PERÚ | Ministerio del Interior

Seguro Saludpol

Fondo de Aseguramiento en Salud de la Policía Nacional del Perú

PLAN DE CONTINUIDAD OPERATIVA DEL FONDO DE ASEGURAMIENTO EN SALUD DE LA POLICÍA NACIONAL DEL PERÚ - SALUDPOL

2024

CONTENIDO

		Pág.
I.	INFORMACIÓN GENERAL	2
II.	BASE LEGAL	2
III.	OBJETIVOS	3
	3.1 Objetivo General	3
	3.2 Objetivos específicos	2
IV.	IDENTIFICACIÓN DE RIESGOS Y RECURSOS	3
	4.1 Matriz de riesgos	3
	4.2 Determinación del nivel de impacto	5
	4.3 Identificación de Recursos	6
V.	ACCIONES PARA LA CONTINUIDAD OPERATIVA	9
	5.1 Determinación de las Actividades Críticas	9
	5.2 Roles y responsabilidades para el desarrollo de las actividades críticas	10
	5.3 Aseguramiento del Acervo Documentario	11
	5.4 Aseguramiento de la Base de Datos mediante la ejecución del Plan de Recuperación de los servicios informáticos	11
	5.5 Recursos Económicos	13
	5.6 Requerimientos de recursos mínimos para la Continuidad Operativa	13
	5.7 Determinación de la Sede Alterna de Trabajo	14
	5.8 Activación del Plan de Continuidad Operativa	14
	5.9 Activación y Desactivación de la Sede Alterna	15
	5.10 Desarrollo de las Actividades Críticas	15
VI.	CRONOGRAMA DE EJERCICIOS DEL PLAN DE CONTINUIDAD OPERATIVA	16
VII.	ANEXOS	16

I. INFORMACIÓN GENERAL

El Fondo de Aseguramiento en Salud de la Policía Nacional del Perú– SALUDPOL se crea con el Decreto Legislativo N° 1174 del 7 de diciembre de 2013, en el marco de la Ley Marco de Aseguramiento Universal en Salud y a partir de esta legislación se reconoce su personería jurídica de derecho público interno con calidad de administradora de fondos intangibles de salud, adscrita al Ministerio del Interior, que cuenta con autonomía técnica, económica, financiera, presupuestal y contable.

Como Institución Administradora de Fondos de Aseguramiento en Salud pública – IAFAS, SALUDPOL recibe, capta y gestiona los fondos destinados al financiamiento de prestaciones de salud dirigidas al personal de la PNP y sus familiares derechohabientes, a través de una cobertura de los riesgos de salud.

La Presidencia de Consejo de Ministros–PCM, órgano rector del Sistema Nacional de Gestión del Riesgo de Desastres SINAGERD, mediante la Resolución Ministerial N° 320-2021-PCM 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"; lineamientos que tienen por objetivo establecer los procedimientos para la implementación de la Gestión de la Continuidad Operativa y la formulación de los Planes de Continuidad Operativa en las entidades públicas de los tres niveles de gobierno, con el fin de continuar funcionando ante un desastre o cualquier evento que interrumpa prolongadamente sus operaciones.

Mediante Resolución de Gerencia General N° 370-2024-SALUDPOL/GG, se conforma el Grupo de Comando para la Gestión de la Continuidad Operativa del Fondo de Aseguramiento en Salud de la Policía Nacional del Perú – SALUDPOL, el cual se encarga de la elaboración del Plan de Continuidad Operativa de la entidad.

El Plan de Continuidad Operativa pretende constituirse en una herramienta de gestión para SALUDPOL, el cual le permitirá generar capacidades de preparación y respuesta ante cualquier tipo de crisis, minimizando el impacto negativo que ocasione un desastre, garantizando, la operatividad básica y optimizando los tiempos de recuperación de la operatividad regular de la entidad en caso de una interrupción imprevista.

II. BASE LEGAL

- Ley Nº 29664, que crea el Sistema Nacional de Gestión de Riesgos de Desastres (SINAGERD) y sus modificatorias.
- Decreto Supremo N.º 048-2011-PCM, y normas modificatorias, que aprueba el Reglamento de la Ley N.º 29664, que crea el Sistema Nacional de Gestión de Riesgos de Desastres (SINAGERD).
- Decreto Supremo N.º 038-2021-PCM, Política Nacional de Gestión del Riesgo de Desastres al 2050.
- Resolución Ministerial N.º 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.
- Resolución de Gerencia General N.° 370-2024-SALUDPOL/GG, que aprueba la conformación del Grupo de Comando para la Gestión de la Continuidad Operativa del Fondo de Aseguramiento en Salud de la Policía Nacional del Perú – SALUDPOL.

III. OBJETIVOS

3.1 OBJETIVO GENERAL

Garantizar la continuidad operativa del Fondo de Aseguramiento en Salud de la Policía Nacional del Perú – SALUDPOL ante la ocurrencia de un desastre de gran magnitud u otro evento que interrumpa sus actividades habituales, ejecutando actividades críticas identificadas previamente hasta lograr su recuperación

3.2 OBJETIVOS ESPECÍFICOS

3.2.1 Identificar las actividades críticas que deben ejecutarse de manera continua y sin interrupciones en caso de desastres u otros eventos que puedan afectar de forma prolongada las operaciones. Además, determinar los recursos humanos, materiales, equipos, infraestructura y sistemas informáticos y de telecomunicaciones necesarios para mantener dichas actividades.

3.2.2 Definir los roles y responsabilidades necesarias para la ejecución de las actividades críticas

IV. IDENTIFICACIÓN DE RIESGOS Y RECURSOS

4.1 MATRIZ DE RIESGOS

El Riesgo (R) es una función del Peligro (P) y la Vulnerabilidad (V) y se expresa como la probabilidad de que ocurra una pérdida en un determinado elemento, como resultado de la ocurrencia de un peligro.

Para evaluar la probabilidad y la gravedad del riesgo asociado a los peligros que afectaría a SALUDPOL, ocasionado por un evento disruptivo, se ha tomado en cuenta la metodología emitida por la RM N° 320-2021-PCM, la cual se realiza tomando en cuenta la intersección del peligro y la vulnerabilidad, tal como indica la matriz siguiente:

Matriz de Riesgo

[illegible]	Riesgo Alto	Riesgo Alto	[illegible]	[illegible]
Peligro Alto	Riesgo Medio	Riesgo Alto	Riesgo Alto	[illegible]
Peligro Medio	Riesgo Medio	Riesgo Medio	Riesgo Alto	Riesgo Alto
Peligro Bajo	Riesgo Bajo	Riesgo Medio	Riesgo Medio	Riesgo Alto
P / V	Vulnerabilidad Baja	Vulnerabilidad Media	Vulnerabilidad Alta	[illegible]

Fuente: RM N° 320-2021-PCM/ Manual para la evaluación de riesgos por fenómenos - CENEPRED

Para la identificación de peligros, se ha considerado aquellos eventos que ocasionarían la interrupción de los servicios en forma total o parcial afectando la infraestructura, recursos y la vida humana sobre todo a las principales actividades administrativas y económicas que soportan el cumplimiento de los objetivos misionales de la institución.

Bajo ese criterio de han identificado los siguientes peligros:

4.1.1 Sismo de gran magnitud

Los sismos son fenómenos que representan la liberación de energía interna de la tierra mediante la ruptura de las capas de corteza y que se manifiesta como movimientos ondulatorios que pueden llegar a alcanzar magnitudes variadas. Cuando los movimientos sísmicos adquieren mayores intensidades cobran la denominación de terremotos.

Lima es la zona del país donde se ha acumulado la mayor cantidad de energía sísmica, esto se sustenta en la investigación científica, la misma que ha puesto en evidencia tres áreas con importante acumulación de energía sísmica las cuales se ubican frente a las costas. La más importante de estas zonas, en términos de tamaño y magnitud estimada se ubica frente a la costa central del Perú (Lima, Ancash e Ica).

De acuerdo con el Instituto Geofísico del Perú, en el caso de Lima se pronostica un movimiento telúrico de magnitud 8.8 Mw por el silencio sísmico desde el terremoto de 1746, cuando cerca del 10% de la población perdió la vida. Un terremoto de esta magnitud dejaría inmersa en un caos a Lima y Callao.

Ante este escenario, las sedes institucionales, ubicadas en Lima, pueden presentar daños severos que comprometerían la estabilidad de sus estructuras, ya que la edificación podría quedar debilitada y colapsar, quedando rezagada o interrumpida la prestación de servicios que brinda la entidad.

El Perú es un país altamente sísmico y corresponde estar preparados. Por lo tanto, el presente plan establecerá los procedimientos mínimos para:

- Continuar con las operaciones y actividades críticas que se realizan en SALUDPOL.
- Movilización del personal en caso ocurra el colapso de las sedes y se requiera continuar las actividades críticas en sede(s) alterna(s).
- Asegurar las acciones que permitan la recuperación y restauración de la infraestructura de las sedes afectadas, bienes muebles, informáticos, entre otras necesidades.

SALUDPOL cuenta con cuatro sedes en la ciudad de Lima:

Cuadro N° 01: Sedes - SALUDPOL

SEDE	ANTIGUEDAD	ESTADO DE CONSERVACIÓN	TIPO DE MATERIAL	ESTADO DE LA INFRAESTRUCTURA	CANTIDAD DE PISOS
CENTRAL	2 años	Muy bueno	Concreto	Muy bueno	7+TERRAZA
UT-LIMA	20 años	Regular	Concreto y drywall	Regular	1 piso
MACHUPICCHU		Regular	Concreto y cobertura ligera	Regular	1 piso
PRONABI	11 años	Regular	Concreto	Regular	4 pisos + terraza

Fuente: Elaboración propia

En base al análisis realizado, se puede identificar que el mayor nivel de riesgo de colapso a nivel de infraestructura es el del local ubicado en la sede UT-LIMA, siendo el menor nivel de riesgo el del local de la sede central.

4.1.2 Incendio

El acontecimiento de un incendio puede afectar la resistencia de las estructuras y la exposición directa al fuego de los colaboradores puede causar graves problemas por inhalación, intoxicación y sofocación por gases tóxicos que se produce en los incendios o perder la vida al quedar atrapados en la edificación.

Existe una probabilidad de ocurrencia de un incendio en las sedes institucionales durante horas laborables y de atención al público, debido al aumento de los espacios dedicados a oficinas, la instalación de equipos eléctricos, electrónicos y la alta concentración de material inflamable en los diferentes pisos.

Si bien se cuenta con dispositivos contra incendios (detectores de humo y temperatura, extintores portátiles y rociadores automáticos de agua) para detectar y extinguir el fuego de fuentes eléctricas, químicas, orgánicas o de otras fuentes; estos no son suficientes, lo que limitaría la capacidad de respuesta. Estar preparados para combatir un incendio, se vuelve un tema central; sobre todo con el objetivo de garantizar la seguridad de las personas y, en un segundo plano, resguardar la inversión en equipos, con el fin de reducir los tiempos requeridos para reiniciar las actividades.

Un incendio puede suceder fuera de horario de trabajo o en días no laborables, teniendo graves consecuencias como la inhabilitación del ambiente físico, el colapso de los sistemas de comunicación y gestión de la información institucional, lo que requeriría la activación del Plan de Continuidad Operativa, con la diferencia que en este caso la afectación es solo en la infraestructura de una de las sedes institucionales.

Es importante señalar que, a mayor cantidad de materiales inflamables presentes, mayor será el impacto de un incendio en el local afectado. En este sentido, de los cuatro locales donde se realizan las distintas actividades del SALUDPOL, el que presenta el mayor riesgo de impacto por incendio es el ubicado en el Lt. N°3 y 19-A de la Mz. L, con frente principal en Calle S/N y frente posterior en Calle Ollantaytambo, Urb. San Juan Bautista de Villa I Etapa, Santiago de Surco. Esto se debe a que en este local se encuentran el Archivo Central, el Archivo de Gestión y el Almacén Central, que contienen una gran cantidad de documentos y materiales susceptibles de ser dañados en caso de incendio

4.2 DETERMINACIÓN DEL NIVEL DE IMPACTO

4.2.2 Determinación del Nivel de Impacto

Consiste en estimar el impacto que tendría una interrupción prolongada de los procesos que soportan el cumplimiento de la misión de SALUDPOL.

En el siguiente cuadro se observa la estimación del nivel de impacto que afectaría a la institución relacionando el peligro con variables de operatividad determinados para el presente plan.

Cuadro N° 02: Estimación del Impacto

Estimación del Nivel de Impacto	Sismo de gran magnitud	Incendio
Colapso total de la infraestructura y servicios básicos del local que requieren evacuación	Riesgo muy Alto	Riesgo muy Alto
Colapso parcial de la infraestructura y afectación de los servicios básicos del local, que pueden requerir evacuación	Riesgo Alto	Riesgo Alto
Afectación de la infraestructura y de los servicios básicos del local, que pueden requerir evacuación	Riesgo Medio	Riesgo Medio
No afecta la infraestructura, no requiere evacuación	Riesgo Bajo	Riesgo Bajo

Fuente: Elaboración propia

4.3 IDENTIFICACIÓN DE RECURSOS

Con la determinación de los peligros y los niveles de impacto que ocasionaría algún evento disruptivo es necesario precisar que SALUDPOL cuenta con recursos para la intervención inicial que permitirá dar respuesta de forma oportuna ante la situación de emergencia o desastre en base al principio de autoayuda.

Cuadro N° 03: Recursos Disponibles de SALUDPOL

Recursos Materiales	Número
Extintores	12
Celulares	20
Camillas	1
Botiquín	5
Camioneta	1

Fuente: Elaboración propia

Cuadro N° 04: Recursos Humanos

UNIDAD ORGÁNICA	CAS	Locadores	Total
Directorio		1	1
Gerencia General	5	42	47
Oficina de Asesoría Jurídica	6	9	15
Oficina de Gestión y Mejora Continua	8	14	22
Oficina de Administración	33	103	136
Oficina de Tecnología de la Información	10	18	28
Dirección de Financiamiento y Planes de Salud	7	11	18
Dirección de Prestaciones de Salud	12	78	90
Dirección del Asegurado	14	73	87
Unidades Territoriales	25		25
TOTAL	**120**	**349**	**469**

Fuente: Elaboración propia

Cuadro N° 05: Recursos Informáticos

EQUIPOS INFORMÁTICOS	CANTIDAD
Acumulador de energía	293
Capturador de imagen – Scanner	10
Computadora personal portátil	61
Equipo multifuncional copiadora impresora scanner y/o fax	123
Monitor	463
Pantalla interactiva	2
Proyector multimedia	9
Sistema de videoconferencia	1
Teclado – Keyboard	491
Unidad Central de Proceso – CPU	412

Fuente: Elaboración propia

Cuadro N° 06 : Equipos de Comunicación

EQUIPOS DE COMUNICACIÓN	CANTIDAD
Punto de acceso inalámbrico – Access Point Wireless	11
Switch para red	42

Fuente: Elaboración propia

Cuadro N° 07: Servidores

SERVIDORES	CANTIDAD
Locales	48
En nube	13
TOTAL	61

Fuente: Elaboración propia

Cuadro N° 08: Software

SOFTWARE	CANTIDAD
Adobe Creative Cloud	3
Herramientas de desarrollo	13
Microsoft Office 2016	86
Microsoft Office 2019	349
Microsoft Office 2021	28
Motores de base de datos	12
Windows 11 PRO	77
Windows 10 PRO	371
Windows 7 PRO	15

SOFTWARE	CANTIDAD
WithSecure Elements Agent	500
Zoom Business	20

Fuente: Elaboración propia

Cuadro N° 09: Centros de Datos

CENTRO DE DATOS	CANTIDAD
Acumulador de energía – equipo de UPS 15 KVA	1
Banco de baterías	1
Cámara de video digital IP tipo fija minidomo	2
Cámara de video tipo tubo lente fijo 2 MP	1
Climatizador	1
Disco duro externo	1
Equipo de aire acondicionado de precisión	1
Equipo de control de acceso biométrico	1
Equipo de iluminación de emergencia	2
Equipo para aire acondicionado tipo doméstico	1
Gabinete de metal	1
Gabinete de metal de pared 24 RU	1
Gabinete de metal para servidores	2
Grabador digital de video y audio - videograbador digital	2
Servidor	4
Servidor Blade	3
Silla fija de metal	1
Sistema de detección y extinción de incendios para data center	2
Sistema de monitoreo y control remoto de ambiente	1
Solución de almacenamiento externo	1
Switch para red	4
Transformador (mayor a 1/4 UIT) de aislamiento trifásico de 20 KVA	1
Transformador trifásico de 12 KVA	1
Unidad de almacenamiento de discos externos	2
Unidad de distribución de energía (PDU) – switched rack PDU	5
Unidad para copia de seguridad	2

Fuente: Elaboración propia

Cuadro N° 09: Sistemas de Información

ÍTEM	SISTEMAS DE INFORMACIÓN	PRIORIDAD
1	Sistema de Gestión de Registro de Asegurados	Alta
2	Sistema de Procedimientos Médicos (SPM)	Alta
3	Sistema de Gestión del Trámite Documentario (STD)	Media
4	Sistema de Gestión de Reembolsos (SGR)	Alta
5	Sistema de Gestión de Asistencia al Usuario y Libro de Reclamaciones (SGAU)	Baja
6	Sistema de Gestión de Pasajes Aéreos (SGPA)	Media
7	Intranet de SALUDPOL	Baja
8	Sistemas de Transferencia de Información de Prestaciones de Salud (STIPS)	Alta
9	Sistema Integrado de Gestión Estratégica Financiera (SIGEF)	Media
10	Sistema de Registro de Prestaciones de Salud (SRPS)	Alta
11	Aplicativo Móvil Stock Farmacias PNP – SALUDPOL	Baja
12	Aplicativo Móvil Salud Policial PNP	Baja
13	Sistema de Gestión de Convocatorias CAS	Baja
14	Sistema de Interacción con Proveedores (SIP)	Media
15	Sistema de Registro de Emergencia Prioridad I (SREP1)	Alta
16	Sistema de Denuncias del Canal de Integridad	Baja
17	Sistema Integrado de Monitoreo del Asegurado (SIMA)	Media
18	Marcaciones Web	Media
19	Sistema de Gestión de Citas de IPRESS NO PNP	Media
20	Sistema de Gestión de Colas	Baja
21	Módulo web de Consulta de Stock de Medicamentos.	Baja
22	Módulo web de Consulta de Convenios y Contratos	Baja
23	Sistema de Gestión Documental	Media
24	Servicios Web Modelo SITEDS (IAFAS)	Media
25	Interoperabilidad basada en SETIAF	Alta

Fuente: Elaboración propia

V. ACCIONES PARA LA CONTINUIDAD OPERATIVA

5.1 DETERMINACIÓN DE LAS ACTIVIDADES CRÍTICAS

El Grupo de Comando, conforme a las disposiciones específicas establecidas en 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", aprobados por Resolución Ministerial N° 320-2021-PCM del 30.12.2021; ha identificado seis (06) actividades críticas, las cuales se indican a continuación:

1. Compra de Prestaciones de Salud

2. Conducción, Monitoreo y Gestión de las Unidades Territoriales
3. Mantenimiento y soporte de los sistemas informáticos
4. Gestión Administrativa
5. Gestión de Recursos Humanos

5.2 ROLES Y RESPONSABILIDADES PARA EL DESARROLLO DE LAS ACTIVIDADES CRÍTICAS

Mediante Resolución de Gerencia General Nº 000370-2024-SALUDPOL/GG se aprueba la conformación del Grupo de Comando para la Gestión de la Continuidad Operativa del Fondo de Aseguramiento en Salud de la Policía Nacional del Perú – SaludPol, el cual estará integrado por los siguientes miembros:

- El/la Jefe/a de la Unidad de Recursos Humanos, quien lo preside.
- Un representante de la Oficina de Tecnología de la Información.
- Un representante de la Oficina de Administración.
- Un representante de la Unidad de Logística y Patrimonio.
- Un representante de la Oficina de Gestión y Mejora Continua.
- Un representante del Área de Comunicaciones e Imagen.

En el artículo tercero de la citada Resolución, se dispone que los integrantes del Grupo de Comando cumplirán sus funciones en mérito a lo dispuesto en 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", aprobados mediante la Resolución Ministerial N° 320-2021-PCM, donde se indica que corresponde al Grupo de Comando realizar las siguientes actividades:

a) Identificar las actividades críticas a cargo de la Entidad, en coordinación con los órganos que desarrollan tales actividades.
b) Identificar los recursos humanos y materiales necesarios para la ejecución de las actividades críticas de la Entidad entre los que se encuentran: locales alternos, materiales, equipos informáticos y data.
c) Realizar las coordinaciones con la unidad responsable del acervo documentario, con el fin de contar con archivos digitales con valor legal, asegurando su conservación ante un desastre de gran magnitud o cualquier evento que pueda interrumpir prolongadamente las operaciones de la entidad.
d) Coordinar con las unidades orgánicas responsables, la verificación del funcionamiento de los grupos electrógenos y las unidades de respaldo de energía de los centros de cómputo, y acceso al correo institucional desde el domicilio del personal, entre otros.
e) Coordinar con las unidades orgánicas responsables, las medidas necesarias para el aprovisionamiento ininterrumpido de los servicios básicos y otros esenciales, para la ejecución de las actividades críticas identificadas.
f) Actualizar el Plan de Continuidad Operativa.
g) Proponer al Gerente General la activación del Plan de Continuidad Operativa de la entidad, cuando corresponda.
h) Verificar el desarrollo de las actividades críticas
i) Verificar el cumplimiento del cronograma de ejercicios del Plan de Continuidad Operativa.

5.3 ASEGURAMIENTO DEL ACERVO DOCUMENTARIO

De acuerdo con el artículo 1 de la Ley Nº 25323, Ley que crea el Sistema Nacional de Archivos, establece que este sistema tiene por finalidad integrar estructural, normativa y funcionalmente los archivos de las entidades públicas existentes en el ámbito nacional, mediante la aplicación de principios, normas, técnicas y métodos de archivo, garantizando con ello la defensa, conservación, organización y servicio del Patrimonio Documental de la Nación.

El Área de Gestión Documentaria y Archivo tiene a su cargo la administración del Archivo Central de SALUDPOL, el cual se encuentra ubicado en el local ubicado en LT. N°3 y 19-A de la MZ. L, con frente principal Calle S/N y frente posterior Calle Ollantaytambo, Urb. San Juan Bautista de Villa I Etapa, Santiago de Surco.

Adicionalmente se deben considerar los archivos periféricos de las diferentes direcciones y oficinas que conforman la organización de SALUDPOL y los archivos desconcentrados a cargo de las Unidades Territoriales de SALUDPOL ubicadas en diversas localidades del interior del país.

A fin de asegurar la conservación del acervo documentario de la entidad, actualmente se viene digitalizando toda la documentación que ingresa a SALUDPOL. Al mismo tiempo, la documentación que producen las unidades orgánicas se genera de manera virtual.

5.4 ASEGURAMIENTO DE LA BASE DE DATOS MEDIANTE LA EJECUCIÓN DEL PLAN DE RECUPERACIÓN DE LOS SERVICIOS INFORMÁTICOS

Mediante Resolución de Gerencia General Nº 000305-2023-SALUDPOL/GG se aprueba el "Plan de Continuidad de Tecnologías de la Información y Comunicaciones (PCTIC) 2023 - 2026 del Fondo de Aseguramiento en Salud de la Policía Nacional del Perú – SaludPol", cuya finalidad es "garantizar la continuidad del servicio de Tecnologías de la Información y Comunicaciones TIC de los procesos en especial los más críticos del SALUDPOL, a fin de que se restablezcan en el menor tiempo posible, en caso ocurra alguna eventualidad que interrumpa su operatividad".

Este Plan considera la siguiente estrategia de recuperación, en caso ocurra un escenario de riesgo:

Escenario N° 01: Indisponibilidad de Infraestructura Física, por causa de algún desastre natural u ocasionados por el hombre.

a) Revisar y realizar un inventario de los equipos informáticos que no fueron afectados por el evento.
b) Implementar una infraestructura tecnológica alterna para los sistemas y servicios que se mantienen en físico dentro de la infraestructura tecnológica afectada.
c) Continuar con la implementación de servidores virtuales.
d) Implementar en el servicio de nube los sistemas virtualizados alojados en físico dentro de la infraestructura tecnológica de la institución.
e) Realizar copias de respaldo de los sistemas de información, aplicaciones, software base y sistemas operativos de manera inmediata y continuar el plan según cronograma establecido y almacenado en el servicio de respaldo contratado.

f) Revisar elementos disuasivos para la extinción de fuego, como extintores

Escenario N° 02: Indisponibilidad del recurso o servicio informático por falla en el Hardware y/o Software.

a) Contar con un procedimiento de alquiler de equipos de comunicación para las instalaciones del SALUDPOL.
b) Realizar copias de respaldo periódicas de la configuración de los equipos de comunicaciones.
c) Solicitar la última copia disponible de los sistemas afectados para la reinstalación, se debe de coordinar con los operadores, el administrador de base de datos, desarrolladores para la reimplementación y puesta en marcha de los servicios afectados.
d) Programación de revisiones anuales de obsolescencia tecnológica de los servidores físicos informáticos, para realizar la renovación de estas, en caso se requiera.
e) Continuar con la implementación de servidores virtuales para mejorar los tiempos de recuperación en caso de falla de hardware.
f) Contar y/o mantener los Acuerdos de Niveles de Servicio (SLA) con los proveedores para que en caso sea necesario, puedan sustituir los servidores físicos y otros equipos de comunicaciones de la infraestructura tecnológica en general, en el menor tiempo posible y/o solucionar los inconvenientes de los servicios que dicho proveedor tiene a cargo y que son monitoreados desde SALUDPOL.
g) Contar con un plan de renovación por obsolescencia o actualización de equipos de cómputo de usuario con el fin de tener equipos con tecnología vigente y reducir los incidentes por fallas relacionadas a la antigüedad de los equipos.

Escenario N° 03: Indisponibilidad de los Servicios Web y/o Sistemas de Información por la ocurrencia de un delito informático.

a) Ejecutar el plan maestro ante ataque informático.
b) Restaurar los servicios afectados con la última versión de respaldo disponible.
c) Recurrir al proveedor de seguridad gestionada (firewall, antivirus, antimalware, etc) realizar los ajustes necesarios con respecto a la seguridad perimetral.
d) De ser el caso comunicar a las autoridades pertinentes acerca del evento.
e) Solicitar apoyo a la Secretaria de Gobierno y Transformación Digital mediante el portal "facilita" para recibir las instrucciones necesarias.
f) Realizar pruebas anuales de Hacking Ético con terceros especializados
g) Realizar el endurecimiento de sistemas en toda la infraestructura bajo el reporte del análisis de Hacking Ético.
h) Contratar el servicio de seguridad de aplicaciones Web.
i) Desarrollar planes de sensibilización en materia de seguridad de la información y buenas prácticas en el uso de los sistemas informáticos.

Escenario N° 04: Caída de Suministro eléctrico.

a) Contratar un servicio de mantenimiento preventivo y correctivo para el UPS y pozo a tierra.
b) Realizar el apagado de los equipos, mientras se cuente con energía del UPS exceptuando el servicio informático de los procesos críticos.

Escenario N° 05: Indisponibilidad de los servicios por ausencia o falta del personal crítico.

a) Capacitar a un reemplazo para cada rol, de tal manera que pueda asumir las funciones en caso el personal principal se encuentre indispuesto.
b) Capacitar al personal de OTI en el proceso de recuperación de los servicios de TI. La capacitación debe ser planificada, estructurada y acorde con las exigencias de recuperación.
c) Para el personal que goce de sus vacaciones deberá dejar por escrito actividades de su rol asignada a otro trabajador.
d) Elaborar una base de datos de conocimiento, en caso el personal encargado de ciertos procedimientos, tanto principal, como de reemplazo se encuentren indispuestos.

Escenario N° 06: Indisponibilidad del servicio de internet.

a) Ante la caída del servicio de internet, el usuario que detecte el incidente deberá reportarlo a la mesa de ayuda usando los medios de comunicación existentes, la OTI brindará el reporte necesario para conocimiento del usuario o usuarios afectados en el incidente, hasta su solución. Los usuarios deberán de usar los medios disponibles de comunicación para la continuidad de sus operaciones
b) De otro lado si no se contara con datos externos de internet, el área que forma parte de los procesos transversales de SALUDPOL, deberá gestionar para estos casos, el levantamiento de información manual con formatos físicos establecidos, hasta que exista la conectividad correspondiente y los procesos core, puedan seguir su operatividad a pesar de esta contingencia.

5.5 RECURSOS ECONÓMICOS

Para el financiamiento de las actividades previstas en el presente plan, la Unidad de Presupuesto de SALUDPOL, realizará las modificaciones presupuestarias necesarias de manera coordinada con la Alta Dirección a fin de asegurar la disponibilidad de recursos para atender la gestión de la emergencia en especial para dar atención a la continuidad operativa.

5.6 REQUERIMIENTOS DE RECURSOS MÍNIMOS PARA LA CONTINUIDAD OPERATIVA

5.6.1 Requerimiento de personal

Para dar continuidad operativa de los servicios y procesos críticos identificados se dispondrá de personal clave que serán convocados para realizar las actividades críticas. Se considerará la restricción de la asistencia a las oficinas, promoviendo la modalidad del trabajo remoto. En el caso que la infraestructura haya colapsado (inoperativo) se dispondrá el desplazamiento del personal clave a la sede alterna designada.

5.6.2 Requerimiento de material y equipo

Son aquellos mobiliarios y bienes mínimos requeridos para facilitar las labores de las actividades críticas previamente identificadas.

5.6.3 Requerimiento de recursos informáticos

indicación de retirarse y estar atentos a ser convocados o en su defecto seguir labores de forma remota.

5.9 ACTIVACIÓN Y DESACTIVACIÓN DE LA SEDE ALTERNA

En el caso que ante un evento de gran magnitud la sede central de SALUDPOL quede inoperativa se ha identificado al local ubicado en Av. Alameda Los Cedros esq. Ca. Tortugas, Mz. G7, Lt. 6 y Lt. 7, Chorrillos, como probable sede alterna en caso de necesidad.

5.9.1 Activación de la sede alterna

a) La Unidad de Logística y Control Patrimonial debe disponer que personal técnico, propio o contratado, realice una evaluación sobre la situación de las sedes de la institución, proponiendo el plan de acción a tomar.
b) La Unidad de Logística y Control Patrimonial se encargará del acondicionamiento y equipamiento de la sede alterna seleccionada, garantizando que se puedan realizar las actividades más urgentes, de acuerdo a las actividades críticas identificadas.
c) La Unidad de Recursos Humanos, de acuerdo a la disponibilidad de espacio y equipamiento, identificará al personal necesario para la continuidad de las actividades críticas identificadas, seleccionando la modalidad de trabajo, presencial o virtual.

5.9.2 Desactivación de la sede alterna

El Grupo de Comando realizará una evaluación permanente del estado situacional de las sedes institucionales, y en su momento, recomendará a la Gerencia General la conclusión del Plan de Continuidad Operativa y el retorno progresivo de las actividades normales de la institución.

5.10 DESARROLLO DE LAS ACTIVIDADES CRÍTICAS

Con el fin de asegurar el desarrollo de las Actividades Críticas, el Grupo de Comando debe realizar el seguimiento y monitoreo correspondiente, para tal efecto deberá utilizar la matriz de Seguimiento y Monitoreo de la ejecución de las Actividades Críticas del Plan de Continuidad Operativa establecida en la R.M. N°320-2021-PCM del 30.12.2021, las que se muestran a continuación.

Cuadro N° 06 : Desarrollo de Actividades Criticas

Se deberá asegurar la disponibilidad de los equipos informáticos (Software y Hardware) ya sea para el trabajo remoto como para las actividades que se ejecutarán en las sedes alternas de activarse, se considerarán los equipos informáticos mínimos necesarios para el personal clave y de apoyo que se convocará para la continuidad operativa de SALUDPOL.

5.7 DETERMINACIÓN DE LA SEDE ALTERNA DE TRABAJO

Con fines de asegurar el menor tiempo de interrupción del funcionamiento institucional, se debe identificar con anticipación por lo menos una eventual ubicación donde se desplazaría SALUDPOL, para seguir operando con sus actividades críticas. Esto implica realizar las coordinaciones para que la potencial sede alterna esté preparada para disponer la implementación necesaria, de tal manera que una vez ocurrido el evento y en cuanto se haya tomado la decisión, sea la alternativa más recomendable para el desplazamiento.

La Sede Alterna más adecuada, en caso que la Sede Central se vea afectada por un evento de gran magnitud, es el local ubicado en Av. Alameda Los Cedros esq. Ca. Tortugas, Mz. G7, Lt. 6 y Lt. 7, Chorrillos, local cedido por el Programa Nacional de Bienes Incautados - PRONABI

5.8 ACTIVACIÓN DEL PLAN DE CONTINUIDAD OPERATIVA

La activación del Plan de Continuidad Operativa del Fondo de Aseguramiento en Salud de la Policía Nacional del Perú se origina ante la ocurrencia de un evento adverso con el fin de continuar brindando los servicios y desarrollando las actividades de la institución. La activación del Plan de Continuidad Operativa estará a cargo del Gerente General de SALUDPOL por recomendación del Grupo de Comando.

Las acciones previstas para la activación del Plan de Continuidad Operativa son las siguientes:

- El Jefe de la Unidad de Recursos Humanos, quien preside el Grupo de Comando, brindará un reporte inicial a la Gerencia General de SALUDPOL, referida a la naturaleza del evento adverso, el impacto del daño generado y la situación operativa de las sedes de SALUDPOL.
- Una vez evaluado el reporte de daños, el Grupo de Comando de SALUDPOL propondrá al Gerente General, la activación del Plan de Continuidad Operativa.
- Se gestionará el acondicionamiento y puesta en operaciones de la sede alterna, asegurando que la misma disponga de ambientes y equipamiento necesario para dar continuidad a las operaciones esenciales de SALUDPOL.
- En cuanto se tenga la confirmación de que la sede alterna se encuentra acondicionada, con los recursos necesarios, con servicios mínimos que aseguren las comunicaciones y la operatividad de los equipos, el personal priorizado (personal clave) se desplazará a la sede alterna.
- El personal no debe ser expuesto a riesgos innecesarios, si las instalaciones no brindan las garantías para la permanencia en las sedes respectivas. Asimismo, será informado sobre los turnos que se dispongan, el horario en el que deben apersonarse de corresponder. En caso de que no se demande la presencia del personal, se dará

VII. ANEXOS

7.1 Plan de Recuperación de los Servicios Informáticos

7.2 Directorio del Grupo de Comando

ACTIVIDAD CRITICA	RESPONSABLE	ACTIVIDADES DESARROLLADAS	PERSONAL ASIGNADO	MATERIAL ASIGNADO	EQUIPO ASIGNADO	PRESUPUESTO ASIGNADO
1. Compra de Prestaciones de Salud	Director de la Dirección de Financiamiento y Prestaciones de Salud	a. Autorización Procedimientos Médicos	2	Útiles de Oficina	PC	25,000.00
		b. Gestión de pago de servicios	3	Útiles de Oficina	PC	
2. Conducción, Monitoreo y Gestión de las Unidades Territoriales	Director de la Dirección del Asegurado	a. Afiliación de asegurados	5	Útiles de Oficina	PC	25,000.00
		b. Compras excepcionales	3	Útiles de Oficina	PC	
3.Mantenimiento y soporte de los sistemas informáticos	Jefe de la Oficina de Tecnología de la Información	a. Alquiler de PCs	1	Útiles de Oficina	PC	50,000.00
		b. Soporte a los sistemas	5	Útiles de Oficina	PC	
		c. Recuperación de datos	5	Útiles de Oficina	PC	
4. Gestión Administrativa	Jefe de la Oficina de Administración	a. Emisión de resoluciones	3	Útiles de Oficina	PC	300,000
		b. Control Interno	8	Útiles de Oficina	PC	
		c. Gestión de Pagos	5	Útiles de Oficina	PC	
5. Gestión de Recursos Humanos	Jefe de la Unidad de Recursos Humanos	a. Supervisión de labores	3	Útiles de Oficina	Vehículo	220,000
		b. Seguridad y Salud en el Trabajo	5	Material Médico	Camillas	
		c. Elaboración de Planillas	3	Útiles de Oficina	PC	

Fuente: Elaboración propia

VI. CRONOGRAMA DE EJERCICIOS DEL PLAN DE CONTINUIDAD OPERATIVA

Con el fin de asegurar la continuidad de los servicios se deberá desarrollar Simulacros y/o Simulaciones.

2025											
ENE	FEB.	MAR.	ABR.	MAY.	JUN.	JUL.	AGO.	SET.	OCT.	NOV.	DIC.

2026											
ENE	FEB.	MAR.	ABR.	MAY.	JUN.	JUL.	AGO.	SET.	OCT.	NOV.	DIC.

2027											
ENE	FEB.	MAR.	ABR.	MAY.	JUN.	JUL.	AGO.	SET.	OCT.	NOV.	DIC.

Fuente: Elaboración propia

Coordinador/a de Continuidad de TIC.

d) Personal Encargado:

Equipo de Emergencia de TIC.

e) Descripción de las actividades después de activar la contingencia

- ✓ Desconectar el fluido eléctrico y alejar líquidos o material inflamable como cajones, entre otros, si corresponde.
- ✓ Evacuar las oficinas de acuerdo a las disposiciones de los Brigadistas de Evacuación, utilizando las rutas establecidas durante los simulacros. Considerar las escaleras de emergencia, señalización de rutas, zonas de agrupamiento del personal, etc. Por ningún motivo utilizar los ascensores.
- ✓ Verificar que todo el personal del SALUDPOL que labora en el área, se encuentre bien.
- ✓ Brindar los primeros auxilios al personal afectado si fuese necesario.
- ✓ Alejarse de las lunas (ventanas) para evitar sufrir cortes por roturas y/o desprendimiento de trozos de vidrio.
- ✓ Evaluación de los daños ocasionados por el sismo sobre las instalaciones físicas, ambientes de trabajo, estanterías, instalaciones eléctricas, documentos, etc.
- ✓ Inventario general de documentación, personal, equipos, etc. y/o recursos afectados, indicando el estado de operatividad de los mismos.
- ✓ Limpieza de las áreas afectadas por el sismo. En todo momento se coordinará con personal de mantenimiento del SALUDPOL, para las acciones que deban ser efectuadas por ellos.
- ✓ En caso se requiera la habilitación del ambiente provisional alterno para restablecer la función de los ambientes afectados, el/la Jefe/a de la OTI, deberá coordinar con el/la Jefe/a de la OA.

f) Duración

- ✓ Los procesos de evacuación del personal del SALUDPOL deberán ser calmados y demorar 5 minutos como máximo.
- ✓ La duración total del evento dependerá del grado del sismo, la probabilidad de réplicas y los daños a la infraestructura.

3. PLAN DE RECUPERACIÓN

a) Personal Encargado

El personal encargado es el/la Coordinador/a de Continuidad de TIC y el Equipo de Restauración de TIC, cuyo rol principal es asegurar el normal desarrollo de los servicios y operaciones de TI del SALUDPOL.

b) Descripción de actividades

El plan de recuperación está orientado a recuperar en el menor tiempo posible las actividades afectadas durante la interrupción del servicio.

En caso, el evento haya sido de considerable magnitud, se deberá:

- ✓ Verificar la disponibilidad de recursos para la contingencia como: manuales técnicos de instalación del sistema de información, almacenamiento de datos, sistemas de comunicación, hardware, y copias de respaldo.
- ✓ Movilizar los equipos de respaldo al sitio alterno de recuperación o en donde necesiten su disponibilidad.
- ✓ Establecer contacto con los proveedores clave y terceros para proporcionar instrucciones inmediatas y/o notificarles cualquier requisito de ayuda sobre la recuperación de las operaciones.
- ✓ Supervisar el progreso de las operaciones de recuperación y de servicios de TI y mantener informado al equipo de Continuidad Operativa.
- ✓ Restauración de los servicios y operaciones de TI en el sitio alterno: El Equipo de Restauración de TIC restaurará el espacio de trabajo para permitir que el personal crítico de la oficina pueda operar, para lo cual deberá ejecutar los procedimientos de recuperación de la plataforma tecnológica.
- ✓ Verificar que las aplicaciones críticas se hayan recuperado y estén funcionando correctamente.
- ✓ Confirmar los puntos de recuperación de datos de las aplicaciones.
- ✓ Verificar que las funcionalidades de comunicación están funcionando correctamente.
- ✓ Verificar que equipos básicos como escáner, impresora estén disponibles y operacionales para dar soporte a los requisitos de la entidad.
- ✓ Asegurar que el ambiente del área de trabajo, las aplicaciones y las

telecomunicaciones están funcionando según lo estimado tanto en el sitio alterno, como al retornar al sitio original, una vez concluida la emergencia o siniestro.

- ✓ Registrar todos los gastos operacionales relacionados con la continuidad de las operaciones.

c) Mecanismos de Comprobación

El/La Coordinador/a de Continuidad de TIC, presentará un informe al equipo de Continuidad Operativa, explicando qué parte de las actividades u operaciones de tecnologías de la información han sido afectadas y cuáles son las acciones tomadas.

d) Desactivación del Plan de Continuidad TIC

El/La Coordinador/a de Continuidad de TIC desactivará el Plan de Contingencia TIC, una vez que se haya tomado las acciones descritas en el presente Plan de Recuperación, mediante una comunicación electrónica al Equipo de Continuidad.

e) Proceso de Actualización

El proceso de actualización será en base al informe presentado por el/la Coordinador/a de Continuidad de TIC, luego del cual se determinará las acciones a tomar.

B) INCENDIO, O CUALQUIER DESASTRE PROVOCADO POR LA MANO DEL HOMBRE

1. PLAN DE PREVENCIÓN

a) Descripción del escenario

- ✓ Todas las oficinas han designado a un delegado para casos de emergencia, así también cada oficina cuenta con un extintor, si bien los delegados han sido capacitados inicialmente, no se considera que la periodicidad de dichas capacitaciones es óptima.
- ✓ Con respecto al mantenimiento de los equipos informáticos, no se tiene un espacio adecuado para realizarlo y reducir el riesgo de incendio al hacer uso de materiales inflamables, como alcohol isopropílico, thinner acrílico o aerosoles. Este riesgo implica un mayor impacto al realizarse trabajos de mantenimiento, por parte de la OTI u otras oficinas, que hacen uso de este tipo de herramientas en horas laborables y en algunos casos lo realizan en los módulos del personal que atiende dicho mantenimiento.

- ✓ Sobre la infraestructura tecnológica, no se tiene una infraestructura tecnológica alterna; sin embargo, en caso que un incendio logre destruir un 50% de las oficinas antes de ser controlado, el impacto en la infraestructura tecnológica sería alto, toda vez que los equipos se verían realmente afectado y la información almacenada ahí también se afectaría, si bien cierta información está en la nube, pero el resto de información se encuentra alojada en servidores virtualizados.
- ✓ La información generada por las aplicaciones alojadas en la nube es respaldada constantemente en línea; la información generada por aplicaciones alojadas en equipos la infraestructura tecnológica se respalda en discos de almacenamiento local de forma diaria y progresiva. Por tanto, de presentarse el incendio en el lapso previo al envío de los respaldos locales a las cintas, se tiene riesgo de pérdida de la información si las mismas no son entregadas al proveedor del servicio de respaldo de backups o se salvaguardan en algún lugar externo a la infraestructura tecnológica.
- ✓ Cabe precisar que no se tiene habilitado un lugar para que la totalidad de empleados trabajen en tanto el inmueble sea restaurado.

  Infraestructura:

  ✓ La infraestructura tecnológica en su totalidad Recursos Humanos:

  ✓ Personal de la entidad.

b) Objetivo

Establecer las acciones que se ejecutarán ante un incendio a fin de minimizar el tiempo de interrupción de las operaciones en el SALUDPOL, sin exponer la seguridad de las personas.

c) Personal Encargado

El/La coordinador/a de Continuidad, es quien debe dar los lineamientos y dar cumplimiento a las Condiciones de Prevención de Riesgo del presente Plan. Por su parte, el Equipo de Prevención debe realizar las acciones descritas en el punto e).

d) Condiciones de Prevención de Riesgo

- ✓ Inspecciones de seguridad realizadas periódicamente a la infraestructura tecnológica.

- ✓ Mantenimiento de las salidas libres de obstáculos.
- ✓ Funcionamiento de los extintores contra incendio.
- ✓ Funcionamiento de las luces de emergencia.
- ✓ Mantenimiento de detectores de humo contra incendio y los rociadores de agua.

e) Acciones del Equipo de Prevención

- ✓ Evaluar en coordinación con el coordinador de Continuidad, las acciones de restauración y respaldo.
- ✓ Establecer, organizar, ejecutar y supervisar procedimientos de respaldo y restauración de información como base de datos, código fuentes y ejecutables.
- ✓ Programar, supervisar el mantenimiento preventivo a los equipos de la infraestructura tecnológica.
- ✓ Mantener vigente o actualizados los extintores contra incendio, a fin de que cumplan su función de forma adecuada.

2. PLAN DE EJECUCIÓN

a) Eventos que activan la contingencia

La contingencia se activará al ocurrir un incendio. El proceso de contingencia se activará inmediatamente después de ocurrir el evento.

b) Personal que autoriza la contingencia informática

El/La Coordinador/a de Continuidad.

c) Personal Encargado

Equipo de Emergencia.

d) Acciones para ejecutar a corto plazo

- ✓ Desconectar el fluido eléctrico y alejar otros líquidos inflamables si corresponde y si se puede.
- ✓ Establecer medidas que permitan garantizar que los respaldos realizados estén totalmente funcionales y que permita recuperar la información exacta a partir de los mismos.

✓Realizar de forma más frecuente el backup de la información en la nube.

✓Evaluar el alcance del desastre en cada área de responsabilidad y notificar y reunir a los demás integrantes del Equipo de Emergencia y Restauración.

e) Duración

La duración total del evento dependerá del grado del incendio y los daños a la infraestructura.

3. PLAN DE RECUPERACIÓN

a) Personal Encargado

El personal encargado es el/la Coordinador/a de Continuidad y el Equipo de Restauración, cuyo rol principal es asegurar el normal desarrollo de los servicios de TI del SALUDPOL.

b) Descripción de actividades

El plan de recuperación está orientado a recuperar en el menor tiempo posible las actividades afectadas durante la interrupción del servicio.

En caso, el evento haya sido de considerable magnitud, se deberá:

- ✓ Verificar la disponibilidad de recursos para la contingencia como: manuales técnicos de instalación del sistema de información, almacenamiento de datos, sistemas comunicación, hardware, y copias de respaldo.
- ✓ Movilizar al Equipo de Restauración al sitio alterno de recuperación.
- ✓ Establecer contacto con los proveedores clave y terceros para proporcionar instrucciones inmediatas y/o notificarles cualquier requisito de ayuda sobre la recuperación de las operaciones.

c) Mecanismos de Comprobación

El Equipo de Emergencia presentará un informe al/el coordinador de Continuidad, explicando qué parte de las actividades u operaciones de tecnologías de la información han sido afectadas y cuáles son las acciones tomadas.

d) Desactivación del Plan de Continuidad TIC

El/La Coordinador/a de Continuidad desactivará el Plan de Continuidad TIC, una vez que se haya tomado las acciones descritas en el presente Plan de Recuperación.

ANEXO 2

DIRECTORIO DEL GRUPO DE COMANDO

CARGO	UNIDAD ORGÁNICA	TELEFONO/ANEXO
PRESIDENTE DEL GRUPO DE COMANDO	UNIDAD DE RECURSOS HUMANOS	(01)-6802710 Anexo 130 - 132
INTEGRANTES DEL GRUPO DE COMANDO	OFICINA DE TECNOLOGÍA DE LA INFORMACIÓN	(01)-6802710 Anexo 700 - 701
	OFICINA DE ADMINISTRACION	(01)-6802710 Anexo 101 - 103
	UNIDAD DE LOGÍSITICA Y PATRIMONIO	(01)-6802710 Anexo 121
	OFICINA DE GESTIÓN Y MEJORA CONTINUA	(01)-6802710 Anexo 300 - 301
	AREA DE COMUNICACIONES E IMAGEN	(01)-6802710 Anexo 909

SALUDPOL V°B° D. BOZA F. UNIDAD DE PLANEAMIENTO

SALUDPOL V°B° OFICINA DE GESTIÓN Y MEJORA CONTINUA

SALUDPOL V°B° R. TOLEDO A. OFICINA DE ADMINISTRACIÓN

SALUDPOL V°B° R. CORREA L. UNIDAD DE PRESUPUESTO