INFORMACIÓN
DTI

Anexo No. 2

CENTRO NACIONAL DE REGISTROS.

Código :

Centro Nacional de Registros (CNR)

EL SALVADOR

MAPA DE CUARTO NIVEL: Procedimiento de resguardo de cintas fuera de oficinas del CNR

OBJETIVO: Garantizar la seguridad de respaldo y resguardo diario de bases de datos o archivo

ALCANCE: Soporte Informático Local y Técnico en Resguardo de Datos.