RESOLUCIÓN DE SECRETARÍA GENERAL

Nº 088 -2015-SUSALUD/SG

Lima, 18 de diciembre de 2015

VISTOS:

El Informe Técnico N° 050-2015-SUSALUD/OGPP mediante el cual la Oficina General de Planeamiento y Presupuesto, pone a consideración y sustenta el proyecto de Procedimiento "EJECUCIÓN DEL PLAN DE CONTINUIDAD DE TECNOLOGÍA DE LA INFORMACIÓN" para su aprobación, y el Memorándum N° 00170-2015-SUSALUD/OGAJ de la Oficina General de Asesoría Jurídica; y,

CONSIDERANDO:

Que, de conformidad con los artículos 9°, 11° y 13° del Texto Único Ordenado de la Ley N° 29344, aprobado por Decreto Supremo N° 020-2014-SA, en armonía con el Decreto Legislativo N° 1158 que dispone medidas destinadas al fortalecimiento y cambio de denominación de la Superintendencia Nacional de Aseguramiento en Salud - SUNASA, se crea la Superintendencia Nacional de Salud – SUSALUD como organismo público técnico especializado, adscrito al Ministerio de Salud, con autonomía técnica, funcional, administrativa, económica y financiera; encargada de promover, proteger y defender los derechos de las personas al acceso a los servicios de salud; registrar, autorizar, supervisar y regular a las Instituciones Administradoras de Fondos de Aseguramiento en Salud - IAFAS, así como supervisar y registrar a las Instituciones Prestadoras de Servicios de Salud - IPRESS y Unidades de Gestión de IPRESS - UGIPRESS, en el ámbito de su competencia;

Que, por Decreto Supremo N° 008-2014-SA, publicado el 10 de junio de 2014, se aprueba el Reglamento de Organización y Funciones - ROF de SUSALUD, y mediante Resolución Ministerial Nº 730-2014/MINSA se aprueba el Cuadro de Asignación de Personal Provisional de SUSALUD, el cual ha sido materia de reordenamiento de cargos mediante Resolución de Superintendencia N° 021-2015-SUSALUD/S;

Que, la Superintendencia Nacional de Salud forma parte integrante del Sistema Nacional de Estadística e Informática, de conformidad a lo establecido en el artículo 7° del Decreto Legislativo N° 604 – Ley de Organización y Funciones del Instituto de Estadística e Informática;

Que, mediante Resolución Ministerial N° 129-2012-PCM se estableció el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001: 2008 EDI Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos", en todas las Entidades que conforman el Sistema Nacional de Estadística e Informática;

Que, mediante Resolución N° 129-2014/CNB-INDECOPI se aprueba la Norma Técnica Peruana "NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de gestión de seguridad de la Información. Requisitos. 2° Edición", que reemplaza a la NTP-SO/IEC 27001: 2008 EDI; en cuyo numeral 17 del Anexo A, se describen los aspectos de seguridad de la información en la gestión de la continuidad del negocio;

Que, mediante Resolución de Superintendencia Nº 052-2014-SUSALUD/S, del 23 de setiembre del 2014, se aprobó la "Política General de Seguridad de la Información de la Superintendencia Nacional de Salud", en cuyo numeral 4.10 "Política sobre la Gestión de la Continuidad" se establece que todos los procesos de negocio críticos cuentan con un plan de contingencias y recuperación en caso de desastres, a fin de mantenerlos disponibles para los clientes, proveedores y otras entidades que deben acceder a ellos;

Que, con Resolución de Secretaría General N° 085-2015-SUSALUD/SG, del 15 de diciembre del 2015, se aprobó el Índice del Manual de Gestión de Procesos y Procedimientos (MGPP), a partir del cual se está desarrollando y gestionando la aprobación de los diversos procesos y procedimientos identificados en SUSALUD;

Que, en el marco del citado numeral 4.10. "Política sobre la Gestión de la Continuidad", se estima pertinente aprobar el Procedimiento "EJECUCIÓN DEL PLAN DE CONTINUIDAD DE TECNOLOGÍA DE LA INFORMACIÓN", con el objetivo de establecer las acciones, responsabilidades y controles a ejecutar ante una situación que afecte los servicios de Tecnología de la Información que dan soporte a los servicios críticos de SUSALUD;

Que, de conformidad con el literal f) del artículo 32° del Reglamento de Organización y Funciones - ROF de SUSALUD, que establece como funciones de la Oficina General de Planeamiento y Presupuesto (OGPP), evaluar y proponer la aprobación de los proyectos de normas de gestión interna formulados por los diversos órganos de SUSALUD, mediante el Informe Técnico de Vistos, la OGPP pone a consideración el Proyecto de Procedimiento "EJECUCIÓN DEL PLAN DE CONTINUIDAD DE TECNOLOGÍA DE LA INFORMACIÓN" para su aprobación, previa coordinación con la Intendencia de Investigación y Desarrollo conforme al artículo 37° del ROF de SUSALUD y con la Oficina General de Asesoría Jurídica – OGAJ conforme al artículo 29° y literales a) y f) del artículo 30° del ROF de SUSALUD;

Que, de acuerdo al artículo 11° y literal i) del artículo 12° del Reglamento de Organización y Funciones - ROF de SUSALUD, aprobado por Decreto Supremo N° 008-2014-SA, la Secretaría General constituye la máxima autoridad administrativa y tiene entre sus funciones, aprobar el Manual de Procedimientos de la entidad;

Con el visado del Intendente de la Intendencia de Investigación y Desarrollo, y de las Encargadas de las funciones de la Oficina General de Planeamiento y Presupuesto, y de la Oficina General de Asesoría Jurídica; y,

Estando a las facultades conferidas por el Reglamento de Organización y Funciones – ROF de SUSALUD.

SE RESUELVE:

Artículo 1°.- APROBAR el Procedimiento "Ejecución del Plan de Continuidad de Tecnología de la Información", que forma parte del Subcapítulo 4.3. Gestión de Seguridad de Información, del Capítulo 4. Gestión de Infraestructura Tecnológica, del Título 3. Procesos de Soporte, del Manual de Gestión de Procesos y Procedimientos de la Superintendencia Nacional de Salud, cuyo índice fue aprobado por Resolución de Secretaría General N° 085-2015-SUSALUD/SG; el mismo que como anexo forma parte integrante de la presente Resolución.

Artículo 2°.- DISPONER que la Intendencia de Investigación y Desarrollo difunda el Procedimiento aprobado por el artículo 1° de la presente Resolución, a los diferentes órganos de SUSALUD para su cumplimiento.

Artículo 3°.- PUBLICAR en la página web e intranet de la entidad, así como difundir la presente Resolución y la Directiva aprobada, según corresponda.

Regístrese y comuníquese

Jorge Luis Cáceres Neyra
Secretario General

SUSALUD
Superintendencia Nacional de Salud

PROCEDIMIENTO
EJECUCIÓN DEL PLAN
DE CONTINUIDAD DE TECNOLOGÍA DE LA INFORMACIÓN

S4.P03 V.1

Revisado por: **Cargo:** **Fecha:**	**José Hamblett Villegas Ortega** **Intendente de IID** **__ /12/2015**	**Firma:**
Aprobado por: **Cargo:** **Fecha:**	**Jorge Luis Cáceres Neyra** **Secretario General** **__ /12/2015**	**Firma:**

ÍNDICE

CUADRO DE CONTROL DE CAMBIOS

Versión	Fecha	Descripción del cambio	Responsable
0	23/11/2015	Creación del documento.	Jenny Castañeda
01	04/12/2015	El documento adopta formato estandarizado y se incluye registros y cuadro de control de cambios.	Jenny Castañeda Jaime Enero

1. OBJETIVO

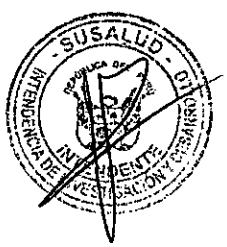
Establecer las acciones, responsabilidades y controles a ejecutar ante una situación de disrupción de los servicios de TI que dan soporte a los servicios críticos de SUSALUD.

2. ALCANCE

2.1. La presente versión alcanza la restauración de los servicios críticos de TI que dan soporte a los servicios de SUSALUD, estos servicios son los siguientes:

- Base de Datos (SQL y Oracle).
- Aplicaciones Web
- Red de Datos.
- Seguridad Perimetral.
- Red SAN.
- Directorio Activo.
- FTP.
- Correo electrónico.
- Virtualización.

2.2. Es de aplicación obligatoria para la Intendencia de Investigación y Desarrollo (IID) de la Superintendencia Nacional de Salud, en adelante -SUSALUD.



3. BASE LEGAL

3.1. Reglamento de Organización y Funciones de SUSALUD, aprobado con Decreto Supremo N° 008-2014-SA.

3.2. Cuadro de Asignación de Personal (CAP) Provisional de SUSALUD, aprobado con Resolución Ministerial N° 730-2014/MINSA.

3.3. Norma Técnica Peruana ""NTP-ISO/IEC 27001:2008 EDI Tecnología de la Información, Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la información. Requisitos" aprobada con Resolución Ministerial N° 129-2012-PCM que establece el uso obligatorio en todas las Entidades que conforman el Sistema Nacional de Informática.

3.4. "NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de gestión de seguridad de la Información. Requisitos" 2° Edición, aprobada con Resolución N° 129-2014/CNB-INDECOPI.

3.5. Ley 29733 - Protección de Datos Personales y sus conexos.

4. DOCUMENTOS RELACIONADOS

4.1. Reglamento Interno de Trabajo de SUSALUD, aprobada con Resolución de Secretaria General N° 046-2015-SUSALUD.

4.2. Política General de Seguridad de la Información de SUSALUD, aprobada con Resolución de Superintendencia N° 052-2014-SUSALUD/S.

4.3. Comité de Gestión de Seguridad de la Información y Comité Técnico de Seguridad de la Información, aprobada con Resolución de Superintendencia N° 046-2014-SUSALUD/S.

4.4. Designación de Oficial de Seguridad de la Información de SUSALUD, mediante Resolución de Superintendencia N° 114-2015 SUSALUD/S.

4.5. Procedimiento gestión de seguridad de la información S4.P01 V.1, aprobada con Resolución de Secretaría General N° 081-2015-SUSALUD/SG

4.6. Procedimiento gestión de servicios informáticos S4.P02 V.1, aprobada con Resolución de Secretaría General N° 081-2015-SUSALUD/SG

5. DEFINICIONES Y ACRÓNIMOS

DEFINICIONES

5.1. **Continuidad de Negocio:** Proceso de gestión que provee un marco conceptual para crear una salvaguarda a los objetos de la organización incluyendo sus obligaciones [ISO 22301].

5.2. **FTP:** Protocolo de transferencia de archivos (en inglés de File Transfer Protocol) entre sistemas conectados a una red TCP (Transmission Control Protocol), basado en la arquitectura cliente-servidor. Desde un equipo cliente se puede conectar a un servidor para descargar archivos desde él o para enviarle archivos, independientemente del sistema operativo utilizado en cada equipo.

5.3. **Incidente:** Situación que pudiera constituir o podría redundar en una interrupción de negocio, pérdida, emergencia o crisis [ISO 22300].

5.4. **Interrupción:** Incidente, ya sea previsto (por ejemplo: una huelga de trabajadores o un huracán) o imprevisto (por ejemplo un apagón o un terremoto), que interrumpe el curso normal de las operaciones de los servicios de TI.

5.5. **Invocación:** Acto de declarar que los acuerdos de la organización de continuidad del negocio deben llevarse a la práctica con el fin de continuar con la entrega de productos o servicios clave. [ISO 22301].

5.6. **ISO 22301:** Norma internacional para la gestión de la continuidad de negocio, en la cual se especifica los requisitos para un sistema de gestión encargado de proteger a la organización de incidentes que provoquen una interrupción en la actividad, reducir la probabilidad de que se produzcan y garantizar la recuperación de la organización.

5.7. **ISO 27031** Norma internacional que explica los principios y conceptos de la tecnología de información y comunicación, la preparación para que continúe el negocio, y la descripción de los procesos y métodos necesarios para señalar e identificar todos los aspectos que sirvan para mejorar la preparación de las tecnologías de la información y comunicación de una organización con la finalidad de garantizar la continuidad del negocio.

5.8. **Plan de Continuidad de TI:** Plan definido y documentado que guían a la organización a responder, recuperar, reanudar los servicios de TI después de una interrupción.

5.9. **Situación disruptiva:** Evento o sucesión de eventos no previstos que afecten a los servicios críticos de TI y que supere un periodo máximo de 8 horas, cuyo impacto no permitiría el desenvolvimiento de las actividades productivas, impidiendo el acceso y/o utilización de los servicios del negocio que se soportan en ellos.

5.10. **Red SAN:** Red de área de almacenamiento (en inglés Storage Area Network), es una red concebida para para transportar datos entre servidores y recursos de almacenamiento, permite conectividad de alta velocidad, de servidor a almacenamiento, almacenamiento a almacenamiento, o servidor a servidor.

ACRÓNIMOS

5.11. **IID:** Intendencia de Investigación y Desarrollo.

5.12. **INDECOPI:** Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual

5.13. **ISO:** Organización Internacional de Normalización

5.14. **MINSA:** Ministerio de Salud.

5.15. **PCM:** Presidencia de consejo de Ministros.

5.16. **SUSALUD:** Superintendencia Nacional de Salud.

5.17. **TI:** Tecnologías de la Información

6. CONSIDERACIONES GENERALES

6.1. El procedimiento para ejecutar el plan de continuidad de TI, incluye además de las actividades y responsables: formatos, recursos y mecanismos para la actuación "antes, durante y después" de una interrupción de los servicios de TI debido a la ocurrencia de eventos y desastres.

La ejecución del plan, debe permitir que la entidad se recupere rápidamente y pueda seguir brindando los recursos críticos de TI.

6.2. El presente documento está enmarcado en lineamiento de estándares internacionales como la ISO 22301, ISO 27031 y adaptado al contexto de SUSALUD.

6.3. La gestión de continuidad de TI añade valor a la organización en la medida que permite minimizar en tiempo de indisponibilidad de los servicios de SUSALUD que son soportados por los servicios de TI.

6.4. Las estrategias que se definieron para reducir el tiempo de respuesta ante interrupciones de los servicios críticos de TI, se muestran a continuación:

- Realizar copias de respaldo de los servidores, BD y aplicativo de seguridad; máquinas virtuales; configuración e información del sistema de almacenamiento (correo electrónico, BD, aplicaciones, etc.); configuración de switches de fibra, LAN, UTM.
- Mantener preparado un servidor Linux y otro Windows con disco local (reemplazo de los servidores de BD)
- Contar con licenciamiento vigente para los servicios críticos
- Realizar monitoreo de los servicios de TI.
- Mantener el soporte del balanceador de servidores.
- Realizar mantenimiento periódico a los sistemas.
- Realizar mantenimiento periódico a los equipos.
- Mantener un equipo firewall de contingencia.
- Monitoreo de las condiciones ambientales del centro de datos (temperatura, humedad).

6.5. Para la invocación del plan de continuidad de TI ante una situación disruptiva, se ha definido cuándo, cómo y el responsable para la ejecución el proceso de recuperación, de los Servicios de TI que se encuentran en el Centro de Datos ubicado en Av. Velasco Astete 1398, Santiago de Surco, así mismo se identifican los siguientes escenarios de invocación:

Escenarios de invocación	Detecta situación	Estrategia	Autorizado para ejecutar el plan	Autorizado para activar el plan
Falla de Hardware o software de un equipo crítico	Personal de SUSALUD	Activación del Plan de Continuidad	Equipo Técnico de la IID	Intendente de IID

Una vez evaluado el siniestro por el órgano correspondiente y decidido iniciar el proceso de recuperación, la persona autorizada para invocar el Plan de Continuidad de TI es el Intendente de IID.

6.6. Estructura de las notificaciones

- El propósito presenta la estructura de notificaciones que ha sido acordada para tal eventualidad, definiendo los niveles de responsabilidad (quien contacta a quién).
  Las listas de notificaciones están presentadas (Anexo 9.1), para facilitar su uso y mantenimiento. Estas listas deben ser utilizadas para llevar un registro de las personas que han sido informadas.

- La notificación de invocación del plan es responsabilidad del Intendente de la IID, el cual está autorizado para invocar el Plan. Específicamente, él informará al personal de Operaciones, y Sistemas que encabezarán los grupos de recuperación quienes a su vez informarán a los miembros del grupo acerca del incidente y de las acciones a ser adoptadas. Así mismo comunicará al Oficial de Seguridad de la Información quien realizará el seguimiento de las acciones adoptadas y de su efectividad. (Anexo 9.2.)

- Se estableció los números telefónicos para: el responsable y de los contactos del equipo de TI (Anexo 9.1.); el responsable y externos (Anexo 9.3.); y emergencia (Anexo 9.4)

6.7. Ante la interrupción de un servicio se cuentan un plan de recuperación para los servicios de TI más importantes con planes de acción (planes de respuesta, recuperación y restauración) orientados a la recuperación del servicio en caso ocurra incidentes con recursos específicos. Las actividades que se desarrollarán en el Centro de Datos, están relacionadas a la recuperación de los siguientes servicios:

- Servicio de BD (Oracle y SQL)
- Aplicaciones Web
- Red de Datos.
- Seguridad Perimetral
- Red SAN.
- Directorio Activo.
- FTP
- Virtualización.
- Correo Electrónico.

A continuación se indica los procedimientos de recuperación y los responsables de elaborar y revisar las actividades específicas de recuperación para cada servicio de TI.

6.8. Luego de ejecutar las tareas "durante" y "después" del plan de continuidad, el Oficial de Seguridad de la Información, o el servidor que haga sus veces deberá elaborar un **"Informe de Ejecución del Procedimiento de Continuidad de TI"**, el cual debe ser presentado al Intendente de la IID, para las gestiones correspondientes.

7. PROCEDIMIENTO

7.1. Plan de acción- BD (oracle).
Componente: Servidor SEPS04 - BD Oracle 11g / con conexión a la Red SAN.

N°	TAREA	RESPONSABLE/ ÓRGANO
Antes de la Contingencia		
1	**Inicio.** Cumplir con el cronograma de backups.	Administrador de Base de Datos IID
2	Guardar una copia de backups en un servidor local y enviar backups al lugar de custodia.	Administrador de Operaciones IID
3	Mantener un servidor de contingencia preparado con SO Linux, motor de BD Oracle y disco local.	Administrador de Operaciones IID
4	Revisar el cumplimiento del procedimiento de backups. Registrar las tareas y acciones realizadas en el "**Cronograma de seguimiento**"	Oficial de Seguridad de la Información IID
Durante la Contingencia		
5	Habilitar servidor de contingencia y copiar el último backup de la BD con que se cuenta.	Administrador de Operaciones IID
6	Restaurar el backup.	Administrador de Base de Datos IID
7	Validar que la información puede ser consultada.	Administrador de Base de Datos IID
8	Revisar la seguridad de la Información en la etapa de contingencia. Registrar las tareas y acciones realizadas en el formato de "**Ejecución del Plan de Continuidad de TI**"	Oficial de Seguridad de la Información IID
Después de la Contingencia		
9	Gestionar la reposición de los recursos afectados.	Jefe de Operaciones IID
10	Instalar y configurar recursos afectados.	Administrador de Operaciones IID
11	Realizar un backup de la BD de contingencia.	Administrador de Base de Datos IID
12	Restaurar la BD de contingencia en la BD de producción recuperada.	Administrador de Base de Datos IID
13	Verificar el cumplimiento del procedimiento de recuperación. Registrar las tareas y acciones realizadas en el formato de "**Ejecución del Plan de Continuidad de TI**" **Fin.**	Oficial de Seguridad de la Información IID

7.2. Plan de acción- BD (SQL)

Componente: Servidor 04 - Windows Server y BD SQL con conexión a la Red SAN antigua.

N°	TAREA	RESPONSABLE/ ÓRGANO
Antes de la Contingencia		
1	**Inicio.** Cumplir con el cronograma de backups	Administrador de Base de Datos IID
2	Guardar una copia de backups en un servidor local y enviar backups al lugar de custodia.	Administrador de Operaciones IID
3	Mantener preparado un servidor Windows Server con un disco local y motor de BD SQL Server.	Administrador de Operaciones IID
4	Revisar el cumplimiento del procedimiento de backups. Registrar las tareas y acciones realizadas en el "**Cronograma de seguimiento**"	Oficial de Seguridad de la Información IID
	Durante la Contingencia	
5	Habilitar servidor de contingencia y copiar el último backup de la BD con que se cuenta.	Administrador de Operaciones IID
6	Restaurar el Backup de la base de datos.	Administrador de Base de Datos IID
7	Validar que la información puede ser consultada	Especialista en gestión de TI/Operador de Procesamiento de Datos IID
8	Revisar la seguridad de la Información en la etapa de contingencia. Registrar las tareas y acciones realizadas en el formato de "**Ejecución del Plan de Continuidad de TI**"	Oficial de Seguridad de la Información IID
	Después de la Contingencia	
10	Gestionar la reposición de los recursos afectados.	Jefe de Operaciones IID
11	Instalar y configurar recursos afectados.	Administrador de Operaciones IID
12	Realizar un backup de la BD de Contingencia	Administrador de Base de Datos IID
13	Restaurar la BD de Contingencia en la BD de producción recuperada.	Administrador de Base de Datos IID

14	Verificar el cumplimiento del procedimiento de recuperación. Registrar las tareas y acciones realizadas en el formato de **"Ejecución del Plan de Continuidad de TI"** **Fin.**	Oficial de Seguridad de la Información IID

7.3. Plan de acción- Sistema de Virtualización

Componentes:

- Servidores: ServerVM1, ServerVM2, BLADESRV01- BLADESRV08
- Hipervisor VMWARE.
- Conexión a la Red SAN.

N°	TAREA	RESPONSABLE/ ÓRGANO
Antes de la Contingencia		
1	**Inicio.** Cumplir con el cronograma de backups	Administrador de Operaciones IID
2	Guardar una copia de backups en un servidor local y enviar backups al lugar de custodia.	Administrador de Operaciones IID
3	Mantener un servidor con hipervisor VMware.	Administrador de Operaciones IID
4	Revisar el cumplimiento del procedimiento de backups. Registrar las tareas y acciones realizadas en el **"Cronograma de seguimiento"**	Oficial de Seguridad de la Información IID
Durante la Contingencia		
5	Mover los servidores virtuales hacia algún otro servidor físico disponible.	Administrador de Operaciones IID
6	Verificar que la comunicación a nivel de red se efectúa con normalidad.	Especialista en Arquitectura de TI IID
7	Realizar pruebas sobre la aplicación.	Coordinador de Desarrollo / Programador de Sistemas IID
8	Revisar la seguridad de la Información en la etapa de contingencia. Registrar las tareas y acciones realizadas en el formato de **"Ejecución del Plan de Continuidad de TI"**	Oficial de Seguridad de la Información IID
Después de la Contingencia		
9	Gestionar la reposición de los recursos afectados.	Jefe de Operaciones IID

10	Instalar el Software de Virtualización en el recurso nuevo o reparado.	Administrador de Operaciones. IID
11	Configurar el Sistema de Virtualización y levantar las máquinas virtuales.	Administrador de Operaciones IID
12	Actualizar las configuraciones de red para los servicios restablecidos.	Especialista en Arquitectura de TI IID
13	Realizar pruebas sobre la aplicación.	Coordinador de Desarrollo Programador de Sistemas IID
14	Verificar el cumplimiento del procedimiento de recuperación. Registrar las tareas y acciones realizadas en el formato de "**Ejecución del Plan de Continuidad de TI**" **Fin.**	Oficial de Seguridad de la Información IID

7.4. Plan de acción- Aplicación Web
Componentes:

- Código fuente de aplicación
- Conexión a la red SAN.

N°	TAREA	RESPONSABLE/ ÓRGANO
Antes de la Contingencia		
	Inicio. Cumplir con el cronograma de backups	Administrador de Operaciones IID
2	Guardar una copia de backups en un servidor local y enviar backups al lugar de custodia.	Administrador de Operaciones IID
3	Revisar el cumplimiento del procedimiento de backups. Registrar las tareas y acciones realizadas en el "**Cronograma de seguimiento**"	Oficial de Seguridad de la Información IID
Durante la Contingencia		
4	Restablecer el backup de la aplicación.	Administrador de Operaciones IID
5	Configurar parámetros de red y verificación.	Especialista en Arquitectura de TI IID
6	Realizar pruebas sobre la aplicación.	Coordinador de Desarrollo /

		Programador de Sistemas IID
7	Revisar la seguridad de la Información en la etapa de contingencia. Registrar las tareas y acciones realizadas en el formato de "**Ejecución del Plan de Continuidad de TI**"	Oficial de Seguridad de la Información IID
Después de la Contingencia		
8	Coordinar con el dueño del proceso soportado por la Aplicación, para identificar la información no recuperada posterior al último backup.	Coordinador de Desarrollo / Programador de Sistemas IID
9	En caso lo soliciten, ejecutar el pase a producción para actualización de información.	Administrador de BD IID
10	Realizar pruebas sobre la aplicación.	Coordinador de Desarrollo / Programador de Sistemas IID
11	Verificar el cumplimiento del procedimiento de recuperación. Registrar las tareas y acciones realizadas en el formato de "**Ejecución del Plan de Continuidad de TI**" **Fin.**	Oficial de Seguridad de la Información IID

7.5. Plan de acción- Servicio FTP/SFTP

Componentes:

- Servidor virtual FTP/SFTP
- Red SAN.

N°	TAREA	RESPONSABLE/ ÓRGANO
Antes de la Contingencia		
1	**Inicio.** Cumplir con el cronograma de backups	Administrador de Operaciones IID
2	Guardar una copia de backups en un servidor local y enviar backups al lugar de custodia.	Administrador de Operaciones. IID
3	Revisar el cumplimiento del procedimiento de backups. Registrar las tareas y acciones realizadas en el "**Cronograma de seguimiento**"	Oficial de Seguridad de la Información IID
Durante la Contingencia		
4	Restablecer el backup de servicio FTP/SFTP.	Administrador de Operaciones IID

5	Configurar parámetros de red y verificar.	Especialista en Arquitectura de TI IID
6	Realizar pruebas sobre el servicio.	Administrador de Operaciones IID
7	Revisar la seguridad de la Información en la etapa de contingencia. Registrar las tareas y acciones realizadas en el formato de **"Ejecución del Plan de Continuidad de TI"**	Oficial de Seguridad de la Información IID
Después de la Contingencia		
8	Coordinar con el encargado del proceso soportado por el servicio, para restablecer la información no recuperada.	Coordinador de Desarrollo Programador de Sistemas IID
9	En caso lo soliciten, ejecutar el pase a producción para actualización de información.	Administrador de Operaciones IID
10	Realizar pruebas sobre el servicio.	Coordinador de Desarrollo/ Programador de Sistemas IID
11	Verificar el cumplimiento del procedimiento de recuperación. Registrar las tareas y acciones realizadas en el formato de **"Ejecución del Plan de Continuidad de TI"** **Fin.**	Oficial de Seguridad de la Información IID

7.6. Plan de acción- Correo Electrónico

Componentes:

- Servidor virtual de correo electrónico.
- Red SAN.

N°	TAREA	RESPONSABLE/ ÓRGANO
Antes de la Contingencia		
1	**Inicio.** Cumplir con el cronograma de backups	Administrador de Operaciones IID
2	Guardar una copia de backups en un servidor local y enviar backups al lugar de custodia.	Administrador de Operaciones. IID
3	Revisar el cumplimiento del procedimiento de backups. Registrar las tareas y acciones realizadas en el **"Cronograma de seguimiento"**	Oficial de Seguridad de la Información IID

Durante la Contingencia		
4	Restablecer el backup de servicio de correo.	Administrador de Operaciones IID
5	Configurar parámetros de red y verificar.	Especialista en Arquitectura de TI IID
6	Realizar pruebas sobre el servicio.	Administrador de Operaciones IID
7	Revisar la seguridad de la Información en la etapa de contingencia. Registrar las tareas y acciones realizadas en el formato de "**Ejecución del Plan de Continuidad de TI**"	Oficial de Seguridad de la Información IID
Después de la Contingencia		
8	Comunica el restablecimiento del servicio a los usuarios.	Administrador de Operaciones IID
9	Verificar el cumplimiento del procedimiento de recuperación. Registrar las tareas y acciones realizadas en el formato de "**Ejecución del Plan de Continuidad de TI**" **Fin.**	Oficial de Seguridad de la Información IID

7.7. Plan de acción- Directorio Activo

Componentes:

- Servidor virtual del directorio activo.
- Red SAN.

N°	TAREA	RESPONSABLE/ ÓRGANO
Antes de la Contingencia		
1	**Inicio.** Cumplir con el cronograma de backups	Administrador de Operaciones IID
2	Guardar una copia de backups en un servidor local y enviar backups al lugar de custodia.	Administrador de Operaciones IID
3	Revisar el cumplimiento del procedimiento de backups. Registrar las tareas y acciones realizadas en el "**Cronograma de seguimiento**"	Oficial de Seguridad de la Información IID
Durante la Contingencia		
4	Restablecer el backup de servicio de directorio activo.	Administrador de Operaciones IID

5	Configurar parámetros de red y verificar.	Especialista en Arquitectura de TI IID
6	Realizar pruebas sobre el servicio.	Administrador de Operaciones IID
7	Revisar la seguridad de la Información en la etapa de contingencia. Registrar las tareas y acciones realizadas en el formato de **"Ejecución del Plan de Continuidad de TI"**	Oficial de Seguridad de la Información IID
Después de la Contingencia		
8	Comunica el restablecimiento del servicio a los usuarios.	Administrador de Operaciones IID
9	Verificar el cumplimiento del procedimiento de recuperación. Registrar las tareas y acciones realizadas en el formato de **"Ejecución del Plan de Continuidad de TI"** **Fin.**	Oficial de Seguridad de la Información IID

7.8. Plan de acción- Red SAN

Componentes: Sistema de almacenamiento (SAN, Switches de FC).

N°	TAREA	RESPONSABLE/ ÓRGANO
Antes de la Contingencia		
	Inicio. Mantener el backup de la configuración del sistema de almacenamiento y switches de fibra.	Especialista en Arquitectura de TI IID
2	Cumplir con el cronograma de backups de los sistemas	Administrador de Operaciones IID
3	Mantener actualizado el diagrama de la configuración y conexiones del sistema de almacenamiento.	Especialista en Arquitectura de TI IID
4	Contar con espacio en disco en los servidores del sistema de virtualización.	Administrador de Operaciones IID
5	Revisar el cumplimiento del procedimiento de backups. Registrar las tareas y acciones realizadas en el **"Cronograma de seguimiento"**	Oficial de Seguridad de la Información IID
Durante la Contingencia		
6	Restablecer el backup de los servicios críticos en los servidores de virtualización.	Administrador de Operaciones IID
7	Configurar parámetros de red y verificar.	Especialista en Arquitectura de TI

		IID
8	Realizar pruebas sobre el servicio.	Administrador de Operaciones IID
9	Realizar pruebas sobre las aplicaciones involucradas.	Coordinador de Desarrollo Programador de Sistemas IID
10	Revisar la seguridad de la Información en la etapa de contingencia. Registrar las tareas y acciones realizadas en el formato de **"Ejecución del Plan de Continuidad de TI"**	Oficial de Seguridad de la Información IID
Después de la Contingencia		
11	Gestionar la reposición de los recursos afectados.	Jefe de Operaciones IID
12	Configurar el hardware y software de los recursos afectados.	Administrador de Operaciones IID
13	Actualizar las configuraciones de red para la red SAN.	Especialista en Arquitectura de TI IID
14	Realizar pruebas sobre las aplicaciones involucradas.	Coordinador de Desarrollo Programador de Sistemas IID
15	Verificar el cumplimiento del procedimiento de recuperación. Registrar las tareas y acciones realizadas en el formato de **"Ejecución del Plan de Continuidad de TI"** **Fin.**	Oficial de Seguridad de la Información IID

7.9. Plan de acción- Red de Datos
Componente: Switch core, switches de servidores.

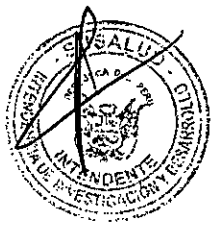
N°	TAREA	RESPONSABLE/ ÓRGANO
Antes de la Contingencia		
1	**Inicio.** Realizar un respaldo de la configuración.	Especialista en Arquitectura de TI IID
2	Mantener un diagrama de conexiones y zonas configuradas en los equipos actualizado.	Especialista en Arquitectura de TI IID
3	Mantener un switch administrable de contingencia.	Especialista en Arquitectura de TI IID
4	Revisar el cumplimiento del procedimiento de respaldo y de la operatividad del equipo de contingencia. Registrar las tareas y acciones realizadas en el "**Cronograma de seguimiento**"	Oficial de Seguridad de la Información IID
Durante la Contingencia		
5	Realizar las configuraciones de red en el equipo de contingencia.	Especialista en Arquitectura de TI IID
6	Verificar la comunicación desde los servidores.	Administrador de Operaciones. IID
7	Revisar la seguridad de la Información en la etapa de contingencia. Registrar las tareas y acciones realizadas en el formato de "**Ejecución del Plan de Continuidad de TI**"	Oficial de Seguridad de la Información IID
Después de la Contingencia		
8	Gestionar la reposición de los recursos afectados.	Jefe de Operaciones IID
9	Configurar el hardware nuevo o reparado.	Especialista en Arquitectura de TI IID
10	Verificar la comunicación desde los servidores.	Administrador de Operaciones IID
11	Verificar el cumplimiento del procedimiento de recuperación. Registrar las tareas y acciones realizadas en el formato de "**Ejecución del Plan de Continuidad de TI**" **Fin.**	Oficial de Seguridad de la Información IID

7.10. Plan de acción- Seguridad Perimetral

Componente: UTM (proveído por el servicio de línea dedicada)

N°	TAREA	RESPONSABLE/ ÓRGANO
Antes de la Contingencia		
1	**Inicio.** Realizar un respaldo de la configuración.	Especialista en Arquitectura de TI IID
2	Mantener actualizado un diagrama de conexiones y documento con la relación de políticas implementadas.	Especialista en Arquitectura de TI IID
3	Mantener un equipo con características de Firewall.	Especialista en Arquitectura de TI IID
4	Revisar el cumplimiento del procedimiento de respaldo y de la operatividad del equipo de contingencia. Registrar las tareas y acciones realizadas en el "**Cronograma de seguimiento**"	Oficial de Seguridad de la Información IID
Durante la Contingencia		
5	Realizar las configuraciones de red en el equipo de contingencia.	Especialista en Arquitectura de TI IID
6	Verificar la comunicación desde los servidores.	Administrador de Operaciones. IID
7	Revisar la seguridad de la Información en la etapa de contingencia. Registrar las tareas y acciones realizadas en el formato de "**Ejecución del Plan de Continuidad de TI**"	Oficial de Seguridad de la Información IID
Después de la Contingencia		
8	Gestionar la reposición de los recursos afectados.	Jefe de Operaciones IID
9	Restablecer las configuraciones de las políticas.	Especialista en Arquitectura de TI IID
10	Revisar el correcto funcionamiento del nuevo hardware.	Especialista en Arquitectura de TI IID
11	Verificar la comunicación desde los servidores.	Administrador de Operaciones IID
12	Verificar el cumplimiento del procedimiento de recuperación.	Oficial de Seguridad de la Información IID

13	Gestionar la reposición de los recursos afectados. Registrar las tareas y acciones realizadas en el formato de "**Ejecución del Plan de Continuidad de TI**" **Fin.**	Jefe de Operaciones IID



8. REGISTROS

CÓDIGO DE REGISTRO	REGISTRO	PROCEDIMIENTO
N/A	Cronograma de seguimiento	Todos los Procedimientos
N/A	Formato: Ejecución del Plan de Continuidad de TI	
N/A	Informe de Ejecución del Plan de Continuidad de TI	

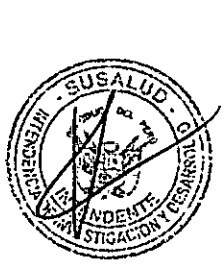
N/A: No Aplica

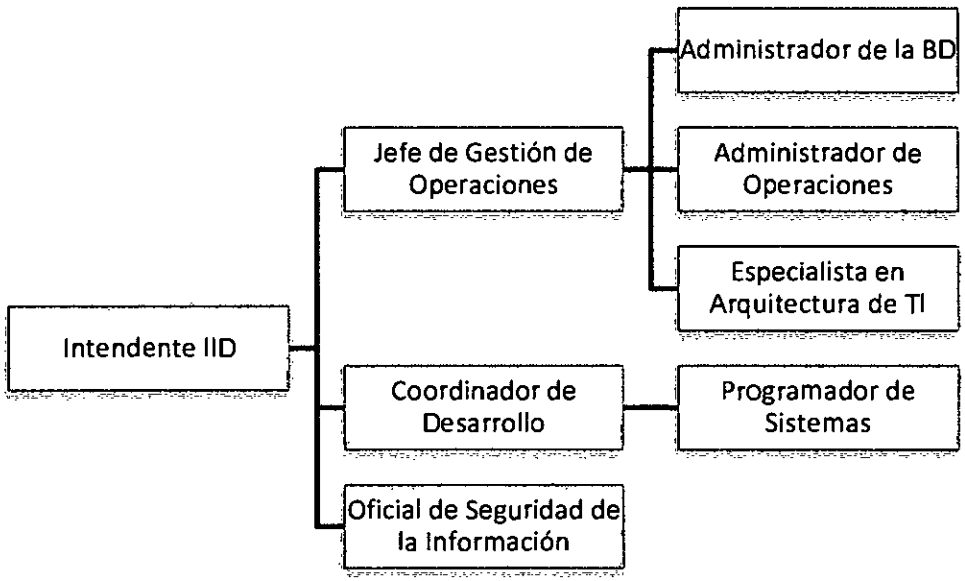
9. ANEXOS

9.1. Información del Árbol de Llamadas: Contactos del Equipo de TI

RESPONSABLE: INTENDENTE DE IID			
NOMBRE DEL PERSONAL	**CARGO**	**ANEXO**	**CELULAR/**
José Villegas	Intendente de IID	5411	999510303
Carlos Maldonado	Jefe de Gestión de Operaciones	5701	987154311
María Urrutia	Administrador de BD	5707	994354280
Joe Malca	Administrador de Operaciones	5708	988799307
Luis Rengifo	Especialista en Arquitectura de TI	5708	993135233
José Huaman	Coordinador de Desarrollo	5707	947007793
Patricia Callupe	Programador de Sistemas	5707	990928690
Jenny Castañeda	Oficial de Seguridad de la Información	5456	949431841

9.2. Árbol de llamadas





9.3. Información del Árbol de Llamadas: Notificación a Contactos Externos

EMPRESA GARANTÍA / SOPORTE	CONTACTO	CARGO	TELÉFONO	CORREO
IT Storage EIRL	Patricia Carrillo	Ejecutiva Comercial	Telf: (511) 221-5186 Movil: 999581361	pcarrillo@itstorage.org, pcarrillo@itstoragecorp.com
Centro Nacional de Servicios - CNS	Katherine A. Velarde Quintanilla	Ejecutivo de Service Desk	Telf:(511) 422-2100 Anexo: 134 Móvil: (511) 998988054	kvelarde@cns.com.pe
	Jair Goyburu Molina	Ejecutivo de Service Desk	Telf:(511) 422-2100 Anexo: 115 Móvil: (511) 995094241	jgoyburu@cns.com.pe
	Freddy Alvarez Carhuayo	Ejecutivo de Service Desk	Telf:(511) 422-2100 Anexo: 121 Móvil: (511) 978218825	falvarez@cns.com.pe
	Nathalya Pastor Bretoneche	Supervisor Service Desk	Telf:(511) 422-2100 Anexo: 117 Móvil: (511) 983419149	npastor@cns.com.pe
	Jorge Siqueiros Yong	Jefe de Proyecto	Telf:(511) 422-2100 Anexo: 124 Móvil: (511) 971163795	jsiqueiros@cns.com.pe
GOALS	Alexis Mejía Aquino	Técnico de Mantenimiento y Soporte	Telf: (511) 221-8680 Anexo: 222 Móvil: 980040508	email: sertec2@goalsnet.net skype: amejia04
IBM (Integra Technologies S.A.C) - CNS	Soporte IBM	Soporte IBM	Central: 0800-50866 Telf Peru: 625-6000 opcion 3	
	Pedro Ordaya Samaniego - ITECH	Gerente	Movil: 988461883	pordaya@itech.com.pe
	Gerson Melgar Lobato - ITECH	Consultor TI	Cel: 990297441 RPM: #990297441 Telefono: 3191111 anexo 204	gmelgar@itech.com.pe Skype: gerson.melgar

Storage Data	Mario Trigoso Saldaña Erick Gonzales	Técnico	Cell: 51-990003843 RPM: #558158 Cel (51) 990004680 /RPM: #558159	mario_trigoso@storagedata.com.pe erick_gonzales@storagedata.com.pe
Optical networks		NOC/SOC	710-7575 500-7575	noc@optical.com.pe operadores@optical.com.pe operadores@optical.pe
AIRTEC SYSTEMAS SAC	Dovin Gomez Alfredo Huaroc Gllberto Moncada	Técnico Supervisor	RPC: 986610805 RPC: 994637280 RPC: 989293653 RPM: *430264	dovin.gomez@cpeaconditioning.pe alfredo.huaroc@cpeaconditioning.pe gmoncada@cpeaconditioning.pe

9.4. Números de Contacto de Emergencia

BOMBEROS	
Central de bomberos	116 / 274-5119
Compañía de Bomberos Santiago Apóstol	Av. Monte de los Olivos. Cdra.9 Urb. Prol. Benavides segunda etapa. Surco. Teléfono: 274-5119.
EMERGENCIAS POLICIALES	
Seguridad ciudadana	Loma de los suspiros s/n. Teléfono: 474-5300 anexo 446
Comisaria Surco	Jr. Arica 388, Calle Arica, 247-1512
DIROVE Emergencia	328 0351, 328 0207
UDEX	431-3177
Central de Policía	105
HOSPITALES Y CLINICAS	
Hospital de Emergencia Casimiro Ulloa	2040900