Firma Digital SUSALUD Superintendencia Nacional de Salud

Firmado digitalmente por AVILA ESPINOZA Yenny Milagros FAU 20377985843 hard
Motivo: Doy V° B°
Fecha: 04.11.2024 17:51:30 -05:00

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”

Firma Digital SUSALUD Superintendencia Nacional de Salud

Firmado digitalmente por PARRA UGAZ Maria Grazia FAU 20377985843 soft
Motivo: Doy V° B°
Fecha: 31.10.2024 10:23:29 -05:00

Firma Digital SUSALUD Superintendencia Nacional de Salud

Firmado digitalmente por LIZARRAGA VALDIVIA Jean Paul FAU 20377985843 soft
Motivo: Doy V° B°
Fecha: 04.11.2024 11:33:41 -05:00

Firma Digital SUSALUD Superintendencia Nacional de Salud

Firmado digitalmente por MARTINEZ AVILES Iliana Consuelo FAU 20377985843 soft
Motivo: Doy V° B°
Fecha: 04.11.2024 09:45:41 -05:00

SUSALUD

Superintendencia Nacional de Salud

Firma Digital SUSALUD Superintendencia Nacional de Salud

Firmado digitalmente por CASTILLO LLAUCE Walt Jimmy FAU 20377985843 hard
Motivo: Doy V° B°
Fecha: 04.11.2024 09:21:47 -05:00

Firma Digital SUSALUD Superintendencia Nacional de Salud

Firmado digitalmente por CRUZADO ESPINOZA Cinthia Lizbeth FAU 20377985843 soft
Motivo: Doy V° B°
Fecha: 04.11.2024 16:16:19 -05:00

PLAN DE CONTINUIDAD OPERATIVA DE LA SUPERINTENDENCIA NACIONAL DE SALUD

2024

Firma Digital SUSALUD Superintendencia Nacional de Salud

Firmado digitalmente por DELGADO FLORES Diego Armando FAU 20377985843 soft
Motivo: Doy V° B°
Fecha: 31.10.2024 16:40:47 -05:00

Firma Digital SUSALUD Superintendencia Nacional de Salud

Firmado digitalmente por PABLO VELASQUEZ Brenda Lizbeth FAU 20377985843 soft
Motivo: Doy V° B°
Fecha: 31.10.2024 13:43:04 -05:00

Firma Digital SUSALUD Superintendencia Nacional de Salud

Firmado digitalmente por LESCANO BAZAN Juan Pablo Martin FAU 20377985843 soft
Motivo: Doy V° B°
Fecha: 31.10.2024 12:01:39 -05:00

Firma Digital SUSALUD Superintendencia Nacional de Salud

Firmado digitalmente por ESPIL CABANILLAS Jackelin Georgette FAU 20377985843 soft
Motivo: Doy V° B°
Fecha: 04.11.2024 16:38:39 -05:00

Firma Digital SUSALUD Superintendencia Nacional de Salud

Firmado digitalmente por MORI GUPIOC Christian Ivan FAU 20377985843 soft
Motivo: Doy V° B°
Fecha: 04.11.2024 16:53:25 -05:00

Firma Digital SUSALUD Superintendencia Nacional de Salud

Firmado digitalmente por OLIVERA CHUMBIAUCA Jorge Alex FAU 20377985843 soft
Motivo: Doy V° B°
Fecha: 04.11.2024 17:01:51 -05:00

Firma Digital SUSALUD Superintendencia Nacional de Salud

Firmado digitalmente por VALVERDE MANRIQUE Beatriz Soledad FAU 20377985843 soft
Motivo: Doy V° B°
Fecha: 04.11.2024 17:12:13 -05:00

Firma Digital SUSALUD Superintendencia Nacional de Salud

Firmado digitalmente por CARHUAYA DIAZ Nancy Yanire FAU 20377985843 hard
Motivo: Doy V° B°
Fecha: 04.11.2024 17:20:36 -05:00

ÍNDICE

ÍNDICE DE TABLAS

I Información General

La Superintendencia Nacional de Salud – SUSALUD, es una entidad pública de alcance nacional cuya misión consiste en promover, proteger y restituir los derechos a los servicios de salud de las personas, con calidad, oportunidad, disponibilidad y aceptabilidad, para lo cual, de forma preventiva, primero supervisa la provisión de los servicios de salud a los usuarios en las IAFAS e IPRESS, así como promueve el conocimiento y ejercicio de sus derechos. Por otro lado, en términos de remediación y en caso de vulneración de los derechos en salud, busca restituirlos a través de acciones de regulación, sanción y conciliación, dentro del ámbito de competencia de SUSALUD. Por último, tiene el deber de modernizar la gestión institucional promoviendo espacios de articulación intersectorial y multisectorial de integración de sistemas de información, así como la transformación digital, para la óptima promoción y protección de los derechos en salud de la ciudadanía. En ese sentido, el Plan de Continuidad Operativa de la Superintendencia Nacional de Salud – SUSALUD, establece la identificación de actividades esenciales y recursos críticos necesarios para la ejecución ininterrumpida de los procesos misionales previamente mencionados. Asimismo, el presente documento es el principal instrumento de la Gestión de la Continuidad Operativa de las Entidades Públicas de los tres niveles de Gobierno, liderada por la Presidencia del Consejo de Ministros, y elaborada conforme los lineamientos contenidos en la Resolución Ministerial N° 320-2021-PCM[1]. Adicionalmente, este instrumento de gestión desarrollado se complementa con la ISO 22301, la norma internacional para la Gestión de la Continuidad de Negocio (SGCN), la cual se basa en una serie de principios clave que deben aplicarse de tal manera que la Gestión de la Continuidad Operativa sea la más apropiada y eficiente para la institución.

La activación del presente plan está prevista ante la ocurrencia de un evento adverso cuya magnitud afecte específicamente la operatividad de las diferentes sedes de SUSALUD. Se tiene como referencia de afectación principal, el escenario definido por un desastre ocasionado por un sismo de gran magnitud y tsunami en Lima y Callao, sin que por ello deje de tomar en cuenta otras amenazas**.**

[1] Resolución Ministerial N° 320-2021-PCM, que aprueba los "Lineamientos para la Gestión de la Continuidad Operativa y la Formulación de los Planes de Continuidad Operativa de las Entidades Públicas de los tres niveles de gobierno".

1.1 Principios

El Plan de Continuidad Operativa (PCO en adelante) de SUSALUD debe contener los siguientes principios indicados por la norma ISO 22301:

- Responsabilidad: Es imprescindible asignar roles en la Gestión de la Continuidad Operativa (GCO en adelante), pues en caso de una interrupción, la ausencia de responsabilidades, autoridades y roles claramente definidos puede hacer que un plan de continuidad del negocio se vuelva ineficaz.
- Objetivos claros: Los objetivos del PCO deben definir claramente las actividades en continuidad esperadas tras algún evento, así como los tiempos de tolerancia para la inactividad y la posible continuidad vigente.
- Impacto y Evaluación de riesgos: La capacidad de identificar y planificar los posibles impactos y riesgos comerciales es clave para un sistema de continuidad de negocio eficaz.
- Comunicación: SUSALUD debe incluir en sus planes de continuidad de negocio cómo y cuándo se comunicarán con servidores y órganos con actividades críticas (como reguladores o proveedores de solución).
- Prueba: El Sistema de gestión de la continuidad de negocio debe probarse periódicamente para evaluar su eficacia y realizar los cambios necesarios, esto implica realizar simulaciones y simulacros según corresponda, permitiendo así actualizar el PCO en base a posibles supuestos.

1.2 Términos y Definiciones:

- *Continuidad de negocio*: Capacidad de una organización para continuar la entrega de productos o servicios a niveles predefinidos y aceptables tras una interrupción.
- *Gestión de la Continuidad Operativa (GCO)*: Proceso continuo que forma parte de las operaciones habituales de la Entidad Publica con el objetivo de que siga cumpliendo con su misión, mediante la implementación de mecanismos adecuados, con el fin de continuar brindando servicios necesarios a la población, ante la ocurrencia de un desastre o evento que produzca una interrupción prolongada de sus operaciones.
- *Plan de Continuidad Operativa (PCO):* Instrumento a través del cual se implementa la continuidad operativa, tiene como objetivo garantizar que la entidad ejecute las actividades

críticas identificadas previamente. Contiene la identificación de riesgos y recursos, acciones para la continuidad operativa y el cronograma de ejercicios.

- *Plan de Recuperación de los servicios informáticos:* Plan que forma parte del Plan de Continuidad Operativa, el cual busca, inicialmente, restaurar los servicios de tecnología de información necesarios para ejecutar las actividades críticas identificadas, permitiendo una posterior recuperación de las condiciones previas a su ocurrencia. Para su desarrollo toma en cuenta la Norma Técnica Peruana NTP ISO/IEC 20071:2014.
- *Análisis de impacto al negocio (BIA):* Proceso de análisis de actividades y el efecto que una interrupción de negocio puede tener sobre ellas.
- *Grupo de Trabajo:* Son espacios internos de articulación, de las unidades orgánicas competentes de cada entidad pública en los tres niveles de gobierno, para la formulación de normas y planes, evaluación y organización de los procesos de gestión del riesgo de desastres en el ámbito de su competencia. En SUSALUD, se encuentra conformado con Resolución de Superintendencia N° 118-2019-SUSALUD/S[2].
- *Grupo de Comando:* Es el conjunto de profesionales responsable de dirigir el desarrollo y ejecución del plan de respuesta y continuidad operativa, declarando una interrupción operativa o situación de emergencia, y proporcionando dirección durante el proceso de recuperación, tanto antes como después del incidente. En SUSALUD, se encuentra conformado con Resolución de Superintendencia N° 057-2023-SUSALUD/S[3].
- *Unidad Orgánica a cargo de la Gestión de la Continuidad Operativa:* Designada por el titular de la entidad. Responsable de articular y coordinar la Gestión de la Continuidad Operativa en la Entidad, y de prestar el soporte y apoyo para asegurar la participación de todo el personal en la continuidad operativa.
- *Interrupción:* Evento anticipado (por ejemplo, una huelga laboral o un huracán) o no anticipado (por ejemplo, un apagón o un terremoto), que causa una desviación negativa no planificada en la entrega esperada de productos o servicios de acuerdo con los objetivos de una organización.

---

[2] Resolución de Superintendencia N° 118-2019-SUSALUD/S, que aprueba la conformación del Grupo de Trabajo para la Gestión del Riesgo de Desastres de la Superintendencia Nacional de Salud.

[3] Resolución de Superintendencia N° 057-2023-SUSALUD/S, que aprueba la conformación del "Grupo de Comando de la Superintendencia Nacional de Salud – SUSALUD".

- *Actividades críticas:* Están constituidas por las actividades que la entidad ha identificado como indispensables y que no pueden dejar de realizarse, conforme a sus competencias señaladas en las normas vigentes sobre la materia.
- *Órganos críticos:* Son aquellos órganos de SUSALUD cuyas actividades se han definido como críticas. Abarca los órganos misionales y la mayoría de los órganos de soporte de la entidad: IPROM, IPROT, ISIAFAS, ISIPRESS, INA, IFIS, IID, IMRN, OFICOR, OGPER, OGA y OGPP. Cabe añadir que cada órgano crítico cuenta con un representante en el Grupo de Comando.
- *Órganos no críticos:* Son aquellos órganos de SUSALUD cuyas actividades no se han definido como críticas, exceptuando a la Alta Dirección por la naturaleza de sus funciones.

1.3 Alcance de la gestión de la continuidad operativa

El alcance de la Gestión de la Continuidad Operativa está enmarcado en el desarrollo de las actividades programadas en el Plan de Continuidad Operativa, el cual abarca las tres sedes de SUSALUD. Cabe añadir que el Plan de Continuidad Operativa deberá actualizarse conforme a la necesidad de la entidad.

II Base Legal

- Ley N° 29664, Ley que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD).
- Ley N° 30831, Ley que modifica el Artículo 19 de la Ley 29664, Ley que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD).
- Ley N° 29783, Ley de Seguridad y Salud en el Trabajo.
- Ley N° 31246, Ley que modifica la Ley N° 29783, Ley de Seguridad y Salud en el Trabajo.
- Ley N° 31572, Ley de teletrabajo, y su modificatoria a través de la Ley N° 32102.
- Decreto Supremo N° 048-2011-PCM, Decreto Supremo que aprueba el Reglamento de la Ley N° 29664, que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD).
- Decreto Supremo N° 060-2024-PCM, Decreto Supremo que modifica el Reglamento de la Ley N° 29664, que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD).
- Decreto Supremo N° 038-2021-PCM, Decreto Supremo que aprueba la Política Nacional del Riesgo Desastres al 2050.

- Decreto Supremo N° 115-2022-PCM, Decreto Supremo que aprueba el Plan Nacional de Gestión del Riesgo de Desastres - PLANAGERD 2022-2030.
- Decreto Supremo N° 005-2012-TR, Decreto Supremo que aprueba el Reglamento de la Ley N° 29783, Ley de Seguridad y Salud en el Trabajo.
- Decreto Supremo N° 051-2010-MTC, Decreto Supremo que aprueba el Marco Normativo General del Sistema de Comunicaciones en Emergencias, entre otros.
- Resolución Ministerial N° 320-2021-PCM, que aprueba los Lineamientos para la gestión de la continuidad operativa y la formulación de planes de continuidad operativa en las entidades públicas de los tres niveles de gobierno.
- Resolución Ministerial N° 046-2013-PCM, que aprueba los Lineamientos que definen el Marco de Responsabilidades en Gestión del Riesgo de Desastres, de las entidades del estado en los tres niveles de gobierno.
- Resolución Ministerial N° 188-2015-PCM, que aprueba los Lineamientos para la formulación y aprobación de Planes de Contingencia.
- Resolución Ministerial N° 050-2020-PCM, que aprueba los Lineamientos para la implementación del Proceso de Preparación y la formulación de los Planes de Preparación en los tres niveles de gobierno.
- Resolución Ministerial N° 149-2020-PCM, que aprueba los Lineamientos para la implementación del proceso de rehabilitación y formulación de los planes de rehabilitación en los tres niveles de gobierno.
- Resolución Ministerial N° 136-2020-PCM, que aprueba los Lineamientos para la formulación y aprobación de los planes de operaciones de emergencia en los tres niveles de gobierno.
- Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "ISO NTP/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática, y su modificatoria por Resolución Ministerial Nº 166-2017-PCM.
- Resolución Directoral N° 010-2022-INACAL/DN, que aprueba las Normas Técnicas Peruanas en su versión 2022: NTP-ISO/IEC 27031:2012 (revisada el 2022) Tecnología de la información. Técnicas de seguridad. Directrices para la adecuación de las tecnologías de la información y las comunicaciones para la continuidad del negocio 1ª Edición, entre otras.

- Resolución de Superintendencia N° 118-2019-SUSALUD/S, que aprueba la reconformación del Grupo de Trabajo de la Gestión del Riesgo de Desastres de SUSALUD.
- Resolución de Superintendencia N° 057-2023-SUSALUD/S, que aprueba la conformación del Grupo de Comando de la Superintendencia Nacional de Salud – SUSALUD.
- Decreto Supremo N° 011-2006-VIVIENDA, Decreto Supremo que aprueba sesenta y seis (66) Normas Técnicas del Reglamento Nacional de Edificaciones-RNE, y sus modificatorias.
- Norma ISO 22301:2020, norma sobre la puesta en marcha y aplicación de controles y medidas para gestionar los riesgos generales a los que esté expuesta la continuidad del negocio de una organización.

III Objetivos

3.1 Objetivo General

Garantizar la continuidad operativa de SUSALUD, para brindar los servicios de protección, promoción y restitución de los derechos en Salud al ciudadano, ante la ocurrencia de cualquier evento que interrumpa sus procesos, ejecutando las actividades críticas identificadas para la operatividad.

3.2 Objetivos Específicos

- Identificar las actividades críticas que requieran ser ejecutadas de manera ininterrumpida.
- Determinar los recursos humanos, materiales, equipos e infraestructura; así como los aplicativos informáticos y planes de contingencia para la protección de información; necesarios para ejecutar las actividades críticas.
- Determinar el requerimiento de presupuesto para efectuar y garantizar la continuidad de las operaciones de acuerdo a las actividades críticas identificadas.
- Lograr la preparación adecuada del personal de SUSALUD, de tal forma que sea posible cumplir con la ejecución de la continuidad operativa.

IV Identificación de Riesgos y Recursos

4.1 Matriz de Riesgos

Para la Identificación de Peligros y Riesgos, el Grupo de Comando de la Superintendencia Nacional de Salud (GC-SUSALUD) en coordinación con las diferentes Unidades Orgánicas, empleó la metodología indicada en el Anexo 2 de la Resolución Ministerial N° 320-2021-PCM, el cual señala que primero se deben identificar los diferentes peligros naturales y antrópicos que puedan interrumpir el desarrollo de las actividades y operaciones, tomando en cuenta los niveles de Bajo, Medio, Alto y Muy Alto. Posteriormente, se identifican las vulnerabilidades de la entidad, enfocadas en la infraestructura y la posible afectación del personal, para evaluarlas cualitativamente con los niveles Bajo, Medio, Alto y Muy Alto. Finalmente, se realiza la intersección de peligro y vulnerabilidad para determinar el riesgo resultante.

En ese sentido, el Grupo de Comando identificó los principales peligros que podrían afectar a las tres sedes de SUSALUD.

Tabla N° 1. Peligros identificados

Peligro	Tipo de Peligro	Descripción
Incendio	Antrópico	Los incendios urbanos son fuegos no controlados de grandes proporciones que ocasionan lesiones, pérdidas de vidas humanas, daños materiales y deterioran el ambiente.
Sismo	Natural	Se define como sismo al proceso de generación y liberación de energía para posteriormente propagarse en forma de ondas por el interior de la tierra; al llegar a la superficie, estas ondas son registradas por las estaciones sísmicas y percibidas por la población y por las estructuras.
Movilización Social	Antrópico	La movilización social es un acto espontáneo de acción social por parte de las masas que implica una ética concreta. Pueden ser actos de protesta, boicots u otras

		manifestaciones. Puede ser pacífica o violenta y llevarse a cabo en el mundo físico o en el virtual.
Pandemia/Epidemia	Antrópico	La Emergencia Sanitaria es un evento extraordinario que constituye un riesgo para la salud pública, afectando a los conciudadanos y ciudadanos de otros Estados, a través de la propagación de la enfermedad y que potencialmente requiere una respuesta inmediata y coordinada.
Fenómenos Meteorológicos	Natural	Es un fenómeno o evento de origen climático relacionado con el calentamiento del Océano Pacífico oriental ecuatorial, el cual se manifiesta de manera más intensa, provocando estragos en la zona intertropical y ecuatorial debido a las fuertes lluvias, afectando principalmente a la región costera del Pacífico de América del Sur.
Inundación	Natural o antrópico	Se define como la ocupación por parte del agua de zonas o regiones que habitualmente se encuentran secas. Puede deberse a causas climáticas, geológicas o antrópicas.
Corte de Energía eléctrica/Internet	Antrópico	Este tipo de peligro puede suceder de manera fortuita o provocada, lo cual genera impactos negativos en equipos y personas.
Ataque cibernético	Antrópico	Los ataques cibernéticos son intentos maliciosos de acceder o dañar un sistema de computadoras o redes. Los ataques cibernéticos pueden ocasionar pérdidas de dinero o resultar en el robo de información personal, financiera o médica. Estos ataques pueden afectar su reputación y su seguridad
Tsunami	Natural	Se define como una ola de grandes dimensiones originada cerca de la costa por un sismo de gran magnitud o erupción volcánica submarina, que puede desplazarse a una velocidad de hasta 50 km/h en cualquier dirección, que

		puede traer como consecuencia la destrucción y muerte de seres humanos al arrastrar grandes masas de agua.

Fuente: Elaboración propia

Se identificaron nueve (09) peligros, los cuales podrían generar una interrupción prolongada en el funcionamiento de la Entidad. Posteriormente, se realizó la evaluación de niveles por sede con respecto al peligro, obteniendo como resultado lo siguiente:

Tabla N° 2. Evaluación de peligro por sedes

SEDE	PROCESO	PELIGROS	PELIGRO	NIVEL DE PELIGRO
SEDE CERCADO DE LIMA	1. Promoción de los derechos y deberes en salud. 2. Protección de los derechos en salud. 3. Prevención de la vulneración de derechos en salud. 4. Restitución de los derechos en salud.	Incendio	Pérdida de personas, equipos y documentación	Muy Alto
		Sismo	Colapso de la infraestructura	Muy Alto
		Movilización Social	Ataques a los trabajadores	Medio
		Pandemia/Epidemia	Contraer enfermedades virales	Alto
		Fenómenos Meteorológicos	Pérdida de enseres y acervo documentado	Medio
		Corte de energía eléctrica/internet	Se suspende uso de equipos informáticos	Alto
		Ataque cibernético	Pérdida de información y datos	Medio
SEDE SANTIAGO DE SURCO	1. Gestión de personas 2. Comunicación	Incendio	Pérdida de personas, equipos y documentación	Muy Alto
		Sismo	Colapso de la infraestructura	Muy Alto
		Movilización Social	Ataques a los trabajadores	Bajo

	integral 3. Gestión logística 4.Gestión presupuestal y financiera 5. Gestión tecnológica	Pandemia/Epidemia	Contraer enfermedades virales	Medio
		Fenómenos Meteorológicos	Pérdida de enseres y acervo documentado	Medio
		Corte de energía eléctrica/internet	Se suspende uso de equipos informáticos	Alto
		Ataque cibernético	Pérdida de información y datos	Medio
		Tsunami	Pérdida de infraestructura acervo documentado	Bajo
SEDE CHICLAYO	1. Protección de derechos en salud	Incendio	Perdida de enseres y acervo documentado	Muy Alto
		Sismo	Daños en la Infraestructura/Inadecuadas rutas de evacuación	Muy Alto
		Fenómenos Meteorológicos	Pérdida de enseres y acervo documentado	Alto
		Corte de energía eléctrica/internet	Se suspende uso de equipos informáticos	Alto
		Pandemia/Epidemia	Ausentismo por personal enfermo	Medio
		Inundación	Daños en infraestructura e inventario	Medio

Fuente: Elaboración propia

Una vez evaluados los niveles de peligro, se consolidaron para toda la entidad, priorizando la calificación más alta y ordenando los peligros en función del nivel de peligro acumulado, para obtener el siguiente resultado:

Tabla N° 3. Evaluación de Peligros, Vulnerabilidad y Riesgos

Valoración de Peligros	Valoración de vulnerabilidad	

Tipo	Valoración	Personas	Patrimonio	Promedio	Valoración de Riesgo
Incendio	Muy Alto	Muy Alto	Alto	Alto	Muy Alto
Sismo	Muy Alto	Muy Alto	Alto	Alto	Muy Alto
Corte de energía eléctrica/internet	Alto	Bajo	Medio	Medio	Alto
Pandemia/Epidemia	Medio	Alto	Bajo	Medio	Medio
Fenómenos Meteorológicos	Medio	Medio	Medio	Medio	Medio
Ataque cibernético	Alto	Bajo	Bajo	Bajo	Medio
Movilización Social	Medio	Medio	Medio	Medio	Medio
Inundación	Medio	Bajo	Alto	Medio	Medio
Tsunami	Bajo	Bajo	Bajo	Bajo	Bajo

Fuente: Elaboración propia

Se muestra la valoración de los peligros naturales y antrópicos, la evaluación de la vulnerabilidad en función de persona y el patrimonio, obteniendo un promedio de vulnerabilidad. Y finalmente la valoración del riesgo, la cual se estima en función del peligro y la vulnerabilidad.

A continuación, se presenta el cuadro resumen de los niveles de riesgo identificados en las diferentes sedes de SUSALUD.

Tabla N° 4. Evaluación de Peligros, Vulnerabilidad y Riesgos

N°	Peligro	Riesgo			
		Bajo	Medio	Alto	Muy Alto
1	Incendio				Muy Alto
2	Sismo				Muy Alto
3	Corte de energía eléctrica/internet			Alto	
4	Pandemia/Epidemia		Medio		
5	Fenómenos Meteorológicos		Medio		
6	Ataque cibernético		Medio		
7	Movilización Social		Medio		
8	Inundación		Medio		
9	Tsunami	Bajo			

Fuente: Elaboración propia

4.2 Determinación del nivel de impacto

A partir de los peligros identificados, se realizó la determinación del impacto bajo un enfoque de prioridad según los niveles de riesgo.

Tabla N° 5. Nivel de impacto del peligro sobre las actividades críticas

SUSALUD	Nivel de impacto del Peligro								
	Incendio	Sismo	Corte de energía eléctrica/internet	Pandemia/Epidemia	Fenómenos Meteorológicos	Ataque cibernético	Movilización Social	Inundación	Tsunami

Actividades criticas operativas y de soporte de la Superintendencia Nacional de Salud	Muy Alto	Muy Alto	Alto	Medio	Medio	Medio	Medio	Medio	Bajo

Fuente: Elaboración propia

Se muestra que existen dos peligros que generan un riesgo “Muy alto” sobre las personas y el patrimonio de la entidad, estas son el incendio y el sismo.

4.3 Identificación de recursos

4.3.1 Determinación de los recursos humanos

El personal calculado para el desarrollo de las actividades críticas en un escenario de continuidad operativa alcanza la cantidad de 125 personas, de las cuales un total de 94 personas participan directamente en los procesos operativos o misionales (IFIS, INA, IPROM, IPROT, ISIAFAS, ISIPRESS e IMRN) y 31 personas están encargadas de llevar a cabo los procesos estratégicos y de apoyo en la entidad (IID, OGA, OGPP, OFICOR y OGPER).

Adicionalmente, cabe mencionar que según el Artículo 17 de la Ley N° 31572, Ley de Teletrabajo, el teletrabajo puede flexibilizarse en casos de situaciones especiales, tales como “circunstancias de caso fortuito o fuerza mayor que requieran que, para garantizar la continuidad de los servicios, se puedan realizar determinadas actividades bajo la modalidad de teletrabajo”, hasta que haya concluido el supuesto que dio origen a la situación especial, contexto perfectamente aplicable en el marco de Gestión de la Continuidad Operativa. En ese sentido, se ha realizado una distribución del personal en función a la naturaleza de sus funciones, según lo evaluado por los responsables de órgano, obteniendo un total de 44 que deberán laborar de forma presencial, 46 que deberán laborar en teletrabajo parcial y 35 en teletrabajo parcial o total, según se muestra en la Tabla N° 6. Cabe precisar que la evaluación previamente realizada está sujeta a variación según lo dispongan la Gerencia General y la OGPER, en cumplimiento del Artículo 36 del Reglamento de Organización y Funciones de SUSALUD.

Finalmente, se precisa que la OGPER maneja una relación con los cargos del personal identificado para su posterior uso en una situación de necesidad frente a una interrupción operativa, la cual se adjunta en el Anexo 04. El personal enlistado se comunicará podrá establecer comunicación según el procedimiento señalado en el Anexo 02 y los medios indicados en el Anexo 05.

Tabla N° 6. Distribución de personal para la gestión de la continuidad operativa

ÓRGANO	NO TELETRABAJABLE O PRESENCIAL	TELETRABAJO PARCIAL	TELETRABAJO PARCIAL O TOTAL	TOTAL
IFIS	0	8	0	8
IMRN	7	0	2	9
INA	13	0	0	13
IPROM	0	2	1	3
IPROT	12	3	26	41
ISIAFAS	0	9	0	9
ISIPRESS	9	2	0	11
SUB-TOTAL Personal operativo	*41*	*24*	*29*	*94*
IID	0	11	2	13
OFICOR	3	0	2	5
OGA	0	7	0	7
OGPER	0	1	2	3
OGPP	0	3	0	3
SUB-TOTAL	*3*	*22*	*6*	*31*

Personal estratégico y de apoyo				
TOTAL	44	46	35	125

Fuente: Elaboración propia.

Así mismo, se ha determinado la cantidad de personal indispensable para las tres sedes en SUSALUD.

Tabla N° 7. Distribución de personal por sede

SEDE	NO TELETRABAJABLE O PRESENCIAL	TELETRABAJO PARCIAL	TELETRABAJO PARCIAL O TOTAL	TOTAL
Sede Cercado de Lima	34	24	27	85
Sede Santiago de Surco	3	22	6	31
Sede Chiclayo	7	0	2	9
TOTAL	44	46	35	125

Fuente: Elaboración propia.

Finalmente, se contabiliza al Grupo de Trabajo, los representantes de los órganos críticos y al Grupo de Comando, los cuales alcanzan la cantidad de 28 personas y deberán ser aquellos que participen en la toma de decisiones, bajo la modalidad que se considere pertinente. Se detalla la distribución en la Tabla N° 8.

Tabla N° 8. Distribución de altos cargos para la gestión de la continuidad operativa

INSTANCIA	INTEGRANTES
Grupo de Trabajo	● Superintendente ● Gerente General

	● Superintendente Adjunto/a de Promoción y Protección de Derechos en Salud ● Superintendente Adjunto/a de Supervisión ● Superintendente Adjunto/a de Regulación y Fiscalización ● Director/a General de la Oficina General de Gestión de las Personas ● Director/a General de la Oficina General de Administración ● Director/a de la Oficina General de Planeamiento y Presupuesto
Representantes de órganos críticos	● Intendente de la Intendencia de Promoción de Derechos en Salud ● Intendente de la Intendencia de Protección de Derechos en Salud ● Intendente de Supervisión de IAFAS ● Intendente de Supervisión de IPRESS ● Intendente de la Intendencia de Normas y Autorizaciones ● Intendente de la Intendencia de Fiscalización y Sanción ● Intendente Macro Regional de la Región Norte de SUSALUD ● Director/a General de la Oficina General de Gestión de las Personas ● Director/a General de la Oficina General de Administración ● Director/a de la Oficina General de Planeamiento y Presupuesto ● Intendente de la Intendencia de Investigación y Desarrollo ● Director/a de la Oficina de Comunicación Corporativa
Grupo de Comando	● Representante de la Intendencia de Promoción de Derechos en Salud ● Representante de la Intendencia de Protección de Derechos en Salud ● Representante de la Intendencia de Supervisión de IAFAS ● Representante de la Intendencia de Supervisión de IPRESS ● Representante de la Intendencia de Normas y Autorizaciones ● Representante de la Intendencia de Fiscalización y Sanción ● Representante de la Intendencia Macro Regional SUSALUD Norte ● Representante de la Oficina General de Administración ● Representante de la Oficina General de Planeamiento y Presupuesto ● Representante de la Intendencia de Investigación y Desarrollo ● Representante de la Oficina de Comunicación Corporativa

	● Representante de la Oficina General de Gestión de las Personas

Fuente: Elaboración propia.

4.3.2 Determinación de los recursos físicos críticos

Según la Tabla N° 6, se han determinado 44 personas en modalidad presencial por la naturaleza de sus actividades, por lo que tendrán que trasladarse a la Sede Alterna para garantizar la continuidad de sus funciones, cuyo detalle para las tres sedes se encuentra en el apartado 5.6. Para dicho fin, se ha identificado el material y equipo necesario para el desarrollo de sus actividades en la Tabla N° 9.

Tabla N° 9. Identificación de recursos físicos críticos

ÓRGANO	ESCRITORIO	SILLA ERGONÓMICA	IMPRESORA	GABINETE O ESTANTE	PACK DE ARTÍCULOS DE OFICINA	CABLE DE RED
INA	13	13	1	1	1	13
IPROT	12	12	1	1	1	12
ISIPRESS	9	9	1	1	1	9
OFICOR	3	3	1	1	1	3
IMRN	7	7	1	1	1	7

Fuente: Elaboración propia.

Así mismo, se identificaron los recursos críticos para las tres sedes en SUSALUD.

Tabla N° 10. Identificación de recursos críticos por sede

SEDE	ESCRITORIO	SILLA ERGONÓMICA	IMPRESORA	GABINETE O ESTANTE	PACK DE ARTÍCULOS DE OFICINA	CABLE DE RED

Sede Cercado de Lima	34	34	3	3	3	34
Sede Santiago de Surco	3	3	1	1	1	3
Sede Chiclayo	7	7	1	1	1	7
TOTAL	44	44	5	5	5	44

Fuente: Elaboración propia.

Los demás órganos con personal identificado como crítico podrán realizar “Teletrabajo parcial” o “Teletrabajo total o parcial” como lo indica la Tabla N° 6, por lo que no se incluyen en este apartado. Así mismo, las instancias involucradas en la toma de decisiones trabajarán bajo la modalidad previamente mencionada.

4.3.3 Determinación de los recursos informáticos e información crítica

a) Equipos informáticos

Se cuenta con noventa cuatro (94) equipos informáticos para el desarrollo de actividades del personal operativo; asimismo, se cuenta con treinta (30) equipos informáticos para el desarrollo de actividades del personal estratégico y de apoyo.

Tabla N° 11. Determinación de equipos informáticos

Órgano	CPU	LAPTOP	MONITOR	TECLADO
IFIS	6	2	6	6
IMRN	5	4	5	5
INA	10	3	10	10
IPROM	3	0	3	3
IPROT	34	7	34	34
ISIAFAS	1	8	1	1
ISIPRESS	3	8	3	3
SUB-TOTAL *Personal operativo*	*62*	*32*	*62*	*62*
IID	13	0	13	13
OFICOR	4	0	6	4
OGA	7	0	7	7
OGPER	2	1	2	2
OGPP	3	0	3	3
SUB-TOTAL *Personal estratégico y de apoyo*	*29*	*1*	*31*	*29*
TOTAL	91	33	93	91

Fuente: Elaboración propia

Así mismo, se realizó la identificación de equipos informáticos por sede.

Tabla N° 12. Determinación de equipos informáticos por sede

SEDE	CPU	LAPTOP	MONITOR	TECLADO
Sede Cercado de Lima	57	28	57	57
Sede Santiago de Surco	29	1	31	29
Sede Chiclayo	5	4	5	5
TOTAL	91	33	93	91

Fuente: Elaboración propia

Por otro lado, se contabilizan 28 equipos informáticos para el desarrollo de actividades del Grupo de Trabajo, los representantes de los órganos críticos y el Grupo de Comando.

Finalmente cabe añadir que, a nivel estructural, únicamente se cuenta con un Centro de Datos ubicado en la sede Surco.

b) Servicios informáticos (aplicativos)

Los servicios informáticos identificados se clasifican en principales y secundarios, siendo los primeros aquellos que usan todos los órganos, y los segundos aquellos que usan algunos órganos, pero indispensables para el desarrollo de actividades críticas.

- Servicios informáticos principales
    - S.O. Windows
    - Office
    - SGD
    - Herramientas de Google (Meet, correo, etc.)
    - Antivirus
    - Firma ONPE
- Servicios informáticos secundarios: Se detallan en la Tabla N° 13.

Tabla N° 13. Determinación de servicios informáticos

Órgano	Plataforma BPM	STD	Sistema de supervisión	Facebook, Twitter, Instagram, YouTube	SIGA
OGPER					X
OGA					X
OGPP					
OFICOR				X	
IID					X
IFIS	X	X			
INA					
IPROT	X				
IMRN	X				
IPROM					
ISIAFAS					X
ISIPRESS			X		
TOTAL	3	1	1	1	4

Órgano	QLICK	ALTERYX	RHNUBE	SIAF	AIRSH
OGPER			X	X	X
OGA			X	X	
OGPP				X	
OFICOR					
IID	X	X		X	
IFIS					
INA					
IPROT					
IMRN					
IPROM					
ISIAFAS					
ISIPRESS					
TOTAL	1	1	2	4	1

Órgano	Casilla electrónica	WINRAR	Oracle	RESUELVE	SITEDS
OGPER					
OGA					
OGPP					
OFICOR					
IID			X	X	X
IFIS	X				
INA		X			
IPROT					
IMRN					
IPROM					
ISIAFAS					
ISIPRESS					
TOTAL	1	1	1	1	1

Órgano	Lotus Cliente	RIPRESS, SETIEPS, RENIPRESS	Convocatorias CAS	BIZAGI	ISABELL	POWER BI
OGPER						
OGA						
OGPP						
OFICOR						
IID						
IFIS						
INA	X	X	X			
IPROT				X	X	X
IMRN						
IPROM						
ISIAFAS						
ISIPRESS						
TOTAL	1	1	1	1	1	1

Fuente: Elaboración propia

c) Información crítica

Se ha identificado que cada órgano maneja una carpeta compartida en el dominio de su respectiva oficina, en la cual se resguarda la información crítica. Existen 22 carpetas a nivel de SUSALUD y 12 carpetas correspondientes a los órganos críticos. Cabe precisar que esta información físicamente se encuentra en los servidores del Centro de Datos de la entidad, por lo que es indispensable garantizar su integridad, para lo cual se disponen acciones en el Anexo 01.

4.3.4 Determinación de los recursos financieros

Para el desarrollo de las actividades de la entidad, se cuenta con la Unidad Ejecutora 001-515: SUPERINTENDENCIA NACIONAL DE SALUD del pliego 134: SUPERINTENDENCIA NACIONAL DE SALUD, en el cual se contemplan las categorías presupuestales 9001: Acciones centrales y 9002: Asignaciones presupuestarias que no resultan en productos, cuyos gastos se justifican en las necesidades de los órganos.

Cabe añadir que es posible la ejecución de modificaciones presupuestales, por lo que también es viable la orientación de recursos a las acciones de implementación de la Gestión de la Continuidad Operativa.

V Acciones para la continuidad operativa

5.1 Determinación de las actividades críticas

Las actividades críticas se definen como aquellas que son indispensables para el cumplimiento de la misión institucional de SUSALUD, en ese sentido, es necesario identificarlas y priorizarlas en un contexto de continuidad operativa. Actualmente, la entidad cuenta con veintisiete (27) actividades críticas, las mismas que están vinculadas a los macroprocesos de SUSALUD. A continuación, se detallan las actividades críticas y su Tiempo Máximo Tolerable de Indisponibilidad - Maximum Tolerable Period of Disruption (MTPD).

Tabla N° 14. Determinación de actividades críticas

N°	CODIGO	ACTIVIDADES CRÍTICAS	MACROPROCESO VINCULADO	ÓRGANO	MTPD (hrs)
1	UOGCO1	Gestionar la continuidad operativa y su articulación con los demás planes del SINAGERD	E.1. PLANEAMIENTO INSTITUCIONAL	UOGCO	25
2	OFICOR3	Monitorear y reportar los casos de vulneración de derechos en salud a través de redes	E.3. COMUNICACIÓN ESTRATÉGICA	OFICOR	25
3	OFICOR2	Monitorear la prensa y redes sociales	E.3. COMUNICACIÓN ESTRATÉGICA	OFICOR	27
4	OGPER2	Asesorar a los servidores en los trámites y procesos necesarios para garantizar su bienestar	S.1. GESTIÓN DE PERSONAL	OGPER	36
5	IID1	Recolectar, transferir, difundir e intercambiar la información generada u obtenida por la IAFAS, IPRESS y Unidades de Gestión de IPRESS con el Registro de Afiliados, RESUELVE y SITEDS.	S.4. GESTIÓN DE INFRAESTRUCTURA TECNOLÓGICA	IID	36
6	IPROT1	Brindar asistencia en la Plataforma de atención al usuario funcionando en beneficio de los ciudadanos a nivel nacional.	M.2. PROTECCIÓN DE DERECHOS EN SALUD	IPROT	48
7	IPROT3	Atender denuncias en salud de forma oportuna a nivel nacional	M.2. PROTECCIÓN DE DERECHOS EN SALUD	IPROT	48
8	IPROT2	Atender solicitudes a través de acciones inmediatas por los delegados en salud	M.2. PROTECCIÓN DE DERECHOS EN SALUD	IPROT	48
9	OGA2	Controlar y garantizar el mantenimiento de los bienes y servicios de la entidad	S.2. GESTIÓN LOGÍSTICA	OGA	48
10	OGPP1	Comunicar y/o administrar autorizaciones del MEF para modificaciones y certificaciones	S.3. GESTIÓN PRESUPUESTAL Y FINANCIERA	OGPP	51
11	INA1	Evaluar y formular proyectos de normas para su posterior aprobación	M.4. RESTITUCIÓN DE DERECHOS EN SALUD	INA	72
12	IFIS1	Regular o sancionar a las Instituciones Prestadoras de Servicios de Salud, Instituciones Administradoras de Fondos de Aseguramiento en Salud y las Unidades de Gestión de Instituciones Prestadoras de Servicios de	M.4. RESTITUCIÓN DE DERECHOS EN SALUD	IFIS	75

		Salud, privadas, públicas o mixtas.			
13	INA2	Administrar los registros de IAFAS, IPRESS, UGIPRESS, Registro de Sanciones, Registro de Corredores de Aseguramiento en Salud, Registro de Sanciones de los Profesionales de la Salud	M.3. PREVENCIÓN DE VULNERACIÓN DE DERECHOS EN SALUD	INA	96
14	OGA1	Gestionar los bienes patrimoniales y custodiar la documentación respectiva	S.2. GESTIÓN LOGÍSTICA	OGA	96
15	OGA4	Administrar los girados, gastos y compromisos de pago de la entidad	S.2. GESTIÓN LOGÍSTICA	OGA	96
16	ISIPRESS 1	Planificar y realizar continuas supervisiones a las IPRESS	M.3. PREVENCIÓN DE VULNERACIÓN DE DERECHOS EN SALUD	ISIPRESS	120
17	IMRN1	Garantizar la óptima atención al usuario por parte del equipo de intermediación en los servicios de salud	M.2. PROTECCIÓN DE DERECHOS EN SALUD	IMRN	169
18	OGPER1	Gestionar la remuneración de los servidores	S.1. GESTIÓN DE PERSONAL	OGPER	170
19	ISIPRESS 3	Gestionar y supervisar la atención de documentos	M.3. PREVENCIÓN DE VULNERACIÓN DE DERECHOS EN SALUD	ISIPRESS	174
20	ISIPRESS 2	Realizar informes legales de las presuntas infracciones de las IPRESS	M.3. PREVENCIÓN DE VULNERACIÓN DE DERECHOS EN SALUD	ISIPRESS	240
21	ISIAFAS1	Fiscalizar a las IAFAS, IPRESS y UGIPRESS	M.3. PREVENCIÓN DE VULNERACIÓN DE DERECHOS EN SALUD	ISIAFAS	288
22	IPROM2	Gestionar acciones para promover derechos y deberes en salud	M.1. PROMOCIÓN DE DERECHOS Y DEBERES EN SALUD	IPROM	336
23	OGA3	Gestionar y supervisar la contratación de bienes y servicios	S.2. GESTIÓN LOGÍSTICA	OGA	336
24	IMRN2	Planificar y realizar continuas supervisiones a las IPRESS	M.3. PREVENCIÓN DE VULNERACIÓN DE DERECHOS EN SALUD	IMRN	344
25	IPROM1	Gestionar la participación ciudadana mediante las JUS	M.1. PROMOCIÓN DE DERECHOS Y DEBERES EN SALUD	IPROM	360

26	IPROM3	Gestionar acciones de asistencia técnica a IAFAS, IPRESS, UGIPRESS	M.1. PROMOCIÓN DE DERECHOS Y DEBERES EN SALUD	IPROM	696
27	OFICOR1	Elaborar y difundir mensajes comunicacionales externos e internos	E.3. COMUNICACIÓN ESTRATÉGICA	OFICOR	720

Fuente: Elaboración propia

Cabe añadir que, si bien los procesos priorizados tienen un MTPD determinado en base a la evaluación de impacto realizada por los ejecutores del proceso, este estará supeditado al tiempo de recuperación objetivo (RTO) de los servicios informáticos empleados para ejecutar dichos procesos, los cuales se detallan en el Anexo 01.

5.2 Aseguramiento del acervo documentario

La documentación que maneja la entidad debe ser adecuadamente conservada, ya sea de forma física o digital.

En ese sentido, se cuenta con el Plan Anual de Trabajo del Archivo Central de la Superintendencia Nacional de Salud, el cual se actualiza cada año y su última versión de 2024 fue aprobada con la Resolución de Gerencia General N° 003-2024-SUSALUD/GG. Este plan contempla entre sus objetivos específicos velar por la conservación y protección integral del patrimonio documental de SUSALUD, mediante la ejecución de actividades archivísticas como la digitalización y la conservación de documentos.

Así mismo, la Directiva N° 004-2019-SUSALUD/GG “Normas Técnicas Archivísticas de SUSALUD” abarca aspectos complementarios que deben cumplirse para la gestión del acervo documentario.

5.3 Aseguramiento de la base de datos mediante la ejecución del plan de recuperación de los servicios informáticos

Para garantizar la continuidad operativa de las diferentes aplicaciones y servicios informáticos se determinó que, a nivel de infraestructura, actualmente solo se cuenta con el Centro de Datos de la sede Surco, por lo que al no contar con un centro alterno, a la fecha únicamente son recuperables

de forma parcial los recursos tecnológicos que soportan los servicios informáticos principales y secundarios de la Tabla N° 15.

Tabla N° 15. Procesos priorizados con sus respectivos servicios informáticos secundarios

Prioridad	Proceso	Código de actividad crítica	Servicios
1	Afiliación de asegurados	IID1	• REGISTRO DE AFILIADOS • RESUELVE
2	Acreditación de asegurados	IID1	• SITEDS CLIENTE • SITEDS WEB • SITEDS PASARELA
3	Registro de IPRESS	INA2	• RENIPRESS
4	Atención al ciudadano	IPROT1	• BPM PAC

El detalle de acciones, responsables y Tiempo de Recuperación Objetivo (RTO) se desarrolla en el Anexo 01, el cual cabe añadir, se basa en un posible siniestro o incidente de magnitud alta, entendiendo este último como la pérdida parcial de infraestructura de HW o SW o telecomunicaciones, por lo que sería aplicable en caso de que los servicios críticos sufran una caída total, gestionando acciones para una recuperación parcial hasta en 28 días.

Finalmente cabe añadir que para mejorar el aseguramiento de la base de datos de forma total y con tal de que abarque todas las actividades críticas identificadas, la Intendencia de Investigación y Desarrollo determina que es necesario priorizar la adquisición de equipos y servicios según el siguiente detalle:

- Equipos de respaldo alterno y del soporte externo para el Sistema de Respaldo de Información COMVAULT
- Contratación del servicio de hosting (On-premise o en la nube) para restaurar, en caso de siniestro, la Base de Datos Oracle 12c
- Disponibilidad de un Centro Alterno para la recuperación de servicios críticos en caso de destrucción parcial o total del Centro de Datos

- Servidores o sistema de registro de información que permita transferir la información procesada de forma automática ante cualquier eventualidad, para así evitar su pérdida.

5.4 Roles y Responsabilidades para el desarrollo de las actividades críticas

En base a la Resolución Ministerial N° 320-2021-PCM, se tienen las siguientes organizaciones involucradas en la Gestión de la Continuidad Operativa:

- Titular de la Entidad
- Unidad Orgánica a cargo de la gestión de la Continuidad Operativa (UOGCO)
- Grupo de Comando

Cada una de estas organizaciones tiene responsabilidades definidas, por lo que en base a ello, se detallan los roles para el desarrollo de las actividades críticas en la Tabla N° 16.

Tabla N° 16. Roles y Responsabilidades para el desarrollo de las actividades críticas

N°	Instancia, órgano o unidad orgánica	Roles y responsabilidades
1	Titular de la entidad	● Liderar la Gestión de la Continuidad Operativa en la entidad. ● Disponer que los funcionarios de la Alta Dirección participen personalmente en la Gestión de la Continuidad Operativa y asuman responsabilidades directas en su implementación, seguimiento y monitoreo. ● Designar la unidad orgánica que será responsable de la Gestión de la Continuidad Operativa (UOGCO). ● Aprobar la conformación del Grupo de Comando, a propuesta de la UOGCO. ● Activar el Plan de Continuidad Operativa a propuesta del Grupo de Comando y comunicarlo a la UOGCO.

2	Grupo de Trabajo	● Garantizar y facilitar las acciones relacionadas a la activación del Plan de Continuidad Operativa. ● Monitorear el cumplimiento del Plan de Continuidad Operativa.
3	Grupo de Comando	● Proponer al titular de la entidad la activación del Plan de Continuidad Operativa cuando corresponda. ● Verificar el desarrollo de las actividades críticas. ● Verificar el cumplimiento del cronograma de ejercicios del Plan de Continuidad Operativa.
4	UOGCO	● Gestionar la realización de los simulacros y simulaciones de la Gestión de la Continuidad Operativa. ● Gestionar la integración de la Gestión de la Continuidad Operativa a la cultura organizacional. ● Convocar a sesión a los miembros del Grupo de Comando para determinar la activación del plan. ● Gestionar el apoyo de los órganos de soporte para la Gestión de la Continuidad Operativa. ● Consolidar la información remitida por los órganos críticos. ● Reportar a los miembros del Grupo de Comando el cumplimiento de acciones previstas, así como cualquier situación no contemplada que repercuta en el éxito de la continuidad operativa. ● Convocar a sesión a los miembros del Grupo de Comando para determinar la desactivación del plan.
5	OGA	● Reportar a la UOGCO el estado de los servicios básicos y de seguridad de las sedes de Cercado, Surco y Chiclayo luego de un evento disruptivo. ● Adoptar las acciones como coordinador para la movilización de personal a la Sede Alterna, así como la habilitación de la misma en caso sea necesario.
6	IID	● Reportar a la UOGCO el estado de los equipos y servicios

		informáticos luego de un evento disruptivo. ● Asumir la activación del Plan de Recuperación de los Servicios Informáticos (Anexo 01) desde la activación del PCO.
7	OFICOR	● Adoptar acciones para la difusión de comunicados internos y externos durante el desarrollo de la continuidad operativa.
8	OGPER	● Reportar a la UOGCO el estado del personal total, tanto crítico como no crítico, luego de un evento disruptivo.
9	OGPP	● Comunicar a la UOGCO y gestionar la habilitación presupuestal disponible luego de un evento disruptivo.
10	Órganos críticos	● Reportar a la OGPER la disponibilidad del personal luego del evento disruptivo. ● Evaluar las interrupciones que afecten o puedan afectar las actividades críticas y comunicarlas a la UOGCO. ● Ejecutar el Plan de Continuidad Operativa en el momento que se comunique su activación. ● Mantener comunicación constante durante la ejecución del Plan de Continuidad Operativa. ● Reportar a la UOGCO el estado de recuperación de las actividades críticas. ● Participar en la realización de los simulacros y simulaciones de la Gestión de la Continuidad Operativa. ● Participar en la integración de la Gestión de la Continuidad Operativa a la cultura organizacional.
11	Órganos no críticos	● Participar en la realización de los simulacros y simulaciones de la Gestión de la Continuidad Operativa. ● Participar en la integración de la Gestión de la Continuidad Operativa a la cultura organizacional.

Fuente: Elaboración propia.

Sin perjuicio de lo considerado en la Tabla N° 17, también se considerarán las funciones o acciones asumidas por el titular de la entidad, la UOGCO y el Grupo de Comando que están consignadas desde el numeral 6.1.1 al 6.1.3 de la Resolución Ministerial N° 320-2021-PCM. Así mismo, cabe añadir que los órganos de soporte mencionados previamente deberán asumir tanto sus roles y responsabilidades de apoyo como las detalladas en su rol de órganos críticos.

5.4.1 Cadena de mando

Para el óptimo desarrollo de las actividades críticas se ha considerado la toma de decisiones en base al ROF, por lo que se detalla la Cadena de Mando en la siguiente tabla.

Tabla N° 17. Cadena de mando

N°	Instancia	Titular	Alterno
1	Alta Dirección	Superintendente	Gerente General
2	Miembros del Grupo de Trabajo	Superintendente Adjunto	Intendente
3	Directores, intendentes y otros directivos	Director, intendente u otro directivo de cada órgano	Jefe/a, coordinador/a o responsable encargado/a de cada órgano
4	Grupo de Comando	Representantes designados	

Fuente: Elaboración propia

En vista de que el Grupo de Comando tiene el propósito principal de formular el proyecto del presente plan y contribuir al desarrollo de actividades críticas, se ha definido como la última instancia con respecto a la toma de decisiones para garantizar la continuidad operativa. La

conformación del Grupo de Comando fue aprobada con la Resolución de Superintendencia N° 057-2023-SUSALUD/S, tal como se detalla en la Tabla N° 8 y cuyos miembros se enlistan en el Anexo 03.

Adicionalmente, cabe mencionar que corresponde al titular de la UOGCO convocar a sesión de Grupo de Comando cuando suceda un evento disruptivo, para que este último determine si debe proponer la activación de Plan de Continuidad Operativa al titular de la entidad.

5.5 Requerimientos

5.5.1 Requerimientos de Personal

Según el numeral 4.3.1, respecto a la Determinación de los recursos humanos, se ha contabilizado la cantidad de 125 servidores para la ejecución de actividades críticas, sin embargo, se ha identificado una brecha de personal debida a que la sostenibilidad de algunos servidores estaba enmarcada en los Decretos de Urgencia (DU). Se detalla el requerimiento de personal para ejecutar el Plan de Continuidad Operativa en la Tabla N° 18. Cabe añadir que la formulación del requerimiento de personal se incrementará en función del alcance territorial de la entidad y del volumen de pendientes relacionados a las actividades críticas. Así mismo, las modalidades de teletrabajo se encuentran sujetas a variación, según lo indiquen la Ley de Teletrabajo, sus modificatorias y la entidad en el marco de su competencia.

Tabla N° 18. Requerimiento de personal por órgano

ÓRGANO	NO TELETRABAJABLE O PRESENCIAL	TELETRABAJO PARCIAL	TELETRABAJO PARCIAL O TOTAL	TOTAL
IFIS	0	12	0	12
IMRN	8	0	5	13
INA	14	0	0	14
IPROM	0	2	1	3
IPROT	12	3	26	41
ISIAFAS	0	9	0	9

ISIPRESS	10	2	0	12
SUB-TOTAL *Personal operativo*	*44*	*28*	*32*	*104*
IID	0	13	2	15
OFICOR	3	0	2	5
OGA	0	7	0	7
OGPER	2	1	2	5
OGPP	0	3	0	3
SUB-TOTAL *Personal estratégico y de apoyo*	*5*	*24*	*6*	*35*
TOTAL	49	52	38	139

Fuente: Elaboración propia

Así mismo, se detalla el requerimiento por sede en la Tabla N° 19.

Tabla N° 19. Requerimiento de personal por sede

SEDE	NO TELETRABAJABLE O PRESENCIAL	TELETRABAJO PARCIAL	TELETRABAJO PARCIAL O TOTAL	TOTAL
Sede Cercado de Lima	36	28	27	91
Sede Santiago de Surco	5	24	6	35

Sede Chiclayo	8	0	5	13
TOTAL	49	52	38	139

Fuente: Elaboración propia

5.5.2 Requerimientos de Material y Equipo

Además de requerir la determinación de una Sede Alterna para la Sede Chiclayo, según el numeral 4.3.2, respecto a la Determinación de los recursos físicos críticos, para el funcionamiento de la Sede Alterna se tienen los recursos indicados en la Tabla N° 9, a los cuales se requiere adicionar lo indicado en la siguiente tabla.

Tabla N° 20. Requerimientos de Material y Equipo

ÓRGANO	Escritorio	Silla ergonómica	Pack de Módem, Router y Switch	Impresora	Gabinete o estante	Pack de papelería y artículos de oficina	Cable de red	Toldos	Grupo electrógeno	Módem de WiFi Portátil	Equipo de radio
INA	14	14	1	1	1	1	14	6	1	7	1
IPROT	12	12					12				
ISIPRESS	10	10					10				
OFICOR	3	3	1	1	1	1	3	1			
OGPER	2	2					2				
IMRN	8	8	1	1	1	1	8	2	1	2	1

Fuente: Elaboración propia

Por otro lado, se detalla el requerimiento por sede en la Tabla N° 21.

Tabla N° 21. Requerimientos de Material y Equipo por sede

SEDE	Escritorio	Silla ergonómica	Pack de Módem, Router y Switch	Impresora	Gabinete o estante	Pack de artículos de oficina	Cable de red	Toldos	Grupo electrógeno	Módem de WiFi Portátil	Equipo de radio
Sede Cercado de Lima	38	38	1	1	1	1	38	6	1	7	1
Sede Santiago de Surco	5	5	1	1	1	1	5	1			
Sede Chiclayo	8	8	1	1	1	1	8	2	1	2	1
TOTAL	51	51	3	3	3	3	51	9	2	9	2

Fuente: Elaboración propia

Se añaden los requerimientos de la IMRN tomando en cuenta que en un futuro se les pueda habilitar una Sede Alterna, además se añaden dos grupos electrógenos, tanto para Lima como para Chiclayo, en caso ocurriera un corte eléctrico; una cantidad considerable de módems de WiFi portátiles en caso se inhabilite la conexión por cable; y dos equipos de radiocomunicación en caso se pierda la señal telefónica.

5.5.3 Requerimiento de Recursos Informáticos

En base al requerimiento de personal, se determina que se requieren ciento cuatro (104) equipos informáticos para el desarrollo de actividades del personal operativo; así como treinta y cinco (35) equipos informáticos para el desarrollo de actividades del personal estratégico y de apoyo. Se detalla en la Tabla N° 22.

Tabla N° 22. Requerimiento de Recursos Informáticos

ÓRGANO	CPU	LAPTOP	MONITOR	TECLADO
IFIS	6	6	6	6
IMRN	5	8	5	5
INA	10	4	10	10
IPROM	3	0	3	3
IPROT	34	7	34	34
ISIAFAS	1	8	1	1
ISIPRESS	3	9	3	3
SUB-TOTAL *Personal operativo*	*62*	*42*	*62*	*62*
IID	15	0	15	15
OFICOR	4	1	6	4
OGA	7	0	7	7
OGPER	2	3	2	2
OGPP	3	0	3	3
SUB-TOTAL *Personal estratégico y de apoyo*	*31*	*4*	*33*	*31*
TOTAL	93	46	95	93

Fuente: Elaboración propia

Así mismo, se determinó el requerimiento de recursos informáticos por sede.

Tabla N° 23. Requerimiento de recursos informáticos por sede

SEDE	CPU	LAPTOP	MONITOR	TECLADO
Sede Cercado de Lima	57	34	57	57
Sede Santiago de Surco	31	4	33	31
Sede Chiclayo	5	8	5	5
TOTAL	93	46	95	93

Fuente: Elaboración propia

5.5.4 Requerimiento Presupuestal

Según lo indicado en el numeral 4.3.4 sobre la Determinación de los recursos financieros, es necesaria la modificatoria presupuestal para dirigir recursos a la implementación de la Gestión de la Continuidad Operativa, y así cubrir la brecha de necesidades que están generando los requerimientos del presente apartado.

5.6 Determinación de la Sede Alterna de Trabajo

La OGA ha determinado la Sede Alterna para el presente plan en función al siguiente detalle:

Tabla N° 24. Determinación de Sede Alterna

SEDE	POSIBLE UBICACIÓN ALTERNA
SURCO - Av. Velasco Astete N° 1398	Cercado de Lima
Cercado de Lima - Av. Nicolás de Piérola N° 529 - Ex. Edif. Crillón	SURCO (ÁREAS LIBRES)

Fuente: INFORME N° 000406-2023-SUSALUD-OGA-LBM

Adicionalmente, la OGA considera que en el caso de la sede IMRN Chiclayo, al no contar con un inmueble aledaño, se estaría considerando en su totalidad las actividades remotas de forma provisional, hasta que se pueda determinar una Sede Alterna.

5.7 Activación del plan de continuidad operativa

La activación del Plan de Continuidad Operativa es propuesta por el Grupo de Comando al titular de la entidad, para ello, el Grupo de Comando debe haber gestionado las actividades de preparación previas al evento disruptivo. Así mismo, deben gestionarse las actividades de ejecución y evaluación, durante y después del evento, según el siguiente detalle:

Antes

- El Grupo de Comando garantiza la aprobación del PCO.
- La UOGCO gestiona la difusión del PCO con todo el personal de SUSALUD.
- SUSALUD realiza ejercicios de simulacros y simulación como parte de la aplicación del PCO.
- La UOGCO en coordinación con los órganos de soporte gestiona la disposición de recursos y medios necesarios para cuando deba activarse el PCO, los cuales debieron ser asegurados y priorizados por el titular de la entidad.
- La UOGCO remite el PCO al INDECI.
- SUSALUD implementa capacitaciones para el personal involucrado en el PCO.

Durante

- SUSALUD gestiona la evacuación de personal y recursos en la medida de lo enmarcado en el SINAGERD.

Después

- La UOGCO convoca al Grupo de Comando para que evalúen la necesidad de activar el PCO.
- El Grupo de Comando elevará la propuesta de activación del PCO al titular de la entidad.
- El titular de la entidad activa el PCO y se lo informa a la UOGCO.
- SUSALUD ejecuta las acciones planteadas en el PCO (Gestión de Crisis).

- El Grupo de Comando en coordinación con la UOGCO evalúa las condiciones para la recuperación progresiva de la entidad, a fin de volver a la normalidad.
- SUSALUD desarrolla las actividades de restablecimiento o rehabilitación.
- El Grupo de Comando documenta las lecciones aprendidas sobre el evento disruptivo para actualización del PCO.

Así mismo, se desarrolla la Gestión de Crisis una vez activado el PCO, en función del siguiente detalle:

- La UOGCO convoca a la Alta Dirección, los representantes de los órganos críticos y no críticos, y al Grupo de Comando, para establecer la Cadena de Mando y definir suplentes en caso sea necesario.
- Los representantes del Grupo de Comando de los órganos críticos supervisan y comunican constantemente a la UOGCO el estado de sus actividades. Con respecto a los órganos no críticos, estos deben designar a un responsable encargado de la misma actividad.
- Se realizan las coordinaciones pertinentes con los órganos de soporte para que se ejecuten las responsabilidades establecidas en el presente plan.

5.8 Activación y desactivación de la Sede Alterna

a) Activación de la Sede Alterna

Una vez que el titular de la entidad active el PCO y la OGA haya determinado que alguna de las sedes actuales se encuentra inaccesible, se procederá de la siguiente forma:

- En caso la Sede Cercado se haya visto gravemente afectada, se gestionará la habilitación de espacios libres en la Sede Surco.
- En caso la Sede Surco se haya visto gravemente afectada, se gestionará la habilitación de los espacios no ocupados en la Sede Cercado.
- En caso la Sede Chiclayo o las demás sedes mencionadas anteriormente se hayan visto gravemente afectadas, se estaría considerando el teletrabajo total, al no contar con un inmueble aledaño.

b) Reunión y traslado del personal crítico

En caso corresponda, la OGA trasladará al personal crítico a la Sede Alterna, el cual deberá ser priorizado en función del MTPD de su actividad crítica vinculada.

c) Desactivación de la Sede Alterna

El director de la UOGCO convocará a sesión a los miembros del Grupo de Comando, para que puedan proponer la culminación de actividades críticas en la Sede Alterna y la desactivación del plan al titular de la entidad.

5.9 Desarrollo de las actividades críticas

Tabla N° 25. Desarrollo de actividades críticas

CÓDIGO	PRIORIDAD	ACTIVIDAD CRÍTICA	SUB ACTIVIDADES A DESARROLLAR
UOGCO1	1	AC3: Gestionar el PCO y su articulación con los demás planes del SINAGERD	Gestión de planes de SINAGERD
			Aseguramiento de la continuidad operativa
OFICOR3	2	AC3: Monitorear y reportar los casos de vulneración de derechos en salud a través de redes	Monitoreo de redes sociales
			Reporte de casos mediáticos con vulneración de derechos en salud
			Elaboración de informe mensual
			Elaboración de matriz de casos reportados
OFICOR2	3	AC2: Monitorear la prensa y redes sociales	Monitoreo de medios de comunicación
			Elaboración de matriz de notas publicadas
			Elaboración de informe mensual sobre publicaciones
			Coordinación de entrevistas en medios
OGPER2	4	AC2: Asesorar a los servidores en los trámites y procesos necesarios para garantizar su bienestar	Brindar información de seguros
			Seguimiento de atención de salud
IID1	5	AC1: Recolectar, transferir, difundir e intercambiar la información generada u obtenida por la IAFAS, IPRESS y Unidades de Gestión de IPRESS con el Registro de Afiliados, RESUELVE y SITEDS	Gestión del área de operaciones e informar a la Intendencia o Grupo de Comando
			Diagnóstico de disponibilidad de servicios, pases a producción y configuración de recursos
			Diagnóstico de disponibilidad de BD, pases a producción y configuración de recursos
			Gestión del área de información e informar a la Intendencia o Grupo de Comando
			Diagnóstico de integridad de arquitectura y gestión de su optimización o aporte a pase a producción
			Diagnóstico de disponibilidad y levantamiento de servicio o aporte a pases a producción
			Diagnóstico de fallos, pases a producción
			Gestión del área de inteligencia de negocios e informar a la Intendencia o Grupo de Comando
			Análisis y explotación de Datos
			Aplicación de Inteligencia de Negocios
			Explotación de datos y Disponibilidad de Tableros
			Opiniones técnicas legales
			Gestión de la intendencia e informar o Grupo de Comando
			Trámite documentario y presupuestal

IPROT1	6	AC1: Brindar asistencia en la Plataforma de atención al usuario funcionando en beneficio de los ciudadanos a nivel nacional.	Recepción de solicitudes a través de canales (presencial oficina, telefónico, virtual y escrito) en Plataforma SUSALUD
			Atención de consultas especializadas en salud por todos los canales
			Derivación de casos a instancias según competencia para atención oportuna en situaciones normales, de emergencia y prioridad nacional
IPROT2	7	AC2: Atender solicitudes a través de acciones inmediatas por los delegados en salud	Atención a través de delegados a nivel nacional
			Acciones de monitoreo y vigilancia en situaciones de emergencia y prioridad para la protección de derechos en salud a nivel nacional
IPROT3	8	AC3: Atender denuncias en salud de forma oportuna a nivel nacional	Atención de denuncias finalizadas con la conformidad del usuario
			Atención de denuncias con informe derivado al órgano instructor
			Evaluación, sistematización y reportes estadísticos de protección de derechos, para toma de decisiones en situaciones de emergencia y prioridad nacional
OGA2	9	AC2: Controlar y garantizar el mantenimiento de los bienes y servicios de la entidad	Controlar, programar y ejecutar los Servicios Generales de mantenimiento, conservación y acondicionamiento de oficinas, equipos y maquinas, excepto equipos computacionales y asociados para mantener la operatividad de la institución.
			Llevar el control de vehículos institucionales para prever contingencias que limitan la operatividad institucional.
			Supervisar las prestaciones de terceros relacionados a Servicios Generales verificando la calidad y el cumplimiento contractual de los proveedores.
OGPP1	10	AC1: Comunicar y/o administrar autorizaciones del MEF para modificaciones y certificaciones	Comunicación y/o transmisión de autorizaciones del MEF para modificaciones y certificaciones
INA1	11	AC1: Evaluar y formular proyectos de normas para su posterior aprobación	Evaluación de los proyectos de normas propuestos por las Intendencias de línea.
			Formulación de proyectos de normas, con exposición de motivos e informe técnico.
			Remisión de proyectos de normas a SAREFIS a fin que continúe su trámite de aprobación.
IFIS1	12	AC1: Regular o sancionar a las Instituciones Prestadoras de Servicios de Salud, Instituciones	Asignación de expedientes
			Evaluación de expedientes
			Elaboración de Resoluciones de Inicio de Procedimiento Administrativo Sancionador

		Administradoras de Fondos de Aseguramiento en Salud y las Unidades de Gestión de Instituciones Prestadoras de Servicios de Salud, privadas, públicas o mixtas.	Elaboración de Informes Finales de Instrucción
			Coordinación e Información con Usuarios
			Elaboración de Asignación de Expedientes
			Elaboración de documentos de gestión de la IFIS
			Coordinación con SAREFIS para los procedimientos administrativos
			Gestionar el inicio del PAS
			Gestión de la IFIS
INA2	13	AC2: Administrar los registros de IAFAS, IPRESS, UGIPRESS, Registro de Sanciones, Registro de Corredores de Aseguramiento en Salud, Registro de Sanciones de los Profesionales de la Salud.	Registro de IAFAS, IPRESS, UGIPRESS, Registro de Sanciones, Registro de Corredores de Aseguramiento en Salud, Registro de Sanciones de los Profesionales de la Salud.
OGA1	14	AC1: Gestionar los bienes patrimoniales y custodiar la documentación respectiva	Programar, coordinar y ejecutar los procedimientos técnicos previstos para el alta, baja adquisición, administración, disposición, supervisión y registro de bienes patrimoniales para el cumplimiento normativo y custodia de los mismos.
			Identificar, codificar y asignar los bienes patrimoniales a los servidores de la Superintendencia Nacional de Salud para conocer a la persona responsable del uso, custodia y conservación de los bienes en mención.
			Asistir en las comisiones de trabajo sobre temas de bienes patrimoniales, alta, baja, donación, venta afectación, cesión, permuta, entre otros; así como elaborar los informes técnicos para la ejecución de estos procesos.
			Constituir, actualizar permanentemente y conciliar el Registro Patrimonial valorizado con contabilidad de forma mensual y trimestral para contar con información confiable.
			Mantener en custodia la documentación sobre la propiedad y los actos de ingreso, alta, baja, venta, transferencia, asignación y otros conceptos de desplazamiento de bienes los muebles, para poder mostrar evidencia sobre las decisiones y actos realizados.
OGA4	15	AC4: Administrar los girados, gastos y	Fase Devengado de todos los compromisos de pago y autorización del mismo en el MADAF

		compromisos de pago de la entidad	Realiza todos los girados de las obligaciones de pago. Prepara información de los pagos tributarios para que se declare a la SUNAT.
			Atiende los gastos de caja chica, uso de los módulos bancarios banca privada para pago de planillas, registra los ingresos recaudados, seguimiento y cobranza de multas impuestas.
ISIPRESS 1	16	AC1: Planificar y realizar continuas supervisiones a las IPRESS	Realizar supervisiones a IPRESS
IMRN1	17	AC1: Garantizar la óptima atención al usuario por parte del equipo de intermediación en los servicios de salud	Intervenir en los hechos o actos que vulneren o pudieran vulnerar el derecho de los usuarios de los servicios de salud.
			Atender, resolver y emitir informes relativos a las consultas y denuncias
			Dirigir y supervisar las labores de los delegados de promoción y protección de los derechos en salud.
			Intervenir en los hechos o actos que vulneren o pudieran vulnerar el derecho de los usuarios en las IPRESS.
OGPER1	18	AC1: Gestionar la información y remuneración de los servidores	Alta y baja de personal
			Control de asistencia
			Ingreso de datos laborales relacionados a planilla
			Cálculo de remuneraciones por servidor y por meta
			Gestión de registros SIAF
ISIPRESS 3	19	AC3: Gestionar y supervisar la atención de documentos	Administrar documentos
ISIPRESS 2	20	AC2: Realizar informes legales de las presuntas infracciones de las IPRESS	Realizar informes legales de presuntas infracciones
ISIAFAS1	21	AC1: Fiscalizar a las IAFAS, IPRESS y UGIPRESS	Programación de fiscalizaciones
			Elaboración de planes de trabajo
			Gestiones administrativas para las notificaciones a los administrados
			Gestiones administrativas para el desplazamiento de los especialistas
			Fiscalización in situ a los administrados
			Elaboración y emisión de los informes de supervisión
			Elaboración y emisión de los informes de presuntas infracciones
IPROM2	22	AC2: Gestionar acciones de instrucción y promoción de derechos en salud	Desarrollo de la sesión informativa virtual y/o presencial sobre derechos y deberes en salud
OGA3	23	AC3: Gestionar y supervisar la contratación de bienes y servicios	Otorgar conformidad por los servicios generales contratados para acreditar la prestación conforme por parte del proveedor contratos. Llevar el control de

			alquileres, energía eléctrica, agua y otros servicios relacionados.
			Gestionar la contratación de bienes y servicios para el cumplimiento del Plan Anual de Contrataciones de la superintendencia Nacional de Salud, monitoreo y supervisión del Plan Anual de Contrataciones.
			Brindar asistencia técnica al Comité de Selección o al Órgano Encargado de las Contrataciones respecto a las consultas, observaciones, impugnaciones, reclamaciones u otros a fin de asegurar el cumplimiento de la normatividad de contrataciones vigente.
			Realizar indagaciones o estudios de mercado de proveedores para determinar el valor estimado, verificar la existencia de pluralidad de marcas y postores, entre otros aspectos relacionados al aseguramiento del éxito de los procedimientos de selección.
			Brindar asistencia técnica a las áreas usuarias para la correcta elaboración de requerimientos de compras o servicios, términos de referencia o especificaciones técnicas.
			Elaborar formatos, informes, proyectos de resoluciones u otros documentos para la aprobación de expedientes de contratación y procesos de selección.
			Conformar Comités de Selección encargados de llevar los actos administrativos de los procedimientos de selección para la contratación de bienes y servicios cuando sea designado
IMRN2	24	AC2: Planificar y realizar continuas supervisiones a las IPRESS	Supervisión inopinada
IPROM1	25	AC1: Gestionar la participación ciudadana mediante las JUS	Recepción y derivación de casos de presunta vulneración de Derechos en Salud reportados por las JUS
			Asistencia técnica para el funcionamiento de las JUS
IPROM3	26	AC3: Gestionar acciones de asistencia técnica en atención al usuario	Garantizar el funcionamiento u operatividad de las Plataformas de Atención al Usuario y la gestión de reclamos
OFICOR1	27	AC1: Elaborar y difundir mensajes comunicacionales externos e internos	Elaboración de notas de prensa y boletines informativos
			Creación de guiones
			Creación de post para redes sociales

			Edición, diseño de mensajes
			Publicación en Redes sociales
			Coordinación con medios de comunicación
			Publicación de programas en la página y redes
			Elaboración de reporte mensual
			Difusión de comunicados
			Difusión de mailings para comunicados internos
			Coordinación de actividades internas
			Elaboración de informe mensual

Fuente: Elaboración propia

VI Cronograma de Ejercicios del plan de continuidad operativa

El Plan de Continuidad Operativa de SUSALUD contempla los peligros que generan mayor riesgo para la ejecución de actividades críticas, por lo que los ejercicios del mismo estarán dirigidos a evaluar su efectividad frente a los eventos disruptivos que podrían generar mayor impacto, para garantizar la actualización y mejora del plan.

Por otro lado, se está adoptando la ejecución de simulacros y simulaciones para el 2024, aprobada por la Resolución Ministerial N° 013-2022-PCM, para simultánea participación y alineamiento con los objetivos del presente plan.

El cronograma anual de ejercicios del Plan de Continuidad Operativa de SUSALUD se detalla en la Tabla N° 26.

Tabla N° 26. Cronograma de ejercicios del Plan de Continuidad Operativa

EJERCICIOS DEL PCO 2024					PROGRAMACION	
N°	SUPUESTO O ACTIVIDAD	TIPO	ÁMBITO	PARTICIPANTES	FECHA	HORA
1	Sismo seguido de tsunami en Lima y Chiclayo	Simulacro	Nivel nacional (sectores)	SUSALUD	04/04/2024	08:30 a 17:30
2	Simulacro Nacional Multipeligro	Simulacro	Nivel nacional	SUSALUD	31/05/2024	10:00
3	Incendio código 3 en la Sede Surco y código 4 en la Sede Cercado de Lima	Simulación	Interno	Alta Dirección, Grupo de Trabajo y Grupo de Comando	31/07/2024	08:30 a 17:30
4	Simulacro Nacional Multipeligro	Simulacro	Nivel nacional	SUSALUD	15/08/2024	15:00
5	Simulacro Nacional Multipeligro	Simulacro	Nivel nacional	SUSALUD	05/11/2024	20:00
6	Simulación Nacional ante desastre de gran magnitud (terremoto de 9° en Lima y Chiclayo, inhabilitación de las 3 sedes físicas)	Simulación	Nivel sectorial	Alta Dirección, Grupo de Trabajo y Grupo de Comando	06/11/2024 y 07/11/2024	08:30 a 17:30
7	Fuertes lluvias en Lima y Chiclayo, inundación de la Sede Chiclayo	Simulación	Interno	Alta Dirección y Grupo de Comando	19/11/2024	16:00

Fuente: Elaboración propia

VII Anexos

ANEXO 01. Plan de recuperación de los servicios informáticos de SUSALUD

ANEXO 02. Procedimiento para la convocatoria del personal involucrado en la ejecución de las actividades críticas

ANEXO 03. Directorio del Grupo de Comando

ANEXO 04. Organización para el desarrollo de las actividades críticas

ANEXO 05. Sistema de comunicaciones de emergencia

ANEXO 06. Cronograma de implementación de la Gestión de la continuidad operativa

“Año del Bicentenario, de la consolidación de nuestra Independencia, y de la conmemoración de las heroicas batallas de Junín y Ayacucho”

ANEXO 01. PLAN DE RECUPERACIÓN DE LOS SERVICIOS INFORMÁTICOS DE SUSALUD

Elaborado por:

Intendencia de Investigación y Desarrollo

Santiago de Surco – Lima

2024

Contenido:

INTRODUCCIÓN

La Gestión de Recuperación de Servicios Informáticos añade valor a la organización en la medida que permite minimizar el tiempo de indisponibilidad de los servicios del SUSALUD que son soportados por los servicios de Tecnologías de Información.

El Plan Recuperación de Servicios Informáticos constituye un elemento importante para que los servicios de Tecnologías de Información de la organización se recuperen rápidamente ante una interrupción debido a fallos tecnológicos.

El presente documento pretende ayudar a comprender mejor la problemática del entorno informático, ya que toda la institución debe estar preparada para el caso de ocurrencias imprevistas, en este sentido, el presente plan de reactivación de los servicios informáticos críticos de SUSALUD, tiene como misión la protección de los derechos en salud de cada peruano, para lo cual se orienta a empoderar y colocar al ciudadano en el centro del sistema de salud nacional,

OBJETIVO

Garantizar la continuidad de los servicios de TI críticos de SUSALUD, ante la presencia de eventos que puedan alterar su normal funcionamiento, restableciendo en tiempos previstos y con el nivel de servicio de acuerdo a los recursos disponibles después del siniestro o de un incidente de magnitud, a través de la puesta en marcha de procedimientos, actividades y elementos requeridos para responder de forma organizada hacia la recuperación de las actividades normales

Objetivos Específicos

- Desarrollar un plan de recuperación para los servicios críticos priorizados: Registro de afiliados, Resuelve. SITEDS, RENIPRESS y BPM-PAC, basados en las normas técnicas peruanas alineado al marco normativo vigente.
- Definir el equipo de recuperación y establecer simulaciones periódicas y en escenarios cercanos a la realidad, según el Plan de recuperación de los servicios informáticos.
- Responder a la reactivación de los servicios informáticos críticos priorizados, en las condiciones mínimas previstas.
- Responder a la reactivación de los servicios informáticos críticos priorizados, en las condiciones normales

ALCANCE

En el marco del plan se considera como servicios a los sistemas de información del Registro de afiliados, Resuelve. SITEDS, RENIPRESS y BPM-PAC, servicios que fueron priorizados por la comisión de elaboración de la Gestión de la continuidad operativa. Este documento permite identificar tanto las personas, cargos, proveedores y recursos a restablecer para cada uno de los servicios priorizados.

BASE LEGAL DE REFERENCIA

- Resolución Ministerial N° 028-2015 - PCM, Aprueban Lineamientos para la gestión de la Continuidad Operativa de entidades públicas en los tres niveles de gobierno.
- ISO 22301:2019 (Requisitos de los Sistemas de Gestión de Continuidad del Negocio)
- Guía de Buenas Prácticas del BCI (Business Continuity Institute - Instituto de Continuidad del Negocio) versión 2018
- Ley Nª 29664, Ley que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD).
- Decreto Legislativo N° 1158 (06.12.2013), que Dispone Medidas Destinadas al Fortalecimiento y Cambio de Denominación de la Superintendencia Nacional de Aseguramiento en Salud, modificado por el Decreto Legislativo N° 1289 (29.12.2016). que dicta disposiciones destinadas a optimizar el funcionamiento y los servicios de la Superintendencia Nacional de Salud.
- Decreto Supremo N° 018-2017 – PCM, Decreto Supremo que aprueba medidas para fortalecer la planificación y operatividad del Sistema Nacional de Gestión de Riesgos de Desastres mediante la adscripción y transferencia de funciones al Ministerio de Defensa a través del Instituto Nacional de Defensa Civil–INDECI y otras disposiciones.
- Decreto Supremo N° 0115-2022-PCM, que Aprueba el Plan Nacional de Gestión del Riesgo de Desastres - PLANAGERD 2022-2030.
- Decreto Supremo Nº 048-2011 - PCM, Decreto Supremo que aprueba el Reglamento de la Ley Nº 29664, que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD).
- Decreto Supremo N° 060-2024-PCM, Decreto Supremo que modifica el Reglamento de la Ley N° 29664, que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD).
- Resolución Ministerial N° 004-2016 - PCM - Aprueban el uso obligatorio de 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. 2a. Edición”, en todas las entidades integrantes del Sistema Nacional de Informática.

1. Glosario de Términos

TÉRMINO	DEFINICIÓN	FUENTE
Riesgo	Combinación de la probabilidad de un evento y sus consecuencias.	[ISO/IEC Guide 73:2002]
Análisis del riesgo	Uso sistemático de la información para identificar fuentes y estimar el riesgo.	[ISO/IEC Guide 73:2002]
Evaluación del riesgo	Proceso general de análisis y evaluación del riesgo.	[ISO/IEC Guide 73:2002]
Valoración del riesgo	Proceso de comparación del riesgo estimado contra el criterio del riesgo dado para determinar el significado de este.	[ISO/IEC Guide 73:2002]
Gestión del riesgo	Actividades coordinadas para dirigir y controlar una organización considerando el riesgo. NOTA: Gestión del riesgo incluye típicamente evaluación del riesgo, tratamiento del riesgo, aceptación del riesgo y comunicación del riesgo.	[ISO/IEC Guide 73:2002]
Tratamiento del riesgo	Proceso de selección e implementación de medidas para modificar el riesgo.	[ISO/IEC Guide 73:2002]

Terceros	Persona natural o jurídica que es reconocida por ser independiente de las partes involucradas concerniente al tema en cuestión.	[ISO/IEC Guide 73:2002]
Amenaza	Causa potencial de un incidente no deseado que puede resultar en daño al sistema u organización.	[ISO/IEC 13335-1:2004]
Vulnerabilidad	Debilidad de un activo o grupo de activos que pueden ser explotados por una o más amenazas.	[ISO/IEC 13335-1:2004]
Crisis	Una situación con un alto nivel de incertidumbre que interrumpe las actividades críticas y/o la credibilidad de una organización, por lo que requiere urgente acción.	[ISO 22301]
Plan de Continuidad de Negocio	Procedimientos documentados que guían a la organización a responder, recuperar, reanudar y restablecer a niveles predefinidos después de una alteración.	[ISO 22301]
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]
Incidente	Situación que pudiera constituir o podría redundar en una interrupción de negocio, pérdida, emergencia o crisis.	[ISO 22301]
Interrupción	Acontecimiento, ya sea previsto (por ejemplo: una huelga de trabajadores o un huracán) o imprevisto (por ejemplo, un apagón o un terremoto), que cause una desviación negativa no planificada con respecto a la entrega esperada de productos o servicios según los objetivos de la organización.	[ISO 27001] [BS 25999]
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 27001]
MBCO (Minimum Business Continuity Objective) ObjetivoMínimo para la Continuidad del Negocio	Un mínimo nivel de servicios y/o productos aceptables para la organización con el fin de lograr sus objetivos durante una interrupción.	[ISO 22301]
MTPD (Maximum Tolerable Period of Disruption) Período Máximo Tolerable de Interrupción	El tiempo que tomaría para que los impactos adversos, que pueden surgir por no brindar un producto/servicio o no realizar una actividad, se vuelvan inaceptables.	[ISO 22301]
Recurso de operación	Todos los bienes, las personas, habilidades, información, tecnología (incluyendo plantas y equipos), los locales, y materiales y la información (ya sean electrónicos o no) que una organización debe tener disponible para su uso, cuando sea necesario, con el fin de operar y cumplir con su objetivo.	[ISO 22301 / DRJ]
RPO (Recovery Point Objective) Punto Objetivo de Recuperación o Tolerancia a Pérdida de Datos	El punto en donde la información usada por una actividad debe ser restaurada para permitir que la actividad funcione a partir de la reanudación. Conocido también como Pérdida Máxima de Datos.	[ISO 22301]
RTO (Recovery Time Objective) Tiempo de Recuperación Objetivo o Expectativa de Recuperación	Periodo de tiempo posterior a un incidente, en el cual un producto o una actividad se debe reanudar o en el cual los recursos se deben recuperar.	[ISO 22301]
Proveedor	Empresa tercera responsable de proveer bienes o	ITIL

	servicios.	
Puestos de trabajo	Lugar o ambiente donde se desarrolla el trabajo.	[ISO 22301]
Servicio TI	Está basado en el uso de tecnologías de la información y apoya a los procesos de negocio del cliente. Es realizado por una combinación de personas, procesos y tecnología que deberían estar definidos en un acuerdo de nivel de servicios.	ITIL (Information Technology Infrastructure Library)
Recursos	Todos los activos, personal, aptitudes, información, tecnología, locales y suministros que una organización tenga que tener disponibles para su uso, cuando sea necesario, para operar y cumplir sus objetivos	[BS 25999]

2. Identificación de los procesos y servicios priorizados

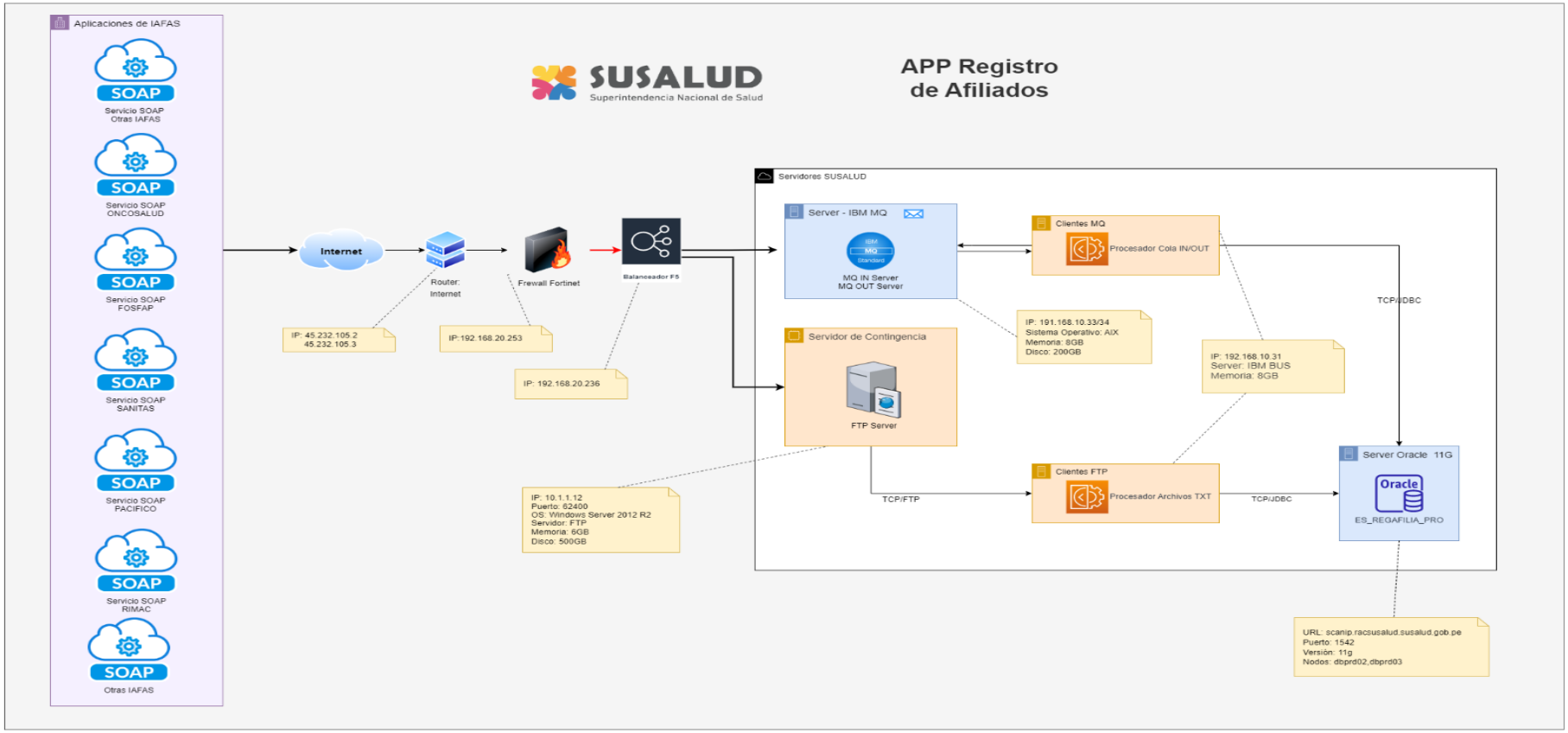
Los procesos y servicios priorizados en el presente documento son los siguientes:

Tabla 1. Procesos y servicios priorizados

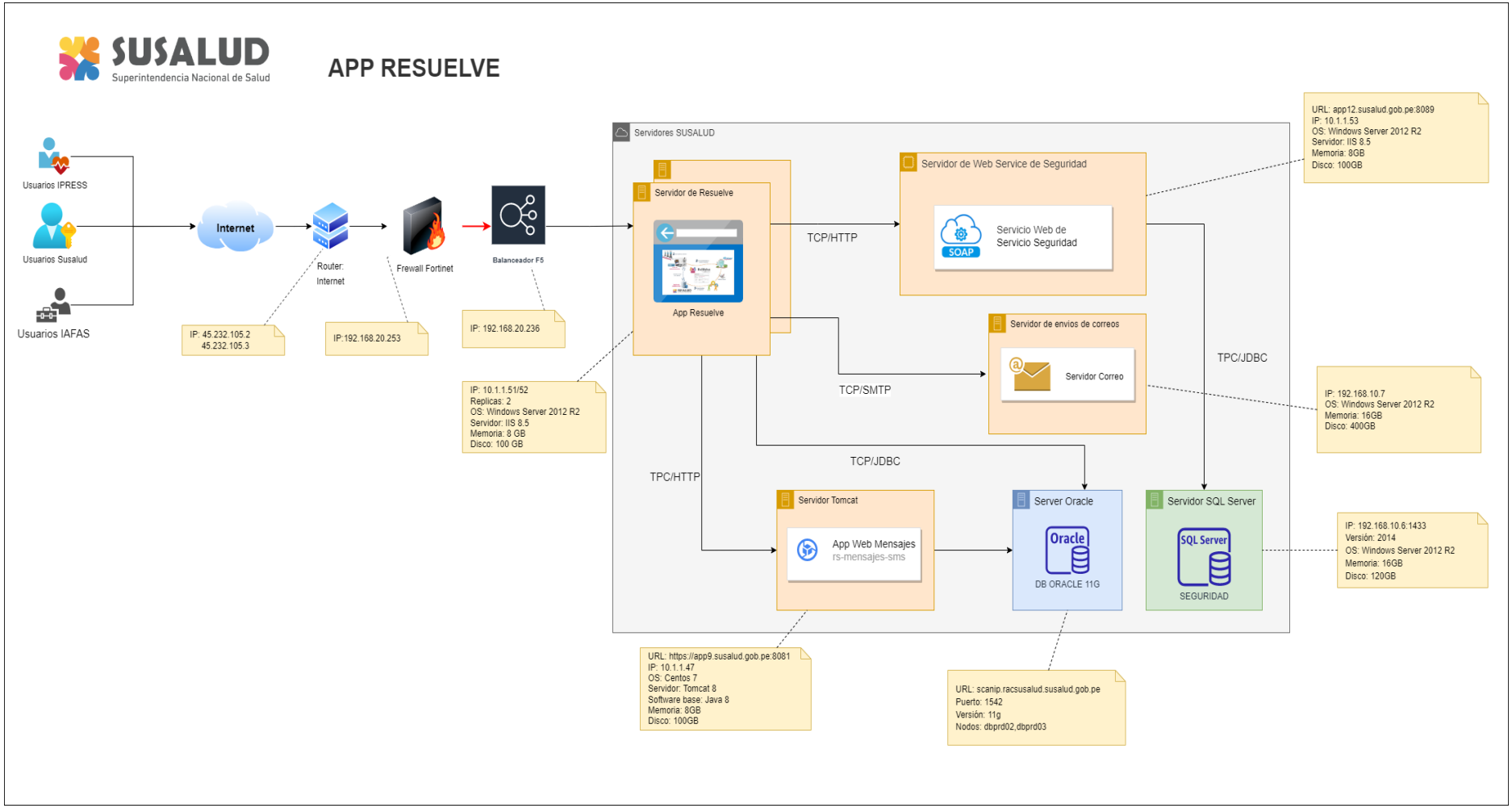
PROCESO	SERVICIOS
AFILIACION DE ASEGURADOS	- REGISTRO DE AFILIADOS - RESUELVE
ACREDITACION DE ASEGURADOS	- SITEDS CLIENTE - SITEDS WEB - SITEDS PASARELA
REGISTRO DE IPRESS	- RENIPRESS
ATENCIÓN AL CIUDADANO	- BPM PAC

3. Arquitectura del servicio

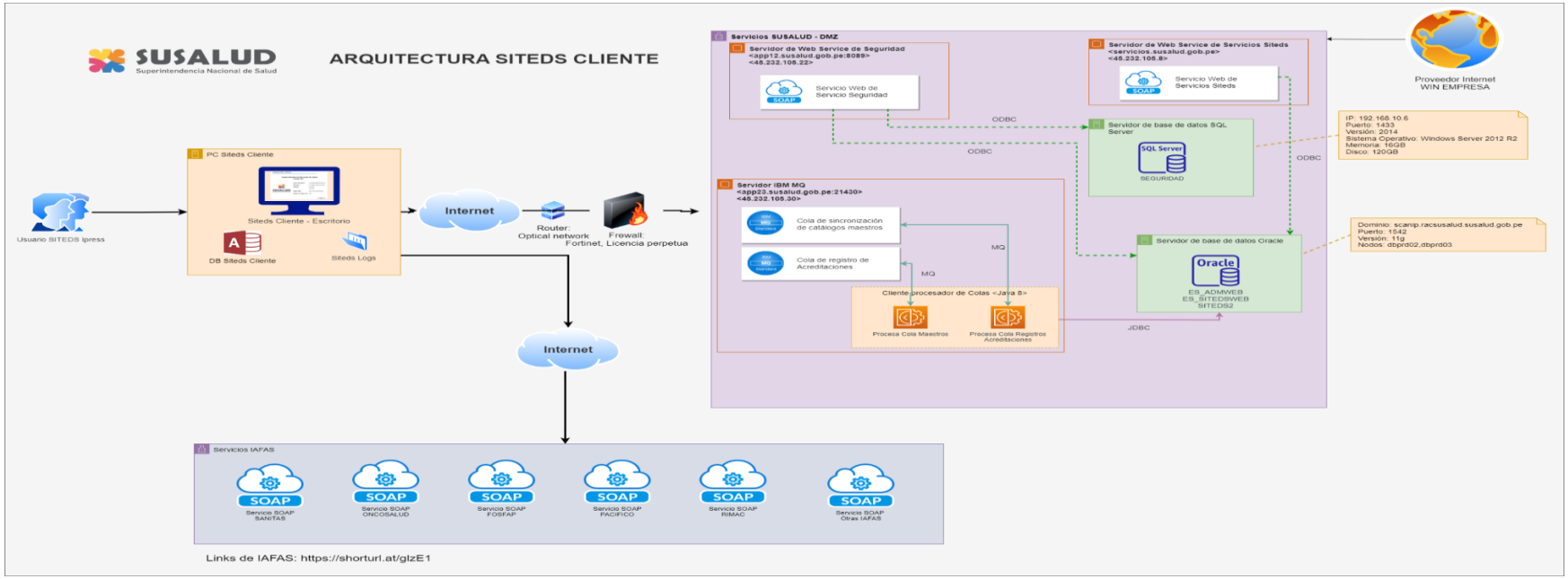
3.1. Arquitectura del servicio RAAUS



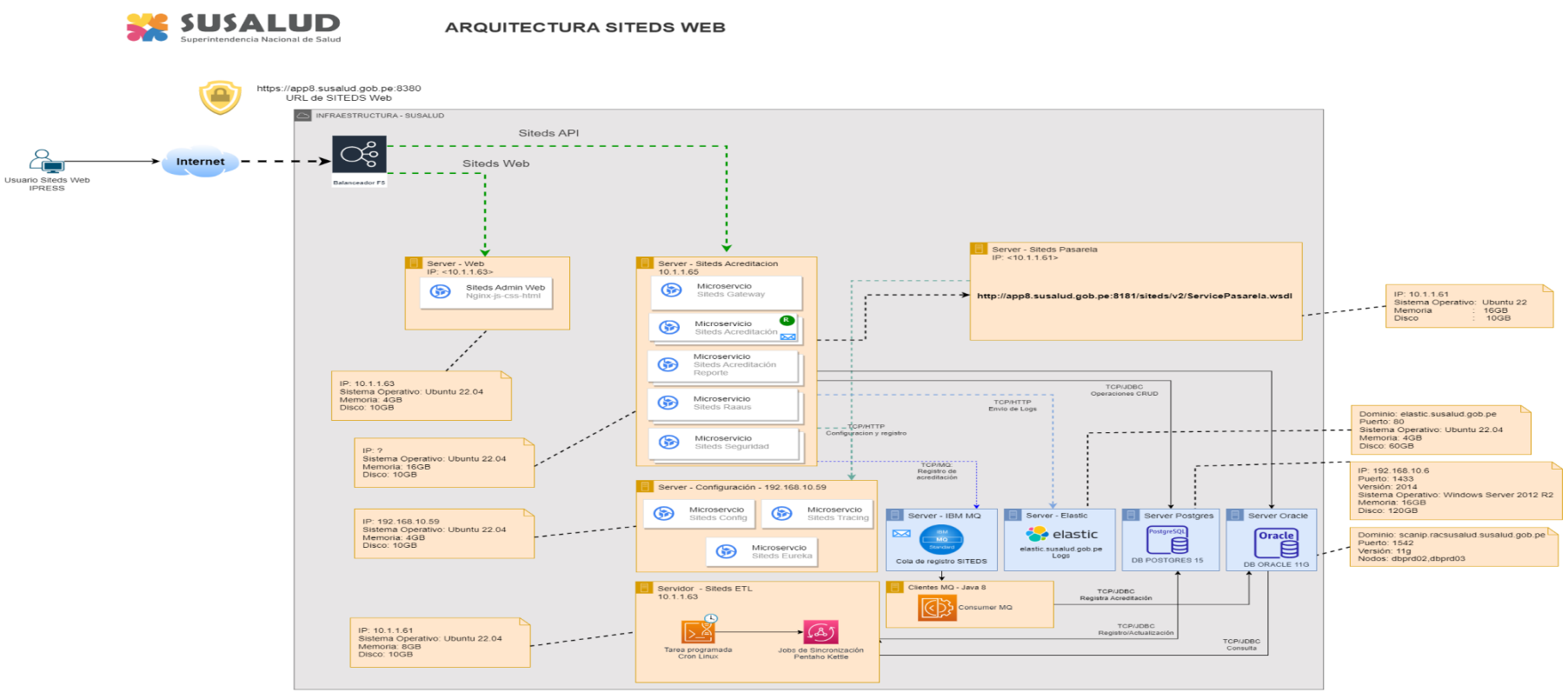
3.2. Arquitectura del servicio RESUELVE



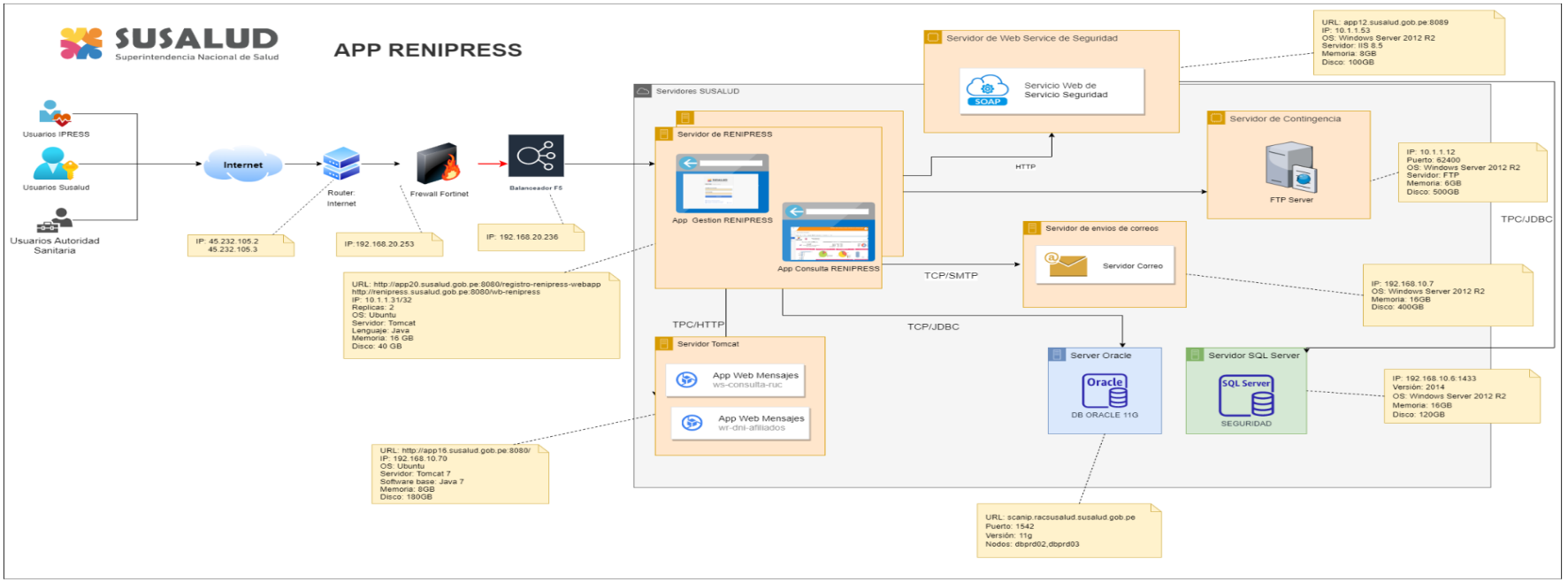
3.3. Arquitectura SITEDS Cliente



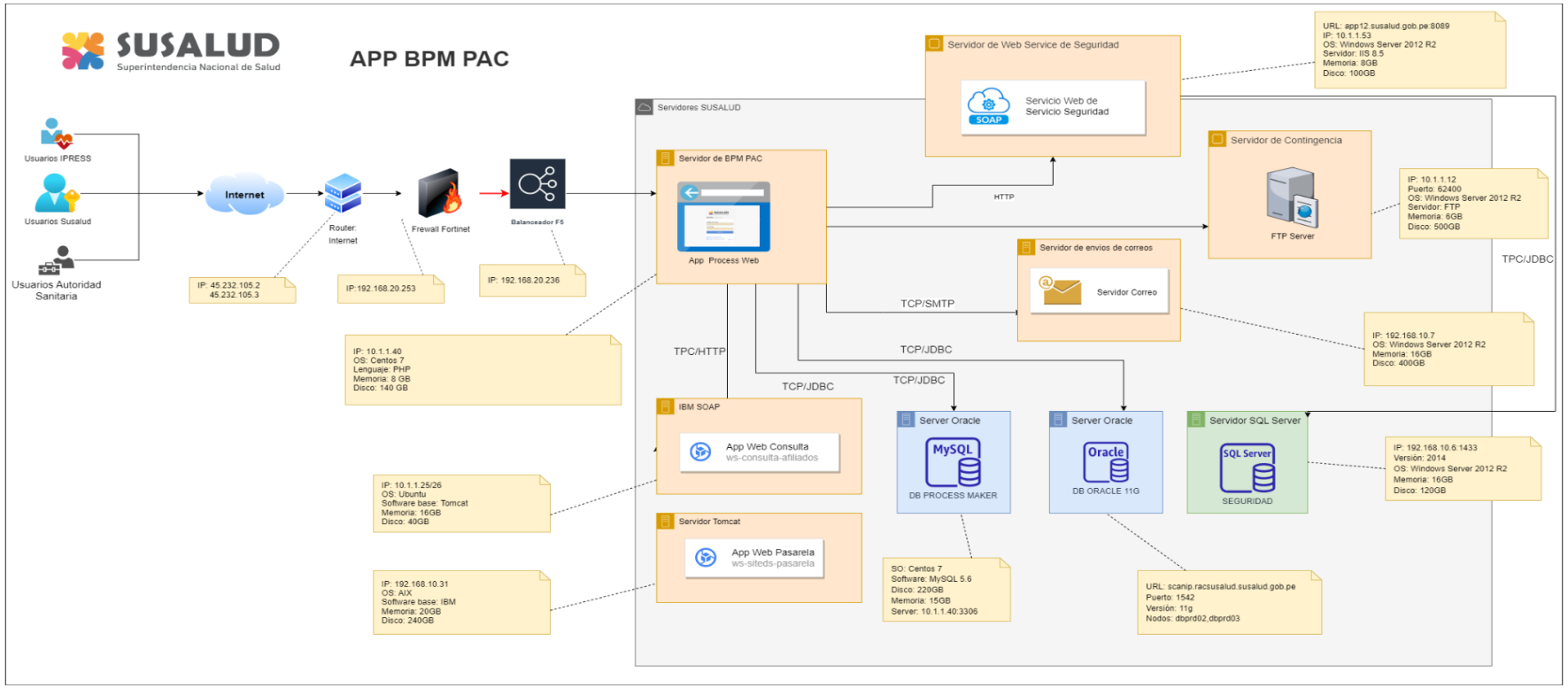
3.4. Arquitectura SITEDS Web



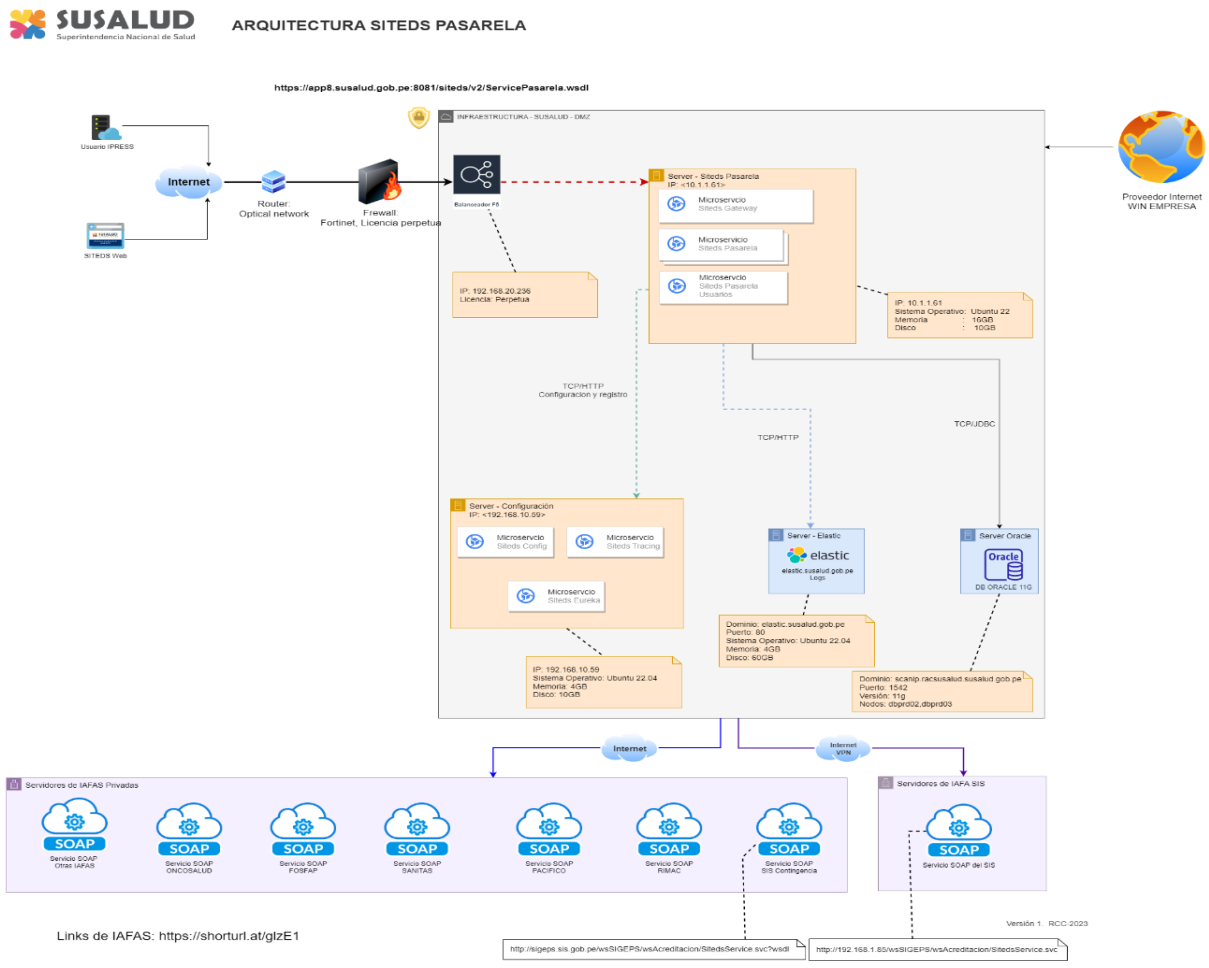
3.5. Arquitectura del RENIPRESS



3.6. Arquitectura del servicio BPM PAC



3.7. Arquitectura SITEDS Pasarela



4. Evaluación de alternativas de infraestructura.

Tabla 2. Relación de alternativas de infraestructura ante un posible siniestro o incidente de magnitud alta:

ALTERNATIVAS	COSTO	VIABLE AL CORTO PLAZO	COMENTARIO
Mirror site	Muy Alto	No	Cumple pero es muy costoso Un centro alterno que está activo funcionando en todo momento en otra locación (propio o de tercero). Alta disponibilidad
Hot site	Alto	No	Cumple, pero es muy costoso (on –off) Un centro alterno que no está activo Se dispone de la infraestructura HW y SW similar al site principal Entra en funcionamiento en el momento que el site principal presente un incidente de magnitud (propio o de tercero)
Warm site	Medio	No	Se dispone de la infraestructura HW y SW mínima requerida, disponible para que en el momento que se requiere se despliegue las aplicaciones y base de datos.
Cold site	Bajo	A mediano plazo	Solo se dispone de local Costo de mantenimiento bajo
In site	Bajo	SI	Infraestructura de HW y SW disponible después de un incidente de magnitud alta (*) Se requiere recuperar los recursos tecnológicos previstos para el funcionamiento de los servicios críticos en condiciones operativas mínimas.

(*) Nota: Incidente de magnitud alta: Pérdida parcial de infraestructura de HW o SW o telecomunicaciones.

SELECCIÓN DE ESTRATEGIAS– INFRAESTRUCTURA ALTERNA DE TI

De este análisis se tienen como única alternativa a corto plazo: In Site

5. Evaluación de servicios críticos

El análisis de impacto de negocio (BIA) nos ayuda a determinar el objetivo de tiempo de recuperación (RTO), las personas necesarias, la infraestructura de TI o las partes externas de la recuperación, los datos esenciales que se utilizan en las actividades críticas, etc.

En esta etapa se ha determinado los niveles de servicio RTO (Tiempo de Recuperación Objetivo)

Tabla 3. RTO para los seis servicios críticos

N°	SERVICIOS CRÍTICOS	RTO Recursos generales	RTO Recursos propios	RTO (en días)	OBSERVACIONES
01	RAAUS / RESUELVE	6.71	6.58	13.29	Se restablecerá EN 6.71 días los Recursos críticos generales del Centro de Datos más 6.58 días para los recursos propios del servicio RAAUS / Resuelve, haciendo un total de:13.29 días.
02	SITEDS CLIENTE		3.5	10.21	Se restablecerá EN 6.71 días los Recursos críticos generales del Centro de Datos más 3.5 días para los recursos propios del servicio SITEDS CLIENTE, haciendo un total de:10.21 días.
03	Registro de SITEDS WEB		2.42	9.13	Se restablecerá EN 6.71 días los Recursos críticos generales del Centro de Datos más 2.42 días para los recursos propios del servicio SITEDS WEB, haciendo un total de:9.13 días.
04	SITEDS Pasarella		2.75	9.46	Se restablecerá EN 6.71 días los Recursos críticos generales del Centro de Datos más 2.75 días para los recursos propios del servicio SITEDS PASARELLA, haciendo un total de:9.46 días.
05	RENIPRESS		3.13	9.84	Se restablecerá EN 6.71 días los Recursos críticos generales del Centro de Datos más 3.13 días para los recursos propios del servicio RENIPRESS, haciendo un total de:9.84 días.
06	bpm PAC		3.58	10.29	Se restablecerá EN 6.71 días los Recursos críticos generales del Centro de Datos más 3.58 días para los recursos propios del servicio BPM PAC, haciendo un total de:10.29 días.
	Total:	**6.71**	**21.96**	**28.67**	

6. Identificación de recursos para los servicios críticos priorizados.

Los servicios críticos de TI son aquellas que soportan procesos críticos de la institución.

A continuación, se detallan los recursos necesarios para la operatividad de los servicios críticos.

Tabla 4. Recursos críticos generales del Centro de Datos

#	SEC	DEP	RECURSO	Ejecutor(es)	# Plan de Acción	Tiempo (horas)
1	1a		Servicio de Internet dedicado con el operador.	Proveedor: Win y Especialista en Arquitectura de TI SUSALUD: ATI / AOP	A.1	4

2	1a		Equipos de Seguridad Perimetral, Lan (Firewall)	Proveedor: Win SUSALUD: ATI / AOP	A.1	4
3	1a		Equipos de Red 2 SW CORE Alta disponibilidad	SUSALUD: ATI / AOP	A.2	4
4	1b		2 switch fibra del 11g y 2 switch para el Flash System y Storage STOREWIZE (1 alterno del otro) SAN: STorage Hitachi, Storage Flash System y Storage STORWIZE	Proveedor: RAZUMTEK (Storewize) JAPAN (Flash System) IT STORAGE (Storage Hitachi) SUSALUD: AOP / ATI	A.3	34
5	2	4	Servidor físico de tecnología RISC sistema operativo AIX IBM Integration BUS y Servidor virtual IBM MQ	IT STORAGE (Servidor Físico RISC) - AOP INSPIRA (IBM BUS, IBM MQ) SUSALUD: - ATI / AOP - EPI / EAS	A.5	28
6	3	4	Plataforma de Virtualización VMware	IT STORAGE SUSALUD: AOP / ATI	A.4	9
7	4	4	Librería de Backup	Centro Nacional de Servicios SUSALUD: AOP / ATI	A.6	6
8	5	7	Software de Backup (COMMVAULT)	Proveedor: Sin soporte externo. SUSALUD: AOP / ATI	A.6	24
9	4	4	Restaurar RMAN de base de datos Oracle 11g (BD de Registro de Afiliados, Resuelve, SITEDS, RENIPRESS y BPM PAC)	Proveedor- Evotech SUSALUD: AOP / ATI	A.10	48
			Total, en días y horas:	**6.71**		**161**

Nota: ATI: Especialista en Arquitectura de Tecnologías
AOP: Administrador de Operaciones
EPI: Especialista en Proyectos Interinstitucionales
EAS: Especialista en Análisis De Sistemas

Tabla 5. Restauración de máquinas virtuales

#	SEC	DEP	RECURSO	Ejecutor(es)	# Plan de Acción	Tiempo (horas)
10	6	8	Restauración de máquinas virtuales: Elastic, BD SQL Server para el Sistema de seguridad, BD del BPM-PAC (Mysql) y Apache para el BPM-PAC Aplicación RENIPRESS, Aplicación: RESUELVE, Aplicación: SITEDS-WEB, WS Seguridad, WS Pasarella, WS de Consulta del registro de afiliados, WS wr-dni-afiliados, WS Consulta de lista de IPRESS, WS para el SITEDS CLIENTE, WS para el DOCKER del SITEDS WEB, WS: chatbot (net),	IT STORAGE SUSALUD: AOP / ATI	A.7	8 por cada mv

			WS para PIDE (java), WS para el SIS (java), FTP del mini batch del RAAUS, FTP interno del BPM PAC útil para guardar archivos anexos a expedientes PAC, mv con S.O. Red Hat 5.5 y Oracle Standar 11g.			

Tabla 6. Recuperación de la máquina virtual del Servidor de correo Lotus

#	SEC	DEP	RECURSO	Ejecutor(es)	# Plan de Acción	Tiempo (horas)
11	6	8	Restaurar mv Servidor de correo Lotus	SUSALUD: AOP / ATI	A.8	6

Tabla 7. Recuperación de la Central telefónica tanto de Surco como de la sede Cercado

#	SEC	RECURSO	Ejecutor(es)	# Plan de Acción	Tiempo (horas)
1	5	CENTRAL TELEFONICA - SURCO	IPNET SAC SUSALUD: ATI / AOP	A.11	12
3	5	CENTRAL TELEFONICA - CERCADO DE LIMA	PERULINUX NG SAC SUSALUD: ATI / AOP	A.11	12
		Total, en días y horas:		**1**	**12**

Tabla 8. Recursos tecnológicos propios del servicio: RAAUS-RESUELVE

#	SEC	RECURSO	Ejecutor(es)	# Plan de Acción	Tiempo (horas)
1	4	Restaurar las mv del RAAUS los WS: chatbot (net), WS: Para la PIDE (java), WS: Para el SIS (java), WS: para el SITEDS CLIENTE, WS: para el DOCKER para el SITEDS WEB	AOP / ATI	A.7	40
2	4	Restaurar la mv del Sistema de Seguridad	AOP / ATI	A.7	9
3	4	Restaurar la mv de ws Seguridad	AOP / ATI	A.7	9
4	4	Restauración de la mv del aplicativo RESUELVE (viene con su IIS)	AOP / ATI	A.7	9
5	4	Interface con la mv del Correo electrónico	AOP / ATI	A.8	8
6	4	Restaurar la mv del Directorio Activo	AOP / ATI	A.9	8

7	4	Restaurar la mv del FTP del mini batch	AOP / ATI	A.7	9
8	3	Restaurar la mv de la BD SQL SERVER - Sistema de Seguridad, para uso de RAAUS-RESUELVE y RENIPRESS	AOP / ATI	A.7	9
9	1	MV con S.O. Red Hat 5.5 y Oracle Standar 11g.	ATI / AOP	A.7	9
10	2	Restaurar RMAN de BD Oracle 11g - RAAUS: ES_HOSTING, ES_REGAFILIA_SYS, ES_MAESTRO, REGAFILIAH_SYS, ES_REGAFILIA_PRO, REGAFILIA_SYS Restaurar la BD de Administrador Web, RENIPRESS, RIAFAS	AOP / ATI	A.10	48
		Total en días y horas:	6.58		**158**

Nota: ATI: Especialista en Arquitectura de Tecnologías
AOP: Administrador de Operaciones

Tabla 9. Recursos tecnológicos propios del servicio: SITEDS CLIENTE

#	SEC	RECURSO	Ejecutor(es)	# Plan de Acción	Tiempo (horas)
1	3	Restaurar la mv de ws Consulta de lista de IPRESS	AOP / ATI	A.7	9
2	3	Restaurar la mv de ws Seguridad	AOP / ATI	A.7	9
3	2	Restauración de bkp de Base de datos seguridad (SQL)	AOP / ATI	A.7	9
4	1	MV con S.O. Red Hat 5.5 y Oracle Standar 11g.	ATI / AOP	A.7	9
5	2	Restaurar Base de datos de SITEDS: ES_SITEDSWEB, Restaurar las bases de datos del Administrador Web, RENIPRESS, RAAUS (Oracle)	AOP / ATI	A.10	48
		Total en días y horas:	**3.50**		**84**

Tabla 10. Recursos tecnológicos propios del servicio: SITEDS WEB

#	SEC	RECURSO	Ejecutor(es)	# Plan de Acción	Tiempo (horas)
1	2	Restauración de BKP Base de datos seguridad (SQL)	AOP / ATI	A.7	1
2	1	MV con S.O. Red Hat 5.5 y Oracle Standar 11g.	ATI / AOP	A.7	9
3	2	Restauración de BKP, Base de datos de RAAUS (Oracle)	AOP / ATI	A.10	48
4	2	Restauración de BKP Base de datos administrador web y BD del SITEDS: ES_SITEDSWEB, REGISTRO, ES_SERVICIOS_SITEDS, SITEDS2 (Oracle)	AOP / ATI	A.10	0
5	2	Restauración de BKP Base de datos de RENIPRESS (Oracle)	AOP / ATI	A.10	0
6	2	Restauración de BKP Base de datos de IAFAS (Oracle)	AOP / ATI	A.10	0
		Total en días y horas:	**2.42**		**58**

Nota: ATI: Especialista en Arquitectura de Tecnologías
AOP: Administrador de Operaciones

Tabla 11. Recursos tecnológicos propios del servicio: SITEDS PASARELA

#	SEC	RECURSO	Ejecutor(es)	# Plan de Acción	Tiempo (horas)
1	3	Web Services de las IAFAS del modelo SITEDS (SIS, RIMAC, SALUDPOL, etc). Administrado por las IAFAS	IAFAS		
2	2	Restauración de BKP Base de datos seguridad (SQL)	AOP / ATI	A.7	9
3	1	MV con S.O. Red Hat 5.5 y Oracle Standar 11g.	ATI / AOP	A.7	9
4	2	Restauración de BKP de Base de datos administrador web: ES_ADMWEB, BD SITEDS: ES_SITEDSWEB, ES_CORE_TRANSAC (Oracle)	AOP / ATI	A.10	48
5	2	Restauración de BKP Base de datos de RAAUS (Oracle)	AOP / ATI	A.10	0
6	2	Restauración de BKP Base de datos de RENIPRESS (Oracle): ES_RENIPRESS	AOP	A.10	0
7	2	Restauración de BKP Base de datos de IAFAS (Oracle): RIAFAS	AOP / ATI	A.10	0
		Total en días y horas:	**2.75**		**66**

Tabla 12. Recursos tecnológicos propios del servicio: RENIPRESS

#	SEC	RECURSO	Ejecutor(es)	# Plan de Acción	Tiempo (horas)
1	5	Restaurar mv del ws de Seguridad	AOP / ATI	A.7	9
2	4	Restauración de backup de BD del Sistema de Seguridad (SQL).	AOP / ATI	A.7	9
3	1	MV con S.O. Red Hat 5.5 y Oracle Standar 11g.	ATI / AOP	A.7	9
4	2	Restauración de backup de la BD de RENIPRESS: ES_RENIPRESS (Oracle) Restauracion de backup de los esquemas relacionados: ES_CORREDORES, ES_REPORTES, ES_SOPORTE_ONLINE, ES_RENIPRESS_LOG, ES_ADMWEB (Oracle)	AOP / ATI	A.10	48
		Total en días y horas:	**3.13**		**75**

Nota: ATI: Especialista en Arquitectura de Tecnologías
AOP: Administrador de Operaciones

Tabla 13. Recursos tecnológicos propios del servicio: BPM PAC

#	SEC	RECURSO	Ejecutor(es)	# Plan de Acción	Tiempo (horas)
1	3	Restauración de la mv FTP interno del BPM PAC útil para guardar archivos anexos a expedientes PAC	AOP / ATI	A.7	9
2	3	Restaurar mv de ws de Consulta del registro de afiliados. wr-dni-afiliados	AOP / ATI	A.7	9
3	3	Interface con la mv del Correo electrónico	AOP / ATI	A.8	2
4	2	Restaurar mv de la BD del BPM-PAC (Mysql) y Apache	AOP / ATI	A.7	9
5	1	MV con S.O. Red Hat 5.5 y Oracle Standar 11g.	ATI / AOP	A.7	9
6	2	Restauración de BKP BD del BPM-PAC (Oracle): ES_BPM_PAC, ES_BPM_SUSALUD.	AOP / ATI	A.10	48
7	2	Restauración de BKP BD del RAAUS, RENIPRESS, IAFAS, UGIPRESS (Oracle)	AOP / ATI	A.10	0
		Total en días y horas:	**3.58**		**86**

Nota: ATI: Especialista en Arquitectura de Tecnologías
AOP: Administrador de Operaciones

7. Recursos de TI críticos, amenazas y escenarios.

Tabla 14. Recursos tecnológicos, amenazas y escenarios

#	RECURSOS	AMENAZAS	ESCENARIOS
1	Servicio de Internet con línea dedicada	Indisponibilidad del servicio	-Falla o mala manipulación del equipo de comunicación - Avería del proveedor
2	Equipos de Seguridad Perimetral, Lan (Firewall)	Falla del equipo UTM o Router	-Falla del único equipo (UTM) con que cuenta el servicio. -Falla del sistema de ambientación (aire acondicionado). Condiciones inadecuadas de temperatura y humedad -Acceso no autorizado debido a Arquitectura de red insegura. Ataque de hackers
3	Equipos de Red 2 SW CORE Alta disponibilidad	Indisponibilidad del servicio	-Falla o mala manipulación del equipo de comunicación -Falla del sistema de ambientación (aire acondicionado). Condiciones inadecuadas de temperatura y humedad Ataque de hackers

4	SAN (2 switch fibra del 11g y 2 switch para el Flash System y Storage STOREWIZE (1 alterno del otro)	Falla de Hardware o software	Falla del Switch SAN Falla del equipo Storage - Falla del sistema de ambientación (aire acondicionado). Condiciones inadecuadas de temperatura y humedad
5	STorage Hitachi, Storage Flash System y Storage STORWIZE	Falla de Hardware o software	Falla de la SAN - Falla del sistema de ambientación (aire acondicionado). Condiciones inadecuadas de temperatura y humedad
6	Plataforma de Virtualización VMware	Falla de software	- Falta de parches o actualizaciones Ataque de hackers
7	Servidor físico de tecnología RISC sistema operativo AIX IBM Integration BUS y Servidor virtual IBM MQ	Falla de Hardware o software	- Falla del sistema de ambientación (aire acondicionado). Condiciones inadecuadas de temperatura y humedad Ataque de hackers
8	Librería de Backup	Falla de Hardware o software	- Falla del sistema de ambientación (aire acondicionado). - Condiciones inadecuadas de temperatura y humedad - Ataque de hackers
9	Software de bkp (COMMVAULT)	Falla de software	- Falta de parches o actualizaciones - Ataque de hackers

10	Restauración de máquinas virtuales: Elastic, BD SQL Server para el Sistema de seguridad, BD del BPM-PAC (Mysql) y Apache para el BPM-PAC Aplicación RENIPRESS, Aplicación: RESUELVE, Aplicación: SITEDS-WEB, WS Seguridad, WS Pasarella, WS de Consulta del registro de afiliados, WS wr-dni-afiliados, WS Consulta de lista de IPRESS, WS para el SITEDS CLIENTE, WS para el DOCKER del SITEDS WEB, WS: chatbot (net), WS para PIDE (java), WS para el SIS (java), FTP del mini batch del RAAUS, FTP interno del BPM PAC útil para guardar archivos anexos a expedientes PAC, mv con S.O. Red Hat 5.5 y Oracle Standar 11g.	BD: Pérdida de la información FTP:Falla de servicios de comunicación Aplicaciones: Indisponibilidad del Sistema Aplicaciones: Mal funcionamiento del Software Aplicaciones: Caída de Sistema por falta de recursos	BD: Falla del sistema de almacenamiento. FTP: Caída del servicio de Internet, Falla de servidor FTP. Aplicaciones: Falla de hardware del servidor de aplicación o BDs que aloja este servicio. Aplicaciones: Caída del servicio de Internet. Saturación del ancho de banda de Internet. Aplicaciones: Mal mantenimiento al software, mal pase a producción del software. Aplicaciones: Insuficiente tiempo para realizar las pruebas antes de pase a producción. Aplicaciones: Falta de recursos en el servidor. Ataque de hackers
11	Servidor de correo	Indisponibilidad del servicio	-Falta de parches o actualizaciones -Encolamiento de mensajería -Falla de hardware o software -Ataque de hackers
12	Restauración de RMAN de base de datos Oracle 11g (BD de Registro de Afiliados, Resuelve, SITEDS, RENIPRESS y BPM PAC)	Pérdida de la información	-Falla del hardware del servidor. -Falla del sistema de almacenamiento. -Ataque de hackers
	Servicio de telefonía	Indisponibilidad del servicio	Falla del hardware o software

Ante la materialización del riesgo se ha consolidado los planes de acción (Anexo 02)

con la finalidad de conocer la secuencia de actividades a realizar así como el responsable de las mismas.

8. Análisis de Impacto del SITEDS, RAAUS, RESUELVE, RENIPRESS y BPM PAC

La ISO 22301 señala que se debe evaluar los efectos en el tiempo de no realizar los subprocesos, a continuación, se detalla los impactos ante una paralización de los subprocesos del alcance:

Tabla 15. Análisis de impacto a nivel operativo, legal, e imagen del servicio: SITEDS

PROCESO	SERVICIO	IMPACTO			OBSERVACION
		OPERATIVO	LEGAL	IMAGEN	
Acreditación	SITEDS CLIENTE/ SITEDS WEB /SITEDS PARARELA	MUY ALTO	ALTO	ALTO	**Impacto Operativo:** Se considera MUY ALTO porque la interrupción del sistema no permitiría a las IAFAS brindar las acreditaciones solicitadas por las IPRESS, dado que retrasa la validación del estado del seguro y la cobertura y por ende la atención oportuna del paciente. Además afecta las prestaciones para su reconocimiento.
					Impacto Legal: Se considera ALTO en caso de pérdida de continuidad del servicio para la acreditación de los asegurados, por lo que se estaría incumpliendo lo dispuesto en la RS 121-2019-SUSALUD/S, RS 072-2021-SUSALUD/S y la Ley del Cáncer Ley N° 31336
					Impacto de Imagen: Se considera ALTO cuando ocurre la pérdida de continuidad del servicio de acreditación de asegurados, causando retraso en la atención de los asegurados y generando desconfianza en los administrados.

Tabla 16. Análisis de impacto a nivel operativo, legal, e imagen del servicio: RAAUS

PROCESO	SERVICIO	IMPACTO			OBSERVACION
		OPERATIVO	LEGAL	IMAGEN	
Registro de Afiliados del AUS.	**RAAUS**	**ALTO**	**MUY ALTO**	**MUY ALTO**	**Impacto Operativo:** Se considera ALTO porque la interrupción del sistema impide que SUSALUD realice la recolección, validación, publicación y brindar los servicios de información sobre el Registro de Afiliados. Así mismo afectaría los proceso de afiliación del SIS principalmente y otros IAFAS.
					Impacto Legal: Se considera MUY ALTO cuando existe una indisponibilidad del sistema, por el cual se puede determinar un incumplimiento del servicio de acuerdo al Decreto Supremo N°034-2010-SA, que obliga tener el registro de afiliado publicado, los 365 días del año. Reglamento de la Ley marco N° 08 – 2010.
					Impacto de Imagen: Se considera MUY ALTO cuando ocurre la interrupción del sistema, causando desconfianza a la opinión pública y las entidades vinculadas.

Tabla 17. Análisis de impacto a nivel operativo, legal, e imagen del servicio: RESUELVE, RENIPRESS y BPM PAC

PROCESO	SERVICIO	IMPACTO			OBSERVACION
		OPERATIVO	LEGAL	IMAGEN	
Registro de Afiliados del AUS.	RESUELVE	MUY ALTO	MUY ALTO	MUY ALTO	**Impacto Operativo:** Se considera MUY ALTO cuando ocurre la interrupción del servicio web, causando que el proceso de afiliación no se dé oportunamente. **Impacto Legal:** Se considera MUY ALTO cuando existe una indisponibilidad de la web, por el cual se puede determinar un incumplimiento del servicio de acuerdo al Decreto Supremo N°034, que obliga tener el registro de afiliado publicado, los 365 días del año. Reglamento de la Ley marco N° 08 – 2010 **Impacto de Imagen:** Se considera MUY ALTO cuando ocurre la interrupción del servicio web, causando malestar a la opinión pública y las entidades vinculadas.
Registro de IPRESS	RENIPRESS	MUY ALTO	ALTO	ALTO	**Impacto Operativo:** Se considera MUY ALTO porque existe un impacto tanto interno como externo, debido a que no se podría recolectar, validar, publicar y dar servicios de información sobre el Registro Nacional de IPRESS, además al ser el registro de IPRESS públicas, privadas y mixtas autorizadas para brindar servicios de salud afectan la interoperabilidad con otros sistemas de información. **Impacto Legal:** Se considera ALTO cuando existe una interrupción del servicio, por el cual se puede determinar un incumplimiento según el Artículo 7 del Decreto Legislativo N° 1158 donde indica que para brindar servicios de salud las IPRESS deberán encontrarse registradas en la Superintendencia Nacional de Salud. **Impacto de Imagen:** Se considera ALTO cuando ocurre la interrupción del servicio, causando retraso y malestar en las IPRESS.
Atención al Ciudadano	BPM PAC	MUY ALTO	MUY ALTO	MUY ALTO	**Impacto Operativo:** Se considera MUY ALTO cuando ocurre la interrupción del servicio web, afectando a la gestión de consultas y denuncias presentadas ante SUSALUD. **Impacto Legal:** Se considera MUY ALTO cuando ocurre la interrupción del servicio web, causando un incumplimiento del servicio de acuerdo al

					Decreto Supremo N°002-2019-SA que aprueba el Reglamento para la Gestión de Reclamos y Denuncias de los Usuarios de las IAFAS, IPRESS y UGIPRESS, públicas, privadas o mixtas.
					Impacto de Imagen: Se considera MUY ALTO cuando ocurre la interrupción del servicio web, causando malestar a la opinión pública y las entidades vinculadas.

Anexo A. Planes de acción de Recursos Críticos

Ante la interrupción de un servicio se cuenta con un plan de recuperación de desastres (DRP) para los servicios de TI más críticos.

Los contactos externos e internos para las comunicaciones respectivas ante una recuperación de servicios de TI priorizados están subidos en la nube de GMAIL en una carpeta compartida denominada "***Plan de Recuperación de Servicios Informáticos***", archivo "***Contactos Internos y Externos***".

A continuación, se detalla el desarrollo de los procedimientos de recuperación y los responsables de elaborar y revisar las actividades específicas de recuperación para cada servicio de TI.

A.1. Plan de acción: Servicio de Internet dedicado con el operador (Router, UTM y enlaces)

Componentes:

- Router, UTM y enlaces de fibra óptica proveído por el servicio de línea dedicado

Etapas:

Antes de la Contingencia

Ejecutante	Actividad
Especialista en Arquitectura de TI	Realizar un respaldo de la configuración del UTM
Especialista en Arquitectura de TI	Elaborar y contar con un diagrama de conexiones actualizado.
Oficial de Seguridad y confianza digital y Especialista en Arquitectura de TI	Revisar el cumplimiento del procedimiento de respaldo y de la operatividad del recurso de contingencia. Registrar las tareas y acciones en las fecha programada según "Cronograma de seguimiento"

Activación de la Contingencia

Activación	Circunstancia
Jefe de Gestión de Operaciones / Especialista en Arquitectura de TI	Falla de Hardware del equipo de seguridad o software del equipo de Seguridad. Falla de Hardware del equipo Router. Falla en el enlace de Fibra óptica.

Durante de la Contingencia

Ejecutante	Actividad
Especialista en Arquitectura de TI	Revisión de conexiones, configuraciones y alertas del equipo de seguridad o router.
Especialista en Arquitectura de TI	En caso de falla del equipo o enlaces de fibra óptica se contacta al proveedor de línea dedicada para la activación del soporte del equipo en arrendamiento o revisión de los enlaces de fibra óptica.
Especialista en Arquitectura de TI y responsables de los servicios	Solucionado el incidente, se realizan las pruebas correspondientes.
Oficial de Seguridad y confianza digital y Especialista en Arquitectura de TI	Revisar la seguridad de la Información en la etapa de contingencia. Registrar las tareas y/o acciones realizadas en el formato de "Ejecución del Plan de Recuperación de servicios informáticos".

Después de la Contingencia

Ejecutante	Actividad
Especialista en Arquitectura de TI	Monitoreo de la operatividad y conectividad los equipos y enlaces.
Oficial de Seguridad y confianza digital y Especialista en Arquitectura de TI	Verificar que se haya cumplido el procedimiento de recuperación. Registrar las tareas y/o acciones realizadas en el formato de "Ejecución del Plan de Recuperación de servicios informáticos". Fin.

A.2 Plan de Acción: Red de Datos

Componentes:

- Switches core Aruba - HP

Etapas:

Antes de la Contingencia

Ejecutante	Actividad
Especialista en Arquitectura de TI	Realizar un respaldo de la configuración de los equipos de red.
Especialista en Arquitectura de TI	Elaborar un diagrama de interconectividad y Vlans.
Especialista en Arquitectura de TI	Contar con equipos en stack.
Oficial de Seguridad y confianza digital y Especialista en Arquitectura de TI	Revisar el cumplimiento del procedimiento de respaldo y de la operatividad del recurso de contingencia. Registrar las tareas y acciones en las fechas programada según "Cronograma de seguimiento"

Activación de la Contingencia

Activación	Circunstancia
Jefe de Gestión de Operaciones / Especialista en Arquitectura de TI	Falla de Hardware del switch core. Falla en el software de configuración.

Durante de la Contingencia

Ejecutante	Actividad
Especialista en Arquitectura de TI	Revisión de conexiones críticas y moverlas a otro equipo operativo que trabaja en alta disponibilidad.
Especialista en Arquitectura de TI	En caso de falla de Hardware se contacta al proveedor para la activación de la garantía o en su defecto reparación del Switch.
Especialista en Arquitectura de TI	Realizar pruebas.

Ejecutante	Actividad
Oficial de Seguridad y confianza digital y Especialista en Arquitectura de TI	Revisar la seguridad de la Información en la etapa de contingencia. Registrar las tareas y/o acciones realizadas en el formato de "Ejecución del Plan de Recuperación de servicios informáticos".

Después de la Contingencia

Ejecutante	Actividad
Especialista en Arquitectura de TI	Switch reparado por garantía de la marca o contrato de mantenimiento.
Especialista en Arquitectura de TI	Configuración del switch reparado y pruebas de operatividad.
Oficial de Seguridad y confianza digital y Especialista en Arquitectura de TI	Verificar que se haya cumplido el procedimiento de recuperación. Registrar las tareas y/o acciones realizadas en el formato de "Ejecución del Plan de Recuperación de servicios informáticos". Fin.

A.3 Plan de Acción: Red SAN

Componentes:

- Sistema de almacenamiento, Hitachi AMS2500, IBM Flash System, IBM Storwize, Switches de FC.

Etapas:

Antes de la Contingencia

Ejecutante	Actividad
Administrador de operaciones	Realizar un backup de la configuración de los 03 sistemas de almacenamiento y switches de fibra.
Administrador de operaciones	Realizar un backup de la información del sistema de almacenamiento (Máquinas virtuales BD, Correo, aplicaciones, etc.).
Administrador de operaciones	Elaborar un diagrama de las conexiones del sistema de almacenamiento y switches de fibra.
Oficial de Seguridad y confianza digital y Administrador de operaciones	Revisar el cumplimiento del procedimiento de respaldo y de la operatividad del recurso de contingencia. Registrar las tareas y acciones en las fecha programada según "Cronograma de seguimiento"

Activación de la Contingencia

Activación	Circunstancia
Administrador de operaciones /Jefe de Operaciones	Falla de Hardware del sistema de almacenamiento o Switches de fibra.

Durante de la Contingencia

Ejecutante	Actividad
Administrador de operaciones	Revisar las configuraciones, conexiones y alertas del equipo.
Administrador de operaciones	En caso de falla de Hardware se contacta al proveedor para la reparación del Switch o sistema de almacenamiento.
Administrador de operaciones	Realizar pruebas de operatividad.

Ejecutante	Actividad
Oficial de Seguridad y confianza digital y Administrador de operaciones	Revisar el cumplimiento del procedimiento de respaldo y de la operatividad del recurso de contingencia. Registrar las tareas y acciones en las fecha programada según "Cronograma de seguimiento"

Después de la Contingencia

Ejecutante	Actividad
Administrador de operaciones /Jefe de Operaciones	Sistema de almacenamiento reparado por garantía de la marca o contrato de mantenimiento.
Administrador de operaciones /Jefe de Operaciones	Configuración del hardware reparado y pruebas de operatividad.
Oficial de Seguridad y confianza digital y Administrador de operaciones /Jefe de Operaciones	Verificar que se haya cumplido el procedimiento de recuperación. Registrar las tareas y/o acciones realizadas en el formato de "Ejecución del Plan de Recuperación de servicios informáticos". Fin.

A.4 Plan de Acción: Virtualización (VCenter) y Hipervisores Esxi.

Componentes:

- Servidor Virtual Vcenter, Hipervisores Esxi.

Etapas:

Antes de la Contingencia

Ejecutante	Actividad
Administrador de operaciones	Realizar un respaldo de la máquina virtual.
Administrador de operaciones	Asegurar capacidad de recursos en los servidores y sistemas de almacenamiento.
Oficial de Seguridad y confianza digital y Especialista Administrador de operaciones	Revisar el cumplimiento del procedimiento de respaldo y de la operatividad del recurso de contingencia. Registrar las tareas y acciones en las fecha programada según "Cronograma de seguimiento"

Activación de la Contingencia

Activación	Circunstancia
Intendente de la IID / Jefe de Operaciones	Falla del servicio de Vcenter
Jefe de Gestión de Operaciones	Caída del servidor.
Jefe de Gestión de Operaciones	Daño parcial del sistema de almacenamiento.

Durante de la Contingencia

Ejecutante	Actividad
Administrador de operaciones	Restablecer el backup del servidor virtual que tiene el Vcenter.
Administrador de operaciones	Revisión y actualización de configuraciones de Vmware.

Ejecutante	Actividad
Administrador de operaciones	Realizar pruebas.
Oficial de Seguridad y confianza digital y Administrador de operaciones	Revisar la seguridad de la Información en la etapa de contingencia. Registrar las tareas y/o acciones realizadas en el formato de "Ejecución del Plan de Recuperación de servicios informáticos".

Después de la Contingencia

Ejecutante	Actividad
Administrador de operaciones /Jefe de Operaciones	Servidor reparado por garantía de la marca o contrato de mantenimiento.
Administrador de operaciones /Jefe de Operaciones	Configuración del hardware reparado y pruebas de operatividad.
Oficial de Seguridad y confianza digital y Administrador de operaciones	Verificar que se haya cumplido el procedimiento de recuperación. Registrar las tareas y/o acciones realizadas en el formato de "Ejecución del Plan de Recuperación de servicios informáticos". Fin.

A.5 Plan de Acción: Servidores RISC sistema operativo AIX IBM, IBM Integration BUS y IBM MQ, IBM Was.

Componentes:

- Plataforma de servidores Risc y sistema de almacenamiento StorWize

Etapas:

Antes de la Contingencia

Ejecutante	Actividad
Administrador de operaciones	Configurar servicios en alta disponibilidad (IBM servic BUS, IBM MQ, IBM Was
Administrador de operaciones	Realizar un respaldo de los servidores.
Administrador de operaciones	Asegurar capacidad de recursos en los servidores y sistemas de almacenamiento.
Oficial de Seguridad y confianza digital y Administrador de operaciones /Jefe de Operaciones	Revisar el cumplimiento del procedimiento de respaldo y de la operatividad del recurso de contingencia. Registrar las tareas y acciones en las fecha programada según "Cronograma de seguimiento"

Activación de la Contingencia

Activación	Circunstancia
Intendente de la IID / Jefe de Operaciones	Falla del servicio de IBM Integration BUS y IBM MQ, IBM Was
Jefe de Gestión de Operaciones	Caída del servidor Risc
Jefe de Gestión de Operaciones	Daño parcial del sistema de almacenamiento.

Durante de la Contingencia

Ejecutante	Actividad
Administrador de operaciones	En caso de falla de Hardware se contacta al proveedor para la reparación del recurso afectado. En caso de falla de Software se contacta al proveedor para la reparación de la configuración del Sistema Operativo.
Administrador de operaciones	Revisión de configuraciones del servidor recuperado y pruebas.
Oficial de Seguridad y confianza digital y Administrador de operaciones /Jefe de Operaciones	Revisar la seguridad de la Información en la etapa de contingencia. Registrar las tareas y/o acciones realizadas en el formato de "Ejecución del Plan de Recuperación de servicios informáticos".

Después de la Contingencia

Ejecutante	Actividad
Administrador de operaciones /Jefe de Operaciones	Servidor reparado por contrato de mantenimiento.
Administrador de operaciones /Jefe de Operaciones	Configuración del hardware reparado y pruebas de operatividad.
Oficial de Seguridad y confianza digital y Administrador de operaciones /Jefe de Operaciones	Verificar que se haya cumplido el procedimiento de recuperación. Registrar las tareas y/o acciones realizadas en el formato de "Ejecución del Plan de Recuperación de servicios informáticos". Fin.

A.6.- Plan de Acción: Librería de Backup y COMMVAULT

Componentes:

- Unidad de Backup. software de backup (Commvault)

Etapas:

Antes de la Contingencia

Ejecutante	Actividad
Administrador de operaciones	Supervisar el mantenimiento periódico a la Librería BK
Administrador de operaciones	Realizar el backup de la configuración del COMMVAULT.
Oficial de Seguridad y confianza digital y Administrador de operaciones /Jefe de Operaciones	Revisar el cumplimiento del procedimiento de respaldo y de la operatividad del recurso de contingencia. Registrar las tareas y acciones en las fecha programada según "Cronograma de seguimiento"

Activación de la Contingencia

Activación	Circunstancia
Intendente de la IID / Jefe de Operaciones	Caída de la unidad de backup Caída del servidor físico donde está instalado el software de Backup.
Jefe de Gestión de Operaciones	Falla en la unidad de backup Falla en el software de backup (commvault)

Durante de la Contingencia

Ejecutante	Actividad
Administrador de operaciones	En caso de falla de Hardware se contactará al proveedor para su reparación
Administrador de operaciones	Revisión y recuperación de configuraciones con el apoyo del proveedor de Soporte del COMMVAULT.
Oficial de Seguridad y confianza digital y Administrador de operaciones /Jefe de Operaciones	Revisar la seguridad de la Información en la etapa de contingencia. Registrar las tareas y/o acciones realizadas en el formato de "Ejecución del Plan de Recuperación de servicios informáticos".

Después de la Contingencia

Ejecutante	Actividad
Administrador de operaciones /Jefe de Operaciones	Unidad de backup reparada por garantía de la marca o contrato de mantenimiento.
Administrador de operaciones /Jefe de Operaciones	Configuración del hardware reparado y pruebas de operatividad.
Oficial de Seguridad y confianza digital y Administrador de operaciones /Jefe de Operaciones	Verificar que se haya cumplido el procedimiento de recuperación. Registrar las tareas y/o acciones realizadas en el formato de "Ejecución del Plan de Recuperación de servicios informáticos". Fin.

A.7 Plan de Acción: Restauración de máquinas virtuales
BD MYsql, WS Seguridad, WS Pasarella, Elastic, SQL Server, Sistema de seguridad, Aplicación RENIPRESS, Registro de RENIPRESS- war (W) y properties(P); RAAUS - RESUELVE, BD del BPM-PAC (Mysql) y Apache, ws de Consulta del registro de afiliados, wr-dni-afiliados, ws Consulta de lista de IPRESS, ws para el SITEDS CLIENTE, ws para el DOCKER para el SITEDS WEB, ws: chatbot (net), publicado en la PIDE (java), publicado para el SIS (java), FTP del mini batch, mv del S.O. Red Hat 5.5 con Oracle Standar 11g.

Componente:

- Plataforma de servidores virtuales y sistema de almacenamiento.

Etapas:

Antes de la Contingencia

Ejecutante	Actividad
Administrador de operaciones	Realizar un respaldo de todas las VM
Administrador de operaciones	Asegurar capacidad de recursos en los servidores y sistemas de almacenamiento
Oficial de Seguridad y confianza digital y Administrador de operaciones	Revisar el cumplimiento del procedimiento de respaldo y de la operatividad del recurso de contingencia. Registrar las tareas y acciones en las fecha programada según "Cronograma de seguimiento"

Activación de la Contingencia

Activación	Circunstancia
Intendente de la IID / Jefe de Operaciones	Caída del servidor Virtual.
Jefe de Gestión de Operaciones	Falla de la aplicación
Jefe de Gestión de Operaciones	Daño parcial en los servidores físicos.
Jefe de Gestión de Operaciones	Daño parcial del sistema de almacenamiento.

Durante de la Contingencia

Ejecutante	Actividad
Administrador de operaciones /Jefe de Operaciones	Restablecer la imagen del servidor virtual. En caso de falla de Hardware se contactará al contratista del mantenimiento para la reparación del servidor o sistema de almacenamiento.
Administrador de operaciones /Jefe de Operaciones	Revisión de configuraciones del servidor virtual recuperado y pruebas.

Ejecutante	Actividad
Oficial de Seguridad y confianza digital y Administrador de operaciones /Jefe de Operaciones	Revisar la seguridad de la Información en la etapa de contingencia. Registrar las tareas y/o acciones realizadas en el formato de "Ejecución del Plan de Recuperación de servicios informáticos".

Después de la Contingencia

Ejecutante	Actividad
Administrador de operaciones /Jefe de Operaciones	Servidor y sistema de almacenamiento reparado por garantía de la marca o contrato de mantenimiento.
Administrador de operaciones /Jefe de Operaciones	Configuración del Servidor y sistema de almacenamiento reparado y pruebas de operatividad.
Oficial de Seguridad y confianza digital y Administrador de operaciones /Jefe de Operaciones	Verificar que se haya cumplido el procedimiento de recuperación. Registrar las tareas y/o acciones realizadas en el formato de "Ejecución del Plan de Recuperación de servicios informáticos". Fin.

A.8 Plan de Acción: Correo Electrónico

Componentes:

- Plataforma de servidores virtuales y sistema de almacenamiento.

Etapas:

Antes de la Contingencia

Ejecutante	Actividad
Administrador de operaciones	Realizar el respaldo de servidor del correo
Administrador de operaciones	Asegurar capacidad de recursos en los servidores y sistemas de almacenamiento.
Oficial de Seguridad y confianza digital y Administrador de operaciones	Revisar el cumplimiento del procedimiento de respaldo y de la operatividad del recurso de contingencia. Registrar las tareas y acciones en las fecha programada según "Cronograma de seguimiento"

Activación de la Contingencia

Activación	Circunstancia
Jefe de Operaciones / Administrador de operaciones	Falla del servicio de correo
Administrador de operaciones	Caída del servidor.
Administrador de operaciones	Daño parcial del sistema de almacenamiento.

Durante de la Contingencia

Ejecutante	Actividad
Administrador de operaciones	Restablecer la imagen del servidor virtual. En caso de falla de Hardware se contacta al proveedor para la reparación del servidor o sistema de almacenamiento.
Administrador de operaciones	Revisión de configuraciones del servidor recuperado y pruebas.
Oficial de Seguridad y confianza digital y Administrador de operaciones	Revisar la seguridad de la Información en la etapa de contingencia. Registrar las tareas y/o acciones realizadas en el formato de "Ejecución del Plan de Recuperación de servicios informáticos".

Después de la Contingencia

Ejecutante	Actividad
Administrador de operaciones /Jefe de Operaciones	Servidor reparado por garantía de la marca o contrato de mantenimiento.
Administrador de operaciones /Jefe de Operaciones	Configuración del hardware reparado y pruebas de operatividad.
Oficial de Seguridad y confianza digital y Administrador de operaciones /Jefe de Operaciones	Verificar que se haya cumplido el procedimiento de recuperación. Registrar las tareas y/o acciones realizadas en el formato de "Ejecución del Plan de Recuperación de servicios informáticos". Fin.

A.9 Plan de Acción: Directorio Activo

Componentes:

- Plataforma de servidores y sistema de almacenamiento.

Etapas:

Antes de la Contingencia

Ejecutante	Actividad
Administrador de operaciones	Configurar tres controladores secundarios del Directorio Activo.
Administrador de operaciones	Realizar un respaldo de servidor Primario del Directorio Activo.
Administrador de operaciones	Asegurar capacidad de recursos en los servidores y sistemas de almacenamiento.
Oficial de Seguridad y confianza digital y Administrador de operaciones	Revisar el cumplimiento del procedimiento de respaldo y de la operatividad del recurso de contingencia. Registrar las tareas y acciones en las fecha programada según "Cronograma de seguimiento"

Activación de la Contingencia

Activación	Circunstancia
Intendente de la IID / Jefe de Operaciones	Falla del servicio de Directorio Activo
Jefe de Gestión de Operaciones	Caída del servidor.
Jefe de Gestión de Operaciones	Daño parcial del sistema de almacenamiento.

Durante de la Contingencia

Ejecutante	Actividad
Administrador de operaciones	Restablecer la imagen del servidor virtual. En caso de falla de Hardware se contacta al proveedor para la reparación del servidor o sistema de almacenamiento.
Administrador de operaciones	Revisión de configuraciones del servidor recuperado y pruebas.
Oficial de Seguridad y confianza digital y Administrador de operaciones	Revisar el cumplimiento del procedimiento de respaldo y de la operatividad del recurso de contingencia. Registrar las tareas y acciones en las fecha programada según "Cronograma de seguimiento"

Después de la Contingencia

Ejecutante	Actividad
Administrador de operaciones /Jefe de Operaciones	Servidor reparado por garantía de la marca o contrato de mantenimiento.
Administrador de operaciones /Jefe de Operaciones	Configuración del hardware reparado y pruebas de operatividad.
Oficial de Seguridad y confianza digital y Administrador de operaciones /Jefe de Operaciones	Verificar que se haya cumplido el procedimiento de recuperación. Registrar las tareas y/o acciones realizadas en el formato de "Ejecución del Plan de Recuperación de servicios informáticos". Fin.

A.10 Plan de Acción: Restauración de RMAN de base de datos oracle 11g (BD de Registro de Afiliados, Resuelve, SITEDS, RENIPRESS y BPM PAC)

Componente:

- Servidores: SEPS05 – SEPS06 (fuera de funcionamiento) - Redhat versión 5.5 / BD Oracle RAC 11g / con conexión a la Red SAN.

Etapas:

Antes de la Contingencia

Ejecutante	Actividad
Administrador de Base de Datos.	Realizar un Backup (RMAN) semanal de la base de datos y enviarlo a un lugar de custodia.
Administrador de Base de Datos.	Preparar un servidor Linux con un disco local: a. S.O. Redhat versión 5.5 b. Espacio disco de acuerdo al último reporte del espacio ocupado en disco de la base de datos y se considera el doble de espacio de data para el backup. c. Procesador equivalente a uno de los nodos del RAC. d. Memoria equivalente al ambiente productivo.
Soporte Técnico / Administrador de Red.	Instalar y configurar el tape backup.
Administrador de Base de Datos.	Instalar el software del motor de BD Oracle. e. Oracle Database Estándar Edition (11g) Release 11.2.0.4.0, Edición Estándar
Oficial de Seguridad y confianza digital y Administrador de Base de Datos.	Revisar el cumplimiento del procedimiento de respaldo y de la operatividad del recurso de contingencia. Registrar las tareas y acciones en las fecha programada según "Cronograma de seguimiento"

Activación de la Contingencia

Activación	Circunstancia
Comité de Crisis / Jefe de Operaciones	1. Destrucción del Data Center.
Jefe de Operaciones	2. Caída de los servidores de BDs.
Jefe de Operaciones	3. Daño irrecuperable del Storage.

Durante de la Contingencia

Ejecutante	Actividad
Administrador de Base de Datos.	Restaurar el Backup (RMAN) de la base de datos. a. Solicitar a centro de datos el último backup en el disco local del servidor de contingencia. b. Restaurar el RMAN c. Comunicar al responsable del servidor de aplicaciones para direccionar las aplicaciones a la BD de contingencia. d. Utilizar restauración de DMP del esquema RENIPRESS para una restauración parcial.
Especialista en gestión de TI.	Validar que las aplicaciones funcionen correctamente.
Oficial de Seguridad y confianza digital, Administrador de Base de Datos y Especialista en gestión de TI.	Revisar el cumplimiento del procedimiento de respaldo y de la operatividad del recurso de contingencia. Registrar las tareas y acciones en las fecha programada según "Cronograma de seguimiento"

Después de la Contingencia

Ejecutante	Actividad
Jefe de Operaciones / Asistente administrativo / Soporte Técnico / Administrador de Red.	Reponer recursos afectados.
Soporte Técnico / Administrador de Red / Administrador de Base de Datos.	Instalar y configurar recursos afectados. Configurar Base de Datos Oracle 11g Standard Edition en un S.O. RedHat 5.5 en una infraestructura RAC de dos nodos con las mismas características del servidor afectado.
Administrador de Base de Datos.	Restaurar el RMAN del ambiente de contingencia.
Administrador de Base de Datos.	Habilitar la estrategia de backup en el nuevo servidor.
Especialista en gestión de TI.	Validar que la aplicación del sistema RENIPRESS funcione correctamente.
Oficial de Seguridad y confianza digital, Administrador de Base de Datos y Especialista en gestión de TI	Verificar que se haya cumplido el procedimiento de recuperación. Registrar las tareas y/o acciones realizadas en el formato de "Ejecución del Plan de Recuperación de servicios informáticos". Fin.

A.11 Plan de acción: Central Telefónica

Componentes:

- Central Telefónica, software.

Etapas:

Antes de la Contingencia

Ejecutante	Actividad
Especialista en Arquitectura de TI	Realizar respaldo de la configuración de las configuraciones.
Especialista en Arquitectura de TI	Mantener contrato de soporte y mantenimiento vigente.
Oficial de Seguridad y confianza digital y Especialista en Arquitectura de TI	Revisar el cumplimiento del procedimiento de respaldo y de la operatividad del recurso de contingencia. Registrar las tareas y acciones en las fechas programada según "Cronograma de seguimiento"

Activación de la Contingencia

Activación	Circunstancia
Jefe de Gestión de Operaciones / Especialista en Arquitectura de TI	Falla de Hardware de la Central Telefónica Falla del software de la central telefónica.

Durante de la Contingencia

Ejecutante	Actividad
Especialista en Arquitectura de TI	Revisión de conexiones, configuraciones y alertas de la central telefónica
Especialista en Arquitectura de TI	En caso de falla de Hardware de la central contactamos al proveedor de soporte para su revisión y mantenimiento correctivo.
Especialista en Arquitectura de TI	Realizar pruebas de operatividad.
Oficial de Seguridad y confianza digital y Especialista en Arquitectura de TI	Revisar la seguridad de la Información en la etapa de contingencia. Registrar las tareas y/o acciones realizadas en el formato de "Ejecución del Plan de Recuperación de servicios informáticos".

Después de la Contingencia

Ejecutante	Actividad
Especialista en Arquitectura de TI	Central telefónica reparada, considerada dentro del contrato de mantenimiento.
Especialista en Arquitectura de TI	Configuración del hardware y software reparados.
Especialista en Arquitectura de TI	Pruebas de operatividad.
Oficial de Seguridad y confianza digital y Especialista en Arquitectura de TI	Verificar que se haya cumplido el procedimiento de recuperación. Registrar las tareas y/o acciones realizadas en el formato de "Ejecución del Plan de Recuperación de servicios informáticos". Fin.

ANEXO 02. Procedimiento para la convocatoria del personal involucrado en la ejecución de las actividades críticas

a. Los medios de comunicación a emplear son los siguientes:
    - WhatsApp
    - Mensajes de texto y llamadas
    - Correos y redes sociales
    - Reuniones virtuales (Meet, Zoom, Teams)

b. Ejecución de la convocatoria y actividades a desarrollar
    - El titular de la UOGCO convoca a los miembros del Grupo de Comando para que puedan proponer la activación del PCO al titular de la entidad.
    - En caso se active el PCO, la UOGCO solicitará a los órganos críticos la disponibilidad del personal.
    - La UOGCO comunicará a cada órgano las actividades críticas que debe ejecutar según el presente plan, para que el responsable pueda determinar un personal sustituto en caso sea necesario.
    - Los órganos críticos remitirán a la OGPER el listado de personal crítico actualizado, así como la modalidad en la que trabajarán mientras el PCO esté activo (el cual puede verse modificado en función a la necesidad de la entidad).
    - Simultáneamente, la UOGCO solicitará el reporte situacional del estado de los servicios básicos y de seguridad de las sedes de Cercado, Surco y Chiclayo a la OGA, la cual además comunicará la necesidad de traslado a la Sede Alterna. Así mismo, la UOGCO solicitará el reporte del estado de los equipos y servicios informáticos a la IID, la cual además asumirá la activación del Plan de Recuperación de Desastres.
    - La OGPER realizará visitas inopinadas para verificar la ejecución de actividades críticas por parte de cada órgano.
    - La UOGCO consolidará el reporte del estado de recuperación de las actividades críticas, para informar al Grupo de Trabajo o a la Alta Dirección en caso alguna acción prevista no se haya ejecutado.

ANEXO 03. Directorio del Grupo de Comando

Se detalla la conformación del Grupo de Comando en el siguiente enlace, el cual es de acceso exclusivo con correo institucional de la entidad: https://docs.google.com/spreadsheets/d/1XzL_WqmEswuIzUBAKfRYKOK8roz5ph_lEKAKqWzXag4/edit?usp=sharing

ANEXO 04. Organización para el desarrollo de las actividades críticas

Se detalla la organización de personal para la ejecución de actividades críticas, las cuales están codificadas.

N°	CÓDIGO	DENOMINACIÓN DEL PUESTO
1	OGPER1	ESPECIALISTA EN ORGANIZACIÓN DEL TRABAJO
2	OGPER1	ASISTENTE DE GESTIÓN DE LA COMPENSACIÓN
3	OGPER2	ESPECIALISTA EN RELACIONES HUMANAS Y SOCIALES
4	OGPER2	MÉDICO OCUPACIONAL
5	UOGCO1	RESPONSABLE DE GESTIÓN DEL RIESGO DE DESASTRES
6	OGPP1	ESPECIALISTA EN PRESUPUESTO
7	OGPP1	ESPECIALISTA EN PRESUPUESTO
8	OGPP1	ESPECIALISTA EN PRESUPUESTO
9	OFICOR1	ESPECIALISTA COMUNICADOR SOCIAL - AUDIOVISUALES
10	OFICOR1	DISEÑADOR GRÁFICO
11	OFICOR1	ESPECIALISTA EN PERIODISMO
12	OFICOR2	ESPECIALISTA COMUNICADOR SOCIAL
13	OFICOR3	ESPECIALISTA EN GESTIÓN Y MONITOREO DE REDES SOCIALES
14	IMRN1	JEFE ZONAL
15	IMRN1	ESPECIALISTA DE LA SALUD - ATENCIÓN RÁPIDA
16	IMRN1	ESPECIALISTA DE LA SALUD - ATENCIÓN RÁPIDA
17	IMRN1	ESPECIALISTA EN SALUD - ATENCIÓN RÁPIDA
18	IMRN2	ESPECIALISTA EN REGIÓN - DELEGADOS EN SALUD
19	IMRN2	ESPECIALISTA EN REGIÓN - DELEGADOS EN SALUD
20	IMRN2	ESPECIALISTA EN REGIÓN - DELEGADOS EN SALUD
21	IMRN2	ESPECIALISTA EN REGIÓN - DELEGADOS EN SALUD
22	IMRN2	ESPECIALISTA EN REGIÓN - DELEGADOS EN SALUD
23	IMRN2	ESPECIALISTA EN PROTECCIÓN DE DERECHOS EN SALUD
24	IMRN2	MÉDICO AUDITOR
25	IMRN2	MÉDICO AUDITOR
26	IMRN2	ESPECIALISTA LEGAL
27	ISIPRESS1	ESPECIALISTA EN SUPERVISIÓN
28	ISIPRESS1	ESPECIALISTA EN SUPERVISIÓN
29	ISIPRESS1	ESPECIALISTA EN SUPERVISIÓN
30	ISIPRESS1	ESPECIALISTA EN ANÁLISIS DE DATOS
31	ISIPRESS1	ESPECIALISTA EN SUPERVISIÓN
32	ISIPRESS1	ESPECIALISTA EN SUPERVISIÓN
33	ISIPRESS1	ESPECIALISTA EN SUPERVISIÓN
34	ISIPRESS1	ESPECIALISTA EN SUPERVISIÓN
35	ISIPRESS2	ANALISTA LEGAL
36	ISIPRESS2	ESPECIALISTA LEGAL
37	ISIPRESS3	ESPECIALISTA ADMINISTRATIVO
38	ISIPRESS3	TÉCNICO EN ARCHIVO
39	IFIS1	ESPECIALISTA LEGAL
40	IFIS1	JEFA DE INSTRUCCIÓN
41	IFIS1	ESPECIALISTA LEGAL
42	IFIS1	ESPECIALISTA LEGAL
43	IFIS1	ASISTENTE LEGAL
44	IFIS1	ESPECIALISTA LEGAL
45	IFIS1	ESPECIALISTA LEGAL
46	IFIS1	ESPECIALISTA LEGAL
47	IFIS1	ESPECIALISTA LEGAL

48	IFIS1	ESPECIALISTA LEGAL
49	IFIS1	ASISTENTE LEGAL
50	IFIS1	ESPECIALISTA LEGAL
51	OGA1	ANALISTA EN CONTROL PATRIMONIAL
52	OGA2	TECNICO EN SEGURIDAD
53	OGA3	JEFE DE GESTIÓN LOGÍSTICA
54	OGA3	ESPECIALISTA EN CONTRATACIONES
55	OGA4	INTEGRADOR CONTABLE
56	OGA4	ANALISTA EN TESORERÍA
57	OGA4	ESPECIALISTA EN TESORERÍA
58	INA1	JEFE DE REGULACION
59	INA1	ESPECIALISTA LEGAL
60	INA1	ESPECIALISTA LEGAL
61	INA1	ESPECIALISTA LEGAL
62	INA1	ESPECIALISTA EN REGULACIÓN ECONÓMICA - CONTABLE
63	INA1	ESPECIALISTA EN REGULACIÓN EN SALUD
64	INA1	ASISTENTE DE GESTIÓN
65	INA2	JEFE DE AUTORIZACIÓN
66	INA2	ESPECIALISTA LEGAL
67	INA2	ESPECIALISTA EN REGISTRO
68	INA2	ESPECIALISTA EN REGISTRO
69	INA2	ESPECIALISTA EN REGISTRO
70	INA2	ESPECIALISTA EN REGISTRO
71	INA2	ASISTENTE LEGAL EN REGISTRO
72	IPROM1	ESPECIALISTA EN PARTICIPACIÓN CIUDADANA
73	IPROM2	ESPECIALISTA EN COMUNICACIONES
74	IPROM3	ESPECIALISTA EN ACCIONES DE IMPLEMENTACIÓN DEL SISTEMA DE ATENCIÓN AL USUARIO
75	ISIAFAS1	JEFE DE SUPERVISION ASISTENCIAL ADMINISTRATIVA Y DE ASEGURAMIENTO
76	ISIAFAS1	COORDINADOR EN ESTUDIO ECONÓMICO ACTUARIAL FINANCIERO Y GESTIÓN DE RIESGO
77	ISIAFAS1	ESPECIALISTA EN PROGRAMACIÓN, CONTROL Y MONITOREO
78	ISIAFAS1	ESPECIALISTA LEGAL
79	ISIAFAS1	ASISTENTE DE GESTIÓN
80	ISIAFAS1	ESPECIALISTA EN SUPERVISIÓN ECONÓMICA FINANCIERA
81	ISIAFAS1	ESPECIALISTA EN SUPERVISIÓN ECONÓMICA FINANCIERA
82	ISIAFAS1	ESPECIALISTA EN SUPERVISIÓN DE SEGUROS DE SALUD
83	ISIAFAS1	ESPECIALISTA EN SUPERVISIÓN DE PROCESOS ASISTENCIALES
84	IPROT1	JEFE DE PLATAFORMA
85	IPROT1	AGENTE DE ATENCIÓN POR CANALES
86	IPROT1	ESPECIALISTA DE ORIENTACIÓN Y ATENCIÓN AL USUARIO
87	IPROT1	ESPECIALISTA DE LA SALUD
88	IPROT1	ESPECIALISTA DE PLATAFORMA DE ORIENTACIÓN Y ATENCIÓN A LA CIUDADANÍA
89	IPROT1	ESPECIALISTA DE PLATAFORMA DE ORIENTACION Y ATENCION A LA CIUDADANIA
90	IPROT2	ESPECIALISTA DE SALUD (INTERVENCIÓN)
91	IPROT2	ESPECIALISTA DELEGADO EN SALUD
92	IPROT2	ESPECIALISTA DELEGADO EN SALUD
93	IPROT2	ESPECIALISTA DELEGADO EN SALUD
94	IPROT2	ESPECIALISTA DELEGADO EN SALUD
95	IPROT2	ESPECIALISTA DELEGADO EN SALUD
96	IPROT2	ESPECIALISTA DELEGADO EN SALUD
97	IPROT2	ESPECIALISTA DELEGADO EN SALUD
98	IPROT2	ESPECIALISTA DELEGADO EN SALUD
99	IPROT2	ESPECIALISTA EN REGIÓN - DELEGADOS EN SALUD
100	IPROT2	ESPECIALISTA EN REGIÓN - DELEGADOS EN SALUD

101	IPROT2	ESPECIALISTA EN REGIÓN - DELEGADOS EN SALUD
102	IPROT2	ESPECIALISTA DELEGADO EN SALUD
103	IPROT3	JEFE DE INTERVENCIONES
104	IPROT3	ESPECIALISTA LEGAL
105	IPROT3	ESPECIALISTA DE LA SALUD EN MONITOREO DE GESTIÓN
106	IPROT3	ASISTENTE DE GESTIÓN
107	IPROT3	ASISTENTE DE ARCHIVO
108	IPROT3	ESPECIALISTA LEGAL
109	IPROT3	ESPECIALISTA LEGAL
110	IPROT3	ESPECIALISTA LEGAL
111	IPROT3	ESPECIALISTA DE LA SALUD
112	IPROT3	ESPECIALISTA DE LA SALUD
113	IPROT3	ESPECIALISTA DE LA SALUD
114	IPROT3	ESPECIALISTA LEGAL
115	IPROT3	ESPECIALISTA LEGAL
116	IPROT3	ESPECIALISTA LEGAL
117	IPROT3	ESPECIALISTA DE LA SALUD
118	IPROT3	ASISTENTE DE GESTIÓN
119	IPROT3	AGENTE DE ATENCIÓN POR CANALES
120	IPROT3	ESPECIALISTA DE LA SALUD
121	IPROT3	AGENTE DE ATENCIÓN POR CANALES
122	IPROT3	ESPECIALISTA DE LA SALUD
123	IPROT3	ESPECIALISTA DE LA SALUD
124	IPROT3	ESPECIALISTA DE LA SALUD
125	IID1	JEFE DE GESTIÓN DE OPERACIONES
126	IID1	ESPECIALISTA EN ARQUITECTURA DE TECNOLOGIAS DE LA INFORMACIÓN
127	IID1	ADMINISTRADOR DE OPERACIONES
128	IID1	ESPECIALISTA DE BASE DE DATOS
129	IID1	ESPECIALISTA EN PROCESAMIENTO DE INFORMACIÓN
130	IID1	JEFE DE GESTIÓN DE LA INFORMACIÓN
131	IID1	ESPECIALISTA EN T.I.
132	IID1	ESPECIALISTA EN PROYECTOS INTERINSTITUCIONALES
133	IID1	ESPECIALISTA EN PROYECTOS INTERINSTITUCIONALES
134	IID1	ESPECIALISTA SENIOR EN CALIDAD DE SOFTWARE
135	IID1	JEFE DE GESTION DE INTELIGENCIA DE NEGOCIOS
136	IID1	ESPECIALISTA EN ANÁLISIS DE DATOS
137	IID1	ESPECIALISTA EN GESTIÓN OPERATIVA
138	IID1	ESPECIALISTA EN POBLACIÓN
139	IID1	ESPECIALISTA LEGAL

ANEXO 05. Sistema de comunicaciones de emergencia

En caso de que los recursos informáticos críticos principales sean los primeros en dejar de funcionar, se plantean las siguientes vías alternas:

- WhatsApp
- Mensajes de texto y llamadas
- Correos y redes sociales
- Plataformas para reuniones virtuales (Meet, Zoom, Teams)

En caso de que las vías previamente mencionadas estén saturadas o inhabilitadas, se ha propuesto el uso de equipos de radiocomunicación como requerimiento, por lo que durante la ejecución de los ejercicios propuestos se deberá contemplar la posibilidad de capacitar al personal e implementar dicha alternativa en la entidad.

ANEXO 06. Cronograma de implementación de la Gestión de la Continuidad Operativa

ACTIVIDAD	PARTICIPANTES	PROGRAMACIÓN
Ejecución de ejercicios del PCO		
Difusión reiterada del cronograma de ejercicios	UOGCO	En 15 días hábiles previos al ejercicio
Organización de las acciones para las simulaciones programadas (puntos de reunión)	UOGCO y Grupo de Comando	En 10 días hábiles previos al ejercicio
Preparación de guiones para las simulaciones programadas	Alta Dirección, Grupo de Trabajo y Grupo de Comando	En 7 días hábiles previos al ejercicio
Organización de recursos para la ejecución de simulacros	UOGCO	En 7 días hábiles previos al ejercicio
Ejecución de simulacros y simulaciones	SUSALUD	Según cronograma de ejercicios
Monitoreo y evaluación de los resultados del PCO		
Evaluación e informe de la ejecución de ejercicios del PCO	UOGCO y Grupo de Comando	Hasta 7 días hábiles después del ejercicio
Modificación de la determinación de recursos	Grupo de Comando	Durante el mes de noviembre
Revisión de requerimientos atendidos del PCO	Grupo de Comando	
Modificación de requerimientos para el PCO	Grupo de Comando	
Actualización de otros aspectos del PCO	Grupo de Comando	
Elevar la propuesta de actualización del PCO	UOGCO y Grupo de Comando	Primera semana de diciembre
Integración de la Gestión de Continuidad Operativa a la cultura organizacional		
Elaboración del listado de propuestas para la integración	Grupo de Comando y UOGCO	05/08/2024 al 16/08/2024
Elección de las actividades para la integración	Grupo de Comando y UOGCO	19/08/2024 al 30/09/2024
Ejecución de actividades para la integración	Grupo de Comando y UOGCO	01/10/2024 al 13/12/2024