Superintendencia Nacional de Servicios de Saneamiento

RESOLUCIÓN DE GERENCIA DE ADMINISTRACIÓN Y FINANZAS

N° 014-2009-SUNASS-GAF

Lima, 9 de septiembre de 2009

VISTO:

El Manual de Contingencias para el área de Sistemas de la SUNASS elevado a la Gerencia de Administración y Finanzas por el Especialista en Sistemas mediante Memorándum N° 076-2008-SUNASS-086 de fecha 23 de diciembre de 2008.

CONSIDERANDO:

Que, en el Informe N° 003-2008-2-4539, "Examen Especial Área de Informática y Sistemas de la Gerencia de Administración y Finanzas de la SUNASS, periodo 01.01.2006 – 31.12.2007", emitido por el Órgano de Auditoria Interna de la SUNASS, se incluyó la recomendación N° 2 que indicaba que "la Gerencia General disponga a la Gerencia de Administración y Finanzas para que se implementen y actualice el Plan de Contingencias del Área de Sistemas e Informática de la SUNASS, el cual deberá ser aprobado y aplicado por el área en mención con las reservas que el caso amerita";

Que, el referido Manual tiene por objeto establecer los procedimientos de almacenamiento y respaldo de la información que genera la institución así como las medidas que se deben adoptar permanentemente con la finalidad de salvaguardar la información de la SUNASS;

Que, mediante el Memorándum N° 076-SUNASS-2008-086 de fecha 23 de diciembre de 2008 el especialista en Sistemas puso a consideración de la Gerencia de Administración y Finanzas el Manual de Contingencia para el área de Sistemas de la SUNASS, el cual fue revisado y aprobado mediante Memorando N° 938-2009-SUNASS-080 de fecha 09 de septiembre de 2009;

En virtud de lo dispuesto en el Manual de Organización y Funciones de la SUNASS, corresponde a la Gerencia de Administración y Finanzas en materia de Tecnología de la Información, formular y proponer la política relativa a la implementación de un plan de sistemas de información con el objeto de preveer que el desarrollo de sus actividades contribuya al logro de los objetivos institucionales, así como diseñar controles con el objeto de salvaguardar los datos fuente de origen, operaciones de proceso y salida de información con la finalidad de preservar la integridad de la información procesada;

SE RESUELVE:

Artículo Primero.- Aprobar el "Manual de Contingencias para el área de Sistemas de la SUNASS".

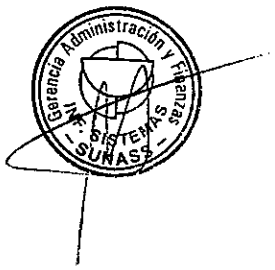
Artículo Segundo.- Disponer que dicho Manual esté disponible en la Intranet de la SUNASS para conocimiento del personal que labora en la Institución.

Regístrese, comuníquese y archívese.

JOSE ZAVALA MUÑOZ
Gerente de Administración y Finanzas (e)

Superintendencia Nacional de Servicios de Saneamiento

PLAN DE CONTINGENCIAS DE LA SUNASS
AREA DE SISTEMAS - 2008



LIMA, DICIEMBRE DEL 2008

INDICE

OFICINA DE INFORMÁTICA Y SISTEMAS

I) Introducción

1. Generalidades.

El Plan de Contingencia tiene como objetivo desarrollar actividades (pautas, normas, procedimientos, etc.) para evitar o minimizar el impacto de una contingencia y a recuperar la operatividad normal de los servicios críticos de redes y comunicaciones, sistemas de información, aplicaciones y bases de datos en el menor tiempo posible ante la ocurrencia de alguna falla.

El Plan de Contingencia permite evitar en un 95 % los problemas que afectan a la mayoría de las tecnologías informáticas y componentes electrónicos. Esto no se limita a las computadoras, software de base y aplicaciones, sino que también puede controlar y prever sistemas de seguridad, sistemas de iluminación, sistemas de refrigeración, de control de proceso, sistemas de control ambientales, centrales telefónicas, sistemas de comunicaciones, que de alguna forma formen parte de nuestra Institución.

Por otro lado, deben tenerse en cuenta no sólo los sistemas propios de la Institución, sino también los sistemas y tecnologías soportadas por proveedores externos, con los cuales se deberán determinar las acciones correctivas necesarias. Además, las interfaces de las aplicaciones de SUNASS con otras aplicaciones o sistemas internos o con otras organizaciones, que deberán evaluarse con detenimiento para asegurar que sean compatibles con los aspectos de seguridad y contingencia propuestos y aprobados por SUNASS y que no afecten a los sistemas internos.

2. Servicios Afectados.

Se presentan varios puntos concretos de la forma como se verán afectados diversos servicios, en caso de no lograrse finalizar a tiempo las acciones requeridas para la reparación y mantenimiento de los sistemas tanto informáticos como no informáticos. Estos puntos son los que dentro del marco de área de sistemas se consideran críticos para la funcionalidad de SUNASS.

Suministros de electricidad:

- La mayoría de las **centrales eléctricas**, cualquiera que sea el combustible que utilicen e incluidas las hidroeléctricas, tendrán más de una unidad vulnerable. Hay muchas otras aplicaciones que utilizan este tipo de promedio variable como verificación de seguridad, por ejemplo, mandos de motores, mandos de vuelo, equipo de mantenimiento de las funciones vitales. Las pruebas con el proveedor del servicio se deberán realizar periódicamente para evaluarlos tiempos de respuesta y cambio de fluido eléctrico continuo, por fluido eléctrico generado.
- Las **redes de electricidad** son incluso más vulnerables debido a un fenómeno conocido como "colapso progresivo", en virtud del cual una falla en una parte del sistema aumenta la carga en el resto, desencadenando fallas adicionales hasta el punto de cierre. La falla de la red afectaría a todos los equipos dependientes de electricidad en otros puntos de la cadena, salvo donde hubiera generación local de energía eléctrica (también estos equipos deberán ser objeto de pruebas y, en caso necesario de modificaciones, para asegurar su correcta operación antes durante y después del evento).

Telecomunicaciones:

- Las **redes telefónicas** dependen en gran medida de microchips y son tan vulnerables al colapso progresivo como las redes de electricidad.
- También los **teléfonos celulares** tienen típicamente microchips que podrían ser vulnerables al colapso progresivo, junto con las centrales telefónicas, particularmente en los sistemas más antiguos.
- Algunos cables submarinos son vulnerables al colapso progresivo. Cualquier problema surgirá principalmente en los componentes en tierra pero no se descarta el reemplazo o la reprogramación de repetidores en el lecho marino.
- La situación relativa a los satélites de telecomunicaciones es menos clara (si bien las estaciones terrestres son ciertamente vulnerables).
- También Internet plantea un interrogante. Se anticipan problemas en la forma en que los datos de encaminamiento son generados y nombrados; es probable que haya fallos de nodos y no se descarta la posibilidad de colapso progresivo.

Sistemas de edificios:

- Las falla potencial en los sistemas de control del edificio SUNASS comprende ascensores, calefacción, iluminación, aire acondicionado, puertas de seguridad de control electrónico, rociadores y alarmas contra intrusos. Para lo cual se debe conocer el ámbito de contingencia de los proveedores de cada uno de los servicios mencionados, y anexarlos al presente plan de contingencias.
- Sé deberá realizar conjuntamente con los proveedores ejercicios pilotos para reducir el riesgo de falla y medir el tiempo de restauración de cada uno de estos servicios, así como determinar los puntos más vulnerables de cada uno de estos elementos, detectar los más débiles y reemplazarlos por otros que aseguren el servicio ante una posible contingencia.

3. Características de los problemas informáticos:

- **No es un problema más de la Institución** sino una real amenaza para la continuidad de las operaciones de la Institución.
- Las **interdependencias cliente-proveedor** pueden provocar perjuicios como consecuencia de problemas presentados en otras organizaciones (reacciones en cadena o efecto dominó)
- Las fallas que podrían producirse en los **servicios públicos** impactarían sensiblemente en todos los sectores de la comunidad.
- El **plazo de finalización** de los proyectos y planes relacionados con el tema de contingencia es **inamovible**.

Por tanto es clave para el éxito de los proyectos de contingencia, que las **máximas autoridades** lideren el Proyecto dándole la **máxima prioridad posible**, y provean los recursos necesarios para asegurar la operatoria normal de la Institución en él mínimo plazo posible.

El **gerenciamiento del Proyecto** es una responsabilidad que no puede delegarse en ningún proveedor externo ó tercero. Es necesario un fuerte trabajo de **planificación y coordinación**, además de ser imprescindible un estricto **control y seguimiento** de todo el proceso de contingencia, que requerirá de personal afectado en forma exclusiva al Proyecto.

También es necesaria una Institución apropiada del Proyecto de contingencia, que permita una gestión eficaz de los responsables y el logro de los objetivos fijados, como también que las máximas autoridades estén informadas de la situación de cada una de las pruebas de contingencia y solución y de los riesgos involucrados para que puedan tomar en forma oportuna las decisiones correspondientes.

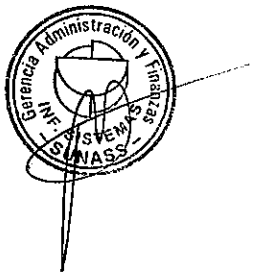
Resulta necesario involucrar a:

- **Los máximos responsables de SUNASS en:**
  - Toma de conciencia de la gravedad del problema
  - Fijación de las metas
  - Provisión de recursos
  - Seguimiento general del Proyecto
- **Los responsables de cada área funcional dentro de SUNASS en:**
  - Identificación de las diferentes funciones de su área y la evaluación del impacto que tendría su discontinuidad o degradación, determinando así las funciones críticas.
  - Determinación, en conjunto con las áreas técnicas, de los recursos informáticos que soportan dichas funciones críticas.
- **Los responsables informáticos para cada área en:**
  - La provisión de soporte técnico a los responsables de cada área, para la determinación de aquellos recursos (hardware, software de base, aplicativos, equipos de comunicación, interfaces.) que soportan las funciones críticas.
  - Identificación del impacto que un problema podría tener sobre la operatoria de estos recursos.

Para la correcta estimación de recursos es importante considerar que los proyectos de contingencia requieren un alto esfuerzo en la etapa de pruebas, para asegurar que los sistemas adecuados mantienen la misma funcionalidad antes de la contingencia y después de la puesta en marcha del plan de seguridad ejecutado.

4. Metodología

El Objetivo del presente plan es presentar las fases en las que se divide el plan de contingencia del área de sistemas e informática de la Superintendencia Nacional de Servicios de Saneamiento – SUNASS. Dentro de cada una de estas fases se detallan las tareas a realizar, procedimientos a definir y los resultados esperados.



II) ANALISIS DE LA SITUACION ACTUAL

2.1 Red de comunicaciones

La red actual está formada por:

* 1 Switch de Fibra (8vo piso)
* 8 Switches Administrables (por piso)
* 1 Router
* 1 Central Telefónica ALCATEL
* 12 Servidores

2.2 Servidores

Se considerarán sólo aquellos servidores y equipos que intervengan en la provisión de los servicios críticos.

2.3 Sala de servidores

La sala de servidores posee un sistema de aire acondicionado para evitar el calentamiento de los equipos, además de un sistema de detección de humo. La sala esta protegida con equipos UPS para garantizar la continuidad de energía eléctrica en caso de corte de energía eléctrica, garantice un mantenimiento rápido y oportuno en las redes de datos y la red eléctrica.

Una puerta de vidrio separa el área de informática de la sala de servidores, restringiendo el acceso a personal no autorizado. Igualmente el acceso al área de sistemas está restringido a personal no autorizado a través de una puerta que está permanentemente cerrada.

2.4 Cintas de backup

Las cintas de backup utilizadas para el almacenamiento de los "Directorios de Respaldo" según Instructivo, son almacenadas temporalmente en el área de Sistemas de la SUNASS para luego ir a un centro de almacenamiento definitivo fuera del local institucional.

El detalle del proceso de Respaldo de Información se presenta en el Anexo II Seguridad (Procedimiento de almacenamiento de la información) en donde se describe las condiciones generales, el procedimiento empleado detallando los directorios y archivos a respaldar, la frecuencia de respaldo y el envío de cintas a los almacenes.

2.5 Protección contra virus

SUNASS cuenta con licencias de McAfee para la protección de servidores y estaciones de trabajo contra virus y otras amenazas.

El antivirus cuenta con las siguientes funcionalidades:

- VirusScan Enterprise v8.7i
- Addon Antiespyware v8.7i
- HIPS (solución firewall e IPS de Host)
- Site Advisor (solución de seguridad en navegación internet)
- Groupshield 7.0 para Lotus Notes

III) Inventario y análisis de impacto preliminar

1. Objetivo

- Realizar un inventario exhaustivo de productos, hardware, sistemas, interfaces, software de base y equipamientos de SUNASS, que puedan verse afectados.
- Efectuar un análisis de impacto preliminar sobre la compatibilidad de las aplicaciones de mantenimiento interno para tener una primera medida de cómo se ven afectadas.
- Estimar los recursos, Costos y tiempos requeridos.

Esta fase comprende las siguientes tareas:

- Inventario de software estándar
- Inventario de sistemas no informáticos (embebidos)
- Inventario de hardware y software de base
- Inventario de sistemas en desarrollo
- Inventario de funciones tercerizadas
- Inventario de aplicaciones de mantenimiento interno y análisis preliminar
- Definición de estrategias de solución
- Estimación de recursos y tiempos

2. Inventario de software estándar

Es necesario identificar con los proveedores de software estándar si son o no compatibles, solicitar su certificación y determinar las acciones de actualización o corrección requeridas (Upgrade a nueva versión, Service Pack, migración a otro producto, etc.).

3. Inventario de sistemas no informáticos o embebidos

Un tema importante a ser tenido en cuenta en esta etapa es la identificación de posibles problemas en sistemas no informáticos que puedan ser afectados por una contingencia. El comportamiento de cualquier sistema que contenga un dispositivo inteligente o funciones críticas con decisiones automáticas que dependen de intervalos de tiempos puede ser impredecible (firmware, PLC's, sistemas de supervisión, regulación y control, protecciones, sistemas de comunicación, etc.).

Para realizar el relevamiento se requerirá la involucración de personal de diversas áreas de SUNASS que deberán ser gestionados adecuadamente y, a posteriori, la consulta con los proveedores de dicho equipamiento a fin de determinar si se requiere la ejecución de acciones adicionales (reparar, reemplazar, desechar, etc.) . (Ver **Anexo I: "Sistemas Embebidos")**

4. Inventario de hardware y software de base

Es necesario identificar con los proveedores de hardware y software de base su compatibilidad, solicitar su certificación y determinar las acciones de actualización o corrección requeridas (Upgrade a nueva versión, Service Pack, migración a otro producto, etc.).

5. Inventario de sistemas en desarrollo

Se deberán revisar todos los proyectos de desarrollo de sistemas que se estén realizando, para determinar, junto con sus responsables, las acciones necesarias para asegurar que los nuevos sistemas no sufran contingencias ya superadas y documentadas. Será oportuno incorporar la compatibilidad de cada uno de los nuevos sistemas dentro de las normas y controles de calidad del plan de seguridad de SUNASS.

6. Inventario de funciones tercerizadas
Se deberán identificar aquellas funciones que son realizadas por terceros y revisar los términos de las contrataciones correspondientes; para determinar, junto con esos proveedores, las acciones necesarias para asegurar que no se vean afectadas por contingencias ya superadas y documentadas.

7. Inventario de aplicaciones y análisis preliminar
Con esta actividad se identifican y localizan todos los programas, lenguajes de control y archivos que se encuentren activos en la Institución.
Es indispensable la participación de: analistas, programadores, usuarios, y administradores de sistemas, que conozcan los sistemas existentes para que la tarea alcance el máximo de confiabilidad. Existen herramientas para ordenar y agilizar el proceso de creación del inventario, pero su mayor o menor efectividad depende del grado de conocimiento que se tenga de los sistemas.

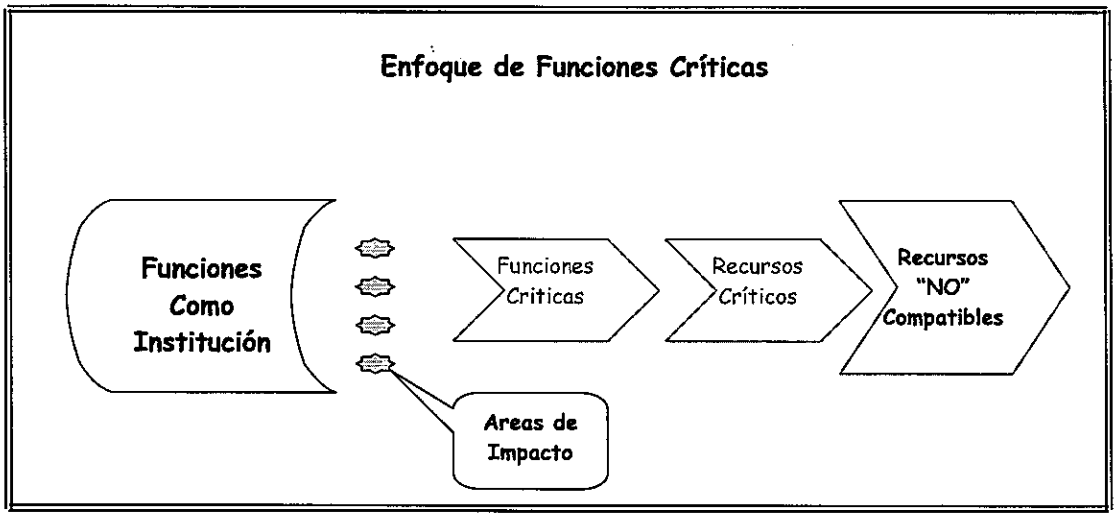
8. Definición de estrategias de solución
Una vez finalizado el inventario y el análisis preliminar se procederán a analizar las estrategias adecuadas a seguir para cada uno de los sistemas afectados:

- **Mantenimiento**: se adecuarán las aplicaciones y datos para asegurar su operatividad como en la revisión anterior a la contingencia. Para los sistemas o aplicaciones en esta categoría será necesario elegir la técnica de mantenimiento a utilizar.
- **Reemplazo**: el sistema afectado puede reemplazarse por uno disponible en el mercado que es compatible y cubre las necesidades del área afectada. En caso de ser necesarias adaptaciones, es importante analizar los tiempos de implementación involucrados.
- **Reescritura**: estas Alternativa pueda darse frecuentemente en los casos donde la SUNASS tuviera dentro sus planes la "reingeniería" de sus sistemas. Dado el poco tiempo disponible, y la poca disponibilidad de recursos humanos, es necesario analizar los riesgos que implica esta Alternativa.
- **Tercerización**: La funcionalidad del sistema sé tercerizará a un proveedor. Este proveedor deberá garantizar que sus sistemas sean compatibles con los estándares de SUNASS para que sea una Alternativa válida.
- **Eliminar**: es una elección extrema, que implica que la funcionalidad provista por ese sistema cesará. Esta decisión es apropiada para las aplicaciones que ya se encontraban en camino de ser eliminadas, debido a procesos de reingeniería o por funciones que quedarán obsoletas.

9. Estimación de recursos y tiempos
A partir del análisis anterior se realizará una primera estimación de los recursos necesarios (humanos, técnicos y económicos) para poder completar la adecuación de los sistemas afectados en el tiempo disponible.
En el caso de haber optado por la estrategia de conversión, es importante considerar al realizar esta estimación, que no es posible delegarla exclusivamente en proveedores externos. Aún en los casos de máxima delegación, siempre será un Proyecto con participación mayoritaria del personal del organismo, por lo que éste debe ser incluido en los Costos.
La participación de los recursos propios del área de sistemas e informática de SUNASS está por debajo del 60 o 70% del esfuerzo total teniendo mayor peso en el gerenciamiento y en las Etapas de inventario, análisis de impacto y pruebas.

IV) Identificación de Funciones Críticas

1. Marco de referencia para el análisis de riesgo.



Debido al corto tiempo disponible antes de la ocurrencia de un desastre y a los pocos recursos disponibles, es necesario definir claramente prioridades de trabajo. Un posible enfoque a seguir para determinar las funciones esenciales de la Institución es el de "funciones críticas" que tendrá como resultado la clasificación de las funciones de la Institución según su criticidad.

2. Clasificación de funciones por su criticidad

El Objetivo de esta etapa es que la Institución identifique las funciones críticas, es decir aquellas cuyo mal funcionamiento o su no-disponibilidad, acarreen consecuencias graves.

2.1. -Determinación de áreas de impacto

Para cada una de las funciones de la Institución se deberá analizar qué áreas serán afectadas en el caso de la falla o degradación de la función. A ellas se las denominará "áreas de impacto". En lo que sigue se determinan seis áreas de impacto. Cada área funcional de SUNASS puede considerar necesario el agregado de otras Sub áreas de acuerdo a sus funciones específicas.

- *Seguridad o bienestar de vidas humanas*: cuando la falla en una función pone en riesgo el bienestar o vidas humanas; por ejemplo: luces de control de tránsito, sistemas de emergencia, suministro de energía eléctrica, telecomunicaciones.
- *Medio ambiente*: cuando la falla o degradación de un sistema impacta negativamente en el medio ambiente.
- *Generación de ingresos o pagos*: cuando la falla en el cumplimiento de una función acarrea consecuencias sobre los pagos de la Institución o los ingresos que debe obtener; por ejemplo no poder pagar o retrasar el pago de remuneraciones, imposibilidad o dificultades para generar obligaciones impositivas o en su cobro, etc.
- *Consecuencias legales o políticas*: por ejemplo juicios por negligencia, ausencia de cumplimiento de servicios o pérdidas económicas.

- *Afectación de la seguridad o confidencialidad*: cuando el mal cumplimiento de una función causa un riesgo de seguridad o pérdida de confidencialidad; por ejemplo divulgación no autorizada de información clave, posibilidad de acceso irrestricto a los datos, posibilidades de fraude, etc.
- *Sobre la operatoria de SUNASS*: imposibilidad de cumplir con funciones básicas propias o que afecten directa o indirectamente a otros organismos, tareas de planificación, etc.

SUNASS, de acuerdo a las funciones que realiza, incluye consecuencias más específicas de los impactos detallados.

2.2. – Calificación de la gravedad de las consecuencias

Para poder medir mejor la criticidad de una función, además de identificar el área de impacto, se han definido niveles de gravedad de las consecuencias de un fallo o falta de cumplimiento de una función de la Institución.

Para cada una de las funciones analizadas y para cada área de impacto se ha calificado su gravedad considerando como escenario base el más desfavorable, suponiendo la ausencia de medidas para reducir el impacto.

La gravedad se ha clasificado según los siguientes criterios:

- ALTA: las consecuencias amenazan la operación continua de SUNASS y requerirían de la intervención de los máximos responsables.
- MEDIA: no está amenazada la operación continua de SUNASS pero se requerirán cambios significativos en las operaciones actuales.
- POCO APRECIABLES: las consecuencias amenazan la eficiencia o efectividad, pero podrían manejarse internamente sin mayor exposición externa

2.3. – Identificación de funciones críticas

Cómo resultado final de esta fase se ha obtenido una matriz ordenada de funciones, clasificadas por su criticidad, permitiendo visualizar a su vez las áreas de impacto afectadas y la gravedad de ese impacto.

Funciones Críticas – Areas de impacto – Gravedad							
Orden por Criticidad	Función Crítica	Seguridad /Bienestar de vidas Humanas	Medio Ambiente	Generación de ingresos y pagos	Consecuencias legales o políticas	Seguridad Confidencialidad	Operatoria
1	Función A	ALTA					
2	Función D		ALTA				
3	Función X			ALTA	MEDIA	ALTA	
4	Función B				MEDIA	ALTA	

FUNCIONES CRITICAS DE LA SUNASS

ORDEN POR CRITICIDAD	FUNCION CRITICA	GENERACION DE INGRESOS Y PAGOS	CONSECUENCIAS LEGALES O POLITICAS	OPERATORIA
1.	Función de Tramite Documentario		ALTA	ALTA
2.	Función de Gestión de Reclamos		ALTA	ALTA
3.	Función de Gestión Administrativa	ALTA		ALTA
4.	Función de Supervisión y Fizcaliz.	MEDIA		MEDIA
5.	Función de Aportes Regulatorios		MEDIA	MEDIA
6.	Función de Digitalización de Doc.		MEDIA	MEDIA

3. Conclusiones

El propósito de este capitulo, es identificar las funciones de la Institución que son más críticas y de las cuales debe asegurarse su operatoria durante y después de una contingencia.

Este enfoque tiende a preservar la operatividad de las funciones críticas, definiendo un criterio para priorizar las tareas, tendiente a minimizar el impacto en caso de que no se disponga de tiempo suficiente para adecuar todos los sistemas y equipamientos.

Para los sistemas o equipamientos no-críticos que no se disponga de tiempo para su adecuación, se tendrán que definir los planes de contingencia correspondientes

Análisis de Riesgo

El análisis de riesgo permitirá identificar las amenazas, el nivel de riesgo de cada amenaza, analizar los activos y definir los servicios críticos. Este análisis ha contemplado evaluar los siguientes procesos y servicios que se consideran importantes para el cumplimiento de los objetivos institucionales de la SUNASS:

A. Proceso de Tramite Documentario
B. Proceso de Gestión de Reclamos
C. Proceso de Gestión Administrativa
D. Proceso de Supervisión y Fiscalización de las EPS
E. Proceso de Digitalización de Documentos
F. Proceso de Apoyo
G. Servicios de TI Institucionales

1 Identificación de las Amenazas

A. Proceso de Tramite Documentario

ITEM	ACTIVO	AMENAZAS
1.	SISTRAM (Sistema de Tramite Documentario) MODULO DE GESTION DE TRAMITE DOCUMENTARIO	- Caída del servicio de Base de Datos - Caída del Servidor de Base de Datos (NOTES) - Caída del arreglo de Disco IBM (NOTES)
2.	NOTIFICACIONES (Archivos Electrónicos)	- Caída del servidor de Archivos (IMGSUNASS) - Caída del Disco (IMGSUNASS)

B. Proceso de Gestión de Reclamos

ITEM	ACTIVO	AMENAZAS
1.	SISTRAM (Sistema de Tramite Documentario) MODULO DE GESTION DE RECLAMOS	- Caída del servicio de Base de Datos - Caída del Servidor de Base de Datos (NOTES) - Caída del arreglo de Disco IBM (NOTES)
2.	EXPEDIENTES Y RESOLUCIONES (Archivos Electrónicos)	- Caída del servidor de Archivos (IMGSUNASS) - Caída del Disco (IMGSUNASS)

C. Proceso de Gestión Administrativa

ITEM	ACTIVO	AMENAZAS
1.	SIGA (Sistema Integrado de Gestión Administrativa)	- Caída del servicio de Base de Datos - Caída del Servidor de Base de Datos (MARTE) - Caída del arreglo de Disco HP (MARTE)
2.	MODULO DE PRESUPUESTO, LOGISTICA, CONTABILIDAD, FINANZAS y RECURSOS HUMANOS	- Caída del Servidor de Aplicaciones (MARTE) - Caída del arreglo de Disco HP (MARTE)

D. Proceso de Supervisión y Fiscalización de las EPS

ITEM	ACTIVO	AMENAZAS
1.	SFIS (Sistema de Fiscalización y Supervisión)	- Caída del servicio de Base de Datos - Caída del Servidor de Base de Datos (MARTE) - Caída del arreglo de Disco HP (MARTE)
2.	SICAP (Sistema de Captura de Datos)	- Caída del servicio de FTP - Caída del arreglo de Disco HP (MARTE)

E. Proceso de Digitalización de Documentos

ITEM	ACTIVO	AMENAZAS
1.	IMAGING SOFT (Sistema de Digitalización de Imágenes: Escaneo, Indexación y Exportación)	- Caída del Servidor de Archivos (IMGSUNASS) - Caída del Disco (IMGSUNASS)

F. Proceso de Apoyo

Este proceso incluye los Servicios que el Área de Informática y Sistemas brinda a las áreas de Logística, Contabilidad, Tesorería, Recursos Humanos, Presupuesto, Etc.

ITEM	ACTIVO	AMENAZAS
1.	SAR (Sistema de Aportes Regulatorios)	- Caída del servicio de Base de Datos - Caída del Servidor de Base de Datos (MARTE) - Caída del arreglo de Disco HP (MARTE)
2.	CONTROL PATRIMONIAL (Sistema de Control Patrimonial)	- Caída del servicio de Base de Datos - Caída del Servidor de Base de Datos (MARTE) - Caída del arreglo de Disco HP (MARTE)

G. Servicios de TI Institucionales

ITEM	ACTIVO	AMENAZAS
1.	COMUNICACIÓN DE DATOS	- Caída de Switch de Fibra - Falla de Cableado UTP - Caída de Suministro Electrónico - Caída del Servidor donde esta el Firewall
2.	COMUNICACION DE VOZ	- Caída de la Central Telefónica - Falla de Cableado UTP - Caída de Suministro Electrónico
3.	CORREO ELECTRONICO	- Caída del Servidor de Correos - Caída del Servidor Firewall - Caída del Antispam - Caída del Servicio de Internet
4.	SERVICIO WEB	- Caída del Servidor Web - Caída del Servicio de Internet - Caída del Servidor Firewall
5.	RESPALDO DE INFORMACION	- Caída del Servidor de Archivos - Caída del Servidor de Base de Datos Oracle - Caída del Servidor de Back-up - Caída de Suministro Electrónico - Falla de Cableado UTP

2 Identificación de los Niveles de Riesgo.

Para la identificación de las amenazas a los servicios brindados por el Área de Informática y Sistemas, se realizará la evaluación de los niveles de riesgo de los eventos. Dicha evaluación resulta del producto aritmético de la probabilidad de ocurrencia de los eventos y el impacto que estos producirían en caso de manifestarse.

La probabilidad y el impacto es un valor sugerido por el personal del Área de Informática y Sistemas en base a la ocurrencia de los sucesos y del conocimiento del estado de los equipos, servicios, aplicaciones y bases de de datos de la SUNASS.

CRITERIOS DE AVALUACION PARA IMPACTO	
1	Muy Bajo
2	Bajo
3	Medio
4	Alto
5	Muy Alto

A. Proceso de Tramite Documentario

FACTORES DE RIESGO	RIESGO	PROBABILIDAD DE OCURRENCIA	IMPACTO	NIVEL DE RIESGO
- Caída de BD de SISTRAM	- Caída del servicio de Base de Datos TRASS	0.0001	5	0.0005
- Caída del Servidor de Base de Datos	- Caída del Servidor de Base de Datos NOTES	0.0001	5	0.0005
- Caída del Servidor de Aplicaciones	- Caída del Servidor de Archivos SIS04	0.0001	5	0.0005
- Caída del Servidor de archivos	- Caída del Servidor de archivos IMGSUNASS	0.0001	4	0.0004

B. Proceso de Gestión de Reclamos

FACTORES DE RIESGO	RIESGO	PROBABILIDAD DE OCURRENCIA	IMPACTO	NIVEL DE RIESGO
- Caída de BD de SISTRAM	- Caída del servicio de Base de Datos TRASS	0.0001	5	0.0005
- Caída del Servidor de Base de Datos	- Caída del Servidor de Base de Datos NOTES	0.0001	5	0.0005
- Caída del Servidor de Aplicaciones	- Caída del Servidor de Archivos SIS04	0.0001	5	0.0005
- Caída del Servidor de archivos	- Caída del Servidor de archivos MARTE	0.0001	4	0.0004

C. Proceso de Gestión Administrativa

FACTORES DE RIESGO	RIESGO	PROBABILIDAD DE OCURRENCIA	IMPACTO	NIVEL DE RIESGO
- Caída de BD de SIGA	- Caída del servicio de Base de Datos SUNDESA	0.0001	5	0.0005
- Caída del Servidor de Base de Datos	- Caída del Servidor de Base de Datos MARTE	0.0001	5	0.0005
- Caída del Servidor de Aplicaciones	- Caída del Servidor de archivos NOTES	0.0001	5	0.0005

D. Proceso de Supervisión y Fiscalización a las EPS

FACTORES DE RIESGO	RIESGO	PROBABILIDAD DE OCURRENCIA	IMPACTO	NIVEL DE RIESGO
- Caída de BD de SFIS	- Caída del servicio de Base de Datos SUNDESA	0.0001	4	0.0004
- Caída del Servidor de Base de Datos	- Caída del Servidor de Base de Datos Marte	0.0001	4	0.0004
- Caída del Servidor de Archivos	- Caída del Servidor de Archivos	0.0001	4	0.0004
- Caída del Servidor de archivos FTP	- Caída del Servidor FTP MARTE	0.0001	4	0.0004

E. Proceso de Digitalización de Documentos

FACTORES DE RIESGO	RIESGO	PROBABILIDAD DE OCURRENCIA	IMPACTO	NIVEL DE RIESGO
- Caída del Servidor de archivos	- Caída del Servidor de archivos IMGSUNASS	0.0001	4	0.0004
- Caída del Servicio WEB	- Caída del Servicio Web TOMCAT	0.0001	4	0.0004

F. Proceso de Apoyo

FACTORES DE RIESGO	RIESGO	PROBABILIDAD DE OCURRENCIA	IMPACTO	NIVEL DE RIESGO
- Caída de BD de SAR, CONTROL PATRIMONIAL	- Caída del servicio de Base de Datos SUNDESA	0.0001	4	0.0004
- Caída del Servidor de Base de Datos	- Caída del Servidor de Base de Datos MARTE	0.0001	4	0.0004
- Caída del Servidor de archivos de Aplicaciones	- Caída del Servidor de archivos NOTES	0.0001	4	0.0004
- Caída del Servicio de Control de Asistencia (TEMPUS)	- Caída del Servidor de Base de Datos MARTE	0.0001	4	0.0004
- Caída del Sistema de TELEBANKING	- Caída del Servidor ARCHIVOS.SUNASS.GOB	0.0001	4	0.0004
- Caída del Sistema TELECREDITO	- Caída del Servidor ARCHIVOS.SUNASS.GOB	0.0001	4	0.0004

G. Servicios de TI Institucionales

FACTORES DE RIESGO	RIESGO	PROBABILIDAD DE OCURRENCIA	IMPACTO	NIVEL DE RIESGO
- Caída de los Switches	- Caída de los Switch	0.0001	4	0.0004
- Falla de Cableado Estructurado	- Falla de Cableado Estructurado	0.0001	4	0.0004
- Caída de Suministro Eléctrico	- Caída de Suministro Eléctrico	0.0001	4	0.0004
- Caída de la Central Telefónica	- Caída de la Central Telefónica	0.0001	4	0.0004
- Caída del Servidor de Firewall	- Caída del Servidor de Firewall FWSUNASS	0.0001	4	0.0004
- Caída del Servidor de Correos	- Caída del Servidor de Correo LOTUS.SUNASS	0.0001	4	0.0004
- Caída del Servicio de Internet	- Caída del Servicio de Internet – Falla del Router	0.0001	4	0.0004
- Caída del Servidor Web	- Caída del Servidor Web WEBSERVER	0.0001	3	0.0003

3 Análisis de Activos.

Tomando como referencia los niveles de riesgo calculados en el punto anterior y, aplicando la ley de Pareto encontramos que para los 26 distintos factores de riesgo analizados bastará con atender al 20% de ellos para tener un impacto de aproximadamente 80% de efectividad sobre el control del total de riesgos identificados.

No obstante, con el fin de mitigar los efectos de los riesgos hemos considerado seleccionar el 25% de los 26 factores de riesgos identificados, es decir los 8 factores de riesgo con mayor nivel de riesgo.

Los eventos críticos de TI mencionados a nivel institucional y las consideraciones técnicas se deben tener en cuenta para minimizar el impacto de ellos. Se debe analizar los distintos agentes que originan los eventos, los activos involucrados en el control del mismo, los controles existentes tanto preventivos como correctivos y los controles a implementar.

4 Sistemas de Información

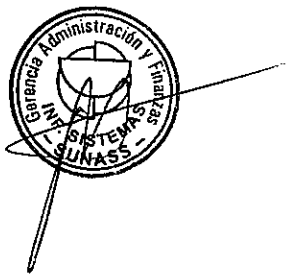
El análisis de riesgos efectuado a los sistemas de información de la SUNASS, ha permitido identificar cuales son los sistemas más críticos que permitan asegurar las funciones principales de la SUNASS para los casos de ocurrir alguna contingencia. A continuación su muestra un cuadro resumen de dicho análisis de riesgo.

OPERACIONES CRITICAS	ACTIVIDADES PRINCIPALES	USUARIO RESPONSABLE
SISTEMA DE RECLAMOS	Permite llevar el registro, seguimiento y control de los expedientes de reclamos que deben ser atendidos por la SUNASS en un plazo determinado.	Luis Espinal Vasquez
SISTEMA DE GESTION DOCUMENTARIA	Recepción, trámite y control de todos los documentos que ingresan y salen de la SUNASS.	Nelly Gutiérrez Porras
SISTEMA DE GESTION ADMINISTRATIVA	Integrar todas las funciones administrativas de las áreas de Logística, Finanzas, Contabilidad, Presupuesto y Recursos Humanos, buscando mejorar su gestión de manera eficiente y eficaz.	José Zavala Muñoz

5 Servicios Críticos

En conclusión, los servicios críticos institucionales Son:

- Caída del Servicio de Base de datos TRASS, SUNDESA.
- Caída del Servidor NOTES.
- Caída del Servidor MARTE.
- Caída del Servidor ARCHIVOS.
- Caída del servidor Web WEBSERVER.
- Caída del Servidor Firewall.
- Caída del Suministro Eléctrico.



Acciones Correctivas

1. Caída de Servidor TRASS, SUNDESA

EVENTO	ACCION CORRECTIVA	RESPONSABLE
Caída del motor de Base de Datos	1. El administrador de Base de Datos procederá a evaluar la gravedad del daño de la base de datos; revisará la bitácora de eventos de la base de datos, o alguna otra fuente de registro para indagar algún código de error (ORA-). Con esta información, el Administrador de Base de Datos revisará en el Knowledge Base de Melalink acerca de cómo solucionar este problema, y así ejecutará las acciones necesarias pare restaurar la operatividad de la base de datos. Caso contrario, el DBA deberá reportar el incidente (Service Request) para ser solucionado por el personal de Oracle a través del Metalink. 2. De no ser resuelto el incidente, el Administrador de base de datos procederá a la búsqueda del backup más reciente de las bases de datos y de los instaladores del motor de base de datos para proceder con la restauración. Asimismo, continuará con la creación del ambiente de producción para la restauración de las bases de datos que corren en el servidor crítico. 3. El administrador de base de datos y el analista de sistemas procederán a realizar las pruebas necesarias para el levantamiento de las bases de datos. 4, Superado el evento, el Administrador de Base de Datos informará al Jefe del Area de Informática y Sistemas, el Gerente de Administración y a los usuarios perjudicados, la habilitación del servicio de Bases de Datos.	- Administrador de Base de Datos - Analista de Sistemas
Falla del Sistema Operativo	1. En caso de que la falla provenga del sistema operativo, el Asistente de Soporte procederá a evaluar la posibilidad de restaurar el mismo. De ser imposible dicha restauración se deberá proceder a la acción correctiva descrita en el punto 2.	- Asistente de Soporte

2. Caída de Servidor NOTES

EVENTO	ACCION CORRECTIVA	RESPONSABLE
Falla del Hardware: Fuente de Alimentación, memorias RAM, procesador, Disco Duro, Mainborad, tarjeta de Red, cable de Red	1. En caso de que la falla provenga del disco duro, memorias RAM, procesador y/o tarjeta de red, el Asistente de Soporte evaluará rápidamente con Soporte técnico su posible cambio de acuerdo a la disponibilidad existente. De ser este cambio imposible y/o sí la falla es una caída irreparable de la Mainboard o del equipo en su conjunto, el Asistente de soporte iniciará las acciones para habilitar el servidor de contingencias. 2.- Al asegurarse de que los servicios necesitan ser restaurados al servidor de contingencias, el Asistente de Soporte informará del hecho al Jefe del Area de informática y Sistemas, al Gerente de Administración y a los usuarios perjudicados con el uso de los servicios y aplicaciones, así como el periodo aproximado de restauración de los mismos. 3.- El Asistente de soporte debe asegurar la habilitación del servidor de contingencias. El Analista de Sistemas procederá a la búsqueda del backup más reciente de los archivos para proceder con la restauración, Asimismo, el analista de sistemas continuará con la creación del ambiente de producción para la restauración de las aplicaciones que corren en el servidor crítico. 4.- El Asistente de soporte, el administrador de base de datos y el analista de sistemas procederán a realizar las pruebas necesarias para el levantamiento de las bases de datos. 5.-Superado el evento, el Asistente de soporte informará al Jefe del Area de Informática y Sistemas, al Gerente de Administración y a los usuarios perjudicados, el reinicio de los servicios y bases de datos.	- Administrador de Base de Datos - Analista de Sistemas
Falla del Sistema Operativo	1. En caso de que la falla provenga del sistema operativo, el Asistente de soporte procederá a evaluar la posibilidad de restaurar el mismo. De ser imposible dicha restauración se deberá proceder a la acción correctiva descrita en el punto anterior – **Falla de Hardware.**	- Asistente de soporte

3. Caída de Servidor MARTE

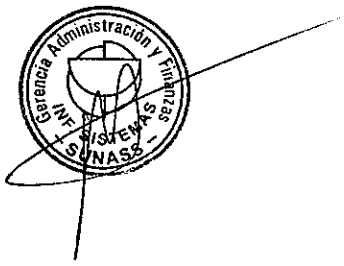
EVENTO	ACCION CORRECTIVA	RESPONSABLE
Falla del Hardware: Fuente de Alimentación, memorias RAM, procesador, Disco Duro, Mainborad, tarjeta de Red, cable de Red	1. En caso de que la falla provenga del disco duro, memorias RAM, procesador y/o tarjeta de red, el Asistente de Soporte evaluará rápidamente con Soporte técnico su posible cambio de acuerdo a la disponibilidad existente. De ser este cambio imposible y/o sí la falla es una caída irreparable de la Mainboard o del equipo en su conjunto, el Asistente de soporte iniciará las acciones para habilitar el servidor de contingencias. 2.- Al asegurarse de que los servicios necesitan ser restaurados al servidor de contingencias, el Asistente de Soporte informará del hecho al Jefe del Area de informática y Sistemas, al Gerente de Administración y a los usuarios perjudicados con el uso de los servicios y aplicaciones, así como el periodo aproximado de restauración de los mismos. 3.- El Asistente de soporte debe asegurar la habilitación del servidor de contingencias. El Analista de Sistemas procederá a la búsqueda del backup más reciente de los archivos para proceder con la restauración, Asimismo, el analista de sistemas continuará con la creación del ambiente de producción para la restauración de las aplicaciones que corren en el servidor crítico. 4.- El Asistente de soporte, el administrador de base de datos y el analista de sistemas procederán a realizar las pruebas necesarias para el levantamiento de las bases de datos. 5.-Superado el evento, el Asistente de soporte informará al Jefe del Area de Informática y Sistemas, al Gerente de Administración y a los usuarios perjudicados, el reinicio de los servicios y bases de datos.	- Administrador de Base de Datos - Analista de Sistemas
Falla del Sistema Operativo	1. En caso de que la falla provenga del sistema operativo, el Asistente de soporte procederá a evaluar la posibilidad de restaurar el mismo. De ser imposible dicha restauración se deberá proceder a la acción correctiva descrita en el punto anterior – **Falla de Hardware.**	- Asistente de soporte

4. Caída de Servidor ARCHIVOS

EVENTO	ACCION CORRECTIVA	RESPONSABLE
Falla del Hardware: Fuente de Alimentación, memorias RAM, procesador, Disco Duro, Mainborad, tarjeta de Red, cable de Red	1. En caso de que la falla provenga del disco duro, memorias RAM, procesador y/o tarjeta de red, el Asistente de Soporte evaluará rápidamente con Soporte técnico su posible cambio de acuerdo a la disponibilidad existente. De ser este cambio imposible y/o sí la falla es una caída irreparabie de la Mainboard o del equipo en su conjunto, el Asistente de soporte iniciará las acciones para habilitar el servidor de contingencias. 2.- Al asegurarse de que los servicios necesitan ser restaurados al servidor de contingencias, el Asistente de Soporte informará del hecho al Jefe del Area de informática y Sistemas, al Gerente de Administración y a los usuarios perjudicados con el uso de los servicios y aplicaciones, así como el periodo aproximado de restauración de los mismos. 3.- El Asistente de soporte debe asegurar la habilitación del servidor de contingencias. El Analista de Sistemas procederá a la búsqueda del backup más reciente de los archivos para proceder con la restauración, Asimismo, el analista de sistemas continuará con la creación del ambiente de producción para la restauración de las aplicaciones que corren en el servidor crítico. 4.- El Asistente de soporte, el administrador de base de datos y el analista de sistemas procederán a realizar las pruebas necesarias para el levantamiento de las bases de datos. 5.-Superado el evento, el Asistente de soporte informará al Jefe del Area de Informática y Sistemas, al Gerente de Administración y a los usuarios perjudicados, el reinicio de los servicios y bases de datos.	- Administrador de Base de Datos - Analista de Sistemas
Falla del Sistema Operativo	1. En caso de que la falla provenga del sistema operativo, el Asistente de soporte procederá a evaluar la posibilidad de restaurar el mismo. De ser imposible dicha restauración se deberá proceder a la acción correctiva descrita en el punto anterior – **Falla de Hardware.**	- Asistente de soporte

5. Caída de Servidor WEB WEBSERVER

EVENTO	ACCION CORRECTIVA	RESPONSABLE
Falla del Hardware: Fuente de Alimentación, memorias RAM, procesador, Disco Duro, Mainborad, tarjeta de Red, cable de Red	1. En caso de que la falla provenga del disco duro, memorias RAM, procesador y/o tarjeta de red, el Asistente de Soporte evaluará rápidamente con Soporte técnico su posible cambio de acuerdo a la disponibilidad existente. De ser este cambio imposible y/o sí la falla es una caída irreparabie de la Mainboard o del equipo en su conjunto, el Asistente de soporte iniciará las acciones para habilitar el servidor de contingencias. 2.- Al asegurarse de que los servicios web necesitan ser restaurados al servidor de contingencias, el Asistente de Soporte informará del hecho al Jefe del Area de informática y Sistemas, al Gerente de Administración y a los usuarios perjudicados con el uso de los servicios y aplicaciones, así como el periodo aproximado de restauración de los mismos. 3.- El Asistente de soporte debe asegurar la habilitación del servidor de contingencias. El Analista de Sistemas procederá a la búsqueda del backup más reciente de los archivos para proceder con la restauración, Asimismo, el analista de sistemas continuará con la creación del ambiente de producción para la restauración de las aplicaciones que corren en el servidor crítico. 4.- El Asistente de soporte, el administrador de base de datos y el analista de sistemas procederán a realizar las pruebas necesarias para el levantamiento de las bases de datos y servicios web. 5.-Superado el evento, el Asistente de soporte informará al Jefe del Area de Informática y Sistemas, al Gerente de Administración y a los usuarios perjudicados, el reinicio de los servicios y bases de datos.	- Asistente de Soporte - Administrador de Base de Datos - Analista de Sistemas
Falla del Sistema Operativo	1. En caso de que la falla provenga del sistema operativo, el Asistente de Soporte procederá a evaluar la posibilidad de restaurar el mismo. De ser imposible dicha restauración se deberá proceder a la acción correctiva descrita en el punto anterior – Falla de Hardware.	- Asistente de Soporte



6. Caída de Servidor de Firewall

EVENTO	ACCION CORRECTIVA	RESPONSABLE
Falla del Hardware: Fuente de Alimentación, memorias RAM, procesador, Disco Duro, Mainborad, tarjeta de Red, cable de Red	1. En caso de que la falla provenga del disco duro, memorias RAM, procesador y/o tarjeta de red, el Asistente de soporte evaluará rápidamente con Soporte técnico su posible cambio de acuerdo a la disponibilidad existente. De ser este cambio imposible y/o sí la falla es una caída irreparable de la Mainboard o del equipo en su conjunto, el Asistente de soporte iniciará las acciones para habilitar el servidor de contingencias. 2.- Al asegurarse de que los servicios necesitan ser restaurados al servidor de contingencias, el Asistente de soporte informará del hecho al Jefe del Area de informática y Sistemas, al Gerente de Administración y a los usuarios perjudicados con el uso de los servicios y aplicaciones, así como el periodo aproximado de restauración de los mismos. 3.- El Asistente de soporte debe asegurar la habilitación del servidor de contingencias. El Analista de Sistemas procederá a la búsqueda del backup más reciente de los archivos para proceder con la restauración, Asimismo, el analista de sistemas continuará con la creación del ambiente de producción para la restauración de las aplicaciones que corren en el servidor crítico. 4.- El Asistente de soporte y el analista de sistemas procederán a realizar las pruebas necesarias para el levantamiento del servicio de Firewall. 5.-Superado el evento, el Asistente de soporte informará al Jefe del Area de Informática y Sistemas, al Gerente de administración y a los usuarios perjudicados, el reinicio de los servicios y bases de datos.	- Asistente de soporte - Analista de Sistemas
Falla del Sistema Operativo	1. En caso de que la falla provenga del sistema operativo, el Asistente de soporte procederá a evaluar la posibilidad de restaurar el mismo. De ser imposible dicha restauración se deberá proceder a la acción correctiva descrita en el punto anterior – **Falla de Hardware.**	- Asistente de Soporte

7. Caída de Suministro Eléctrico

Todos los Servidores, equipos de comunicación Central Telefónica están conectados a un sistema ininterrumpido de energía (UPS).

EVENTO	ACCION CORRECTIVA	RESPONSABLE
Caída de suministro Eléctrico	1.- Ante una eventual caída de suministro eléctrico, el Administrador de base de datos procederá de manera inmediata a realizar el apagado correcto de las bases de datos en producción, para este caso se necesita que el Administrador de base de datos haga uso de métodos que le permita el apagado inmediato de las bases de datos en un tiempo mínimo, Comunicaciones, seguidamente se confirmará el hecho al Jefe del Area de informática y Sistemas y al Asistente de Soporte. 2.- El Asistente de soporte procederá inmediatamente al apagado de los servicios, de la central telefónica y a continuación de los servidores, Para el apagado correcto de los servidores en un tiempo mínimo, el Asistente de Soporte procederá a ejecutar un script que le permita el apagado automático de los servidores, 3.- El Jefe del Area de Informática y Sistemas procederá a indagar acerca del tiempo de duración del corte de suministro eléctrico a fin de comunicarlo al Asistente de soporte, De ser un corte prolongado de suministro eléctrico, el Asistente de soporte procederá a coordinar la contratación de un Proveedor de Generador Eléctrico cuya capacidad sea la adecuada para permitir el normal funcionamiento de los equipos de la red informática, 4.- El Jefe del Área de Informática y Sistemas y el Asistente de soporte, con ayuda del personal de Soporte Técnico, comunicarán vía teléfono celular a las distintas áreas y oficinas descentralizadas del evento sucedido. 5.- Luego de restablecido el suministro eléctrico con el generador eléctrico contratado, el Asistente de soporte procederá a encender los equipos de comunicaciones, servidores y Central telefónica, Seguidamente, el Administrador de Base de Datos procederá al levantamiento de las bases de datos y servicios. 6.- El Administrador de la Red y Comunicaciones, conjuntamente con personal del Area de Informática y Sistemas procederán a realizar las pruebas de los servicios y aplicaciones, dispositivos de comunicación y central telefónica para asegurar su correcto funcionamiento. 7.- El Jefe de informática y Sistemas y el Asistente de soporte con ayuda del personal de soporte Técnico, comunicarán vía telefónica a las distintas áreas y oficinas descentralizadas del funcionamiento de los servicios y equipos. 8.- Al restablecer el servicio de suministro eléctrico y proceder al retiro del Generador eléctrico contratado, el Asistente de Soporte procederá a coordinar con el personal del Area de Informática y Sistemas el apagado adecuado de los equipos siguiendo los pasos 1 y 2 en un horario que no interrumpa las labores de los usuarios, 9.- Al restablecerse el servicio de suministro eléctrico, ya sea por el apagado del generador eléctrico contratado o por el restablecimiento del suministro eléctrico; dentro de las tres horas establecidas como no críticas, se procederá al prendido de los equipos y a la prueba de los mismos siguiendo los pasos 5 , 6 y 7.	- Jefe del Area de Sistemas - Administrador de Base de Datos - Asistente de Soporte

Si el corte de fluido eléctrico es prolongado se procederá a solicitar la autorización a la Gerencia de Administración y Finanzas a fin de contratar un grupo electrógeno y restituir los servicios básicos que permitan a la institución a seguir operando.

En caso de ser necesario se podrá optar por los registros de los datos de los sistemas de información de forma manual hasta que sea superado el evento. Para esto, se anexan los formatos a ser utilizados por cada sistema.

Acciones Correctivas para eventos Externos

5.1 Fuego

5.1.1 Acciones previas al evento

SUNASS cuenta con un sensor de humo en la sala de cómputo principal, el cual, por medio de una alarma, hará de conocimiento del personal de seguridad la ocurrencia de un suceso de este tipo. La ubicación de los extintores de fuego deberá estar señalizada y se deberá designar y capacitar al personal encargado de manipular los mismos.

5.1.2 Acciones durante el evento

El jefe del área de Informática y Sistemas será el responsable de realizar las siguientes acciones:

- Informar a vigilancia de la ocurrencia del incidente para que ellos informen a la compañía de bomberos
- Organizar al personal encargado de manipular los equipos de extinción de fuego.

5.1.3 Acciones después del evento

El Asistente de Soporte y el personal de Soporte Técnico deberán verificar la operatividad de los equipos, y proceder con el plan de contingencia por Fallas de hardware. El analista de sistemas será el responsable de aplicar el plan de contingencia de sistemas de información durante el periodo de recuperación de los servicios.

5.2 Terremoto

5.2.1 Acciones previas al evento

Deberán realizarse labores de respaldo de información de acuerdo a las políticas de respaldo y recuperación establecidas. Las cintas de backup deberán ser enviadas al archivo externo de la institución.

5.2.2 Acciones durante el evento

Las acciones durante el evento no aplican al presente plan ya que durante esta emergencia, el recurso humano que administra los equipos de cómputo procederá a evacuar las instalaciones de manera rápida y ordenada con el fin de salvaguardar sus vidas.

5.2.3 Acciones después del evento

Los administradores de los servidores determinarán la magnitud del daño en los equipos. De encontrarse sin daños tanto el edificio como los equipos, estos últimos podrían ser puestos en funcionamiento. De lo contrario, los equipos que todavía se encuentren operativos, tendrían que ser trasladados a otro espacio físico para proceder con la restauración de los servicios.

Si el evento hubiese ocasionado daño en los equipos, deberá tenerse en cuenta el uso de equipos de contingencia contratados a un proveedor y/o su adquisición rápida y efectiva ante esta emergencia. Seguidamente, se procederá a la restauración de la información desde las cintas de backup procedentes del archivo externo.

5.3 Inundación

5.3.1 Acciones previas al evento

Ubicar a los equipos a una altura minima de aproximadamente 12 cm de alto del piso, para asegurar que los equipos de la sala de cómputo no se vean afectados por problemas de inundación. Asimismo, las tomas eléctricas y de red deberán encontrarse a una altura adecuada sobre el piso, y el cableado eléctrico, de voz y de datos deberán estar protegidos por canaletas, bandejas y/o tubo corrugado, de manera que pueda evitarse posibles cortos circuitos por el contacto con agua.

5.3.2 Acciones durante el evento

El Asistente de Soporte junto con el personal de Soporte Técnico, deberán informar a los usuarios que se procederá a realizar el corte de los servicios de los distintos sistemas, permitiendo así que dichos usuarios se desconecten de los sistemas y almacenen su información, disminuyendo los riesgos de pérdida de información.

Seguidamente, se procederá a apagar los equipos y desconectarlos de la línea de alimentación eléctrica.

5.3.3 Acciones después del evento

El Asistente de Soporte conjuntamente con el personal de Soporte Técnico, deberán asegurarse de que no existan contactos húmedos. Luego, deberán encender los equipos y verificar la integridad de los servicios de red ofrecidos; y por último, comunicar a los usuarios la disponibilidad de los dichos servicios.

V. PRUEBAS

1. Introducción

Las pruebas son una parte muy significativa del Proyecto de contingencia de las aplicaciones, no sólo por su importancia en el logro de resultados correctos sino por el tiempo y recursos requeridos.

En la fase de pruebas se debería comprometer a toda la Institución segmentada según la aplicación que le corresponde, siendo el usuario final quien certificará la "aceptación" del sistema que utiliza.

Las pruebas de cambios para aplicaciones tienen características particulares. Mientras para los cambios tradicionales se debe probar que los sistemas tienen un nuevo comportamiento, acorde con los cambios establecidos, en éstas se deberá verificar que:

a) Se mantenga inalterado el comportamiento de los sistemas, con datos anteriores al cambio
b) Los sistemas deben ser capaces de procesar en forma correcta la información anterior y posterior al cambio, del próximo y de la transición entre ambos
c) No deberán aparecer nuevos campos, por no haber sido identificados en fases anteriores.

2. El Plan de Pruebas

En el desarrollo de las Pruebas participaran representantes de distintas áreas y niveles, dado que no son tareas exclusivas del área de sistemas de la organización, sino que los usuarios son parte fundamental en la tarea de verificación de la correcta operación. La extensión de los cambios y la trascendencia que puede tener una falla, requiere que en las pruebas se involucren los responsables del más alto nivel.

Deberá preverse pruebas de:

a) Hardware y Software de Base
b) Programas utilitarios estándar
c) Programas aplicativos
d) Equipamiento no informático
e) Interfaces.

Es necesario probar los sistemas y equipamientos, independientemente de que sus programas hayan o no sufrido adecuaciones, priorizando aquellos que soportan funciones críticas.

El Plan de Pruebas establecerá la preparación de informes, fijando su periodicidad, formato y contenido. No deberá perderse de vista la alta trascendencia de esta parte de las actividades, que constituye más de la mitad del Proyecto total, y merece un especial seguimiento y control.

3. Metodología

Dentro de la metodología para las pruebas se deberán tener en cuenta dos aspectos fundamentales:

1. Definición de pautas claras para generar el ambiente de prueba
2. Procedimientos operativos para los distintos niveles y tipos de pruebas

3.1 Ambiente de Prueba

Básicamente se interpreta como "Ambiente de Prueba" al conjunto formado por:

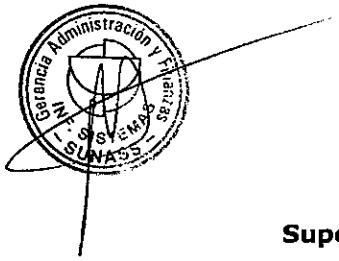
- Recursos físicos (equipamiento, almacenamiento de discos, etc.)
- Conjunto de Lotes de Prueba

- Escenarios de Prueba

El ambiente de prueba deberá ser aislado del de producción y soportar los cambios del sistema, sin afectar:

- Autorizaciones
- Seguridad
- Licencias
- Archivos y Bases de datos
- Acceso de red
- Aplicaciones activadas por tiempos de ejecución

Finalmente se debe indicar que para la realización de pruebas del presente plan se recomienda realizar por lo menos una vez al año, para lo cual se sugiere realizar esta prueba en el mes de OCTUBRE de cada año, este cronograma debe ser aprobado por la Gerencia de Administración y Finanzas.



VI. ACTUALIZACION DEL PLAN

El plan de contingencias deberá ser revisado por el Jefe del Área de Informática y Sistemas, Administrador de Base de Datos, el Asistente de Soporte y el Analista de Sistemas en forma periódica para proponer cambios y/o adaptaciones como mejoras, buenas prácticas y/o las correspondientes actualizaciones por cambios de equipos informáticos y de seguridad.

Los Proyectos de contingencia deberán considerar los siguientes puntos:

- **Objetivo del Proyecto:** se indicara aquellos componentes de la función crítica que se pretenden cubrir frente a la contingencia considerada. Estos componentes pueden variar, así como su grado de cobertura para las distintas contingencias analizadas. Ej. continuar con operaciones normales o con restricciones, continuar operando manualmente, etc.
- **Criterio para ejecución del Proyecto:** condiciones bajo las cuales se considera que debe comenzar a aplicarse el plan de contingencia. Ej. No se concluye a término el plan de adecuación, falta de disponibilidad de hardware o software de base.
- **Tiempo esperado** de duración del Proyecto. Es decir, el tiempo máximo que se puede continuar operando bajo estas condiciones de contingencia.
- **Roles, responsabilidades y autoridad**
- **Pruebas** de los planes y **Capacitación**
- Procedimientos para **iniciar** y **operar** en modo de contingencia
- **Requerimiento de recursos** para operar en modo contingencia
- Criterio y procedimientos para **volver al modo operativo** normal
- Procedimientos de **recuperación** de datos perdidos o dañados.

ANEXO I Sistemas Embebidos

1. Introducción

La denominación de Sistemas embebidos (embedded) refleja que son una parte integral (interna) del sistema, y en general son dispositivos utilizados para controlar o asistir la operación de diversos equipamientos. El problema se origina en los circuitos integrados (chips) con lógicas sensibles al tiempo y en los microprocesadores en general. Cuando los fabricantes necesitan incluir capacidades de medición de *"intervalos de tiempo"* en sus sistemas, generalmente utilizan chips de propósito general (*"timer chips"*), dado que los circuitos a medida resultan antieconómicos.

2. Fases de adecuación de sistemas embebidos:

- Inventario de equipamiento
- Análisis y Evaluación
- Adecuación

FASE 1: Inventario de equipamiento.

1. Definición de áreas de impacto y riesgo asociado

Para poder asignar prioridades, se han definido diferentes categorías ó áreas de impacto, que se verán afectadas en caso de falla o mal funcionamiento de un equipamiento.

En lo que sigue se especifican las categorías como guía de referencia, y cada área puede considerar necesario el agregado de otras tareas de acuerdo a sus funciones específicas:

- *Impacto ambiental:* cuando la falla o degradación de un sistema impacta negativamente el ambiente de trabajo.
- *Impacto operacional:* la falla de un sistema afecta la operatividad de una determinada área SUNASS.
- *Otros:* dependiendo de cada área se definirán categorías adecuadas a sus funciones específicas.

Con el Objetivo de ordenar y focalizar el análisis posterior en los sistemas más críticos, se establece tres niveles de gravedad (ej. : alto, medio y bajo) que permiten evaluar el riesgo de las consecuencias de un fallo o mal funcionamiento de los equipos y sistemas inventariados.

EQUIPOS CRITICOS DE LA SUNASS

ITEM	NIVEL DE GRAVEDAD	EQUIPOS
1.	ALTO	- Equipos de Comunicación - UPS, Establizadores - Central Telefónica
2.	MEDIO	- Impresoras - Fotocopiadoras, Escanner
3.	BAJO	- Proyectores

2. Definición de datos a relevar
En esta etapa se han definido los datos que se relevarán de los distintos equipamientos, que podrían ser los siguientes:

- Datos del área: nombre, instalación, nombre o persona de contacto.
- Datos del equipo o sistema: Nro. de serie, marca, modelo, tipo, uso, fecha de adquisición, población, etc. En caso de estar compuesto por diferentes componentes o subsistemas se detallará la relación entre ellos y los datos anteriores para cada uno (sistema o equipo provisto por un integrador que contiene diversas componentes de distintos fabricantes)
- Interfaces internas y externas que soporta el sistema o equipamiento relevado.
- Categoría y nivel de gravedad
- Sensibilidad: identificar el conocimiento de la persona entrevistada sobre características sensibles a fallas del sistema, equipamiento o interfase.

Es importante no olvidar que todo los sistemas pueden ser sensibles a fallas aún si no presenta ninguna de las características anteriores, como sistemas que no tienen funciones criticas.

3. Relevamiento de datos
Se ha definido la estructura del equipo que llevará adelante el relevamiento de los datos, responsabilidades y tareas a realizar, como así también en caso de ser necesario, subdivisiones en diferentes áreas o sectores, para poder obtener una mayor paralelización del trabajo.

Tarea	Responsable Cargo	Nombre
Coordinación General	Especialista en Sistemas e Informática	Cesar Gamarra
Equipos de Usuario Final	Técnico en Soporte	Oliver León
Servidores	Encargado en Infraestructura y Comunic.	Emerson Pastor
Dispositivos de Comunicación	Encargado en Infraestructura y Comunic.	Emerson Pastor
Sistemas de Información	Especialista en Sistemas/Analista Prog.	Iván Galván/Jorge Salazar

Se debe normar la forma en que se comunicará e informará al personal de SUNASS sobre las tareas que se llevarán adelante.
Se han definido los procedimientos de recolección de datos, de almacenamiento, reportes, para su posterior tratamiento y uso, como también los criterios para considerar concluido el relevamiento y pautas generales.

FASE 2: Certificación de fabricantes y proveedores.

Esta fase comprende el proceso de certificación con fabricantes y proveedores y las acciones para determinar si el equipamiento y sistemas toleraran fallas de contingencia, así como el desarrollo de las acciones más efectivas para su solución.

1. Pedido de certificaciones
Del inventario desarrollado en la fase 1, se ha dispuesto de la lista de fabricantes y proveedores a contactar. Para ordenar el proceso de certificación, se han definido procedimientos para el pedido de certificaciones y acciones para el sistema o equipamiento correspondiente y su posterior seguimiento y control.
Deberá pedirse certificación escrita del fabricante o proveedor de la compatibilidad del sistema o equipo, planes para los equipos no compatibles, Costos de actualizaciones y acciones necesarias para su compatibilización. Además se incluirá una fecha límite de

respuesta. Para acelerar el proceso se deberá utilizar el correo electrónico para obtener una respuesta más rápida a la vez que se envía la carta por correo convencional.
Los pedidos de certificación deberán adecuarse a las normar y procedimientos internos de SUNASS, tipo de contrato, licencias y garantías del producto, acordadas en los contratos celebrado por los proveedores y SUNASS.

TABLA DE PROVEEDORES I

COSAPI DATA S.A.	Contacto: Ing. Miguel Carmen Telf.: 2154530-2324 Celular: 997570274 mcarmen@cosapidata.com.pe Calle Dean Valdivia 205 San Isidro
OPTICAL IP S.A.	Teléfono Central de Soporte: 7107500 Contacto: Ing. Juan Carlos Espinoza. 250011 anexo 243 - Celular 8704755 jespinoza@optical.com.pe Calle Carlos Krumdlieck 287 Panamá 4069 Surquillo
TELMEX DEL PERU	Teléfono Central de Soporte: 610-555 Contacto: Jimmy Carrión 610-2057 – 99759-4972 jimmy_carrion@temex.com Av. Larco 1301 Torre Parque Mar, Miraflores
EBD - ALCATEL	Telefono Central de Soporte: 712-5000 Contacto : Edwin Galindo 7125040 – 993524094 *egalindo@ebdperu.com* Av. Jose Galvez Barrenechea 996 San Isidro
TELEFONICA MOVILES	Teléfono Central de Soporte: 2109000 Contacto : Ricardo Bezada 210-9605 – 996592057 jrbezada@tp.com.pe Av. Jorge Basadre 592 piso 2 San Isidro
ASP SYSTEM	Teléfono de Soporte: 242-9470 Contacto : Jaime Sandoval 834,8122612 jsandoval@aspsperu.com Jr. Porta N° 170 Of. 409 Miraflores

TABLA DE PROVEEDORES II

EMPRESA	TIPO DE CONTINGENCIA	PERSONA	TELEFONO
PERSONAL	Central Telefónica	Téc. Edwin Galindo	9057784
ALCATEL	Central Telefónica	Sr. Alfredo Mejia	4401715
TELEFONICA	Comunicación	Sra. Gisella Navarro	210-9560
ALCATEL	Comunicación	Sr. Edwin Galindo	712-5040
EDELNOR	Energía	Atención al Cliente	103
Sist. Eléctrico	Energía	Juan Céspedes Navarro	9348113

2. Determinación de compatibilidad
Una vez recibidas las respuestas de los proveedores, se identificarán las que no respondan claramente o estén incompletas para un análisis posterior. Las certificaciones se deben revisar cuidadosamente. Es importante notar que diferentes entornos de prueba pueden llevar a resultados distintos y que un sistema o equipamiento puede ser compatible en un cierto entorno y no en el propio. Esto requerirá de un examen de los datos de prueba provistos por el proveedor y de los procedimientos seguidos, todo lo cual podrá requerir un mayor grado de detalle en las pruebas realizadas, especialmente para aquellos sistemas críticos (TEMPUS, FIREWALL, ANTIVIRUS, NOTES).

3. Pruebas de compatibilidad
Estas pruebas se realizan en los casos de que no se tenga respuesta del fabricante y/ proveedor, de sistemas o equipos críticos, sistemas o equipos en desarrollo específico. El Objetivo de la prueba es observar el comportamiento del sistema o equipo en escenarios adversos al normal funcionamiento.

Plan de pruebas:
En cada caso se ha determinado el nivel de pruebas apropiado para cada sistema, entorno, condiciones de prueba, recursos, y sistemas de interfaces que será necesario incluir en los niveles de la prueba.
Cada sistema debería tener su plan individual de prueba, e incluir especificaciones, rutinas, procedimientos de prueba y el cronograma de trabajo correspondiente a cada uno de los proyectos de contingencia.
Para las pruebas se deberá contactar al fabricante o proveedor para averiguar sobre procedimientos de pruebas disponibles, manuales de operador y coordinación de las actividades de prueba.

Niveles de prueba: para cada sistema y/o equipamiento se ha determinado el nivel de pruebas a realizar, que el cual esta agrupado de la siguiente forma:

- **Nivel de instalación**: prueba de múltiples todos los sistemas de SUNASS con interfases internas y externas.
- **Nivel de sistema**: prueba dentro de los límites de cada una de las aplicaciones de SUNASS, asegurando que se maneja correctamente las funciones y procedimientos y no se producen errores.
- **Nivel de componente**: al azar se determina y prueba un componente aisladamente.

El nivel de prueba se determinará dé acuerdo con las características y requerimientos particulares de cada área. Para el sistema SIGA, el cual cuenta con múltiples interfases y cuya falla tiene un alto impacto deben realizarse todos los niveles de prueba.

4. Evaluación de riesgo

Esta actividad comprende el análisis de escenarios de falla de los componentes no-compatibles. Requiere la evaluación de la criticidad o gravedad en relación con los otros componentes dentro de la misma área de impacto; tipos de riesgos del componentes e impacto de fallas asociados; costo estimado de las fallas; y vulnerabilidad del sistema (cómo falla) y tiempo de recuperación del sistema.

Una vez finalizado el inventario y al disponer de la información de los fabricantes de cada uno de los sistemas, y de las acciones para determinar la compatibilidad, se deberá redefinir su importancia y pase a ser nominado como componente crítico para SUNASS. Será necesario reevaluar aquellos componentes que se han determinado no-compatibles o de los cuales se desconoce su estado dentro de la categoría de riesgo y de su gravedad.

Se revisarán nuevamente los sistemas completos con sus interdependencias, e identificarán los riesgos involucrados y los impactos que resultarán de la falla de alguno de sus componentes.

Vulnerabilidad del sistema:

- **Severa**: El componente identificado fallará en su operación normal sin adecuación. El tiempo de recuperación del sistema es significativo y no aceptable.
- **Moderada**: El componente identificado fallará en su operación normal o requerirá de intervención manual para restablecer sus condiciones normales de operación. Se requerirá intervención más de una vez por turno o ciclo de operación de máquina.
- **Mínima**: El sistema o componente identificado puede requerir intervención manual para restablecer sus condiciones normales de operación sólo una vez. Probablemente no serán requeridas futuras intervenciones.

El análisis de vulnerabilidad con los demás análisis de riesgo asistirá en la toma de decisiones cuando se determinen las prioridades de adecuación de los sistemas y se desarrollen las estrategias de adecuación.

Luego de evaluados los posibles riesgos e impactos asociados con las fallas de los sistemas, se deberán trabajar en conjunto con los responsables de las distintos áreas de SUNASS para revisar lo encontrado y desarrollar una lista ordenada por prioridades de todos los sistemas que requieren adecuación. Esta lista de prioridades se utilizará para desarrollar las estrategias de adecuación. Esta Priorizacion asegurará que los sistemas más críticos y de alto riesgo, sean tratados primero y los esfuerzos de adecuación se realicen en forma metódica.

5. Desarrollo de estrategia de adecuación

Básicamente las estrategias de adecuación se han agrupado entre las siguientes:

- **No adecuar**: El sistema y/o componentes es compatible; no se utiliza más; no es esencial para el departamento; o no se puede actualizar o reemplazar.
- **Actualizar**: Se encuentra disponible una versión o Release compatible.
- **Reemplazar**: No existe versión o Release compatible o no es deseable por el costo, requerimientos adicionales o tiempos. Existe un sistema y/o equipamiento funcionalmente equivalente o compatible disponible por un proveedor o fabricante.
- **Rodeo**: solución temporaria o permanente como acciones manuales o similares para mantener su funcionalidad hasta que la contingencia sea corregida.
- **Indeterminada**: no se puede determinar un proveedor o fabricante responsable; como en el caso del sistema SIGA. Requerirá un manejo especial.

FASE 3: Adecuación.

La fase de adecuación incluye el desarrollo de los planes de adecuación y contingencia, y su implementación.

1. *Plan de adecuación*
   Esta actividad comienza con la revisión de las estrategias de adecuación de los sistemas y/o equipamiento, para determinar el curso de acción para su implementación.
   Esto implica el desarrollo de planes detallados y los requerimientos de adquisiciones, especificaciones y procedimientos de prueba, requerimientos de herramientas o equipamientos, y personal propio de o del fabricante o proveedor necesarios para soportar las actividades de instalación y pruebas.
   Se considerara con especial cuidado las interfases en esta etapa, para coordinar con las distintas áreas involucradas la forma de implementación.
2. *Desarrollo de la contingencia*
   Es altamente improbable que todos los sistemas embebidos sean adecuados después del desarrollo de una contingencia y algunos sistemas validados como compatibles seguramente no funcionarán apropiadamente. Por tanto, es esencial que las áreas de SUNASS desarrollen contingencias que contemplen posibles escenarios de fallas y determinen la mejor forma de minimizar el impacto de dichas fallas dentro de los costos y restricciones disponibles.
   Las áreas de SUNASS deberán considerar el desarrollo de contingencias para aquellos sistemas determinados como críticos, independientemente de la certificación del proveedor o fabricante; para aquellos que su compatibilidad es indeterminada; y para todo sistema que no demuestre exitosamente su compatibilidad luego de las pruebas realizadas.
3. *Ejecutar plan de adecuación*
   En esta actividad se procederá dé acuerdo con el plan de adecuación para llevar adelante las acciones planificadas. Para la mayoría de los sistemas, la adecuación implicará la instalación del nuevo sistema/equipamiento de acuerdo a las Instrucciones y recomendaciones hechas por el fabricante. Es recomendable, realizar inicialmente las actividades de instalación y prueba en las áreas de SUNASS.
4. *Pruebas de aceptación*
   De acuerdo a lo especificado en los planes de adecuación, se realizarán las pruebas de aceptación. Estas comprenderán todas los componentes de los sistemas, incluyendo interfases internas y externas, probadas en su conjunto para determinar la compatibilidad de los sistemas. Se deberá coordinar con el personal usuario involucrado, para asegurar el mínimo impacto de las pruebas sobre los entornos productivos.

ANEXO II Seguridad.

PROCEDIMIENTOS PREVENTIVOS PARA LA INFORMACION ALMACENADA EN LOS SERVIDORES

A. INTEGRIDAD FISICA DE LA INFORMACIÓN (COPIAS DE RESPALDO):

La Unidad de Sistemas de Información procede a respaldar la información contenida en los servidores utilizando un dispositivo de librería de cintas de respaldo Marca Hewlett Packard modelo StorageWorks MSL2024 Ultratrim 1840.

Se cuenta con una Librería de Cintas Hewlett Packard modelo StorageWorks MSL2024 Ultratrim 1840, el mismo que trabaja en conjunto con el Software ARCSERVE v11, solución que permite obtener las cintas de respaldo de la información contenida en los servidores críticos, la misma que se procesa de Lunes a Viernes a la 10:00 pm. (solo la información actualizada) y el día sábado a la 11:00 de la mañana se realiza el backup total de la información contenida en los Servidores Institucionales.

Este esquema de respaldo de la información contempla dos pool de cintas, de acuerdo a lo siguiente:

1.- El pool de cintas diarias, 5 cintas, (Lunes a Viernes), permite mantener en el robot la cinta con la información respaldada del día anterior, esta información se refiere exclusivamente a todos los datos que son administrados por los sistemas de información y los archivos de trabajos de los usuarios.

2.- El pool de cintas semanal, 3 cintas, (Se obtiene el día sábado), permite almacenar un histórico en conjunto de la información de los datos que son administrados por los sistemas de información, los archivos de trabajos de los usuarios así como los programas fuentes y compilados almacenados en los servidores institucionales.

3.- Las copias de Respaldo (Backup de programas fuentes, ejecutables y base de datos), serán almacenados en el Local del Almacén Central de la SUNASS, Av. Materiales N° 2762, Lima-Cercado.

4.- El procedimiento alternativos de respaldo automático de la información es el siguiente: Los archivos DMP que se generan diariamente de los servidores críticos de Base de Datos (SISTRAM, SIGA, SAR y SFIS), son centralizados diariamente en el equipo del Asistente de Soporte Técnico, para que semanalmente estos archivos se quemen en CD's ó DVD's, para su envío posterior al Local de Materiales junto con los archivos correspondientes de respaldo de los Archivos de los usuarios y de los archivos de las imágenes digitalizadas.

B. INTEGRIDAD LOGICA DE LA INFORMACIÓN (ARREGLO DE DISCOS):

Los servidores críticos de la red institucional cuentan con arreglos de discos (RAID) de hardware y software, lo que permite que en el caso de fallar un disco del arreglo, la información contenida en él, pueda seguir siendo procesada, además tienen la característica de ser removibles, aún estando en producción, HOT SWAPPING, la misma que permite que en el caso de haber fallado un disco este pueda ser cambiado sin necesidad de apagar el servidor al que pertenece el disco, por lo cuál los usuarios que

estén trabajando con él, no se verán desconectados de la sesión y por lo cuál podrán seguir laborando, con menor perfomance. Estos servidores son:

- 02 Servidores de Aplicaciones (IBM e-server) servidor de Archivos y servidor de Pagina Web
- 02 Servidores de Aplicaciones (HP Proliant DL 380 G3) servidor de base de datos ORACLE y servidor de Correo Lotus Notes
- 01 Servidor de Aplicaciones (IBM X-SERIES 346) servidor de base de datos ORACLE.

TABLA DE PROGRAMACION DE BACKUP

SISTEMA Y/O APLICATIVO	DETALLE DE LA INFORMACION	SERVIDOR	SISTEMA OPERATIVO	DIRECCION IP	RUTA	TAMAÑO	L	M	M	J	V
Correo Electronico	Archivos	Lotus	Windows 2000 Server	192.168.1.13	C:\Install	1996.8 Mb	X	X	X	X	X
SIGA	Archivos				D:\APP	697 Mb	X	X	X	X	X
SIGA	Archivos				D:\Fuentes_APP	228 Mb	X	X	X	X	X
Correo Electronico	BD				D:\Lotus\Domino\data\mail	46592 Mb	X	X	X	X	X
Correo Electronico	Archivos				D:\Lotus\Domino\data\Ids	383 Mb	X	X	X	X	X
Correo Electronico	BD				D:\Lotus\Domino\data\Libreta Presidencial	23 Mb	X	X	X	X	X
BD Oracle	Archivos	Notes	Windows Server 2003 R2 STD	192.168.1.15	D:\backup	55 Mb	X	X	X	X	X
	Archivos				D:\Lotus\Domino\data	46489.6 Mb	X	X	X	X	X
	Archivos				E:\Escaneo	29491.2 Mb	X	X	X	X	X
	Archivos				E:\Install	1996.8 Mb	X	X	X	X	X
	Archivos				G:\Escaneo	31436.8 Mb	X	X	X	X	X
	Archivos				G:\transferenda	830 Mb	X	X	X	X	X
	Archivos				G:\oracle	26009.6 Mb	X	X	X	X	X
SisTram	Archivos	Sis 04	Windows Server 2003 R2 STD	192.168.1.186	D:\Fuentes	215 Mb	X	X	X	X	X
	Archivos				D:\Procedimiento de Instalacion y Configuracion	2.26 Mb	X	X	X	X	X
FileServer	Archivos	Archivos	Windows Server 2003 ENT	192.168.1.212	D:\CDSPU	4915.2 Mb	X	X	X	X	X
	Archivos				D:\INVENTARIO	1075.2 Mb	X	X	X	X	X
	Archivos				D:\TELECREDITO	115 Mb	X	X	X	X	X
	Archivos				D:\TELEWISE	143 Mb	X	X	X	X	X
	Archivos				E:\	30617.6 Mb	X	X	X	X	X
	Archivos				H:\	30617.6 Mb	X	X	X	X	X
Imaging	Archivos	Img	Windows Server 2003 R2 STD	192.168.1.6	C:\IMG_SUNASS	80486.4 Mb	X	X	X	X	X
	Archivos				C:\Inetpub\wwwroot	4.77 Mb	X	X	X	X	X
	Archivos				D:\ImagingSoft	1945.6 Mb	X	X	X	X	X
	Archivos				D:\pase	423 Mb	X	X	X	X	X
	Archivos				D:\Tempus	53.4 Mb	X	X	X	X	X
	Archivos				D:\Toad for Oracle9	61.7 Mb	X	X	X	X	X
	Archivos				D:\Tomcat	10.7 Mb	X	X	X	X	X
Intranet	Archivos	ImgSunass	Windows XP	192.168.1.34	C:_ImagingView	85913.6 Mb	X	X	X	X	X
	Archivos				C:\bvsde	149 Mb	X	X	X	X	X
	Archivos				C:\IMGS	20172.8 Mb	X	X	X	X	X
	Archivos				C:\imgsoft	160 Mb	X	X	X	X	X
	Archivos				C:\Inetpub\wwwroot	810 Mb	X	X	X	X	X
	Archivos				C:\sicap	144 Mb	X	X	X	X	X
	Archivos				C:\Web	423 Mb	X	X	X	X	X
	Archivos				C:\WorkSpace - EPS	28.5 Mb	X	X	X	X	X
	Archivos				C:\wwwsite	13.8 Mb	X	X	X	X	X
WebServer	Archivos	WebServer	Windows 2000 Server	192.168.1.24	D:\web	8652.8 Mb					
					TOTAL	442.76 Gb					

PROCEDIMIENTOS PREVENTIVOS PARA EL FUNCIONAMIENTO DE LOS SERVIDORES

El encargado en Infraestructura y Comunicaciones deberá tener en cuenta lo siguiente:

A.- VERIFICACIONES ANTES DE ENCENDER LOS SERVIDORES:

Todos los servidores cuentan con el respaldo de equipos UPS (Unidad de Poder Suplementario), activar el dispositivo y sólo cuando las luces de activación se hubieran apagado, encender el equipo de cómputo. En el caso de que las luces de activación no encendieran, proceder a conectar directamente los cables de alimentación eléctrica de los servidores a la toma corrientes de color marfil de fibra de vidrio, cada UPS esta debidamente identificado con una etiqueta que indica a que servidor esta atendiendo.

B. VERIFICACIONES EN EL CASO DE NO ENCENDER EL SERVIDOR:

- Que la alimentación eléctrica de los equipos sea la correcta, 220 Voltios en la línea estabilizada, la misma que será identificada por poseer los enchufes color marfil de fibra de vidrio (no de metal), adosados a la pared, o estar sobrepuestos en el suelo en cuyo caso serán de bronce.

- Que los Cables de Comunicación entre la CPU. (Unidad Central de Proceso), monitor, teclados y los de la red institucional estén correctamente conectados.

- Que los interruptores de encendido estén activados, estos se encuentran en la parte frontal de todos los servidores, también hay que proceder a abrir la tapa frontal del equipo para los equipos IBM e-server.

C. DURANTE EL FUNCIONAMIENTO:

Preventivas

- Se deberá trabajar en un lugar fresco y ventilado.

- La unidad de Aire Acondicionado debe estar operativa y trabajar a una temperatura de 21°c.

Correctivas

- En el caso de un incendio o cortocircuito se procederá a utilizar el extingüidor de fuegos cargado con Halon, el cuál se encuentra ubicado dentro de la sala de servidores.

- El juego de llaves de la bóveda y de la sala de servidores está en poder del Especialista de Sistemas e Informatica, encargado de la red institucional, una copia de las mismas las tiene el área de finanzas en la caja fuerte de la institución para ser utilizada SOLO en caso de emergencia.

MANTENIMIENTO PREVENTIVO Y CORRECTIVO DE LOS EQUIP0OS DE CÓMPUTO

Los servidores institucionales de la SUNASS, cuentan con servicio de mantenimiento preventivo y correctivo realizado como un servicio facturable por atención de llamada, previa autorización de la Jefatura de la Unidad de Sistemas de Información.

Estos servicios podrán ser realizados por los proveedores autorizados por las casas proveedoras para cada caso.

Para el mantenimiento correctivo se ha considerado una cobertura de servicio de todos los días de la semana por 24 horas de atención y un tiempo máximo de respuesta de 04 horas, luego de haberse originado la llamada.,

Todos los servicios realizados en el servidor deben estar registrados en la bitácora de ocurrencias detallando el trabajo realizado, motivo y personal que autorizo el mismo. Además se establece que en el caso de ser retirado el equipo por más de 24 horas la compañía tendrá que dejar por el tiempo necesario un equipo de similares o mejores características a la retirada de manera que no se perjudique la labor operativa de la SUNASS.

ANEXO III Procedimientos Alternativos.

PROCEDIMIENTO ALTERNATIVO DE COPIAS DE RESPALDO

PROCEDIMIENTOS PARA BACKUP DEL SISTEMA OPERATIVO LINUX

CD /HOME/ORACLE/BACKUP

ESTE ES EL DIRECTORIO DONDE SE VA A CREAR EL BACKUP

****

EXP SYSTEM/MARTE FILE =COPYU15022008.DMP LOG=COPY15022008.LOG FULL=Y OWNER=GREP,PRESU,SIGA,SIGA,SIGA_VARIOS COMPRESS=Y

** PARA BAJAR DESDE UNA PC LO EXPORTADO DEL LINUX EN ESTE CASO EL COPY15022008.DMP Y COPY15022008.LOG SE HACE LO SIGUIENTE.

SE INGRESA AL DIRECTORIO DONDE QUIERE QUE SE BAJE EL EXPOR EN MODO DOS O SE EJECUTA LA INTRUCCION (FTP Y ÉL NUMERO DE IP) DE LA BASE DE DATOS ORACLE QUE SE ENCUENTRA EN LINUX DESDE CUALQUIER PC HACIENDO LO SIGUIENTE:

C:\> FTP 192.168.1.70 (enter)

FTP> LOGIN: ESCRIBIR EL ROOT

FTP> PASSWD: CLAVE SECRETA DEL ORACLE

FTP> CD /HOME/ORACLE/BACKUP

FTP> BIN COPYU15022008.DMP
FTP> GET COPYU150220008.DMP

UNA VEZ QUE TERMINO DE MIGRAR EL COPYU15022008.DMP SE PROCEDE HACER LO MISMOS PASOS CON EL COPYU15022008.LOG.
LUEGO DE TERMINADO LOS PROCESOS SE REALIZAN LA ULTIMA INSTRUCCIÓN ES:

FTP> BYE (enter)

C:\>EXIT (enter)

PROCEDIMIENTOS PARA BACKUP DEL SISTEMA OPERATIVO WINDOWS – 2003 Y BASE DE DATOS ORACLE

POSICIONARSE EN EL DIRECTORIO DONDE SE QUIERE QUE SE HAGA EL BACKUP DEL WINDOWS 2003-ORACLE BASE DE DATOS.

C:\> EXP80 SYSTEM / MINERVA@SUNASSU FILE=COPYN15022008.DMP LOG=COPYN15022008.LOG FULL=Y COMPRESS=Y

PARA ACCESAR HACER LAS MIGRACIONES RESPECTIVAS SE REALIZA LO SGT.

ORACLE FOR WINDOWS
SQL PLUS

USE NAME:	SYSTEM
PASSWD :	MANAGER
HOST STRING	ORANT

NOTA: SI EXIXTE ALGUNA CREACION ANTERIOR AL PROCESO HABRA QUE BORRARLO REALIZANDO LOS SGT:

SQL> DROP USER SIGA_VARIOS ó SIGA CASCADE;

UNA VEZ APLICADO EL DROP SE PROCEDE HACER LO SGT:

SQL> CRÉATE USER SIGA_VARIOS IDENTIFIED by SIGA_VARIOS DEFAULT TABLESPACE CONTSIGA TEMPORARY TABLESPACE TEMPORARY_DATA;

DESPUES APLICAR La siguiente Instrucción

SQL> GRANT CONNECT, RESOURCE TO SIGA_VARIOS;

UNA VEZ REALIZADO LOS PROCESOS RESPECTIVOS NOS VAMOS AL PROMT DEL C; \> A REALIZAR LO SGT Y POR SUPUESTO DENTRO DEL DIRECTORIO DONDE QUEIRO QUE SE GUARDE EL COPYN15022008.DMP Y EL COPYN15022008.LOG ejemplo;

C:\ >IMP SYSTEM / MANAGER FILE=D: \PRUEBA\COPYN15022008.DMP FROMUSER=SIGA_VARIOS TOUSER=SIGA_VARIOS LOG=D: \PRUEBA\COPYN15022008.LOG IGNORE=Y

UNA VEZ TERMINADO EL PROCESO SIN PROBLEMAS NOS VA AL PROMT DEL SQL Y EJECUTAMOS LO SGT:

SQL > @GRANT

SQL > @PUBLIC

NOTA: LOS PROCESOS SE DESARROLLAN COMBINANDO UNA SERIE DE PARAMETROS PARA QUE LOS RESULTADOS SEAN OPTIMOS Y LA BASE DE DATOS SE IMPORTE O EXPORTE CON TODA NORMALIDAD.

PROCEDIMIENTO PARA BACKUP DE PARA LAS APLICACIONES LOTUS NOTES

INGRESAR AL LOTUS NOTES Y EFECTUAR PARA CADA APLICACIÓN DE LOTUS NOTES LO SIGUIENTE:

HACER CLICK EN EL ÍCONO DE LA APLICACIÓN A REALIZAR EL BACKUP.
EJECUTAR LAS OPCIONES: ARCHIVO, BASE DE DATOS, COPIAR Y LUEGO ESPECIFICAR:
EL SERVIDOR: LOCAL,
TITULO: [NOMBRE BASE DE DATOS]+[FECHA:DDMMAAAA], Y LA CARPETA DE DESTINO DEL COPIADO.

LOS PARAMETROS A TENER EN CUENTA AL COPIAR SON:

- DISEÑO Y DOCUMENTOS.
- LISTA DE CONTROL DE ACCESO.

PROCEDIMIENTO ALTERNATIVO ANTE ATAQUE DE VIRUS

1. Verificar que se encuentre instalado en el equipo infectado, la última versión del Software Antivirus. (Última versión en las estaciones de trabajo y/o posteriores).

   - Se procederá a desconectar el equipo infectado de la red. Luego, pasar el Software Antivirus.
   - Se comprueba la existencia de virus en el equipo, y se procede a colocar los archivos infectados en cuarentena.

2. Cuando no se logra recuperar la funcionalidad del equipo infectado, es decir no inicializa correctamente el Sistema Operativo, se procede a verificar vía Internet en la página Web del fabricante del Antivirus, así como también otras posibles soluciones de otros fabricantes sobre la recuperación de equipos atacados por el virus.

3. Si a pesar de aplicar los puntos anteriores persiste el problema, proceder a realizar una copia de respaldo del equipo y reinstalar el sistema operativo, software y aplicaciones.

En un Servidor:

- ✓ Para recuperar un Servidor infectado con virus, se procede de la misma manera considerando únicamente los puntos 1 y 2
  Después de aplicar el procedimiento y no se logra la eliminación del virus y tampoco la operatividad de el servidor.

- ✓ Proceder a realizar una copia de respaldo de los archivos más recientes, para complementarlos con los backups que se realizan periódicamente, para una posible restauración del Servidor.

- ✓ Como última medida, se debe contactar con el proveedor indicado. Para este caso, el proveedor a contactar es McAfee.

PROCEDIMIENTO PREVENTIVO ANTE FALLA EN EL FIREWALL / LINEA DEDICADA

Simultáneamente al realizar los procedimientos establecidos en el plan de Contingencias, se procede a tomar las siguientes acciones:

Firewall

1. Verificar la última actualización del Software Checkpoint, así como el correcto licenciamiento.

2. Verificación de los servicios Inicializados correctamente.

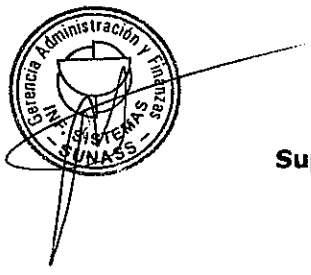
3. Realizar unas pruebas de seguimiento con y a través del Servidor, para llegar a identificar que todos los niveles de seguridad así como las políticas establecidas se estén llevando a cabo apropiadamente.

4. Si no se comprobara la adecuada funcionalidad del equipo, proceder a llamar al área de Soporte de la empresa Cosapi data Ver Relación de Proveedores.

Servicio de Internet y Correo

La SUNASS, cuenta actualmente con los servicios de la empresa OPTICAL IP, para poder brindar el derecho a navegar vía Internet y como servicio de correo electrónico se utiliza el software Lotus Notes de la Empresa IBM,.

De presentarse problemas con la Línea, dependerá únicamente de la solución por parte del proveedor de Servicios. Ver Relación de Proveedores.



ANEXO IV Equipos de Comunicación:

EQUIPOS DE COMUNICACIÓN.

La SUNASS cuenta en la actualidad con los siguientes dispositivos de comunicación conectados bajo cableado estructurado y dentro de una topología estrella con backbone colapsado de fibra óptica BAJO:

CANTIDAD	DISPOSITIVO	MODELO	MARCA
1	SWITCH DE FIBRA	OMNISWITCH 6850-24	ALCATEL
4	SWITCH ADMINISTRABLE	OMNISTACK OS-LS-6224	ALCATEL
4	SWITCH	SUPER STACK 3 3226	3COM
8	DATA SWITCH	SUPERSTACK II SWITCH 3300	3COM
1	DATA SWITCH	COREBUILDER 3500	3COM
1	ROUTER	CISCO 800 SERIES	CISCO

En caso de presentarse una falla o irregularidad en el dispositivo, el área de soporte tratará de resolver dicho problema, si por algún motivo (por ejemplo, necesidad de repuestos debido a desgaste de piezas y accesorios) el área de soporte no pudiera corregir la falla, dicha actividad será realizada como un servicio facturable por atención de llamada (ver relación de proveedores), previa autorización de la Jefatura de la Unidad de Sistemas de Información.

Además se establece que en el caso de ser retirado el equipo por más de 24 horas la compañía tendrá que dejar por el tiempo necesario una dispositivo de comunicación de similares características a la retirada, de manera que no se perjudique la labor del personal al cual se le hubiera asignado el dispositivo con problemas.

DIAGRAMA DE CONNECTIVIDAD DE LA RED DE LA SUNASS.

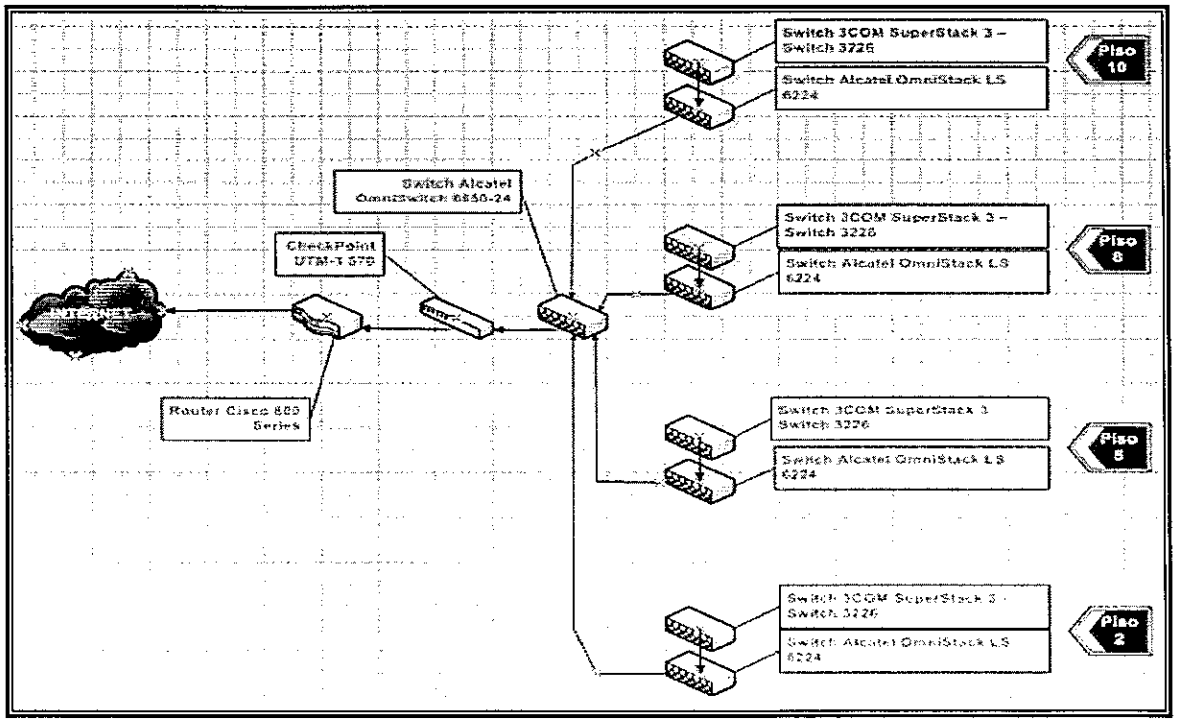
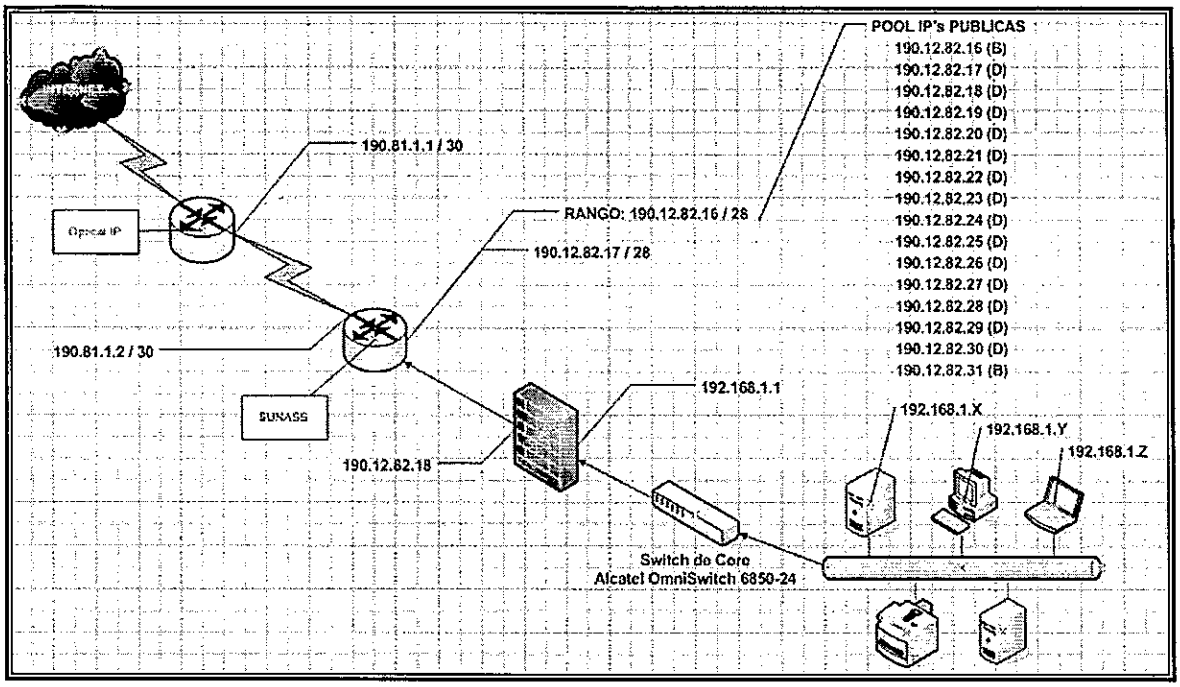


DIAGRAMA DE DIRECCIONES IP DE LA RED DE LA SUNASS.



ANEXO V Software:

Esta constituido por los sistemas operativos, software de desarrollo de sistemas, software de comunicaciones, antivirus, software de ofimática (hoja de cálculo, procesador de textos, etc.) y utilitarios para la gestión de oficina. En la actualidad la SUNASS dispone de las siguientes licencias:

SOFTWARE	IDIOMA	LICENCIAS
Software de Aplicaciones		
Windows Server 2003 OEM	Ingles	1
Windows Server 2003 Standard	Inglés	1
Windows Server 2003 R2 Standard	Inglés	2
Windows Server 2000 OLPC	Inglés	2
Linux Red Hat Enterprise V3	Español	1
Sun Solaris 2.6	Ingles	Ilimitada
Upgrade Solaris 8, (RTU 3 -4 SPARC PLATAFORM EDITION)	Ingles	1
Lotus Notes Collaboration v7	Español	58
Lotus Notes Collaboration /Notes Messaging v7	Español	40
Lotus Domino Application Server v7	Español	1
Lotus Domino Designer v7	Español	2
Lotus Domino Mail Server v7	Inglés	1
Lotus CC-Mail	Inglés	100
Lotus CC-Mail (Router)	Inglés	1
Checkpoint Firewall One VS 4.1 For Next Generation	Inglés	1
Microsoft Foxpro v.2.6 for DOS	Inglés	1
Microsoft Foxpro v.2.6 for Windows	Inglés	10
Brighstor Arcserve Manager for Windows	Inglés	1
Brighstor Arcserve Agent for Oracle	Inglés	1
Brighstor Arcserve Agent for UNIX	Inglés	1
Brighstor Arcserve Client for LINUX	Inglés	1
Brighstor Arcserve Oracle Agent for LINUX	Inglés	1
Brighstor Arcserve Agent for Lotus Notes	Inglés	2
Brighstor Arcserve Disaster Recovery	Inglés	1
Brighstor Arcserve Open Files for Windows	Inglés	1
Brighstor Arcserve Cliente Agents for Windows	Inglés	4
Oracle Database 10g Standard Edition para un Procesador	Inglés	2
Oracle Internet Developer Suite 10g	Inglés	1
Oracle Application Server Standard Edition	Inglés	1
Toad For Oracle Standard Edition	Inglés	1
Visual Studio V. 6.0	Inglés	1
SICAP V_2.2	Español	Ilimitada
Herramientas Gráficas		
Corel Draw 6.00	Inglés	1
Page Maker 6.00	Inglés	1

Microsoft Publisher	Inglés	1
Visio Profesional 2007 OLP	Español	1
Corel Draw Graphics Suites 12.0 Full	Español	3
Adobe Page Maker 7.00 Full	Español	2
Adobe PhotoShop 8.0 Full	Español	3
DreamWeaver MX 2004	Inglés	2
Macromedia Studio MX 2004 c/Flash Pro	Inglés	2
Omni Page (Scanner)	Inglés	10
Cannon File 2.52 (Administrador de Digitalización)	Inglés	1
Google Earth Pro	Inglés	1
Imaging Sof (View / Web)	Español	Ilimitada
Software de Ofimática		
Microsoft Project 2007	Inglés	2
Microsoft Office XP Pro Oem	Español	15
Microsoft Office XP Pyme	Español	19
Microsoft Office 2003 Standard	Español	81
Microsoft Office Basic 2007/Small Businnes	Español	98
Microsoft Office 2003 Profesional	Español	10
Microsoft Office 2007 Profesional	Español	20
Sistema Peruano de Información Jurídica (SPIJ)	Español	14
Sistema Operativo		
Windows XP Home Edition	Español	15
Windows XP Professional	Español	228
Microsoft Windows Server CAL 2003 Single OPEN No level	Inglés	120
Firewall Statefull Inspection Fortigate 60 p/100nodos	Inglés	1
Trend Micro OfficeScan Client Antivirus + Imss	Inglés	120
McAfee Agent VirusScan Enterprise	Inglés	211

Adicionalmente se dispone de los siguientes programas:

- **Sistema de Gestión Bibliotecaria:** Sistema basado en WIN-ISIS ver.1.4, maneja la información bibliográfica de la Institución, distribuida a través de CENDOC.
- **Sistema De Administración Telefónica (Sentinel Phone 2008):** Software que permite controlar las llamadas entrantes y salientes de la Institución. Este software es administrado por el personal de sistemas.

- **SISTEMAS EN PRODUCCIÓN DE LA SUNASS**

La SUNASS dispone de sistemas administrativos y sistemas técnicos, el primer grupo de ellos está orientado a la automatización de las tareas administrativas y los segundos sirven para el desarrollo de las tareas propias de la función reguladora y fiscalizadora de la SUNASS.

Estos sistemas han sido desarrollados con la herramienta de desarrollo Developer en base de datos relacional Oracle. A continuación se presentan los sistemas que se encuentran en producción:

SISTEMAS ADMINISTRATIVOS

	SISTEMAS ADMINISTRATIVOS	Realizado	Ambiente	Situación	Nº Usuarios
1.	SIGA – Modulo de Logística	2000	Developer Oracle	Operativo	10
2.	SIGA – Módulo de Finanzas	2000	Developer Oracle	Operativo	4
3.	SIGA- Módulo de Contabilidad	2000	Developer Oracle	Operativo	4
4.	SIGA – Módulo de Presupuestos	2000	Developer Oracle	Operativo	1
5.	SIGA – Módulo de Recursos Humanos	2000	Developer Oracle	Operativo	2
6.	SAR – Sistemas de Aportes por Regulación	2005	Developer Oracle	Operativo	2
7.	Sistema de Control Patrimonial	2005	Developer Oracle	Operativo	2
8.	Sistema Documentario de la SUNASS (Tramite Documentario, Atención de Reclamos y Orientación al Usuario)	2007	Developer Oracle - Web	Operativo	40

- **Sistema Integrado de Gestión Administrativa (SIGA):** Este sistema esta constituido por cinco módulos los cuales soportan las actividades de las áreas de Logística, Finanzas, Contabilidad, Presupuesto y Recursos Humanos. Este sistema ha sido elaborado bajo un mismo estándar de desarrollo utilizando el Developer/2000 y la base de datos relacional Oracle. Su conceptualización es integrar todas las funciones administrativas involucradas buscando mejorar su gestión de manera eficiente y eficaz.

  A continuación se describen a cada uno de los módulos mencionados:

  - Logística: Se considera desde la solicitud de Pedidos de Bienes y Servicios, los cuales deberán ser autorizados por el jefe del área correspondiente, para luego ser atendidos por el área de logística. En algunos casos su atención es directa y se realiza a través del área de almacén, en otros casos hay realizar todo un proceso que considera la elaboración de una Orden de Compra ú Orden de Servicio. Al ser atendidas estas ordenes se elabora el documento sustentatorio para luego ser enviado al área de Finanzas. Este módulo considera el compromiso y la ejecución presupuestal de manera automática y de igual manera realiza el asiento de provisión contable.

  - Finanzas: Este módulo considera el pago de los Bienes y Servicios y otras obligaciones. Esto se realiza mediante el registro del Comprobante de Egreso y la elaboración de los

cheques de pago. Del mismo modo, considera todos los tipos de ingresos, para ello registra el comprobante de ingresos. Como proceso automatizado complementario, incluye la rendición de caja chica y el tratamiento de las operaciones de transferencia de fondos de las EPS a la SUNASS.

- Contabilidad: El módulo de Contabilidad realiza asientos automáticos de un gran número de operaciones, disminuyendo la labor de digitación al área contable. Del mismo modo, permite el ingreso de asientos manuales para otro tipo de transacciones, así como el proceso de ajuste por inflación. Este módulo considera la emisión de los Libros Contables, el Balance de Comprobación y los Estados Financieros con sus respectivos anexos. De manera automática realiza la ejecución contable cerrándose el ciclo contable.

- Presupuestos: Mediante este módulo la SUNASS formula su presupuesto anual considerando las actividades a realizar cada una de las áreas de la SUNASS. La desagregación del presupuesto considera el uso de partidas presupuéstales asignadas a cada una de las actividades establecidas en la etapa de formulación. La ejecución presupuestal se realiza automáticamente a través de los procesos involucrados en los módulos anteriores. También se puede elaborar reportes de ejecución presupuestal y realizar la reformulación al presupuesto cuando sea requerido.

- Recursos Humanos: Está constituido por dos sub-módulos, el primero de ellos es la Planilla de Empleados y la segunda es la Evaluación del Personal de la SUNASS. Para el primero de ellos considera la asignación de conceptos y uso de fórmulas registradas directamente por el usuario, ello permite hacer el proceso de cálculo de los conceptos de ingresos, egresos y aportaciones. Además, dispone del ingreso de datos específicos para los empleados y finalmente emite todos los reportes propios para el área, así como los que se relacionan al área de contabilidad. Los asientos contables correspondiente a la planilla mensual se realizan de manera automática.

➢ **Sistema de Trámite Documentario:** Este sistema permite manejar el proceso de atención de los documentos que ingresan o se envían a la SUNASS. Este sistema ha sido desarrollado en Developer con Base de Datos ORACLE, programa que se caracteriza por establecer un flujo de atención para los diversos documentos que trata la SUNASS. **Sistema de Reclamos:** Este sistema permite manejar el proceso de atención de reclamos de los usuarios en segunda instancia administrativa. Este sistema ha sido desarrollado en Developer con Base de Datos ORACLE, programa que se caracteriza por establecer un flujo de trabajo para el procedimiento de atención de reclamos, estableciendo tiempo de atención para cada uno de ellos. Este sistema considera cuadros estadísticos que se emiten mensualmente.

➢ **Sistema de Aportes por Regulación (SAR):** Desarrollado en Ambiente Oracle, utilizando la herramienta Developer, permite el control de los aportes de las EPS, registrando todos los aportes que las EPS hacen a la SUNASS. Su conceptualización es la de atender todas las necesidades de los pagos de aportes regulatorios y fraccionamiento de las EPS, buscando mejorar su control de manera eficiente, al final se busca su integración con el sistema SIGA.

➢ **Sistema de Control Patrimonial:** Desarrollado en Ambiente Oracle , utilizando la herramienta Developer, permite llevar el control de los bienes patrimoniales, registrando el ingreso de nuevos bienes, los movimientos que se realizan y finalmente el registro de baja.

- **COMENTARIO**

Todas las áreas de la SUNASS se conectan al SIGA a través de sus pedidos de Bienes/Útiles y de Caja Chica, la interconexión propiamente dicha se realiza con dos herramientas, la primera es

a través del Correo institucional y en segundo lugar esta la Intranet, a la cual tienen acceso todo el personal de la Sunass y acceden a todos los temas de todas las Gerencias. Otro medio de interconexión es la Pagina Web de la SUNASS. También existen sistemas que realizan tareas propias de la función reguladora y fiscalizadora de la SUNASS.

A continuación se enumeran otros sistemas con que cuentan operativamente la SUNASS.

SISTEMAS TECNICOS

	SISTEMAS TÉCNICOS	Realizado	Ambiente	Situación	Nº Usuarios
1.	SFIS - Sistema de Fiscalización y Supervisión	2003	Developer Oracle	Operativo	**10**
2.	SICAP - Sistema de Captura y Transferencia de Datos	2004	Visual Fox	Operativo	**49**
3.	Sistema de Calidad del Agua	1999	Developer Oracle	Operativo	**2**
4.	Sistema de Registro de EPS	2006	Java Oracle – Web	Operativo	**Ilimitado**