RENIEC

REGISTRO NACIONAL DE IDENTIFICACIÓN Y ESTADO CIVIL

RENIEC

GUIA DE PROCEDIMIENTOS

PLAN DE CONTINGENCIA INFORMÁTICO

RESOLUCIÓN SECRETARIAL N° 124-2019-SGEN/RENIEC		
GP-445-GTI/SGSTO/005	VERSIÓN: 01	FECHA DE APROBACIÓN:
	N° PÁGINAS: 42	22 NOV. 2019

ÍNDICE

PÁG.

I. OBJETIVO

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.

Asimismo, establecer un plan de recuperación, conformación de equipos y entrenamiento para restablecer la operatividad en el menor tiempo posible de los siguientes sistemas:

a) Sistema de emisión de DNI.

b) Sistema de Registros Civiles.

c) Sistema de Trámite Documentario.

II. ALCANCE

El presente documento es administrado por la Sub Gerencia de Soporte Técnico Operativo de la Gerencia de Tecnología de la Información del RENIEC, siendo de aplicación obligatoria por el equipo de contingencias de la GTI, para atender situaciones de contingencia, para restaurar los sistemas informáticos o servicios por algún problema interno o externo que pudiera presentarse; cuya ejecución corresponde al personal responsable de dicha labor.

III. BASE LEGAL

3.1 Ley N° 26497, Ley Orgánica del Registro Nacional de Identificación y Estado Civil (RENIEC), del 12 julio de 1995 y modificatorias.

3.2 Ley N° 28716, Ley de Control Interno de las Entidades del Estado del 18 de abril de 2006 y modificatorias.

3.3 Resolución de Contraloría N° 320-2006-CG, aprueban Normas de Control Interno, del 03 de noviembre del 2006.

3.4 Resolución Jefatural N° 347-2001-INEI, aprueba la Directiva N° 018-2001-INEI/DTNP, "Normas y Procedimientos Técnicos para Garantizar la Seguridad de la Información Publicada por las Entidades de la Administración Pública", del 07 de noviembre de 2001.

3.5 Resolución Jefatural N° 073-2015/JNAC/RENIEC, aprueba la Política de Seguridad de la Información y los Objetivos de Seguridad de la Información del RENIEC, del 30 de marzo del 2015.

3.6 Resolución Jefatural N° 073-2016/JNAC/RENIEC, aprueba el Reglamento de Organización y Funciones y la Estructura Orgánica del RENIEC, del 31 de mayo de 2016 y modificatoria.

3.7 Resolución Jefatural N° 074-2016/JNAC/RENIEC, aprueba el Cuadro de Codificación y Siglas de los órganos y unidades orgánicas del RENIEC, del 14 de junio de 2016 y modificatoria.

3.8 Resolución Secretarial N° 055-2017/SGEN/RENIEC, aprueba la DI-200-GPP/001 "Lineamientos para la Formulación de los Documentos Normativos del RENIEC", sexta versión, del 28 de agosto de 2017 y modificatoria.

3.9 Resolución Gerencial N° 004-2016/GCI/RENIEC, aprueba la DI-372-OSDN/006 "Gestión de Riesgo de Seguridad de la Información" segunda versión, del 22 de noviembre de 2016.

3.10 Norma Técnica Peruana "NTP ISO/IEC 27001:2014, Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a Edición", del 01 de diciembre del 2014.

IV. DEFINICIÓN DE TÉRMINOS

4.1 Acceso

Es el proceso responsable de permitir que los usuarios hagan uso de los servicios de TI, datos u otros activos. Proceso que ayuda a proteger la confidencialidad, integridad y disponibilidad de los activos, garantizando que sólo los usuarios autorizados pueden accederlos o modificarlos.

4.2 Amenaza

Es interferir con el funcionamiento adecuado de una computadora personal, o causar la difusión no autorizada de información confiada a una computadora. Ejemplo: Fallas de suministro eléctrico, virus (malware), saboteadores o usuarios descuidados.

4.3 Ataque

Término general usado para cualquier acción o evento que intente interferir con el funcionamiento adecuado de un sistema informático, o intento de obtener de modo no autorizado la información confiada a una computadora.

4.4 Ataque Activo

Acción iniciada por una persona que amenaza con interferir el funcionamiento adecuado de una computadora, o hace que se difunda de modo no autorizado información confiada a una computadora personal. Ejemplo: El borrado intencional de archivos, la copia no autorizada de datos o la introducción de un virus (o malware) diseñado.

4.5 Ataque Pasivo

Intento de obtener información o recursos de una computadora personal sin interferir con su funcionamiento, como espionaje electrónico, telefónico o la intercepción de una red. Todo esto puede dar información importante sobre el sistema, así como permitir la aproximación de los datos que contiene.

4.6 Atención Aceptable

Es aquella que se realiza día a día y durante 8 horas diarias para atender al público que necesita el DNI y necesita de los Registros Civiles.

4.7 CID

Confidencialidad, Integridad y Disponibilidad de la información.

4.8 Continuous Access (CA)

Es un software, el cual replica la data grabada sincrónicamente a través de discos en pares, tanto discos primarios como secundarios.

4.9 Datos

Los datos son hechos y cifras que al ser procesados constituyen una información, sin embargo, muchas veces datos e información se utilizan como sinónimos. En su forma más amplia los datos pueden ser cualquier forma de información: campos de datos, registros, archivos y bases de datos, texto (colección de palabras), hojas de cálculo (datos en forma matricial), imágenes (lista de vectores o cuadros de bits), vídeo (secuencia de tramas), etc.

4.10 Emergencia

Asunto o situación imprevistos que requieren una especial atención y deben solucionarse lo antes posible. Ejemplo: La necesidad de procesamiento y balanceo de carga por sobrecarga en los sistemas actuales. o cortes de energía intempestivos.

4.11 Escenario

Un escenario es la combinación de una amenaza con una actividad. Se define como la posibilidad para que una amenaza determinada se materialice como una emergencia en un sitio determinado.

4.12 Golpe (Breach)

Es una violación con éxito de las medidas de seguridad, como el robo de información, el borrado de archivos de datos valiosos, el robo de equipos, PC, etc.

4.13 Grupo Electrógeno

Es una máquina que mueve un generador eléctrico a través de un motor de combustión interna. Son comúnmente utilizados cuando hay déficit en la generación de energía eléctrica de algún lugar, o cuando son frecuentes los cortes en el suministro eléctrico.

4.14 Incidente

Evento único o una serie de eventos no deseados o inesperados que compromete las operaciones y amenazan la seguridad de la información del proceso o del área. Cuando se produce un ataque o se materializa una amenaza, tenemos un incidente, como por ejemplo las fallas de suministro eléctrico o un intento de borrado de un archivo protegido

4.15 Infraestructura Informática

Agrupa y organiza el conjunto de elementos tecnológicos que integran un proyecto, soportan las operaciones de la organización o sustentan una operación. Conforma los distintos elementos de hardware y software empleados para optimizar la productividad y el funcionamiento, así como mejorar la seguridad de la información.

4.16 Integridad

Se refiere a que los valores de los datos se mantengan tal como fueron puestos intencionalmente en un sistema. Las técnicas de integridad sirven para prevenir que existan valores errados en los datos provocados por el software de la base de datos, por fallas de programas, del sistema, hardware o errores humanos. El concepto de integridad abarca la precisión y la fiabilidad de los datos, así como la discreción que se debe tener con ellos.

4.17 Metroclúster

Es una configuración que permite crear un clúster entre dos arrays de almacenamiento ubicados en distintos lugares. Un clúster MC/ServiceGuard es un grupo de servidores conectados por red, que tienen redundancia en software (SW) y hardware (HW), suficientes para que el fallo de uno de los componentes del clúster no interrumpa de forma significativa el servicio informático proporcionado por estos ordenadores.

4.18 Plan de Contingencia

Es un conjunto de procedimientos alternativos a la operatividad normal de la institución, cuya finalidad es la de permitir el funcionamiento de ésta, aun cuando alguna de sus funciones deje de hacerlo debido algún incidente, desastre o sabotaje tanto interno como ajeno a la institución.

4.19 Privacidad

Se define como el derecho que tienen los individuos y organizaciones para determinar, ellos mismos, a quién, cuándo y qué información referente a ellos serán difundidos o transmitidos a otros.

4.20 RAID

Arreglo Redundante de Discos Independientes, hace referencia a un sistema de almacenamiento de datos que utiliza múltiples unidades de almacenamiento de datos: HDD (discos duros) o SSD (disco duro en estado sólido) entre los que se distribuyen o replican los datos.

4.21 Respaldo

Es la obtención de la copia de los datos en otro medio magnético, de tal modo que a partir de dicha copia es posible restaurar el sistema. Por lo tanto, los respaldos se hacen con regularidad, frecuencia preestablecida a efectos de hacerlos correctamente.

4.22 Servidor de Aplicaciones

Es el Servidor que proporciona servicios de aplicación a las computadoras cliente como parte de una aplicación de tres niveles, que consta de un servidor gráfico de interfaz de usuario (GUI), un servidor de aplicaciones (lógica empresarial) y un servidor de bases de datos y transacciones.

4.23 Servidor de Archivos

Es el servidor en una red de ordenadores cuya función es permitir el acceso remoto a archivos almacenados en él o directamente accesibles por este.; almacena y distribuye diferentes tipos de archivos informáticos entre los clientes de una red. Algunos protocolos de servidores de archivos son: SMB/CIFS (en Windows), Samba (en Unix) y NFS (en Unix). En internet, estos programas utilizan a menudo el FTP.

4.24 Servidor de Base de Datos

Es el servidor que provee servicios de base de datos a otros programas, es definido por el modelo cliente-servidor. Los sistemas gestores de bases de datos; (DBMS) son un tipo de software muy específico, que sirve de interfaz entre la base de datos, el usuario y las aplicaciones que la utilizan.

4.25 Servidor Blade

Se trata de un chasis o carcasa que alberga múltiples servidores físicos o cuchillas dentro de él. Todo el sistema está a menudo montado en bastidor. Cada Servidor Blade es una delgada "tarjeta" que contiene sólo microprocesador, memoria y buses. Los servidores de tecnología Blade hacen uso de herramientas que permiten generar imágenes del Sistema Operativo (SO) instalado localmente, imagen que puede ser restaurada de ocurrir imprevistos a nivel Hardware o SO.

4.26 Seguridad

Se refiere a las medidas tomadas con la finalidad de preservar los datos o información que, en forma no autorizada, sea accidental o intencionalmente, puedan ser modificados, destruidos o simplemente divulgados.

4.27 Situación de Contingencia

Se presenta cuando se suspende o inhabilita la operatividad de cualquiera de los sistemas considerados críticos, en el Centro de Cómputo de Producción - Sede Operativa, durante un plazo estimado como NO aceptable para los objetivos de disponibilidad del servicio. El tiempo promedio de respuesta en una Situación de Contingencia es relativo y variable, debido a diversos factores internos y/o externos que afecten la operatividad del servicio.

4.28 UPS (Uninterruptible Power Supply)

Son llamados en español SAI (Sistema de Alimentación Ininterrumpida). Es un dispositivo que, gracias a sus baterías u otros elementos almacenadores de energía, puede proporcionar energía eléctrica por un tiempo limitado a todos los dispositivos que tenga conectados.

4.29 Urgencia

Es una medida de cuánto tiempo pasará hasta que un incidente, problema o cambio tenga un impacto significativo en la organización. Ejemplo: Calculo del tiempo necesario de procesamiento adicional por parte del equipo principal por mantenimiento, aniegos. necesidad de corte de energía, accidentes o situaciones imprevistas.

V. DISPOSICIONES GENERALES

La Gerencia de Tecnología de la Información (GTI), es responsable de velar por el cumplimiento del presente documento normativo.

El equipo del Plan de Contingencia, es liderado por el Gerente de Tecnología de la Información (GTI), y está conformado orgánicamente por las SGSTO, SGOT, SGGBD y SGIS, que se encargaran operativamente de la gestión de la contingencia. Ver Anexo N° 03.

5.1 EL EQUIPO DE PLAN DE CONTINGENCIA

5.1.1 SUB GERENTE DE SOPORTE TÉCNICO OPERATIVO - SGSTO

a. Coordina, dirige y decide respecto a acciones o estrategias a seguir en un escenario de contingencia dado.
b. Toma la decisión de activar el Plan de Contingencia.
c. Notifica y comunica a la GTI acerca del incidente, posibles problemas ocurridos durante la ejecución del plan y el progreso de la recuperación.
d. Supervisa la recuperación de la infraestructura de las TICs en el Centro de Cómputo de Contingencia.
e. Coordina con la Sub Gerencia de Servicios Generales y la Oficina de Seguridad y Defensa Nacional, la evaluación del daño físico en la sede de producción.
f. Supervisa el cumplimiento de los controles que permitan asegurar el CID de la información durante la situación de la emergencia y recuperación.
g. Plantea soluciones alternativas en sistemas, procesos, procedimientos ante situaciones de contingencia.

SUPERVISOR DE CENTRO DE CÓMPUTO

a. Asegura que toda la documentación relacionada a estándares, operaciones, registros vitales, programas de aplicación, se encuentren actualizados y almacenados en un ambiente seguro.
b. Evalúa el daño en la plataforma tecnológica básica del RENIEC, coordina las acciones necesarias para su recuperación en el Centro de Cómputo de Contingencia y su restauración a condiciones normales.

c. Supervisa el funcionamiento de los equipos de cómputo principales y de los demás recursos informáticos del centro de cómputo.

d. Recupera las cintas de respaldo del almacenaje externo y entrega al sitio de recuperación (traslado y custodia de cintas backups).

e. Administración, ejecución y recuperación de los backups de las bases de datos del RENIEC.

ADMINISTRADORES DE SERVIDORES

A) ADMINISTRADOR DE APLICACIONES Y ARCHIVOS

a. Mantiene actualizado los procedimientos de operaciones de los servidores de aplicaciones del Sistema del RENIEC.
b. Supervisa y administra la operatividad de los servidores virtuales de las aplicaciones de los sistemas informáticos del RENIEC.
c. Monitorea el rendimiento de los servidores blade en base a parámetros de desempeño de procesadores, memoria, input/output, entre otros.
d. Contacta a los proveedores para el reemplazo de algún componente de los sistemas afectados: servidores blades.

B) ADMINISTRADOR DE INFRAESTRUCTURA Y EQUIPOS DE ALMACENAMIENTO

a. Asegura la disponibilidad de los servidores y equipos de almacenamiento, mediante la administración y configuración del clúster.
b. Monitorea la funcionalidad del Metroclúster y su correcta sincronización.
c. Supervisa el funcionamiento de los equipos servidores físicos, su conexión con los sistemas de almacenamiento y con la red de datos.
d. Ejecuta el plan de contingencia a nivel infraestructura.
e. Contacta a los proveedores para el reemplazo de algún componente de los sistemas afectados: storages, librerías de backup.

C) COMITÉ DE PRUEBAS

El Comité de Pruebas es liderado por el Gerente de Tecnología de la Información (GTI) el mismo que puede ser delegado al Coordinador PCI quien cumple las funciones del Gerente de TI para estos casos de Contingencia según el anexo N° 03.

Tiene asignadas las siguientes responsabilidades:

a) Elaborar el Plan de Pruebas, supervisar y dar apoyo durante la ejecución de las pruebas y garantizar la ejecución de las mismas en los tiempos planeados.
b) Registrar los resultados de las pruebas y participar activamente en las pruebas a los sistemas de aplicación críticos.
c) Apoyar al personal de las líneas de negocio involucradas en la ejecución de las pruebas.
d) No importa cuán bien diseñado y planificado parezca el Plan de Contingencia, una prueba realista puede revelar las áreas que requieren mayor atención. Si los resultados de la prueba resultan sin defectos, se debe examinar la adecuación y realismo de las pruebas.
e) La mayoría de los componentes del plan deben ser probados y actualizados basándose en los resultados de cada prueba. Es importante que cada componente sea probado individualmente. Las pruebas pueden ser disruptivas,

por tanto, se requiere el apoyo por parte de la Alta Dirección para asegurar la disponibilidad de una cantidad suficiente de recursos.

5.1.2 SUB GERENTE DE GESTIÓN DE BASE DE DATOS – SGGBD

a. Garantiza la integridad, confiabilidad y seguridad en el acceso y modificación de la base de datos del RENIEC.
b. Administra y supervisa componentes de acceso a datos y los servicios en línea.
c. Participa en la elaboración de planes de seguridad y contingencia de los sistemas de información.

A) ADMINISTRADOR DE BASE DE DATOS

a. Administra el funcionamiento de la Base de Datos de producción.
b. Levanta los servicios de Base de Datos, con la data restaurada, válida, íntegra, probada y disponible para los usuarios, en coordinación con los administradores de servidores.

5.1.3 SUB GERENTE DE INGENIERÍA DE SOFTWARE – SGIS

a. Administra los proyectos informáticos orientados a la satisfacción de las necesidades del usuario.
b. Organiza, supervisa y designa los equipos de proyectos informáticos.

A) JEFE DE PROYECTOS DE APLICACIONES

a. Administra la documentación actualizada de los proyectos informáticos a cargo: Lenguaje o Paquete con el que fue creado el Sistema, programas que lo conforman: programas fuentes, de objetos, rutinas, macros, etc. El volumen de los archivos que trabaja el Sistema. El volumen de transacciones diarias, semanales y mensuales que maneja el sistema.
b. Diagrama, esquematiza y actualiza el catálogo de servicios, donde muestra dependencias detallando URLs de acceso y datos de configuración de las aplicaciones o sistemas de la institución.
c. Asegura el correcto funcionamiento de los diferentes sistemas de aplicación una vez restablecidas las operaciones tecnológicas en el CD Contingencia.
d. Define las actividades de recuperación para los casos de pérdida de información y/o contingencia.
e. Establece los requerimientos del sistema operativo, archivos utilitarios, librerías y documentación indispensable para la operatividad de los aplicativos.
f. Valida con el usuario del negocio acerca del adecuado desempeño de las aplicaciones posterior al restablecimiento de las operaciones en el Centro de Datos de Contingencia.

5.1.4 SUB GERENTE DE OPERACIONES TELEMÁTICAS - SGOT

a. Gestiona, administra y supervisa la infraestructura de telecomunicaciones a nivel nacional.
b. Asegura la operatividad de la conectividad y seguridad de la red de datos del Sistema de la institución.

c. Participa en la ejecución del plan de contingencia de los sistemas y recursos informáticos.

A) NETWORKING

a. Gestiona las diferentes herramientas de análisis de tráfico a fin de efectuar un adecuado diagnóstico de la operación y crecimiento de las redes de transmisión de datos.
b. Mantiene actualizado el diagrama de conexiones de dispositivos, diagrama alterno y el inventario de equipos de telecomunicaciones a ser usado en situaciones de contingencia.

B) SEGURIDAD INFORMÁTICA

a. Administra los servicios de intercambio de información, del acceso a equipos de cómputo, de la transferencia de archivos y del respaldo de la información.

C) INFRAESTRUCTURA

a. Asegura la disponibilidad de la infraestructura de telecomunicaciones a nivel nacional
b. Ejecuta el plan de contingencia relacionada con la infraestructura de telecomunicaciones

VI. DESCRIPCIÓN DE PROCEDIMIENTOS

6.1 SITUACIÓN ACTUAL DE LOS SISTEMAS DNI, REGISTROS CIVILES Y TRÁMITE ADMINSTRATIVO

6.1.1 SITUACIÓN ACTUAL DEL SISTEMA DNI

- Los centros de cómputo cuentan con una infraestructura informática de última generación, tanto para servidores de cómputo, unidades de almacenamiento, como para respaldo de información, los cuales interactúan con el sistema del DNI. Ver Anexo N° 01.
- El RENIEC cuenta con tres (03) Centro de Datos CD, de los cuales dos (02) se encuentran ubicados el Sistema del DNI:
  - Sede Operativa - Producción
  - Sede Administrativa - Contingencia

  Ambos están unidos por una red SAN extendida, la cual sirve de plataforma para las soluciones de "Replicación de Datos" y "Clúster de Aplicaciones". Anexo N° 02.
- Físicamente la data se encuentra en el Sistema de Almacenamiento (Storage). La Base de Datos (BD) del sistema del DNI se encuentra en un servidor HP SUPERDOME SERVER SD32B, con Sistema Operativo (SO) HP-UX v.11.31.
- Los Storages configurados para la replicación de datos se describen en el cuadro siguiente.

SITE	DESCRIPCIÓN	SEDE
Producción	Funciona como	Operativa

	Primario	
Contingencia	Funciona como Alterno	Administrativa

- Los volúmenes asignados se crean de acuerdo a las necesidades de crecimiento de la BD, con un nivel de Raid5, con discos de paridad los cuales son utilizados para reconstruir la data de bloques erróneos de discos.
- La Replicación de Datos (RD) a través del Arreglo de Discos, es mediante un software llamado Continous Access (CA), el cual replica la data a través de discos en pares, tanto discos primarios como secundarios. El estado óptimo de cada réplica es pair. La RD es grabada sincrónicamente desde el Sistema de Almacenamiento Site Producción al otro Sistema de Almacenamiento Site Contingencia.
- Las aplicaciones y subsistemas del clúster se agrupan en paquetes. Estos son las unidades básicas del clúster en los que se agrupan todos los recursos hard/soft que se necesitan para el funcionamiento de una aplicación.
- En caso falle un nodo, red o servicio, MC/ServiceGuard transfiere de forma automática, el control de todos los recursos del sistema que forman un paquete, para que se ejecuten en otro nodo del clúster con una interrupción mínima.
- El RENIEC dispone de una plataforma de respaldo y recuperación de datos, con la capacidad de hacer el respaldo en caliente y con el sistema en producción. Anexo N° 02.
- En el siguiente cuadro se describen las características del hardware de los servidores del Sistema del DNI.

DESCRIPCIÓN	SERVIDORES DEL SISTEMA DEL DNI		
	BASE DE DATOS	APLICACIONES	RESPALDO DE BASE DE DATOS
PROCESADORES	12	06	08
TIPO DE PROCESADOR	Intel(R) Itanium 2 9100 1.6 GHz, 24 MB	Intel(R) Xeon 2.69 Ghz.	Intel(R) Itanium 2 9100 1.6 GHz, 24 MB
MEMORIA RAM	143.81 GB	14 GB	127.87GB
DISCO	68 GB	50 GB	68 GB

6.1.2 SITUACIÓN ACTUAL DEL SISTEMA DE RRCC

- El RENIEC cuenta con tres (03) Centros de cómputo (CD), de los cuales dos (02) se encuentran ubicados el Sistema de RRCC:
  - Sede Operativa - Producción
  - Sede San Borja - Producción

Ambos están unidos por una red SAN extendida, la cual sirve de plataforma para las soluciones de "Replicación de Datos" y "Clúster de Aplicaciones". Anexo N° 2A.

- Físicamente la data se encuentra en el Sistema de Almacenamiento (Storage). La Base de Datos (BD) del sistema del RRCC se encuentra en un servidor HP SUPERDOME2 32S, con Sistema Operativo (SO) HP-UX v.11.31.
- Los Storages configurados para la replicación de datos se describen en el cuadro siguiente.

SITE	DESCRIPCIÓN	SEDE
Producción	Funciona como Primario	Operativa
Producción	Funciona como Primario	San Borja

- Los volúmenes asignados se crean de acuerdo a las necesidades de crecimiento de la BD, con un nivel de Raid5, con discos de paridad los cuales son utilizados para reconstruir la data de bloques erróneos de discos.
- La Replicación de Datos (RD) a través del Arreglo de Discos, es mediante un software llamado Oracle RAC (Real Application Cluster).
- El software del Oracle RAC maneja el acceso a los datos, los cambios en los datos son coordinados entre las instancias y cada instancia ve imágenes consistentes de la BD. El Interconnect del clúster permite que las instancias se pasen entre ellas información de coordinación e imágenes de los datos.
- La RD es grabada sincrónicamente desde el Sistema de Almacenamiento Site Producción (Sede Operativa) al otro Sistema de Almacenamiento Site Producción (Sede San Borja). La réplica de la data es a través de discos en pares, tanto discos primarios como secundarios. El estado óptimo de cada réplica es pair.
- La arquitectura RAC basada en una infraestructura compartida, asegurando una alta disponibilidad, escalabilidad y agilidad para cualquier aplicación. En el caso de que un nodo quede inutilizado, la aplicación continúa accediendo a los datos vía el resto de las instancias disponibles, lo que permite que los usuarios y aplicaciones se beneficien de la potencia de procesamiento de múltiples máquinas.
- El RENIEC dispone de una plataforma de respaldo y recuperación de datos, con la capacidad de hacer el respaldo en caliente y con el sistema en producción. Anexo N° 2A.
- En el siguiente cuadro se describen las características del hardware de los servidores del Sistema del RRCC.

DESCRIPCIÓN	SERVIDORES DEL SISTEMA DE RRCC		
	BASE DE DATOS	APLICACIONES	RESPALDO DE BASE DE DATOS
PROCESADORES	04	04	04
TIPO DE PROCESADOR	Intel(R) Itanium (R) 9350	Intel(R) Xeon 2.69 Ghz.	Intel(R) Itanium (R) 9350

	1.73 GHz, 24 MB		1.73 GHz, 24 MB
MEMORIA RAM	511.58 GB	16 GB	511.58 GB
DISCO	300 GB	30 GB	300 GB

6.1.3 SITUACIÓN ACTUAL DEL SISTEMA DE TD.

- El RENIEC cuenta con tres (03) centros de cómputo, de los cuales dos (02) se encuentran ubicados el Sistema de TD:
  - Sede Operativa - Producción
  - Sede Administrativa - Contingencia

  Ambos están unidos por una red SAN extendida, la cual sirve de plataforma para las soluciones de "Replicación de Datos" y "Clúster de Aplicaciones". Anexo N° 02.
- Físicamente la data se encuentra en el Sistema de Almacenamiento (Storage). La Base de Datos (BD) del sistema de TD se encuentra en un servidor HP SUPERDOME SERVER SD32B, con Sistema Operativo (SO) HP-UX v.11.31.
- Los Storages configurados para la replicación de datos se describen en el cuadro siguiente.

SITE	DESCRIPCIÓN	SEDE
Producción	Funciona como Primario	Operativa
Contingencia	Funciona como Alterno	Administrativa

- Los volúmenes asignados se crean de acuerdo a las necesidades de crecimiento de la BD, con un nivel de Raid5, con discos de paridad los cuales son utilizados para reconstruir la data de bloques erróneos de discos.
- La Replicación de Datos (RD) a través del Arreglo de Discos, es mediante un software llamado Continuos Access (CA), el cual replica la data a través de discos en pares, tanto discos primarios como secundarios. El estado óptimo de cada réplica es pair. La RD es grabada sincrónicamente desde el Sistema de Almacenamiento Site Producción al otro Sistema de Almacenamiento Site Contingencia.
- Las aplicaciones y subsistemas del clúster se agrupan en paquetes. Estos son las unidades básicas del clúster en los que se agrupan todos los recursos hard/soft que se necesitan para el funcionamiento de una aplicación.
- En caso falle un nodo, red o servicio, MC/ServiceGuard transfiere de forma automática, el control de todos los recursos del sistema que forman un paquete, para que se ejecuten en otro nodo del clúster con una interrupción mínima.
- El RENIEC dispone de una plataforma de respaldo y recuperación de datos, con la capacidad de hacer el respaldo en caliente y con el sistema en producción. Anexo N° 02.

- En el siguiente cuadro se describen las características del hardware de los servidores del Sistema de TD.

DESCRIPCIÓN	SERVIDORES DEL SISTEMA DE TRAMITE DOCUMENTARIO (TD)		
	BASE DE DATOS	APLICACIONES	RESPALDO DE BASE DE DATOS
PROCESADORES	04	04	04
TIPO DE PROCESADOR	Intel(R) Itanium 2 9000 1.6 GHz, 24 MB	Intel(R) Xeon 2.70 Ghz.	Intel(R) Itanium 2 9000 1.6 GHz, 24 MB
MEMORIA RAM	23.93 GB	08 GB	23.93 GB
DISCO	73.4 GB	32 GB	73.4 GB

6.2. DESCRIPCIÓN DEL PROCEDIMIENTO DE CONTINGENCIA

Una situación de contingencia es aquella que suspende o inhabilita total o parcialmente la operatividad de los sistemas informáticos de la institución para atender al público. Entre ellos están el Sistema de DNI, el Sistema de Registros Civiles y el Sistema de Trámite Documentario. Por ello, se definen los escenarios que pueden ocasionar problemas en el centro de cómputo considerado área crítica para el funcionamiento de los sistemas en mención.

6.2.1 ESCENARIO 1: CORRUPCIÓN DEL SISTEMA OPERATIVO (SO)

Puede presentarse en los servidores de Aplicaciones, archivos o de Base de Datos	
CAUSA	**CONSECUENCIAS**
a. Perdida de datos, corrupción física o lógica o borrado involuntario de archivos o programas del SO	a. Imposibilidad de acceder al SO. b. La inoperatividad del SO impide la normal operación de la Base de Datos o Software de Aplicación. c. Servicios del Sistema inoperativos.
ACTIVIDADES A SEGUIR	
a. Recibir notificación "error en el Sistema". b. Verificar la operatividad a nivel infraestructura, aplicaciones y base de datos (BD) de los servidores del Sistema. c. Identificar el error a nivel SO en los servidores de: Base de Datos, Aplicaciones y/o Archivos. d. Activar el Plan de Contingencia.	

Verificar operatividad del Sistema.
RESPONSABLE: SUBGERENCIA DE SOPORTE TÉCNICO OPERATIVO (SGSTO)

CONTINGENCIA A NIVEL SERVIDORES	
BASE DE DATOS	**APLICACIONES Y ARCHIVOS**
Restauración de la imagen backup del SO correspondiente a este servidor.	Restauración del backup realizado al servidor de Aplicaciones y servidor de Archivos en el centro de cómputo de Producción.

6.2.2 ESCENARIO 2: CORRUPCIÓN DE DATOS

La corrupción de datos en la Base de Datos (datafile) y/o Software de Aplicación.	
CAUSA	**CONSECUENCIAS**
a. Pérdida de datos, corrupción física o lógica o borrado involuntario de archivos de la Base de Datos y/o Software de Aplicación.	a. Imposibilita el acceso de los usuarios al Sistema. **b.** Servicios del Sistema inoperativos.
ACTIVIDADES A SEGUIR a. Recibir notificación "error en el System". b. Verificar la operatividad a nivel Base de Datos y Software de Aplicaciones en los servidores del Sistema. c. Identificar el error a nivel Datos (datafile) en la Base de Datos y en las Aplicaciones. d. Activar el Plan de Contingencia. e. Verificar operatividad del Sistema	
RESPONSABLE: SUBGERENCIA DE SOPORTE TECNICO OPERATIVO (SGSTO) Y SUBGERENCIA DE GESTION DE BASE DE DATOS (SGGBD)	

CONTINGENCIA A NIVEL SERVIDORES		
BASE DE DATOS		**APLICACIONES Y ARCHIVOS**
OPCIÓN 01	OPCIÓN 02	Restauración del backup realizado al servidor de Aplicaciones y servidor de Archivos en el centro de cómputo (CD) de
Levantar los servicios del Metroclúster, para redireccionar la BD en un servidor del centro de cómputo (CD) de Contingencia, el cual cuenta con los mismos	Restauración de la data, producto de los backups realizados a la BD.	

volúmenes y son replicados entre los 02 sistemas de almacenamiento con los que cuenta RENIEC en ambos centros de cómputo (CD). En el caso de Oracle RAC el direccionamiento es automático, por lo tanto, sólo se debe verificar que el servicio este activo.		Producción

6.2.3 ESCENARIO 3: FALLO FÍSICO

El fallo físico (hardware) puede presentarse en los sistemas de almacenamiento, en los servidores de: Base de Datos, Aplicaciones y/o Archivos.

CAUSA	CONSECUENCIAS
a. Falta de mantenimiento de la infraestructura informática del Sistema. b. Falla física de los sistemas de almacenamiento o de los servidores del sistema.	a. Imposibilidad de poner operativo el servicio de la Base de Datos y/o el Software de Aplicación. **b.** El no acceso de los usuarios al Sistema.

ACTIVIDADES A SEGUIR

a. Recibir notificación a través del sistema de alarmas.

b. Verificar operatividad a nivel Hardware en los sistemas de almacenamiento de la Base de Datos y servidores.

c. Determinar el tipo de error en el Hardware del sistema.

d. Activar Plan de Contingencia.

e. Verificar Operatividad del Sistema.

RESPONSABLE: SUBGERENCIA DE SOPORTE TÉCNICO OPERATIVO (SGSTO)

CONTINGENCIA A NIVEL SERVIDORES	
BASE DE DATOS	**APLICACIONES Y ARCHIVOS**
Levantar los servicios del Metroclúster, para re direccionar la BD en un servidor del centro de cómputo de Contingencia, el cual cuenta con los mismos volúmenes y son replicados entre los 02 sistemas de almacenamiento con los que cuenta RENIEC en ambos centros de cómputo. En el caso de Oracle RAC el direccionamiento es automático, por lo tanto, sólo se debe verificar que el	Restauración del backup realizado al servidor de Aplicaciones y servidor de Archivos en el centro de cómputo de Producción.

servicio este activo.	

6.2.4 ESCENARIO 4: INOPERATIVIDAD DEL CENTRO DE CÓMPUTO DE PRODUCCIÓN

Comprende el apagado total del Centro de Cómputo de Producción – Sede Operativa	
CAUSA a. Incidentes Internos como fallas eléctricas, incendios, aniegos, etc. b. Incidentes Externos como desastres naturales, actos terroristas entre otros.	**CONSECUENCIAS** a. Inaccesibilidad total a los servicios del sistema.
ACTIVIDADES A SEGUIR a. Recibir notificación de estado de emergencia del centro de cómputo de producción. b. Evaluar operatividad del Centro de Cómputo. c. Determinar el tipo de desastre: interno o externo. d. Declarar Centro Cómputo de Producción Inoperativo. e. Activar el Plan de Contingencia. f. Verificar Operatividad del Sistema.	
RESPONSABLE: SUBGERENCIA DE SOPORTE TÉCNICO OPERATIVO (SGSTO)	

CONTINGENCIA A NIVEL SERVIDORES	
BASE DE DATOS	**APLICACIONES Y ARCHIVOS**
Levantar los servicios del Metroclúster, para re direccionar la BD en un servidor del centro de cómputo (CD) de Contingencia, el cual cuenta con los mismos volúmenes y son replicados entre los 02 sistemas de almacenamiento con los que cuenta RENIEC en ambos centros de cómputo (CD). En el caso de Oracle RAC el direccionamiento es automático, por lo tanto, sólo se debe verificar que el servicio este activo.	Activar el servidor de Aplicaciones y servidor de Archivos en el centro de cómputo (CD) de Contingencia.

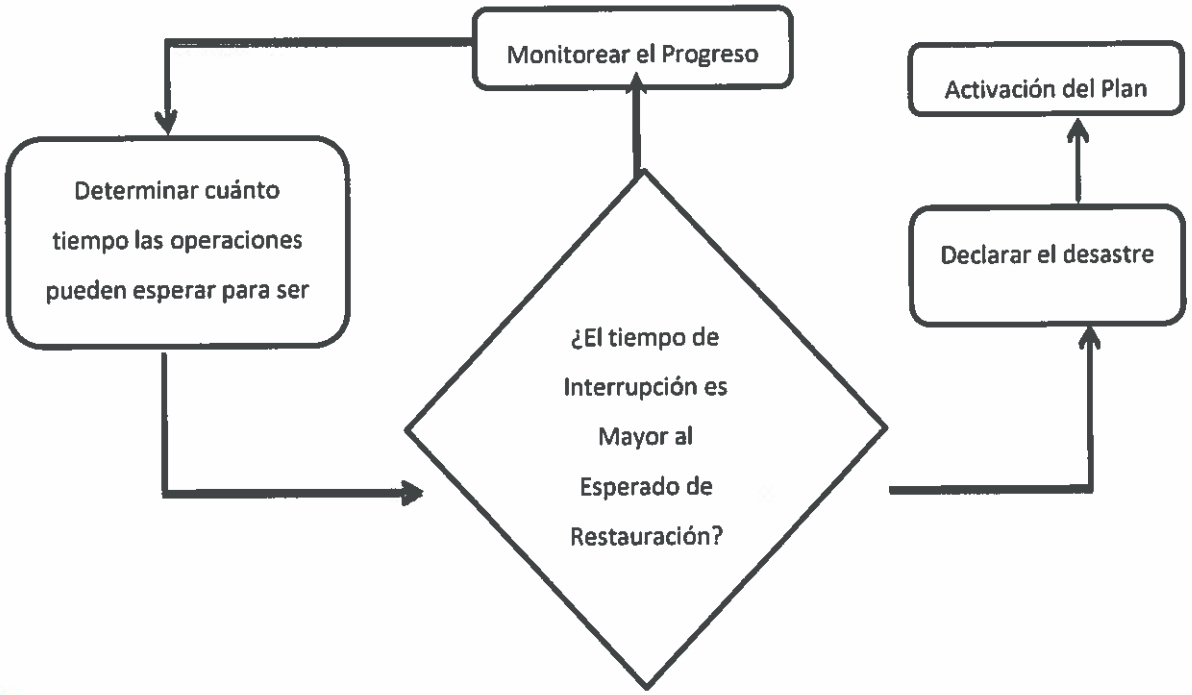
6.3 PROCEDIMIENTO DE ACTIVACIÓN DEL PLAN

Este procedimiento tiene como objetivo evaluar el tipo de contingencia al cual se vería enfrentado el Centro de Datos (CD) Primario del RENIEC y tomar las acciones que correspondan en caso de una situación de emergencia o un desastre.

El Equipo de Evaluación del Desastre es conformado por:

a) Subgerente de Soporte Técnico Operativo (SGSTO)
b) Subgerente de Gestión de Base de Datos (SGGBD)
c) Subgerencia de Operaciones Telemáticas (SGOT)
d) Subgerencia de Ingeniería de Software (SGIS)

El siguiente diagrama muestra los criterios que deberán ser usados para activar el Plan de Contingencia:



Debe notarse que una interrupción no es solamente un evento que reduce la efectividad de los sistemas, es un evento extraordinario que causa una pérdida de procesos de negocio clave y tiene un impacto alto en la Institución.

En una situación de emergencia, se deberá proceder de la siguiente manera:

N°	Acción	Descripción	Responsable	Referencia
1	Notificar emergencia	Cuando se presente una situación de emergencia, esta deberá ser notificada al Coordinador del Plan de Contingencia. Si la persona que detecta la emergencia no puede contactarse con el responsable, entonces deberá notificar uno a uno a los miembros del Equipo del Plan de Contingencia hasta poder contactarse con algunos de ellos.	Trabajador Reniec	Anexo N° 03 Equipo del Plan de Contingencia

		Dependiendo del escenario.		
2	Recibir y confirmar Notificación	Cuando la notificación de una contingencia potencial es recibida, se debe obtener una descripción breve de la naturaleza del incidente y cualquier tipo de daño. Si es necesario, se debe confirmar que la notificación es verídica a través de un medio secundario	Coordinador del plan de Contingencia	Anexo N° 03 Equipo del Plan de Contingencia
3	Contactar Servicios de Emergencia	Si la situación lo amerita, se deberá efectuar el contacto con los servicios de emergencia. Dependiendo del escenario.	Coordinador del plan de Contingencia o OSDN	
4	Notificar a la seguridad del RENIEC	Notificar inmediatamente al personal de seguridad del RENIEC, dependiendo del tipo de incidente, si es de tipo físico y externo notificar al personal de seguridad física u OSDN, si es de tipo acceso al Computador o aplicaciones notificar al Administrador de seguridad informática.	Coordinador de Seguridad o OSDN	
5	Reunión de Coordinación	Coordinar una reunión a la brevedad posible con el Equipo del Plan de Contingencia, con la finalidad de hacer una evaluación preliminar de los daños. Dependiendo de la criticidad del desastre, esta reunión se puede realizar en el local del CD primario o en un lugar cercano al mismo	Coordinador del plan de Contingencia	
6	Evaluar el Incidente	Evaluar el incidente de desastre y determinar la cantidad de tiempo requerido para completar la reparación. El daño ocasionado a la infraestructura y a las instalaciones deberá ser evaluado y documentado	Equipo de Evaluación del Desastre	
7	Declarar la Contingencia	En caso que el tiempo requerido para completar la reparación de los daños sea	Coordinador del plan de	

		mayor al tiempo de recuperación requerido por el negocio, se declara la situación de emergencia y se da por activado el Plan de Contingencia	Contingencia	
8	Preparar los recursos requeridos para el CD alterno	Proveer transporte para el equipo de recuperación, personas y suministros requeridos para el restablecimiento de las operaciones en el CD alterno	Coordinador del plan de Contingencia	
9	Contactar al personal involucrado	Se deberá contactar a todos los miembros del Equipo del Plan de Contingencia que no se encuentre presentes en el momento de la declaración de la situación de emergencia. progresivamente se deberá avisar y orientar a todo el personal de la institución	Coordinador del plan de Contingencia	Anexo N° 03 Equipo del Plan de Contingencia
10	Ejecutar el Procedimiento del Plan de Contingencia	Iniciar las actividades de recuperación en el CD alterno de acuerdo a los procedimientos de recuperación definidos	Coordinador del plan de Contingencia	

6.4 ACCIONES PARA LA ACTIVACIÓN DE PROCEDIMIENTOS

Estas acciones se realizan previamente a la ejecución del procedimiento de la continuidad en RENIEC y son aplicadas y coordinadas por la Sub Gerencia de Soporte Técnico Operativo de la Gerencia de Tecnología de la Información de RENIEC.

Interrupción intempestiva:

a) Coordinar con el Sub Gerente de Soporte Técnico Operativo para la verificación, identificación y solución de la incidencia.

b) Comunicar a la Gerencia de Tecnología de la Información sobre las coordinaciones efectuadas, así como de la magnitud del incidente, para efectos de la autorización de las acciones de contingencia.

c) Coordinar con las unidades orgánicas afectadas, previa a la aplicación de las acciones de contingencia.

RENIEC en un tiempo prudencial contados desde que toma conocimiento del incidente, debe diagnosticar y determinar el tiempo estimado en el cual los servicios informáticos se encontrarán operativos o indicar que no ha culminado el diagnóstico y por consiguiente debe proceder con las acciones de contingencia, lo cual debe ser informado por la Sub Gerencia de Soporte Técnico Operativo, vía correo electrónico o telefónica, a las Subgerencias de la Gerencia de Tecnología de la Información o a la Jefatura Nacional según corresponda.

Interrupción programada:

a) La Gerencia de Tecnología de Información comunica al Sub Gerencia de Soporte Técnico Operativo la programación del día y hora de la interrupción de los servicios informáticos.

b) El Sub Gerente de Soporte Técnico Operativo coordina con las unidades orgánicas que serán afectadas.

c) La Gerencia de Tecnología de la Información publicará un comunicado en el portal RENIEC para conocimiento de las áreas usuarias con un tiempo mínimo de anticipación de 2 días útiles.

6.4.1 ACCIONES PREVIAS PARA EL SISTEMA DNI

Se identifican varias actividades previas antes de poner en práctica el Plan de Contingencia del Sistema del DNI.

SERVIDOR DE BASE DE DATOS DEL DNI

1. Verificar la operatividad de conectividad y seguridad de la red de datos del Sistema del DNI.

   Responsable: SGOT.

2. Verificar la funcionalidad del Metroclúster del DNI y la correcta sincronización de la data en el Sistema de Almacenamiento, del centro de cómputo de Contingencia.

   Responsable: SGSTO.

3. Presentar y configurar a nivel SO los nuevos volúmenes añadidos y replicados en el sistema de almacenamiento del centro de cómputo de Contingencia a servidores destinados para tal fin.

   Responsable: SGSTO.

4. Configurar la Base de Datos de Contingencia en forma automática y/o manual.

   Responsable: SGGBD.

5. Realizar procedimientos de verificación de la Base de Datos de Contingencia; levantar en modo lectura. Verificar la funcionalidad a nivel Base de Datos.

   Responsable: SGGBD.

6. Realizar procedimientos de verificación de las aplicaciones a nivel de disponibilidad de servidores virtuales y URL de las aplicaciones web.

   Responsable: SGSTO.

7. Realizar procedimientos de verificación de funcionalidad a nivel de usuario de las aplicaciones que consultan a la Base de Datos de DNI.

   Responsable: SGIS.

8. Revisar y comprobar el funcionamiento del Plan de Contingencia del Sistema de DNI, mediante la ejecución de tres (03) pruebas anuales.

   Responsable: SGSTO, SGGBD, SGIS, SGOT.

SERVIDOR DE APLICACIONES DEL DNI

1. Verificar la sincronización de los aplicativos del DNI en el sistema de almacenamiento ubicados en ambas sedes: centro de cómputo de Producción y el centro de cómputo de Contingencia.

   Responsable: SGSTO.

2. Verificar la correcta ejecución del backup, realizado al Servidor de Aplicaciones.

   Responsable: SGSTO.

3. Verificar que la dirección Url: http://sio3.reniec.gob.pe/inicio/login.do sea la indicada, como el link al cual se acceda vía web al servicio del Sistema Integrado Operativo (SIO), considerado como el aplicativo núcleo del Sistema del DNI.

   Responsable: SGSTO.

6.4.2 ACCIONES PREVIAS PARA EL SISTEMA DE RRCC

Se identifican varias actividades previas antes de poner en práctica el Plan de Contingencia del Sistema del RRCC.

SERVIDOR DE BASE DE DATOS DEL RRCC

1. Verificar la operatividad de conectividad y seguridad de la red de datos del Sistema del RRCC.

   Responsable: SGOT.

2. Verificar la funcionalidad del Oracle RAC de RRCC y la correcta sincronización de la data en el Sistema de Almacenamiento, del centro de cómputo de Sede San Borja.

   Responsable: SGGBD.

3. Presentar y configurar a nivel SO los nuevos volúmenes añadidos y replicados en el sistema de almacenamiento del centro de cómputo de Sede San Borja a servidores destinados para tal fin.

   Responsable: SGSTO.

4. Configurar la Base de Datos de Sede San Borja en forma automática y/o manual.

   Responsable: SGGBD.

5. Realizar procedimientos de verificación de la Base de Datos de Sede San Borja; levantar en modo lectura. Verificar la funcionalidad a nivel Base de Datos.

   Responsable: SGGBD.

6. Realizar procedimientos de verificación de las aplicaciones a nivel de disponibilidad de servidores virtuales y URL de las aplicaciones web.

   Responsable: SGSTO.

7. Realizar procedimientos de verificación de funcionalidad a nivel de usuario de las aplicaciones que consultan a la Base de Datos de RRCC.

   Responsable: SGIS.

8. Revisar y comprobar el funcionamiento del Plan de Contingencia del Sistema de RRCC, mediante la ejecución de tres (03) pruebas anuales.

   Responsable: SGSTO, SGGBD, SGIS, SGOT.

SERVIDOR DE APLICACIONES DEL RRCC

1. Verificar la sincronización de los aplicativos del sistema de RRCC en el sistema de almacenamiento ubicados en ambas sedes: centro de cómputo de Sede Operativa y el centro de cómputo de Sede San Borja

   Responsable: SGSTO.

2. Verificar la correcta ejecución del backup, realizado al Servidor de Aplicaciones.

   Responsable: SGSTO.

3. Verificar que la dirección Url: http://rrcc.reniec.gob.pe sea la indicada, como el link al cual se acceda vía web al servicio de RRCC.

   Responsable: SGSTO.

6.4.3 ACCIONES PREVIAS DEL SISTEMA DE TRAMITE DOCUMENTARIO

Se identifican varias actividades previas antes de poner en práctica el Plan de Contingencia del Sistema de TD.

SERVIDOR DE BASE DE DATOS DE TD

1. Verificar la operatividad de conectividad y seguridad de la red de datos del Sistema de TD.

   Responsable: SGOT.

2. Verificar la funcionalidad del Metroclúster de TD y la correcta sincronización de la data en el Sistema de Almacenamiento, del centro de cómputo de Contingencia.

   Responsable: SGSTO.

3. Presentar y configurar a nivel SO los nuevos volúmenes añadidos y replicados en el sistema de almacenamiento del centro de cómputo de Contingencia a servidores destinados para tal fin.

   Responsable: SGSTO.

4. Configurar la Base de Datos de Contingencia en forma automática y/o manual.

   Responsable: SGGBD.

5. Realizar procedimientos de verificación de la Base de Datos de Contingencia; levantar en modo lectura. Verificar la funcionalidad a nivel Base de Datos.

   Responsable: SGGBD.

6. Realizar procedimientos de verificación de las aplicaciones a nivel de disponibilidad de servidores virtuales y URL de las aplicaciones web.

   Responsable: SGSTO.

7. Realizar procedimientos de verificación de funcionalidad a nivel de usuario de las aplicaciones que consultan a la Base de Datos de TD.

   Responsable: SGIS.

8. Revisar y comprobar el funcionamiento del Plan de Contingencia del Sistema de TD, mediante la ejecución de tres (03) pruebas anuales.

   Responsable: SGSTO, SGGBD, SGIS, SGOT.

SERVIDOR DE APLICACIONES DE TD

1. Verificar la sincronización de los aplicativos de TD en el sistema de almacenamiento ubicados en ambas sedes: centro de cómputo de Producción y el centro de cómputo de Contingencia.

   Responsable: SGSTO.

2. Verificar la correcta ejecución del backup, realizado al Servidor de Aplicaciones.

   Responsable: SGSTO.

3. Verificar que la dirección Url: http://td1.reniec.gob.pe/forms/frmservlet?config=tramite sea la indicada, como el link al cual se acceda vía web al servicio de TD.

   Responsable: SGSTO.

6.5 PROCEDIMIENTO GENERAL DE RECUPERACIÓN

Este procedimiento general tiene como objetivo la activación del CD alterno para el restablecimiento de la totalidad de operaciones tecnológicas requeridas a fin de garantizar la continuidad de los procesos críticos del RENIEC identificados como resultado del análisis de impacto en el negocio.

A continuación, se detallan las acciones que conforman el procedimiento general de recuperación:

Tabla 1. Acciones generales de recuperación en casos de emergencias.

No.	Acción	Descripción	Responsable
1	Contactar al SGSTO	El SGSTO debe ser notificado y movilizado a las instalaciones del CD alterno	SGSTO
2	Notificar a la empresa de custodia para el restablecimiento de las cintas de respaldo	Notificar vía email o teléfono a la empresa de custodia acerca de la situación de desastre y que estén listos para enviar las cintas de respaldo sin retrasos, según los acuerdos contractuales definidos y en el lugar y tiempo acordado	Administrador del Centro de Cómputo
3	Notificar al proveedor de comunicaciones	Notificar al proveedor de comunicaciones acerca de la situación de desastre para monitorear el restablecimiento de Líneas de contingencia en el CD alterno	SGOT

4	Activar el CD alterno	Declarar el CD alterno como CD en contingencia. Se debe revisar el checklist inventario de aplicaciones del Anexo 09 Requisitos en el CD alterno y Análisis de Aplicaciones. Adicionalmente, se deberá tener en cuenta los insumos necesarios de HW y SW requeridos para el correcto funcionamiento del mismo	Administrador de Centro de Cómputo
5	Identificar la pérdida de plataforma tecnológica	Identificar la infraestructura tecnológica perdida en el CD primario	Administrador de Centro de Cómputo
6	Determinar los equipos que pueden ser reutilizados	Determinar equipos que puedan ser reutilizados luego de la contingencia. Revisar su operatividad, y confiabilidad, para validar que la misma no se haya visto afectada como consecuencia del evento de desastre ocurrido en el CD	Administrador de Centro de Cómputo
7	Determinar necesidades adicionales y coordinar compras de emergencia	Determinar los elementos adicionales que son necesarios para facilitar la recuperación de los procesos críticos. Estos artículos se deben comprar inmediatamente	Administrador de infraestructura y equipos de almacenamiento (SGSTO)
8	Movilizar equipos disponibles hacia el sitio alterno	De ser necesario, mover servidores y/u otros equipos disponibles que se encuentren operativos al sitio alterno.	Administrador de infraestructura y equipos de almacenamiento (SGSTO) + GAD
9	Recuperar copias de seguridad de aplicaciones	Recuperar de ser necesario, las copias de seguridad ya sean del CD o del almacenamiento externo y restaurar los datos. Validación en el repositorio de Gestión de Cambios	Jefe de Proyectos de Aplicaciones – SGIS. SGSTO
10	Preparar la plataforma tecnológica para la recuperación de los procesos	De ser necesario, instalar software base, aplicar parches, restaurar los últimos backups y aplicar script de recuperación sobre la plataforma tecnológica del CD alterno	SGSTO SGGBD SGOT
11	Verificar los enlaces de red	Ejecutar el procedimiento de verificación de los enlaces de Red y Comunicaciones. Procedimiento: • Verificación de conectividad de agencias del RENIEC hacia CD alterno.	SGOT

12	Recuperar Consultas en Línea - Vía Dedicada	Ejecutar el procedimiento de recuperación de la aplicación de Consultas en Línea - Vía Línea Dedicada. Procedimiento: • Verificar y/o activar el pase de los servicios del metrocluster. • Aperturar la base de datos de los sistemas de producción. • Activar y verificar los servicios de servidor MQ. • Confirmación telefónica con cada institución cliente del servicio.	SGSTO
13	Recuperar Agencias	Ejecutar el procedimiento de recuperación de aplicaciones de Agencias	Coordinador del plan de Contingencia
14	Recuperar el controlador de Dominio	Verificar la operatividad del controlador de Dominio	Administrador de seguridad informática
15	Recuperar la Línea de Procesamiento de RRCC	Ejecutar el procedimiento de recuperación de la Línea de Procesamiento de Registros Civiles.	Coordinador del plan de Contingencia
16	Recuperar la Línea de Emisión DNI	Ejecutar el procedimiento de recuperación de la Línea de Emisión del DNI.	Coordinador del plan de Contingencia
17	Recuperar Consultas en Línea - Vía web	Ejecutar el procedimiento de recuperación de la aplicación de consultas en Línea Vía web. Procedimiento: • Verificar y/o activar el pase de los servicios del metrocluster. • Aperturar la base de datos de la línea de producción del DNI. • Activar y verificar los servicios del OAS. • Verificar la correcta funcionalidad del aplicativo.	Coordinador del plan de Contingencia
18	Recuperar Correo Institucional	Verificar la operatividad del Correo Institucional.	Administrador de seguridad informática

19	Recuperar Portal Institucional	Ejecutar el procedimiento de recuperación del Portal Institucional.	Coordinador del plan de Contingencia
20	Recuperar acceso a Internet	Verificar la operatividad del servicio de Acceso a Internet	Administrador de seguridad informática
21	Recuperar Trámite Documentario	Ejecutar el procedimiento de recuperación del aplicativo de Trámite Documentario. Procedimiento: • Verificar y/o activar el pase de los servicios del metro cluster.	Coordinador del plan de Contingencia
22	Recuperar Intranet Institucional	Ejecutar el procedimiento de recuperación de la Intranet Institucional. Procedimiento: • Verificar y/o activar el pase de los servicios del metro cluster. • Aperturar la base de datos de la línea de producción del DNI. • Activar y verificar los servicios del OAS.	Coordinador del plan de Contingencia
23	Informar a los usuarios críticos del negocio	Informar a los usuarios clave del negocio acerca del restablecimiento de las operaciones, para la verificación de la operatividad global de sus procesos de negocio. Adicionalmente, se debe tener información relacionada a la cantidad de datos perdidos durante el evento de desastre, ya que esto significará exigencias de reconstrucción y reproceso para las diferentes áreas de negocio. Referencia NAI 443	Coordinador del Plan de Contingencia SGSTO
24	Habilitar los controles de Operación en CD alterno	Habilitar los procedimientos de backups y controles normales de operaciones en el CD alterno	Administrador de Centro de Cómputo
25	Notificar el término de las actividades de recuperación	Declarar el término de la ejecución de las operaciones del plan, cuando las operaciones del CD primario hayan sido totalmente restablecidas en el CD alterno	SGSTO

6.6 ESTRATEGIAS DE PRUEBAS

Existen varias estrategias ver tabla 2, que pueden ser adoptadas para probar el plan:

Tabla 2. Tipos de Pruebas.

Tipos de Pruebas	Descripción
Prueba de Capacidad	El objetivo de esta prueba es asegurar una adecuada capacidad y disponibilidad de los recursos cuando el plan se active. Los puntos a considerar incluyen espacio en oficina alternativa, aire acondicionado y requerimiento de energía para los equipos a ser utilizados en la activación del plan.
Verificación Manual	El objetivo de esta prueba es asegurar la disponibilidad de los materiales de recuperación requeridos según se estableció en el plan. Esta prueba requiere revisar toda la data requerida, suministros y/u otras copias impresas de documentos que se encuentran actualmente respaldados y correctamente resguardados externamente.
Ensayo Estructurado	El objetivo de esta prueba es liderar el equipo hacia una recuperación simulada a fin de determinar la suficiencia del plan. La prueba se debe conducir como sigue: • Todos los líderes de equipo se reúnen en una habitación donde se les hará entrega del escenario a probar. • Cada uno debe trabajar sus procedimientos de recuperación prestando particular atención en la interacción con los otros equipos. • Los puntos identificados serán anotados y serán materia de seguimiento.
Convocatoria no Anunciada del Equipo del Plan de Contingencia	El objetivo de esta prueba es asegurar que la lista de equipos de movilización de recuperación se encuentre al día y que los equipos puedan ser movilizados en el momento requerido. Esta prueba debe ser conducida en tiempos diferentes (fuera y durante horas de trabajo) a manera de identificar cualquier defecto en el plan.
Prueba Paralela	El objetivo de la prueba paralela es verificar el correcto funcionamiento del CD alterno, validando que los equipos y aplicaciones funcionen correctamente, soporten la carga de trabajo estimada en contingencia y que se cumpla con los tiempos estimados de recuperación. Esta prueba se realiza sólo en el CD alterno sin afectar las operaciones del CD primario. Al igual que en las otras pruebas se deben tomar notas de fallas y posibles mejoras identificadas para poder actualizar y mejorar el plan. Se debe involucrar a personal de las áreas de negocio para que las pruebas incluyan la aprobación y observaciones de los mismos

	con respecto a sus expectativas de funcionalidad y rendimiento.
Prueba Total	Al igual que la prueba paralela, se busca verificar el correcto funcionamiento del CD alterno, sin embargo, la prueba total es más completa, e incluye la desactivación del CD primario para lograr un mayor realismo de la prueba. Este tipo de pruebas deben realizarse en momentos de carga de trabajo baja para el negocio y de preferencia en fines de semanas de TI y personal vital involucrado de las áreas de negocio.

6.7 PLAN DE PRUEBAS

El plan preparado por el equipo del plan de contingencia está compuesto de una serie de actividades orientadas a mantener actualizado y vigente el Plan de Contingencia. Estas pruebas están enmarcadas dentro de un calendario de pruebas, y se compone de las siguientes partes:

- Definir el propósito de la prueba.
- Definir la prueba.
- Designar el equipo de prueba.
- Estructurar los aspectos a probar.
- Ejecutar las pruebas.
- Analizar los resultados y actualizar el Plan de Contingencia, si fuese necesario.

VII. VIGENCIA

Entrará en vigencia a partir de su aprobación.

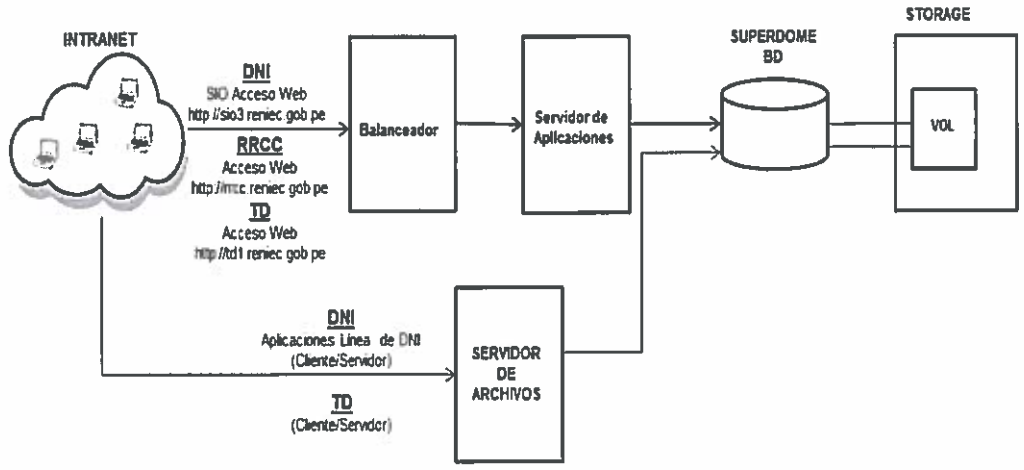
VIII. APROBACIÓN

Será aprobada mediante Resolución Secretarial.

IX. ANEXOS

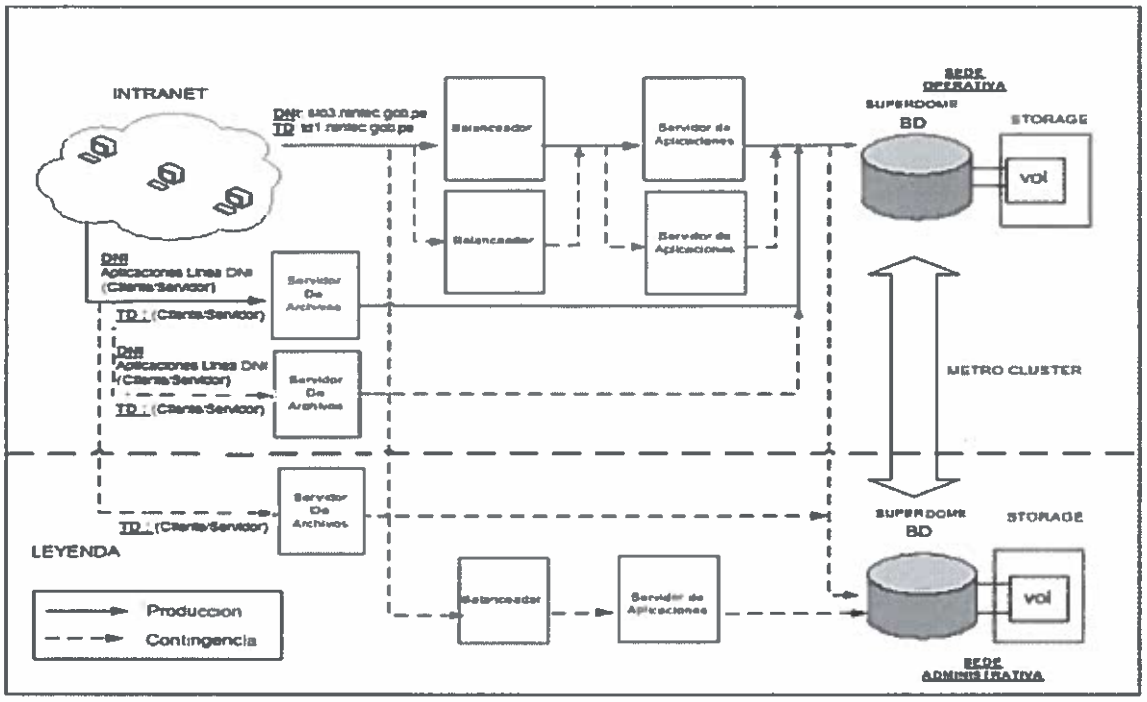
ANEXO N° 01

ESQUEMA FUNCIONAL DE LOS SISTEMAS DNI (DNI), REGISTROS CIVILES (RRCC) Y TRAMITE DOCUMENTARIO (TD)



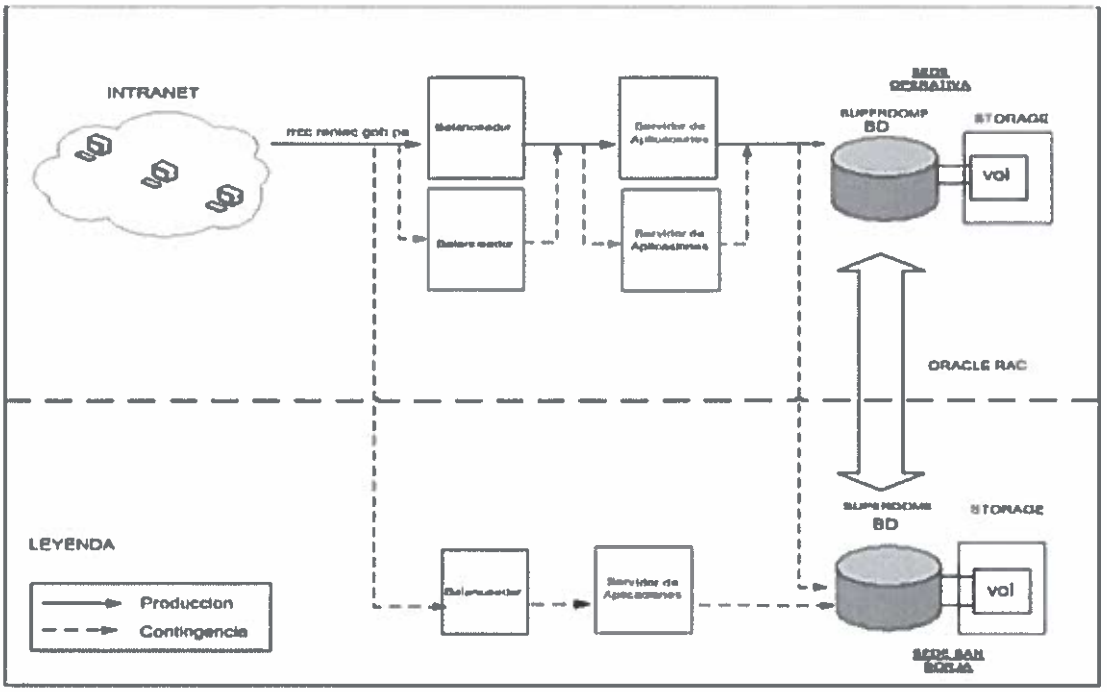
ANEXO N° 02

ESQUEMA ACTUAL DE LOS SISTEMAS DNI (DNI) y TRAMITE DOCUMENTARIO (TD) INCLUYENDO LOS SUBSISTEMAS DE CONTINGENCIA

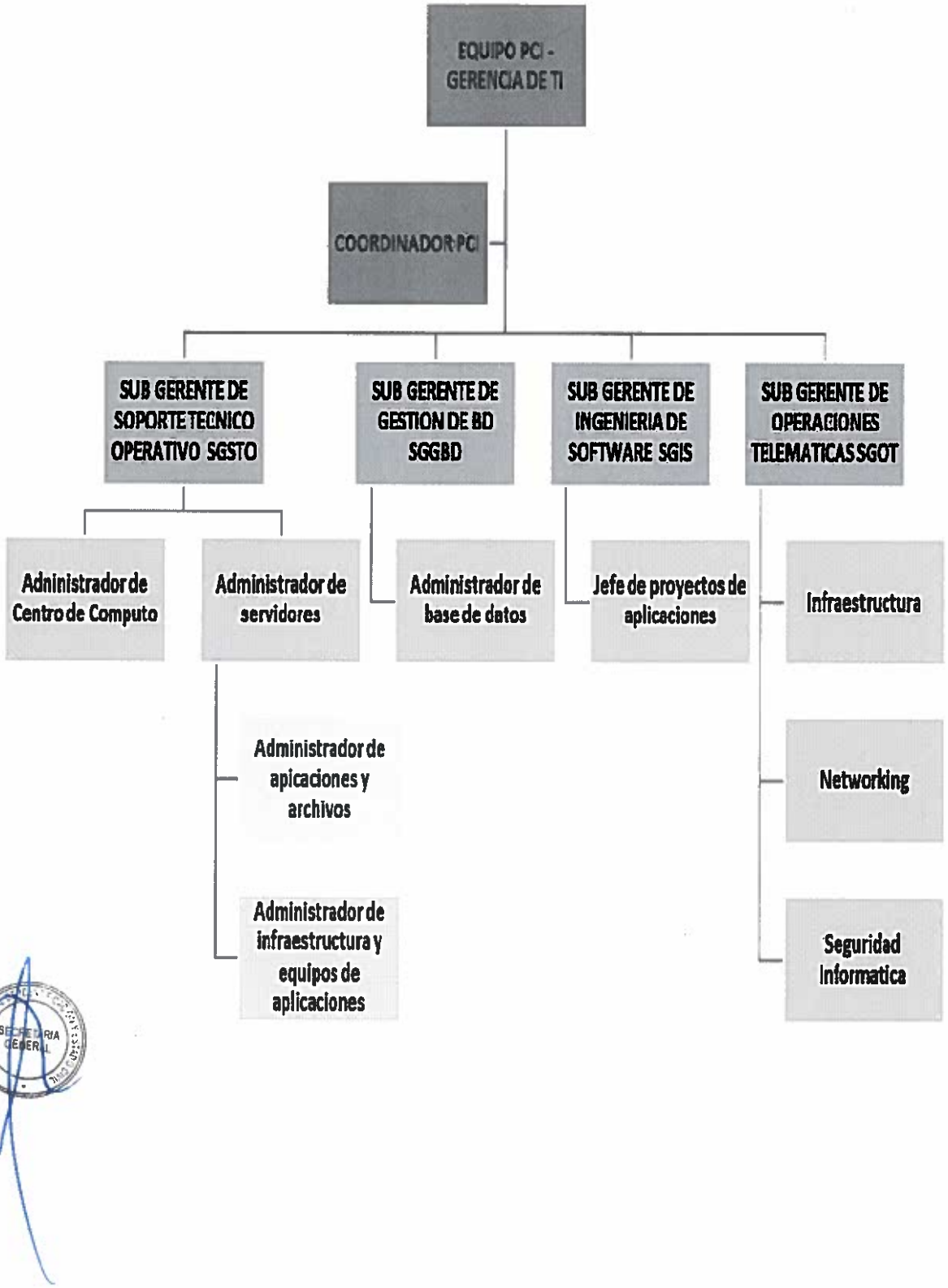


ANEXO N° 02A

ESQUEMA ACTUAL DEL SISTEMA DE REGISTROS CIVILES (RRCC) INCLUYENDO LOS SUBSISTEMAS DE CONTINGENCIA



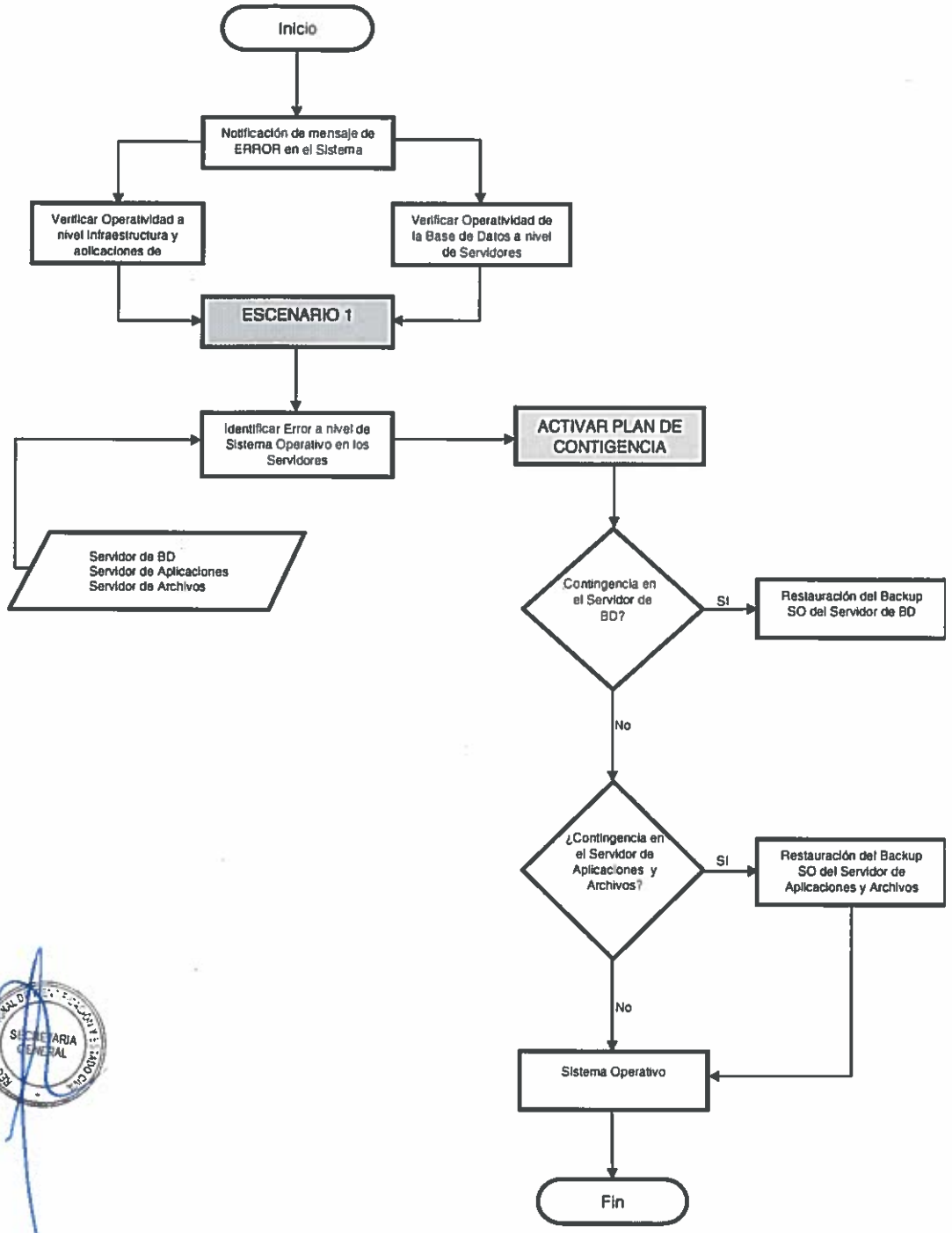
ANEXO N° 03
EQUIPO DE PLAN DE CONTINGENCIAS



ANEXO N° 04

DIAGRAMA DE FLUJO ESCENARIO 01 (SGSTO)

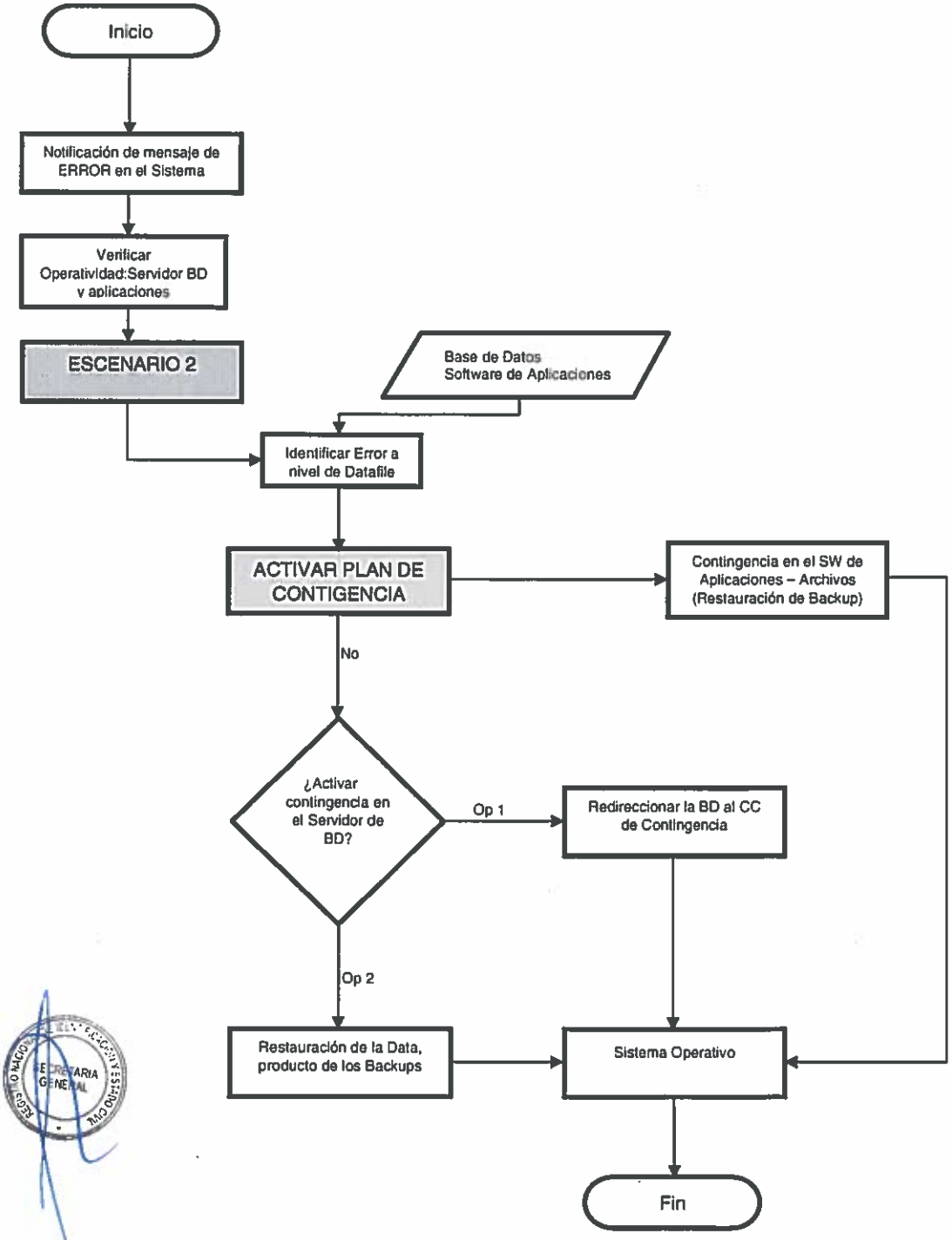
(Corrupción del Sistema Operativo)



ANEXO N° 05

DIAGRAMA DE FLUJO ESCENARIO 02 (SGSTO-SGGBD)

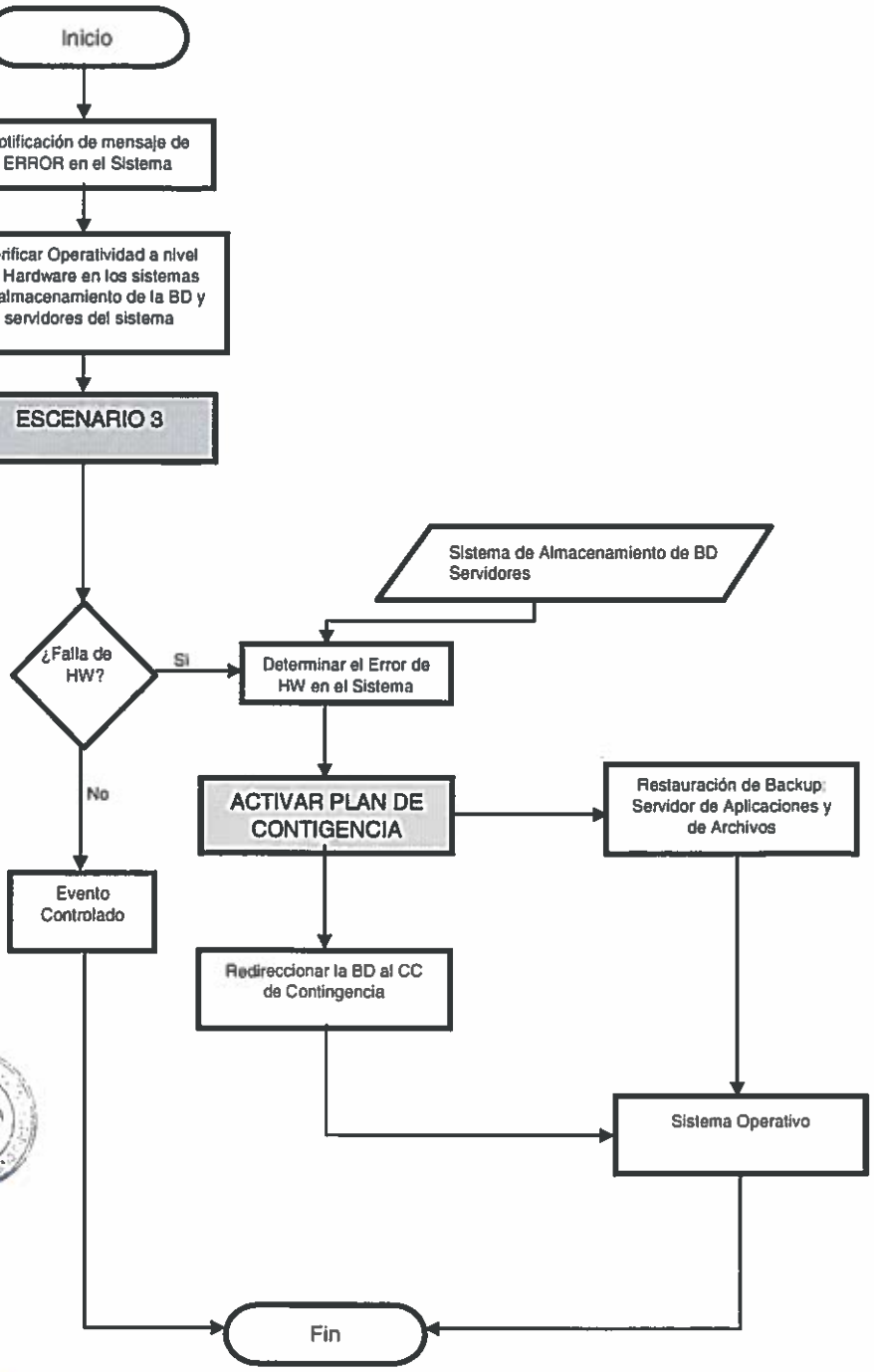
(Corrupción de Datos)



ANEXO N° 06

DIAGRAMA DE FLUJO ESCENARIO 03 (SGSTO)

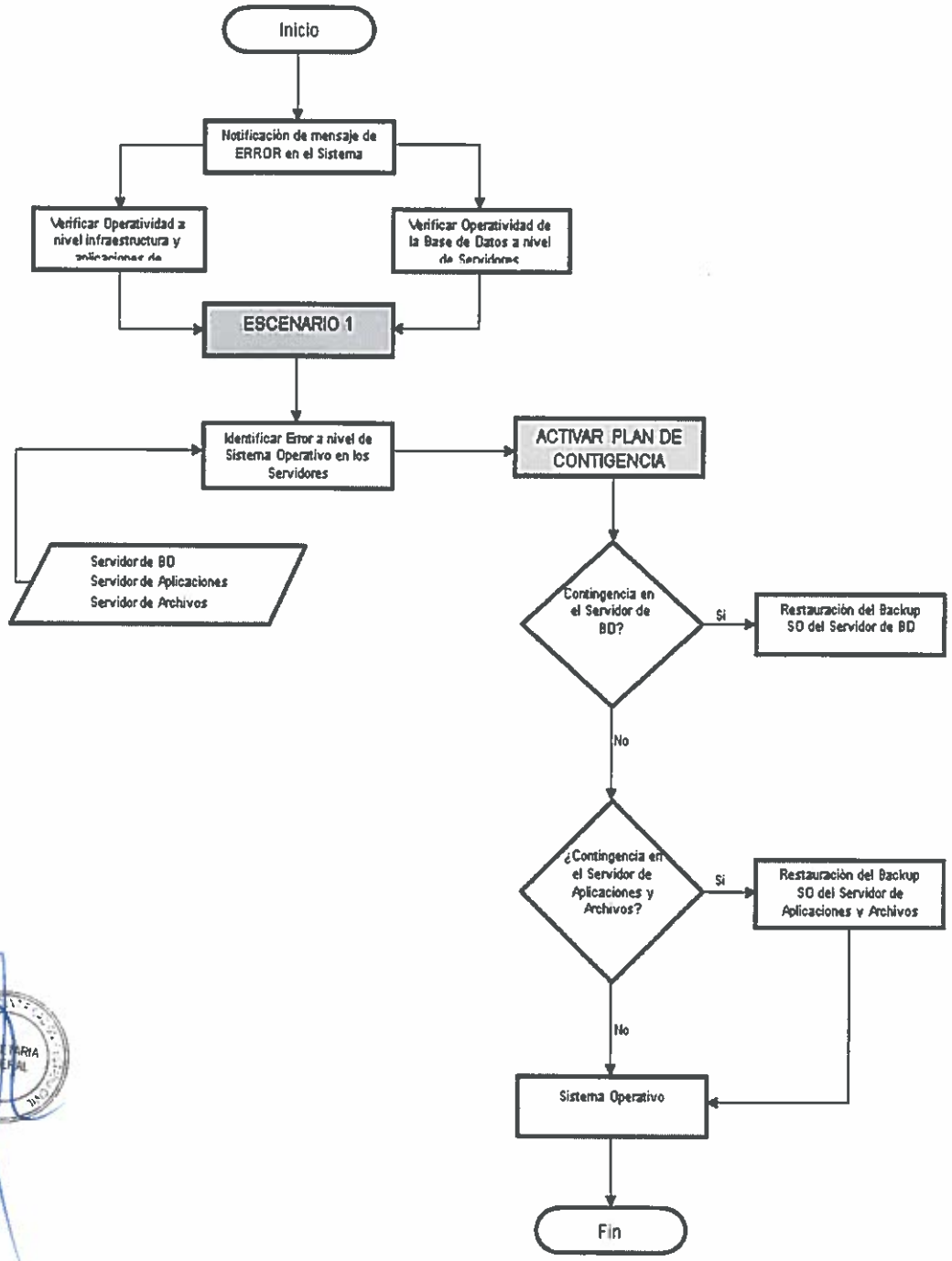
(Fallo Físico)



ANEXO N° 07:

DIAGRAMA DE FLUJO ESCENARIO 04 (SGSTO)

(Inoperatividad del Centro de Cómputo de Producción)



ANEXO N° 08

RELACION DE SERVICIOS Y PROVEEDORES

N°	Descripción del Servicio	Proveedor del Servicio	Contacto	Teléfono
1	Servicio de soporte técnico y mantenimiento correctivo para plataforma de servidores Superdome.	Inversiones Palo Alto SAC	Jennyfer Lara Vela	987859761
2	Renovación de licencias de software (servicio de renovación de mantenimiento de software Microsoft).	Corporación Sapia	Carlos Carrion Romero	2154530 Anexo2497
3	Servicio de soporte al software (soporte integral de plataforma de software Unicenter ca).	Clarity Consulting SAC	Lissette Zarate	994626421
4	Servicio de soporte y actualización de software websphere mq series.			
5	Servicio de soporte integral de software Microsoft.	Microsoft Perú SRL	Georgette Martinez	999891879
6	Servicio de soporte para la plataforma de respaldo y recuperación de datos.			
7	Servicio de traslado y custodia de cintas magnéticas.	Hermes Transportes Blindados	Yashmine Mendieta Cordova	6174000 Anexo1228
8	Mantenimiento preventivo de equipos de aire acondicionado.			
9	Servicio de mantenimiento preventivo y correctivo de servidor blade	Adexus Perú SA	Alejandro Leon	997501327
10	Mantenimiento preventivo y correctivo de fotocopiadoras	Syscosmel SAC - Delta System Plus SAC		4619239 - 4636033
11	Servicio de soporte, mantenimiento preventivo y correctivo para la infraestructura de los kioskos plataforma virtual multiservicios (pvm).	Hiper SA	Miguel Choque	945072709
12	Servicio de soporte y actualización de licencias Oracle	Sistemas Oracle del Perú	Masami Yamaguchi	6151071
13	Servicio de mantenimiento preventivo de equipos de aire acondicionado para			

	servidores			
14	Servicio de soporte y mantenimiento de sistema automático de identificación biométrica (ABIS)	Identibio SAC	Alfredo Narváez	968888958
15	Servicio de mantenimiento preventivo y correctivo de equipos de impresión para el documento nacional de identidad	Xerox del Perú SA	Luis Vallejo	981004237

ANEXO N° 09

SERVIDORES DE LOS TRES SISTEMAS (DNI, RRCC Y TRÁMITE DOCUMENTARIO)

SISTEMA DEL DNI

SITE	DESCRIPCIÓN	SEDE
Producción	Funciona como Primario	Operativa
Contingencia	Funciona como Alterno	Administrativa

DESCRIPCIÓN	SERVIDORES DEL SISTEMA DEL DNI		
	BASE DE DATOS	APLICACIONES	RESPALDO DE BASE DE DATOS
PROCESADORES	12	06	08
TIPO DE PROCESADOR	Intel(R) Itanium 2 9100 1.6 GHz, 24 MB	Intel(R) Xeon 2.69 Ghz.	Intel(R) Itanium 2 9100 1.6 GHz, 24 MB
MEMORIA RAM	143.81 GB	14 GB	127.87GB
DISCO	68 GB	50 GB	68 GB

SISTEMA DE RRCC

SITE	DESCRIPCIÓN	SEDE
Producción	Funciona como Primario	Operativa
Producción	Funciona como Primario	San Borja

DESCRIPCIÓN	SERVIDORES DEL SISTEMA DE RRCC		
	BASE DE DATOS	APLICACIONES	RESPALDO DE BASE DE DATOS
PROCESADORES	04	04	04
TIPO DE PROCESADOR	Intel(R) Itanium (R) 9350 1.73 GHz, 24 MB	Intel(R) Xeon 2.69 Ghz.	Intel(R) Itanium (R) 9350 1.73 GHz, 24 MB

MEMORIA RAM	511.58 GB	16 GB	511.58 GB
DISCO	300 GB	30 GB	300 GB

SISTEMA DE TRAMITE DOCUMENTARIO (TD)

SITE	DESCRIPCIÓN	SEDE
Producción	Funciona como Primario	Operativa
Contingencia	Funciona como Alterno	Administrativa

DESCRIPCIÓN	SERVIDORES DEL SISTEMA DE TRAMITE DOCUMENTARIO (TD)		
	BASE DE DATOS	APLICACIONES	RESPALDO DE BASE DE DATOS
PROCESADORES	04	04	04
TIPO DE PROCESADOR	Intel(R) Itanium 2 9000 1.6 GHz, 24 MB	Intel(R) Xeon 2.70 Ghz.	Intel(R) Itanium 2 9000 1.6 GHz, 24 MB
MEMORIA RAM	23.93 GB	08 GB	23.93 GB
DISCO	73.4 GB	32 GB	73.4 GB