



PERÚ

Ministerio  
del Interior



---

# PLAN DE CONTINUIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES (PCTIC) DEL FONDO DE ASEGURAMIENTO EN SALUD DE LA POLICÍA NACIONAL DEL PERÚ – SALUDPOL 2023 - 2026

---

Oficina de Tecnología de la Información

2023



BICENTENARIO  
DEL PERÚ  
2021 - 2024



## INDICE

<b>I.- INTRODUCCIÓN .....</b>	<b>3</b>
<b>II.- FINALIDAD.....</b>	<b>4</b>
<b>III.-OBJETIVO .....</b>	<b>4</b>
<b>IV.- OBJETIVOS ESPECÍFICOS.....</b>	<b>4</b>
<b>V.- BASE LEGAL.....</b>	<b>4</b>
<b>VI.-TERMINOLOGÍA.....</b>	<b>6</b>
<b>VII.- METODOLOGÍA DE TRABAJO .....</b>	<b>9</b>
<b>VIII.-DESARROLLO DE LAS FASES PARA LA ELABORACIÓN DEL PLAN DE CONTINUIDAD TIC..</b>	<b>9</b>
<b>8.1. FASE 1: DETERMINACIÓN DEL ALCANCE .....</b>	<b>10</b>
<b>8.2. FASE 2: ANÁLISIS DE LA ORGANIZACIÓN .....</b>	<b>10</b>
<b>8.3. FASE 3: DETERMINACIÓN DE LA ESTRATEGIA DE CONTINUIDAD .....</b>	<b>20</b>
<b>8.4. FASE 4: RESPUESTA A LA CONTINGENCIA .....</b>	<b>27</b>
<b>8.5. FASE 5: DEFINICIÓN Y EJECUCIÓN DEL PLAN DE PRUEBAS.....</b>	<b>33</b>
<b>8.6. FASE 6: MONITOREO .....</b>	<b>34</b>
<b>IX.- APROBACIÓN Y ACTUALIZACIÓN .....</b>	<b>34</b>
<b>ANEXO I: FORMATO DE CONTROL Y CERTIFICACIÓN DE LAS PRUEBAS DEL PLAN DE CONTINUIDAD TIC Y RECUPERACIÓN DE SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES EN SALUDPOL.....</b>	<b>36</b>
<b>ANEXO II: INVENTARIO DE SISTEMAS DE INFORMACIÓN DEL SALUDPOL VIGENTE .....</b>	<b>37</b>
<b>ANEXO III: PROCEDIMIENTOS DE RESTAURACIÓN DE SERVICIOS DE TIC SEGÚN LOS PRINCIPALES ESCENARIOS DE RIESGO .....</b>	<b>39</b>

## I.- INTRODUCCIÓN

Actualmente las instituciones públicas están expuestas a diversos riesgos que pueden afectar su capacidad para cumplir con sus objetivos, así como su continuidad operativa. Debido a ello se establecen planes de continuidad o de contingencia de Tecnologías de la Información y Comunicaciones, con el fin de reducir al mínimo el impacto de los riesgos que se generan por causa de las amenazas existentes que traen conexas.

Ahora bien, el contar con un Plan de Continuidad de Tecnologías de la Información y Comunicaciones (PCTIC) del Fondo de Aseguramiento en Salud de la Policía Nacional del Perú – SALUDPOL<sup>1</sup> (en adelante Plan de Continuidad TIC), sólido y estructurado, permitirá prever la cantidad mínima de escenarios de riesgo o situaciones adversas, así como los ataques internos o externos los cuales podrían materializarse y afectar a la entidad en su recurso o servicio informático que soportan sus procesos, afectando directa o indirectamente al conjunto de beneficiarios dentro de ellos se encuentra al personal de la PNP y sus familiares derechohabientes, por ende, de la importancia de salvaguardar a dicho recurso o servicio informático.

El presente Plan de Continuidad TIC, describe la planificación de las acciones que se requieren ante una situación de emergencia, contemplando la recuperación de los recursos y servicios TIC, que soportan los procesos de forma preponderante a los procesos misionales, actuando como un proceso continuo de estrategias y procedimientos, ante situaciones inesperadas que puedan dañar a dicha continuidad en las operaciones en el SALUDPOL.

El Plan de Continuidad TIC, cuenta con una estructura que, en conjunto permiten la gestión, ejecución, pruebas y mantenimiento, esto conlleva a una fácil y ágil operación por los responsables autorizados, ante situaciones de desastres.

Finalmente, el Plan de Continuidad TIC, contempla el uso de estándares internacionales tales como la “NTP ISO/IEC 22301: Sistema de Gestión de la Continuidad de Negocio”, la “NTP-ISO/IEC 27001:2022. Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. 3ª Edición” y otras buenas prácticas, que en su conjunto permitirán extraer los puntos esenciales para la actuación ante tales

---

<sup>1</sup> SALUDPOL: es el Fondo de Aseguramiento en Salud de la Policía Nacional del Perú, el cual 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, la cual 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.

escenarios de riesgo por parte del equipo a cargo de dichas responsabilidades, si es que llegaran a materializarse.

## II.- FINALIDAD

Garantizar la continuidad del servicio de 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.

## III.-OBJETIVO

Elaborar el Plan de Continuidad<sup>2</sup> TIC, el cual permita garantizar la continuidad de las operaciones del servicio informático en el SALUDPOL.

Asimismo, el Plan de Continuidad TIC, se encuentra articulado al Objetivo Estratégico “04. Fortalecer la implementación del Sistema Integrado de Gestión (SIG), a través de la modernización de la gestión pública, transparencia, transformación digital, así como el posicionamiento institucional del SALUDPOL”, así como a la Acción Estratégica “04.06 Fortalecimiento del desarrollo de TIC para la articulación Interinstitucional, del Plan Estratégico (PE) 2022-2026 del SALUDPOL<sup>3</sup>”.

## IV.- OBJETIVOS ESPECÍFICOS

- a) Conocer los procesos que tiene SALUDPOL a fin de realizar su identificación, determinar su criticidad y cuáles son los riesgos relacionados con los activos de información relacionados con las TIC, que son más relevantes a los que están expuestos, mediante el análisis de riesgo realizado.
- b) Determinar los escenarios de riesgos más frecuentes para luego planificar las estrategias que ayuden a salvaguardar los activos de información del servicio informático.
- c) Establecer los procedimientos a tener en cuenta por cada escenario de riesgo identificado, a fin de responder adecuadamente ante la contingencia presentada.

## V.- BASE LEGAL

- Resolución de Secretaría de Gobierno y Transformación Digital N° 002-2023-PCM/SGTD que aprueba la Directiva que establece el perfil y responsabilidades del Oficial de Seguridad y Confianza Digital, vigente desde el 8 de setiembre de 2023.

---

<sup>2</sup> Definición de Plan de continuidad (o de contingencia) TIC: Es un conjunto de procedimientos que permiten la recuperación en casos de desastres, un plan formal que describe todos los pasos que se tienen que seguir en caso de que suceda una emergencia.

<sup>3</sup> Resolución de Directorio N.° 011-2023-IN-PD, que aprueba la Ampliación del Horizonte Temporal del Plan Estratégico (PE) 2022-2026 del SALUDPOL.

- Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD que “Establece la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información en las Entidades Públicas, vigente desde el 8 de setiembre del 2023.
- Decreto Supremo N° 085-2023-PCM, que aprueba la Política Nacional de Transformación Digital al 2030, vigente desde el 28 de julio de 2023.
- Resolución Directoral N° 022-2022-INACAL/DN - Aprueban Normas Técnicas Peruanas sobre turismo, acuicultura y otros:
  - NTP-ISO/IEC 27001:2022: “Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de Gestión de la Seguridad de la Información. Requisitos. 3ª Edición”.
  - NTP-ISO/IEC 27002:2022. “Seguridad de la información, ciberseguridad y protección de la privacidad. Controles de seguridad de la información. 2ª Edición”.
  - NTP-ISO/IEC 27005:2022. “Seguridad de la información, ciberseguridad y protección de la privacidad. Orientación sobre la gestión de los riesgos de seguridad de la información. 3ª Edición” vigente desde el 12 de enero de 2023.
- Decreto Supremo N° 157-2021-PCM, que aprueba el Reglamento del Decreto de Urgencia N° 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital, vigente desde el 25 de setiembre de 2021.
- Decreto Supremo N° 029-2021-PCM, que aprueba el Reglamento del Decreto Legislativo N°1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo, vigente desde el 19 de febrero del 2021.
- Resolución Directoral N° 004-2020-INACAL/DN, que aprueba la NTP ISO/IEC 22301:2020. “Seguridad y resiliencia. Sistema de gestión de la continuidad de negocio. Requisitos. 1º Edición, vigente desde el 07 de abril de 2020.
- Resolución de Gerencia General N.º 0048-2020-IN-SALUDPOL-GG, que aprueba el Manual de Procedimientos (MAPRO) denominado Nivel 1: P.A.6.1: Gestión de Dirección y Administración de TI perteneciente a la Oficina de Tecnología de Información; P.A.6.2. Gestión de Soluciones y Desarrollo de TI; y P.A.6.3. Gestión de Servicios e Infraestructura de TI del SALUDPOL, vigente el 25 de febrero del 2020.
- Decreto de Urgencia N° 007-2020. Aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento, vigente desde el 09 de enero de 2020.
- Resolución de Secretaría de Gobierno Digital N° 004-2018-PCM/SEGDI que aprueban los “Lineamientos del Líder de Gobierno Digital”, vigente desde el 22 de diciembre de 2018.

- Resolución de Secretaría de Gobierno Digital N° 005-2018-PCM/SEGDI, que aprueban los Lineamientos para la formulación del Plan de Gobierno Digital, vigente desde el 22 de diciembre de 2018.
- Decreto Legislativo N.° 1412, que aprueba la Ley de Gobierno Digital. Vigente desde el 13 de setiembre del 2018.
- Resolución Directoral N° 014-2018-INACAL/DN - Aprueban Normas Técnicas Peruanas, Especificación Técnica Peruana y Reporte Técnico Peruano sobre cereales y menestras, gestión del riesgo y otras... NTP-ISO 31000:2018. Gestión del riesgo. Directrices. 2a Edición, vigente desde el 04 de julio de 2018.
- Decreto Supremo N° 050-2018-PCM - Aprueban la definición de Seguridad Digital en el ámbito nacional, vigente desde el 15 de mayo de 2018.
- Resolución Ministerial N.° 119-2018-PCM, que aprueba el Comité de Gobierno Digital, vigente desde 08 de mayo de 2018.
- Resolución Ministerial N.° 166-2017-PCM, “(...) Artículo 3.- Priorización del alcance del Sistema de Gestión de la Seguridad de la Información (...)”, vigente desde el 20 de junio del 2017.
- 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.

## VI.-TERMINOLOGÍA

- **Amenaza:**  
Causa potencial de un incidente de seguridad de la información no deseado, que puede resultar en un daño para la organización o el sistema.
- **Área Usuaría:**  
Forma parte de las unidades orgánicas de la entidad.
- **Continuidad:**  
Es un término que se refiere al vínculo que mantienen aquellas cosas que están, de alguna forma, en continuo.
- **Confianza Digital:**  
Es el estado que emerge como resultado de cuán veraces, predecibles, éticas, proactivas, transparentes, seguras, inclusivas y confiables son las interacciones digitales que se generan entre personas, empresas, entidades públicas o cosas en el entorno digital, con el propósito de impulsar el desarrollo de la economía digital y la transformación digital. Es un

componente de la transformación digital y tiene como ámbitos la protección de datos personales, la ética, la transparencia, la seguridad digital y la protección del consumidor en el entorno digital.

- **Copia no controlada:**

Todo documento impreso o digital libre de control.

- **Contingencia:**

Evento o suceso que ocurre, en la mayoría de los casos, en forma inesperada y que causa alteraciones en los patrones normales de funcionamiento de una organización.

- **Cuarto de comunicaciones:**

Ambiente donde se alojan los equipos que proveen de red e internet a todo SALUDPOL.

- **Endurecimiento:**

El hardening o endurecimiento de sistemas es una práctica de Ciberseguridad que sienta las bases de una infraestructura informática segura y ayuda a reducir el perfil de amenaza general, protegiendo así sus redes, hardware y datos valiosos.

- **Incidente:**

Circunstancia o suceso que sucede de manera inesperada y que puede afectar al desarrollo de una actividad. En el contexto informático, es una interrupción de las condiciones normales de operación en cualquier proceso informático en el SALUDPOL.

- **Infraestructura Tecnológica:**

Son los equipos que proveen todos los servicios de tecnología de información a SALUDPOL, estos están resguardados en un ambiente seguro, protegido contra el acceso al personal no autorizado y monitoreado por el personal especializado de la OTI.

- **Metodología de análisis de riesgos:**

Los métodos de análisis de riesgos son técnicas que se emplean para evaluar los riesgos de un proyecto o un proceso. Estos métodos ayudan a tomar decisiones que permiten implementar medidas de prevención para evitar peligros potenciales o reducir su impacto.

- **MTD (Maximum Tolerable Downtime):**

Es el tiempo Máximo Tolerable de caída, es decir es el tiempo límite máximo de indisponibilidad (incluido el tiempo de recuperación (RTO)), que se establece para señalar el momento en que se considera continuar con la actividad o restauración de productos y/o servicios de la entidad.

- **Norma:**

Regla que se debe seguir o a que se deben ajustar las conductas, tareas, actividades, etc. (RAE, 2023).

- **Oficial de Seguridad y Confianza Digital:**

Es el rol responsable de coordinar la implementación y mantenimiento del Sistema de Gestión de Seguridad de información (SGSI) en la entidad, atendiendo las normas en materia de Seguridad Digital, Confianza Digital, Transformación Digital y Gobierno Digital.

- **Plan de prevención:**

Es el conjunto de actividades orientadas a prevenir la presencia de un evento no deseado, con el propósito de disminuir y mitigar la probabilidad de ocurrencia de los escenarios identificados en el presente plan. El plan de prevención es la parte principal del Plan de Continuidad o de Contingencia TIC, porque permite aminorar y atenuar la probabilidad de ocurrencia de un estado de contingencia.

- **Plan de emergencia:**

Es el conjunto de actividades a realizar en el momento que se presenta el incidente y activa la contingencia como un mecanismo alterno que permitirá reemplazar a la actividad normal cuando este no se encuentra disponible.

- **Plan de Continuidad TIC o Plan de contingencia TIC (PCTIC):**

Es un documento que reúne un conjunto de procedimientos alternativos para facilitar el normal funcionamiento de las Tecnologías de Información y de Comunicaciones (TIC), cuando alguno de sus servicios se ha afectado negativamente por causa de algún incidente interno o externo a la organización. Este plan permite minimizar las consecuencias en caso de incidente en el SALUDPOL.

- **Plan de recuperación:**

Es el conjunto de actividades que tienen por objetivo restablecer oportunamente la capacidad de las operaciones, procesos y recursos del servicio que fueron afectados por un evento de contingencia.

- **Procedimiento:**

Acción de proceder. Método de ejecutar algunas cosas.

- **Probabilidad:**

Posibilidad de que un evento determinado ocurra en un periodo de tiempo dado.

- **Registro:**

Documento que presenta los resultados obtenidos o proporcione evidencia de las actividades desempeñadas.



- **Riesgo:**  
Posibilidad de que suceda algún evento adverso que tendrá un impacto sobre el cumplimiento de los objetivos institucionales o de los procesos para la presentación de servicios al ciudadano. Se expresa en términos de probabilidad y consecuencias.
- **ROL (Revised Operating Level):**  
Es el nivel mínimo de recuperación que debe tener una actividad para que la consideremos como recuperada, aunque el nivel de servicio no sea el óptimo.
- **RPO (Recovery Point Objective):**  
Este valor determina el impacto que tiene sobre la actividad la pérdida de datos. Este valor es crítico a la hora de determinar las políticas de copias de la organización, y no guarda relación con el RTO.
- **RTO (Recovery Time Objective):**  
Es el tiempo que lleva solucionar el incidente antes de que todos los sistemas y/o el servicio informático vuelvan a su normalidad.
- **Vulnerabilidad:**  
Debilidad de un activo o grupo de activos o controles, que pueden ser explotadas por una o varias amenazas. Una vulnerabilidad en sí misma no causa daños.

## VII.- METODOLOGÍA DE TRABAJO

La metodología para elaborar un plan de contingencia, generalmente incluyen identificar los riesgos, evaluar su recurrencia e impacto, definir las medidas preventivas y correctivas necesarias, establecer un equipo responsable de implementar el plan y realizar pruebas periódicas para asegurarse de que el plan esté actualizado y sea efectivo.

Para el desarrollo del plan se ha contemplado seis (6) fases:

FASE 1: Determinación del alcance.

FASE 2: Análisis de la entidad.

FASE 3: Determinación de la estrategia de continuidad.

FASE 4: Respuesta a la contingencia.

FASE 5: Definición y Ejecución del Plan de Pruebas.

FASE 6: Monitoreo.

## VIII.-DESARROLLO DE LAS FASES PARA LA ELABORACIÓN DEL PLAN DE CONTINUIDAD TIC

En este apartado se detallan los factores que se deben considerar para garantizar la continuidad de las operaciones TIC en SALUDPOL en circunstancias adversas, el cual implica las siguientes fases:

## 8.1. FASE 1: DETERMINACIÓN DEL ALCANCE

SALUDPOL tiene en su mapa general de procesos, los relacionados a la parte estratégica, los que refieren a los core o misionales y los de apoyo; el enfoque para la realización del Plan de Continuidad TIC en mención, será al recurso y servicio informático que soportan principalmente los procesos misionales de la entidad<sup>4</sup> del SALUDPOL, tal y como se aprecia a continuación:

Imagen. 1. Mapa de Procesos del SALUDPOL



Fuente: Resolución Ministerial N° 158-2019-IN y su modificatoria

En ese sentido, el Plan de Continuidad TIC involucra la **recuperación de recursos y servicios de Tecnología de la Información y Comunicaciones del SALUDPOL**, el cual incluye, los elementos referidos a los sistemas de información, redes y comunicaciones, bases de datos, equipos e instalaciones tecnológicas, personal, servicios y otros administrados por la Oficina de Tecnologías de la Información (OTI), direccionado a minimizar eventuales riesgos ante situaciones adversas que atentan contra el normal funcionamiento de los servicios informáticos de la entidad.

## 8.2. FASE 2: ANÁLISIS DE LA ORGANIZACIÓN

La Oficina de Tecnología de la Información es el área de donde proviene la dotación de los activos de información (recurso y/o servicio informático) para otras áreas o departamentos, los cuales necesitan ser salvaguardados para su respectiva continuidad, la misma que sustenta la elaboración del presente plan.

<sup>4</sup> Si bien, dentro del alcance se define en primera instancia tomar los procesos misionales de la IAFAS SALUDPOL, eso no exime a que también, de darse el caso, el Plan de Continuidad TIC, atienda a los procesos estratégicos o de apoyo por parte del equipo de Continuidad TIC, según el grado de afectación que se tenga, de acuerdo al escenario que se presente.

Imagen. 2. Estructura orgánica del SALUDPOL



Fuente: Anexo N° 01 de la Resolución Ministerial N° 1270-2019-IN, que modifica la Resolución Ministerial N° 158-2019-IN

De otro lado, según la Resolución de Ministerial (RM) N°158-2019-IN-SALUDPOL del 24 de enero de 2019, el cual aprueba el Manual de Operaciones del SALUDPOL, se detalla que la OTI, tiene las siguientes funciones que se relacionan con el presente Plan de Continuidad TIC, las cuales son:

“(…)

*a) Planificar, ejecutar, controlar, supervisar y evaluar los procesos, actividades y el control de riesgos en materia de su competencia, para el cumplimiento de sus objetivos, en el marco de las políticas y lineamientos dispuestos vigentes.*

*b) Diseñar, implementar y mantener los sistemas de información, infraestructura tecnológica y redes y comunicaciones, necesarios para el cumplimiento de los objetivos del SALUDPOL.*

*c) Mantener actualizada la plataforma informática y administrar los recursos informáticos, según necesidad de los diferentes órganos del SALUDPOL.*

(…)

*e) Formular y proponer las normas sobre la seguridad de los sistemas de información, red informática y de comunicaciones del SALUDPOL, implementando medidas para el respaldo de la información.*

*f) Ejecutar y evaluar las actividades y el uso de los recursos asignados para el cumplimiento de sus funciones, según la normatividad vigente.*

(…)

*i) Formular y proponer los documentos normativos y procedimientos técnicos en materia de su competencia.*

(…)”

De los procesos críticos que tiene SALUDPOL, se han identificado los siguientes activos de información:

### A) Activos de Información:

Del conjunto de procesos críticos, se han determinado los siguientes activos de información, denotando su nivel de importancia, los cuales se han tomado en cuenta para el presente análisis afín de identificar las posibles amenazas, vulnerabilidades y riesgos a los que se exponen, estos activos se detallan a continuación:

**Tabla. 1. Activos de información identificados en los procesos misionales de SALUDPOL**

Identificación del Activo						
Código del Activo	Tipo de Activo	Activo	Atributos del Activo Priorizado	Descripción del Activo	Nivel de importancia o prioridad del Activo	Propietario del Activo
ECO1-MON.SGSI-01-2023	Económico o monetario	Dinero	Disposición económica	Recurso económico relacionado al costo de la implementación del SGSI.	Alta	Alta Dirección/ Líder del Gobierno Digital.
HU01-DIR.SGSI-01/02-2023	Recurso Humano.	Usuario que utiliza el recurso y/o servicio informático.	Personal que forman parte de los procesos core y de las oficinas o departamentos.	Persona que se encarga de utilizar el recurso y/o servicio informático, que soportan los procesos del SALUDPOL.	Alta	Alta Dirección/ Jefe y/o Director de Oficina o Dirección.
HU02 RH-SGSI-02-2023	Recurso Humano	Usuario que dota el recurso y/o servicio informático.	Personal del área de OTI.	Persona que se encarga de brindar al recurso y/o servicio informático del SALUDPOL.	Alta	Alta Dirección/ Jefe de la OTI
IF03-SGSI-01-2023	Infraestructura Física	Zona o ambiente	Ambientes físicos de los procesos core y demás instalaciones de las áreas.	Forma parte de la Infraestructura física en donde se aloja a los activos de información de los procesos core del SALUDPOL.	Alta	Alta Dirección/ Gerente/Director de cada área.
HW02-SGSI-01-2023	Hardware	Pc que utiliza el personal	Hardware que se utiliza dentro de los procesos core y otros.	Pc que se utiliza para acceder a los aplicativos y/o sistemas del SALUDPOL.	Alta	Alta Dirección/ Jefe y/o Director de Oficina o Dirección.
SE03-SEL.SGSI-01-2023	Servicio: Eléctrico	Suministro de energía eléctrica	Servicio que se utiliza dentro de los procesos core.	Servicio que se utiliza para el encendido de equipos de cómputo y demás activos físicos de información.	Alta	Alta Dirección/ Jefe y/o Director de Oficina o Dirección.
SE02-IYC.SGSI-01-2023	Servicio de comunicación	Servicio de conexión a internet	Servicio de red y comunicaciones, que se utiliza dentro de los procesos core.	Servicio que se utiliza para brindar conectividad a los equipos de cómputo y demás activos de red y comunicaciones que dan soporte a la información.	Alta	Alta dirección/ Jefe de la OTI.
RYC9-CAB.SGSI-1-2023	Red y Comunicaciones	Cableado de red	Componente de red y comunicaciones, que se utiliza dentro de los procesos core	Cable coaxial de Categoría - 6, que se utiliza para la interconexión entre los puntos de red de cada PC y los equipos de red y comunicaciones tales como Switch, Router, etc.	Mediana	Alta dirección/ Jefe de la OTI.
RYC1-SCH.SGSI-01-2023	Red y Comunicaciones	Switch de comunicaciones	Dispositivo que permite interconectar redes informáticas. El Switch es un dispositivo que permite que la conexión de computadoras y periféricos a la red para que puedan comunicarse entre sí y con otras redes.	Ubicado en el Rack de comunicaciones de la infraestructura tecnológica de la entidad, así como de las diferentes sedes de la entidad a nivel nacional.	Alta	Alta dirección/ Jefe de la OTI.

Identificación del Activo						
Código del Activo	Tipo de Activo	Activo	Atributos del Activo Priorizado	Descripción del Activo	Nivel de importancia o prioridad del Activo	Propietario del Activo
			Componente de red y comunicaciones, que se utiliza para soportar la conectividad referida a los recursos y servicios tecnológicos que soportan los procesos Core de la entidad.			
RYC2-SCH.SGSI-01-2023	Red y Comunicaciones	Router	Componente de red y comunicaciones, que se utiliza dentro de los procesos core	Ubicado en el Rack de comunicaciones de la infraestructura tecnológica de la entidad, así como de las diferentes sedes de la entidad a nivel nacional. sirve para la interconexión a internet que alimenta a todas las Pcs de las oficinas, en aras del Soporte de los procesos misionales del SALUDPOL.	Alta	Alta Dirección/ Proveedor OPTICAL NETWORKS S.A.C.
SW01-SRV.SGSI-01-2023	Software	Servidor virtual	Componente de red que soporta los procesos core de la institución.	Servidor virtual que se encuentra en la nube y que aloja a los Sistemas de Información.	Alta	Alta Dirección/ Jefe de la OTI.
SW03-SIN.SGSI-01-2023	Software	Sistemas de Información	Sistemas de información que forma parte de los procesos core de SALUDPOL	Sistemas de información que gestionan los procesos del SALUDPOL.	Alta	Alta Dirección/ Jefe y/o Director de Oficina o Dirección.
SW03-APW.SGSI-01-2023	Software	Sistemas de Información	Aplicaciones Web que se relacionan con los procesos core de SALUDPOL	Aplicaciones Web, que permiten realizar diferentes consultas o extracción y/o registro de la información a las diferentes Base de Datos que tiene SALUDPOL.	Alta	Alta Dirección/ Jefe y/o Director de Oficina o Dirección.
SW07-BD.SGSI-01-2023	Software	Base de datos	Base de datos que guardan la información de los procesos core de la entidad	Conjunto de registros de datos que contiene información producto su tratamiento en los sistemas que soportan los procesos core del SALUDPOL	Alta	Alta Dirección/ Jefe y/o Director de Oficina o Dirección.

Fuente: Elaboración realizada por la OTI del SALUDPOL

De la misma forma, se ha identificado las siguientes amenazas y riesgos los cuales se detallan:

## B) Amenazas

Se ha identificado en primera instancia aquellas amenazas que pudieran aprovechar las vulnerabilidades que tienen los activos de información en el proceso core del alcance, en el SALUDPOL, considerando la ubicación geográfica, el contexto actual y los activos que se relacionan con la infraestructura tecnológica.

**Tabla. 2. Amenazas identificadas en la evaluación de riesgos**

Ítem	Amenaza	Tipo
1	*Restricción del presupuesto. *Cambios de Gestión.	Económico
2	* Infección viral crónica o grave. *Situación pandémica.	Sanitaria

Ítem	Amenaza	Tipo
	*Fallecimiento.	
3	Documentación Excesiva	Información
4	Desastres naturales/ambientales o los provocados por el hombre (Terremoto o sismo, Tsunami, Corriente del niño, Humedad, Incendio, explosiones, etc.)	Siniestros naturales o provocados por el hombre
5	Dispositivos o componente inadecuados, con fallas o con un límite de capacidad	Tecnológico
6	Altas Temperaturas extremas del medio ambiente	Ambiental
7	Virus informático (Ransomware, Troyanos, etc.)	Tecnológico
8	Cortes de energía eléctrica	Físico
9	Ataque físico a las torres o instalaciones incluso satelitales, de donde se provee la conectividad	Tecnológico
10	Sobrecarga de energía	
11	Agentes externos: Intemperie, óxido de hierro, envejecimiento, proyección de partículas incandescentes.	Tecnológico
12	Ataque de Manipulación de STP (Spanning Tree Protocol)	Tecnológico
13	Ataque: Escaneo de Puertos	Tecnológico
	Accesos con privilegios incorrectos	Tecnológico
14	Ataque de Inyección SQL.	Tecnológico
15	Inconsistencias en el guardado de datos	Tecnológico
16	*Ataque Distribuido de Denegación de Servicio DDOS. *Alto tráfico de datos.	Tecnológico

Fuente: Elaboración realizada por la OTI del SALUDPOL.

### C) Probabilidad de ocurrencia

Es la cuantificación de que ocurra o se produzca una determinada amenaza, realmente. Para el cálculo de probabilidad utilizaremos la siguiente tabla:

**Tabla. 3. Nivel de Valoración de la ocurrencia de las amenazas**

PROBABILIDAD				
Improbable	Ocasional	Posible	Probable	Recurrente
1	2	3	4	5
Se puede presentar al menos una vez en 5 años o más	Se puede presentar al menos una vez en 3 años o más	Se puede presentar al menos una vez en 2 años	Se puede presentar al menos una vez al año	Se puede presentar más de 1 vez cada seis meses

Fuente: Elaboración realizada por la OTI del SALUDPOL.

### D) Identificación del Impacto

El impacto del riesgo mide la gravedad o magnitud del efecto adverso a causa de la ocurrencia de la amenaza. Es una calificación aplicada a la amenaza, para describir el grado de afectación. La medición puede ser cualitativa o cuantitativa.

Para nuestro caso, la clasificación del impacto será en una escala 1 al 5 categorizando desde el nivel insignificante hasta el estado catastrófico, tal como se muestra en la siguiente tabla:

**Tabla. 4. Nivel de impacto del riesgo ante la posible**

IMPACTO		
1.Insignificante	1	No representa un impacto importante. Se cuenta con controles suficientes que responden a un programa de mantenimiento (evaluado y mejorado), se evidencia que han respondido a acontecimientos ocurridos y ejercicios realizados, se puede prescindir del activo o servicio por un tiempo limitado.
2.Moderado	2	El impacto sobre la confidencialidad, integridad y disponibilidad de la información es moderado en tiempo y alcance. Su efecto para una actividad específica puede subsanarse en corto plazo.
3.Serio	3	El impacto sobre la confidencialidad, integridad y disponibilidad de la información es limitado en tiempo y alcance. Su efecto es para una actividad específica que puede subsanarse en corto plazo.
4.Critico	4	Impacta en forma grave al activo, se puede llegar a comprometer documentos internos clasificados como confidenciales, paralizar o retrasar procesos claves por un tiempo considerable.
5.Catastrófico	5	Impacta en forma severa paralizando el accionar en todo el SALUDPOL y su efecto no solo se limita a éste, compromete la confidencialidad o integridad de información.

Fuente: Elaboración realizada por la OTI del SALUDPOL.

#### E) Identificación del nivel de riesgo

Es así que, teniendo en cuenta los patrones de valoración antes descritos, se describió la matriz de riesgo, dependiendo de la probabilidad de ocurrencia de la amenaza y nivel de impacto al aprovechar la vulnerabilidad, el riesgo adopta un respectivo color tal y como se detalla:

**Tabla. 5. Matriz de riesgo para determinar el nivel de afectación a la entidad**

MATRIZ DE RIESGO						
		PROBABILIDAD				
		Improbable	Ocasional	Posible	Probable	Recurrente
IMPACTO		1	2	3	4	5
Insignificante	1	1	2	3	4	5
2.Moderado	2	2	4	6	8	10
3.Serio	3	3	6	9	12	15
4.Critico	4	4	8	12	16	20
5.Catastrófico	5	5	10	15	20	25

Fuente: Elaboración realizada por la OTI del SALUDPOL.

La interpretación de cada cuadrante de calor o nivel de riesgo de la ocurrencia de la amenaza y el impacto que causa en la evaluación, se detalla a continuación:

**Tabla. 6. Descripción del nivel de riesgo**

GRADO	NIVEL DE RIESGO	DESCRIPCIÓN
1 al 4	ACEPTABLE	Riesgo aceptable, sin revisión y no se requieren acciones.
5 al 9	TOLERABLE	Riesgo tolerable con revisión del Jefe de la OTI, y se evalúa tomar acciones.
10 al 12	ALTO	Riesgo no aceptable, se requiere de una acción correctiva, pero se permite planificar plazos y compromisos.
15 al 25	EXTREMO	Riesgo no aceptable, se requiere acción correctiva inmediata.

Fuente: Elaboración realizada por la OTI del SALUDPOL.

De lo anteriormente descrito se identificó para los procesos misionales de SALUDPOL los siguientes riesgos:

**Tabla. 7. Evaluación de riesgos del SALUDPOL**

N°	Identificación del Activo		Identificación del Riesgo			Valorización del Riesgo
	Código del Activo	Activo	Amenaza	Vulnerabilidad	Descripción del Riesgo Identificado	Nivel o Valor del Riesgo
1	ECO1-MON.SGSI-01-2023	Dinero	*Restricción del presupuesto. *Cambios de Gestión.	Falta de sustento y/o concientización en la importancia de la Implementación del SGSI.  Inestabilidad organizacional.	Extinción del presupuesto para implementación del SGSI	EXTREMO
2	HU01-DIR.SGSI-01/02-2023	Usuario que utiliza el recurso y/o servicio informático.	* Infección viral crónica o grave.  *Situación pandémica.  *Fallecimiento.	Falta de personal alternativo para la ejecución del proceso o procedimiento.	Posibilidad de que exista alguna infección viral crónica, grave o situación pandémica o fallecimiento del personal, que ocasione <b>paralización en la ejecución del proceso o procedimiento de forma habitual</b> , por falta de personal alternativo que pueda suplir dichas funciones.	EXTREMO
3	HU02 RH-SGSI-02-2023	Usuario que dota el recurso y/o servicio informático	Documentación Excesiva	Contratación insuficiente de personal adicional como apoyo en la ejecución del proceso o procedimiento	Probabilidad de que llegue excesiva documentación, que ocasione <b>desatención por parte de la persona que se encarga de la recepción y/o tratamiento de documentos</b> , debido a la contratación insuficiente de personal adicional como apoyo en la ejecución del proceso o procedimiento.	EXTREMO
4	IF03-SGSI-01-2023	Zona o ambiente	Desastres naturales/ambientales o los provocados por el hombre (Terremoto, Tsunami, Corriente del niño, Humedad, Incendio, explosiones, etc.)	Infraestructura física construida con material de Drywall, el cual, no es apropiado, en relación al lugar o ubicación del terreno, ya que dicho material, está sometido a un mayor porcentaje de humedad y otros.	Posibilidad de que ocurran desastres naturales/ambientales o los provocados por el hombre, las cuales <b>dañen a la entidad en su infraestructura física</b> construida en su mayoría, con material de Drywall, el cual, no es apropiado en referencia al lugar o ubicación del terreno, sometido a un mayor porcentaje de humedad y otros.	EXTREMO
5	IF03-SGSI-01-2023	Zona o ambiente	Desastres naturales/ambientales o los provocados por el hombre (Terremoto, Tsunami, Corriente del niño, Humedad, Incendio, explosiones, etc.)	Ambientes físicos que no cuentan con zonas de seguridad	Probabilidad de que ocurran desastres naturales/ambientales o provocados por el hombre que <b>dañen a los activos de información</b> , ante la Inexistencia de zonas seguras.	EXTREMO
6	HW02-SGSI-01-2023	Pc que utiliza el personal	Dispositivos o componente inadecuados, con fallas o con un límite de capacidad	Dimensionamiento (Sizing) inadecuado de las partes internas de la Pc.	Posible falla física en la Memoria RAM y/o tarjeta de video de la PC, ocasionan la <b>ralentización o demora en el rendimiento de la misma</b> , en el desarrollo de los procesos, debido a un dimensionamiento inadecuado acorde a los requerimientos del usuario.	EXTREMO



N°	Identificación del Activo		Identificación del Riesgo			Valorización del Riesgo
	Código del Activo	Activo	Amenaza	Vulnerabilidad	Descripción del Riesgo Identificado	Nivel o Valor del Riesgo
7	HW02-SGSI-01-2023	Pc que utiliza el personal	Altas Temperaturas extremas del medio ambiente	Falta de mantenimiento a los ventiladores u otro componente de la PC que utiliza el usuario.	Probabilidad de que genere algún <b>sobrecalentamiento de componentes internos de la PC</b> que utiliza el usuario, <b>que genere paralización temporal de la continuidad de las operaciones</b> , debido a las altas temperaturas extremas provenientes del medio ambiente, ante la falta de mantenimiento a los ventiladores u otro componente interno de dicha PC.	EXTREMO
8	HW02-SGSI-01-2023	Pc que utiliza el usuario	Virus informático (Ramsonware, Troyanos, etc.)	Falta de antivirus actualizado y/o parches de actualización en el Sistema Operativo de la PC.	Posibilidad de que exista una intrusión en la red a causa de un virus informático, que infecte el Sistema operativo, aplicaciones y/o el sistema de archivos de la PC del usuario, por la falta de antivirus actualizado <b>causando incluso pérdida o fuga de información.</b>	ALTO
9	SE03-SEL.SGSI-01-2023	Suministro de energía eléctrica	Cortes de energía eléctrica	Falta de Grupo Electrónico y/o UPS	Probabilidad de que ocurra un corte de energía eléctrica en cualquier momento y <b>los procesos y/o procedimiento se paralicen</b> , esto debido a la falta de Grupo Electrónico y/o UPS, que salvaguarde la continuidad de las operaciones.	EXTREMO
10	SE03-SEL.SGSI-01-2023	Suministro de energía eléctrica	Sobrecarga de energía	Falta de ampliación de Potencia del suministro eléctrico.	Probabilidad de que ocurra una sobrecarga de energía por conexión de equipos adicionales, que conlleven a un <b>corte del suministro eléctrico</b> , propiciando que los procesos y/o procedimiento se paralicen, esto debido a la falta de ampliación de potencia en el suministro eléctrico.	ALTO
11	SE02-IYC.SGSI-01-2023	Servicio de conexión a internet	Ataque físico a las torres o instalaciones incluso satelitales, de donde se provee la conectividad	Falta de monitorización continua por parte del personal de Redes y Comunicaciones de OTI.	Probabilidad de que se perpetre un ataque físico a las torres o instalaciones incluso satelitales, de donde se provee la conectividad a la página de SALUDPOL, provocando la caída del servicio web, trayendo como consecuencia <b>la suspensión del servicio, pérdida de reputación, así como pérdidas económicas y robo de datos</b> , esto por la falta de monitorización continua por parte del personal de Red y Comunicaciones de OTI.	EXTREMO
12	RYC9-CAB.SGSI-1-2023	Cableado de red	Agentes externos: Intemperie, óxido de hierro, envejecimiento, proyección de partículas incandescentes.	Falta de canaletas físicas para protección de los cables de red.	Posibilidad de que exista exposición de los cables de red, ante la falta de canaletas físicas de protección y eso traiga deterioro en dichos cables que <b>no permita la conexión de forma adecuada.</b>	TOLERABLE
13	RYC1-SCH.SGSI-01-2023	Switch de comunicaciones	Ataque de Manipulación de STP (Spanning Tree Protocol)	Inadecuada configuración del switch.	El Ataque de Manipulación del STP, es propenso a manifestarse si no se tiene una adecuada configuración del Switch, ya que la seguridad básica del Switch no evita los ataques malintencionados. Por ello es necesario hacer cambios en la configuración de los Switches, <b>a fin de evitar accesos no autorizados.</b>	TOLERABLE

N°	Identificación del Activo		Identificación del Riesgo			Valorización del Riesgo
	Código del Activo	Activo	Amenaza	Vulnerabilidad	Descripción del Riesgo Identificado	Nivel o Valor del Riesgo
14	RYC2-SCH.SGS I-01-2023	Router	Ataque: Escaneo de Puertos	Inadecuada configuración del router.	Probabilidad de que se tenga un ataque de escaneo de puertos que afecte al/los Router(s), por no contemplar una adecuada configuración del dispositivo la cual no permite controlar las conexiones entrantes y los dispositivos conectados por medio de un filtrado MAC, manteniendo un firewall activado e ir controlando los puertos abiertos, generando como consecuencia el robo de la información, credenciales y ofreciendo una entrada para controlar dispositivos conectados a una red.	TOLERABLE
15	SW01-SRV.SGS I-01-2023	Servidor virtual	Accesos con privilegios incorrectos	No se gestionan los usuarios de cuentas Privilegiadas. Claves de usuario de administrador de servidores no protegidas.	Probablemente, si no se tiene la gestión de cuentas privilegiadas, la información que se encuentra en los servidores, puede ser violada por ellos mismos, sin tener rastros de auditoría, ocasionando <b>manipulación o robo de información.</b>	ALTO
16	SW03-SIN.SGSI -01-2023	Sistemas de Información	Ataque de Inyección SQL	<p>*No se implementa un desarrollo de código seguro de las aplicaciones Web correspondiente.</p> <p>*No se realizan copias de seguridad diariamente.</p> <p>No se cuentan en los sistemas con módulos y/o reportes de auditoría.</p>	El sistema, esta propenso a recibir un ataque de inyección SQL, el cual inyecta líneas de código SQL maliciosas en la propia aplicación web obteniendo acceso parcial o completa a los datos de la BD, para la <b>extracción, modificación o robo de información</b> , debido a que los desarrolladores web, no siguen las recomendaciones basadas en el diseño o desarrollo de código seguro generando que la información pierda su integridad, confidencialidad y disponibilidad y más aún si no se generan copias de seguridad de dicha data diariamente, así como no se cuenta con módulos y/o reportes de auditoría que pueda conllevar a revisar por los propietarios de la información.	EXTREMO
17	SW03-SIN.SGSI -01-2023	Sistema de Información	Inconsistencias en el guardado de datos	<p>*En el desarrollo de código fuente en algunos sistemas, no se direcciona adecuadamente a la BD para las funcionalidades con las que fue creado, ni mucho menos se tienen campos definidos para interoperar.</p> <p>*No se tiene una metodología de desarrollo para guiar el proceso de desarrollo de Software.</p> <p>*No se cuenta con una integración de los sistemas.</p> <p>*Manuales de usuario desactualizados.</p>	Es posible que sea recurrente las inconsistencias en el guardado de datos reflejados en otro sistema, si no se direcciona correctamente a la BD del sistema actual con quien se interactúa, y/o se tiene la intención de integrar los sistemas, con una metodología que se estandarice para el desarrollo de software, en donde se tenga inmerso las buenas prácticas de código seguro (Por ejemplo OWASP, etc.), así como gestionar una normalización de la BD, junto con un buen desarrollo de código seguro, actualizando de forma paralela los manuales de usuario, que nos permiten entender e interpretar el uso de los sistemas, todo ello para <b>evitar una mala reputación y pérdidas de dinero en SALUDPOL.</b>	EXTREMO
18	SW03-SIN.SGSI -01-2023	Sistema de Información	Inconsistencias en el guardado de datos.	<p>*No se cuenta con la integración de sistemas.</p> <p>*No se tiene una metodología de desarrollo de Software.</p>	Es posible que sea recurrente el tema de las inconsistencias en el guardado de datos, si no se direcciona y gestiona una normalización de la BD, junto con la utilización de una metodología de desarrollo de software desde la creación de los proyectos de implementación,	EXTREMO

N°	Identificación del Activo		Identificación del Riesgo			Valorización del Riesgo
	Código del Activo	Activo	Amenaza	Vulnerabilidad	Descripción del Riesgo Identificado	Nivel o Valor del Riesgo
					<b>propiciando una mala reputación al SALUDPOL.</b>	
19	SW03-SIN.SGSI-01-2023	<b>Sistemas de Información</b>	*Ataque Distribuido de Denegación de Servicio DDOS.  *Alto tráfico de datos.	*Falta de cambios o actualizaciones seguras, que se deben de realizar en los sistemas/ página web y demás plataformas conexas.	Probabilidad de que se perpetre un ataque DDOS a la página de SALUDPOL, provocando la caída del servicio web, trayendo como consecuencia <b>la suspensión del servicio, pérdida de reputación, así como pérdidas económicas y robo de datos</b> , esto por la falta de cambios o actualizaciones seguras, que se deben de realizar en los sistemas/ página web y demás plataformas conexas.  Asimismo, podría ocurrir la probabilidad de recurrencia de que surja un alto tráfico de datos que conlleven a la caída del sistema en entorno web o de la página web, por falta de monitorización continua por parte del personal de Red y Comunicaciones de OTI.	EXTREMO
20	SW07-BD.SGSI-01-2023	<b>Base de datos</b>	Ataque de Inyección SQL	*No se implementa un desarrollo seguro de las aplicaciones Web que soportan la BD correspondiente. * No se realizan copias de seguridad diariamente	La Base de Datos, esta propensa a recibir un ataque de inyección SQL, el cual inyecta líneas de código SQL maliciosas en la propia aplicación web obteniendo <b>acceso parcial o completa a los datos de la BD, para la extracción, modificación o robo de información</b> , debido a que los desarrolladores web, no siguen las recomendaciones basadas en el diseño seguro y/o desarrollo de código seguro generando que la información pierda su integridad, confidencialidad y disponibilidad y más aún si no se generan copias de seguridad de dicha data diariamente.	EXTREMO
21	SW07-BD.SGSI-01-2023	<b>Base de datos</b>	Inconsistencias en el guardado de datos	* No se tiene una normalización de la BD mencionado. * No se cuenta con diccionario de datos	Es posible que sean recurrente las inconsistencias en el guardado de datos, si no se direcciona y gestiona una normalización de la BD, y se implemente un diccionario de datos actualizado, que nos permiten entender e interpretar un conjunto de datos o base de datos al proporcionar información básica sobre los campos o variables que contiene, <b>generando nuevo código confuso.</b>	ALTO
22	SW07-BD.SGSI-01-2023	<b>Base de datos</b>	Virus informático (Ransomware, Troyanos, etc.)	No se realizan copias de seguridad diariamente y que las mismas sean restablecidas mediante cronogramas correspondientes a modo de prueba y cuando suceda un incidente grave o catastrófico.	Posibilidad de que exista una intrusión en la red a causa de un virus informático, <b>que infecte las BD</b> y peor aún si no se tienen generadas copias de seguridad diarias, <b>propiciando la pérdida de la información.</b>	ALTO

Fuente: Elaboración realizada por la OTI del SALUDPOL

A partir de la reflexión sobre los impactos, se identificaron actividades relacionadas con los procesos misionales del SALUDPOL, definiendo con los órganos, los indicadores de máximo tiempo tolerable de interrupción (MTD), impactos para cada actividad crítica, esencial y relevante, lo cual

sirvió como factor principal para clasificar las actividades según el nivel de criticidad y determinándose los tiempos objetivos de recuperación (Tiempo Objetivo de Recuperación – RTO).

### 8.3. FASE 3: DETERMINACIÓN DE LA ESTRATEGIA DE CONTINUIDAD

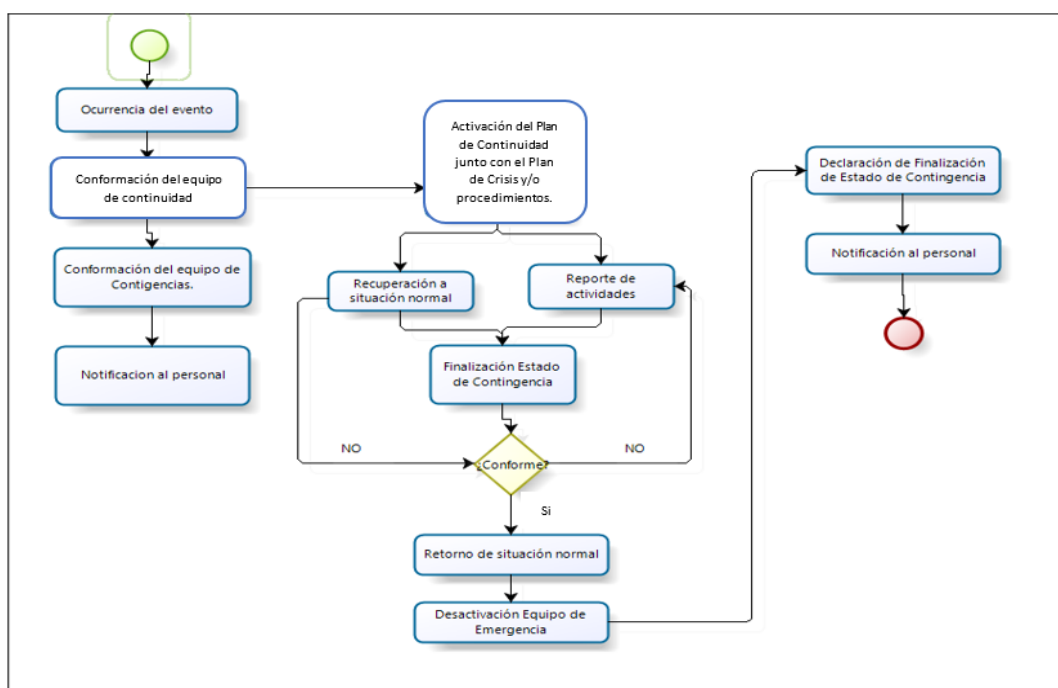
SALUDPOL, establece en su estrategia de continuidad de las tecnologías de la información bajo las siguientes precisiones:

#### 8.3.1. Establecer el proceso general de continuidad ante una contingencia

Para ello se tiene que tomar en cuenta, el inicio de identificación del estado de emergencia, y quién será el responsable de declarar dicho estado, para la parte informática, el responsable será el Jefe de la OTI o quien él designe formalmente para dicha responsabilidad, para comunicar las decisiones, se utilizarán los canales establecidos en SALUDPOL.

A continuación, se establece el diagrama del proceso de continuidad ante una contingencia en SALUDPOL:

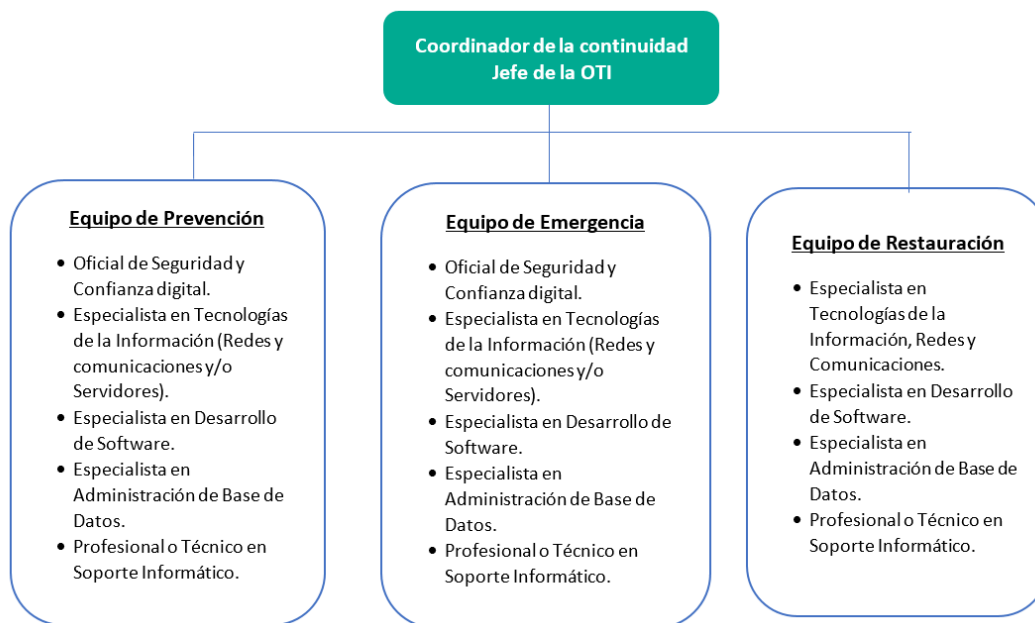
**Imagen. 3. Proceso de continuidad ante una Contingencia Informática**



#### 8.3.2. Organización operativa del Plan de Continuidad TIC

Para el funcionamiento del presente plan, se ha establecido la siguiente organización operativa, basada en roles, lo cuales estarán sujetas a los puestos contemplados en el Manual de Clasificador de Cargos del SALUDPOL, aprobado por Resolución de Gerencia General N.° 167-2019-IN-SALUDPOL-GG y a los cambios que se puedan realizar en la normativa interna y externa, conformado exclusivamente por personal de la OTI de SALUDPOL.

**Imagen. 4. Organizativa funcional para el Plan de Continuidad de TIC del SALUDPOL**



La relación del personal de los equipos de trabajo que forma parte del Plan de Continuidad TIC debe ser actualizada de manera permanente y socializada a los siguientes:

- ❖ Personal de la OTI.
- ❖ Alta Dirección.
- ❖ Equipo técnico de la Seguridad Física.

Las actividades planificadas como parte del presente plan, podrán ejecutarse en forma presencial, semipresencial o en remoto, conforme a los escenarios que pudieran darse ante los diversos eventos de mayor impacto considerados para el presente Plan de Continuidad TIC, así como, conforme a las disposiciones vigentes.

A continuación, se detallan los perfiles del personal que participará:

#### **a) DEL COORDINADOR DE LA CONTINUIDAD**

Este rol está a cargo del Jefe de la OTI o quien lo represente, el cual, ante una contingencia, tiene las siguientes funciones:

- ❖ Coordinar, dirigir y decidir respecto a acciones o estrategias a seguir en un escenario de contingencia dado.
- ❖ Monitorear y/o supervisar y vigilar la recuperación de la infraestructura de TI.
- ❖ Tomar la decisión de activar el Plan de Continuidad TIC.
- ❖ Guiar y supervisar a los equipos operativos de continuidad TIC, en el desarrollo de sus actividades.

- ❖ Evaluar la extensión de la contingencia y sus consecuencias potenciales sobre la infraestructura tecnológica.
- ❖ Notificar y mantener informados a los miembros de la Alta Dirección acerca del evento de desastre, el progreso de la recuperación y posibles problemas ocurridos durante la ejecución del plan.
- ❖ Coordinar con la Oficina de Administración para el reemplazo de hardware, software y/o activación para los servicios de TIC afectados.
- ❖ Declarar el evento de término de la ejecución de las operaciones del Plan de Continuidad TIC cuando las operaciones hayan sido restablecidas.
- ❖ Presentar un informe a la Gerencia General explicando las actividades u operaciones de tecnologías de la información afectadas y las acciones tomadas.

## **b) DEL EQUIPO DE PREVENCIÓN**

Es el encargado de ejecutar las acciones preventivas antes que ocurra un siniestro o desastre. Su finalidad es evitar la materialización y tener todos los medios requeridos para que los equipos de Emergencia y de Restauración puedan realizar la recuperación de los servicios de tecnologías de la información y comunicaciones, en el menor tiempo posible.

A continuación, se detallan las funciones por cada integrante del Equipo de Prevención:

### **b.1) Oficial de Seguridad y Confianza Digital**

- ❖ Evaluar y/o proponer los procedimientos de seguridad de los servicios de TIC a la OTI, así como los de restauración de información base de datos, código fuentes y ejecutables, gestión de incidentes, entre otros, y supervisar los mismos.
- ❖ Participar en la realización de las pruebas de restauración del hardware y software y relacionados con la temática informática.
- ❖ Participar en las pruebas y simulacros de desastres.
- ❖ Verificar la realización del mantenimiento preventivo a la infraestructura de TI.
- ❖ Participar en el monitoreo de la red y proponer las medidas preventivas para minimizar o evitar las contingencias informáticas en SALUDPOL.
- ❖ Desarrollar planes de sensibilización en materia de seguridad de la información y confianza digital aunado a las buenas prácticas en el uso de los sistemas informáticos.
- ❖ Recomendar a las diferentes unidades u órganos del SALUDPOL determinar los procedimientos que les permitan continuar con las actividades esenciales ante la ausencia o inoperatividad de los servicios TIC.

### **b.2) Especialista en Tecnologías de la Información (Redes y comunicaciones y/o Servidores)**

- ❖ Monitorear la red y el funcionamiento de los servidores.
- ❖ Mantener actualizado el inventario del hardware y software.

- ❖ Coordinar oportunamente las actualizaciones de los servidores.
- ❖ Acoplar las copias de respaldo y clasificarlas por base de datos, aplicativos y sistemas de información.
- ❖ Elaborar informes técnicos de conformidad, luego de cada mantenimiento efectuado, así como elaborar informes periódicos del funcionamiento de la infraestructura de TI.
- ❖ Verificar el estado de las garantías y/o licencias de los componentes de la plataforma tecnológica, los cuales estén acordes y actualizados con las fechas correspondientes.
- ❖ Monitorear el funcionamiento de la Central Telefónica.
- ❖ Realizar revisiones de obsolescencia tecnológica de los servidores y equipos de telecomunicación de forma anual.
- ❖ Gestionar las copias de respaldo de los servidores, así como realizar la restauración de los mismos, teniendo en cuenta el cronograma establecido en coordinación con el Oficial de Seguridad y Confianza Digital y el Jefe de la OTI.

#### **b.3) Especialista en Desarrollo de Software**

- ❖ Llevar un control y/o un inventario del activo de información software de forma más detallada, a fin de contemplar el número de sistemas de información y su conceptualización, para ello Se detalla en el “Anexo II: Inventario de Sistemas de Información del SALUDPOL vigente”, todos los sistemas actuales que tiene SALUDPOL.
- ❖ Verificar que los desarrollos de software sean realizados teniendo en cuenta la normativa vigente y la metodología que se establezca, así como se apliquen las buenas prácticas del desarrollo seguro.
- ❖ Realizar copias de respaldo de los aplicativos y sistemas de información de la entidad, y llevar un control de las versiones.
- ❖ Llevar un control de cambios de los mantenimientos y/o cambios realizados a los sistemas de información.
- ❖ Revisar la documentación, consolidación, actualización y validación de los manuales de los sistemas en producción, según corresponda.
- ❖ Realizar periódicamente las pruebas de restauración de los sistemas de información en producción de la entidad según el cronograma que establecerán.

#### **b.4) Especialista en Administración de Base de Datos.**

- ❖ Monitorear y revisar el funcionamiento interno de los servidores virtuales existentes y preparar los mismos para el reinicio en el caso se requiera.
- ❖ Realizar el hardening de las bases de datos

- ❖ Realizar copias de respaldo de las bases de datos y llevar un control de dichas copias.

#### **b.5) Profesional o Técnico en Soporte Informático.**

- ❖ Mantener actualizada la lista de anexos y teléfonos.
- ❖ Mantener actualizado el inventario hardware y software del usuario final.
- ❖ Verificar el estado de las garantías y/o vigencias tecnológicas de los equipos informáticos de usuario final.

### **c) DEL EQUIPO DE EMERGENCIA**

Este equipo es el encargado de ejecutar las actividades requeridas durante la materialización del siniestro o desastre. Su finalidad es mitigar su impacto sobre los equipos tecnológicos y de la información del SALUDPOL, procurando salvaguardar su pérdida o deterioro.

Por ende, se mencionan las actividades que se realizarán durante la contingencia, según los miembros del equipo:

#### **c.1) Oficial de Seguridad y Confianza Digital**

- ❖ Apoyar en las labores de verificación y validación de operación de los servicios de TIC.

#### **c.2) Especialista en Tecnologías de la Información (Redes y comunicaciones y/o Servidores)**

- ❖ Informar el desastre o incidencia al coordinador de continuidad TIC.
- ❖ Ejecutar las actividades de emergencia detalladas en el Plan de Continuidad TIC, de acuerdo con el escenario de riesgo presentado.
- ❖ Realizar la evaluación de condiciones de la infraestructura de TI del SALUDPOL, durante la emergencia.
- ❖ Comunicar al Coordinador de la continuidad sobre las acciones de emergencia ejecutadas.
- ❖ Realizar la evaluación de las condiciones de la información almacenada en los diferentes sistemas durante la emergencia.
- ❖ Ejecutar las acciones de emergencia detalladas en el Plan de continuidad TIC y restauración relacionada a la central telefónica instalada en el SALUDPOL de acuerdo con el escenario de riesgo presentado.
- ❖ Ejecutar las acciones de emergencia detalladas en el Plan de continuidad TIC y restauración relacionada a la central telefónica instalada en el SALUDPOL de acuerdo con el escenario de riesgo presentado.



### **c.3) Especialista en Desarrollo de Software**

- ❖ Realizar las labores de verificación y validación de operación relacionadas a los sistemas de información junto con las bases de datos instalados y ejecutados en el entorno de Producción.
- ❖ Realizar la evaluación de las condiciones de los aplicativos informáticos y sistemas de información durante la emergencia.
- ❖ Apoyar en las acciones que se requieran.

### **c.4) Especialista en Administración de Base de Datos.**

- ❖ Realizar la evaluación de las condiciones de la información almacenada en las diferentes bases de datos durante la emergencia.
- ❖ Levantar la última copia guardada en relación a la Base de Datos, en el caso se haya dañado la data o la información que tiene inmersa, esto en coordinación con el Oficial de Seguridad y Confianza Digital y el Coordinador de la Continuidad.
- ❖ Registrar los eventos que ocurren en el restablecimiento de la data que se restaure.

### **c.5) Profesional o Técnico en Soporte Informático.**

- ❖ Apoyar en la evaluación de condiciones de los equipos de telecomunicaciones durante la emergencia.
- ❖ Realizar la evaluación preliminar de la afectación a los equipos informáticos de usuario final (computadoras, teléfonos, impresoras, entre otros) así como actualizar el registro de las incidencias presentadas en el mismo.
- ❖ Notificar los casos críticos en cuanto a equipos usuario final, que afecte la continuidad de operaciones y/o la pérdida de información de los usuarios del SALUDPOL.
- ❖ Apoyar en las acciones que se requieran.

## **d) DEL EQUIPO DE RESTAURACIÓN DE TIC**

Este equipo es el encargado de ejecutar las acciones necesarias luego de que el siniestro o desastre esté controlado. Su finalidad es restituir en el menor tiempo posible el funcionamiento de los equipos tecnológicos y recuperar el estado de los servicios informáticos del SALUDPOL.

### **d.1) Oficial de Seguridad y Confianza Digital**

- ❖ Monitorear la restauración de aplicativos y ejecución de pruebas para verificación de funcionalidad.
- ❖ Monitorear la restauración de los servicios de TI y elaborar informes con las acciones realizadas.

- ❖ Validar y actualizar, en caso corresponda, la información documentada del Plan de Continuidad TIC de acuerdo con el escenario de riesgo presentado.
- ❖ Generar una bitácora o registro de lecciones aprendidas sobre el evento suscitado.

#### **d.2) Especialista en Tecnologías de la Información (Redes y comunicaciones y/o Servidores)**

- ❖ Iniciar el proceso de recuperación de los servicios de tecnología de la información realizando las pruebas de funcionamiento en los equipos afectados de la infraestructura informática y los equipos de la infraestructura tecnológica del SALUDPOL.
- ❖ Establecer contacto con los proveedores clave y/o terceros para notificarles cualquier requisito de ayuda sobre la recuperación de los activos tecnológicos de la entidad, en caso se requiera.
- ❖ Notificar las actividades de recuperación ejecutadas al Coordinador de la continuidad.
- ❖ Elaborar un informe técnico que incluya las acciones de recuperación de los equipos de comunicaciones, los servidores y los equipos de la infraestructura tecnológica del SALUDPOL.
- ❖ Alimentar la bitácora o registro colaborativo de lecciones aprendidas.

#### **d.3) Especialista en Desarrollo de Software**

- ❖ Verificar el estado de los sistemas institucionales del SALUDPOL, en caso se requiera desplegar y/o reinstalar los sistemas de información, de lo contrario verificar que se encuentren funcionando correctamente.
- ❖ Elaborar un informe técnico que incluya las acciones de recuperación realizadas.
- ❖ Alimentar la bitácora o registro colaborativo de lecciones aprendidas.

#### **d.4) Especialista en Administración de Base de Datos**

- ❖ Restaurar las copias de respaldo de las bases de datos correspondientes establecidas en el Plan de Continuidad TIC, en caso sea necesario.
- ❖ En caso sea requerido, realizar la creación de base de datos en servidores virtuales alternos.
- ❖ Verificar el funcionamiento de las bases de datos institucionales.
- ❖ Elaborar un informe técnico que incluya las acciones de recuperación realizadas.
- ❖ Alimentar la bitácora o registro colaborativo de lecciones aprendidas.

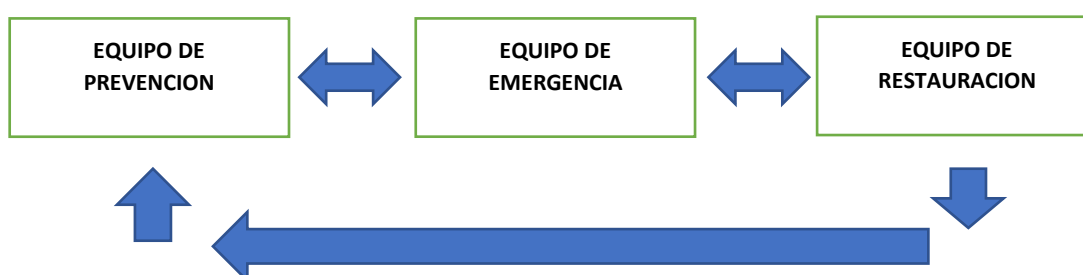
#### **d.5) Profesional o Técnico en Soporte Informático**

- ❖ Coordinar e iniciar el proceso de recuperación de los servicios relacionados a la central telefónica instalada en el SALUDPOL.

- ❖ Verificar el funcionamiento de los Equipos de usuarios finales en las sedes afectadas del SALUDPOL.
- ❖ Apoyar en la evaluación de condiciones de los equipos de telecomunicaciones.
- ❖ Solucionar los problemas de conexión y funcionamiento de los equipos de usuarios finales, impresoras, escáner entre otros, en caso sea necesario.
- ❖ Elaborar un informe técnico que incluya las actividades de recuperación de los equipos de los usuarios finales y la central telefónica.

Los equipos podrían ejecutar sus actividades paralelamente, de acuerdo con el siguiente orden de operación:

**Imagen. 5. Interacción de los equipos involucrados en el Plan de Continuidad TIC**



Fuente: Elaboración realizada por la OTI del SALUDPOL

## 8.4. FASE 4: RESPUESTA A LA CONTINGENCIA

### 8.4.1. Establecer los escenarios de riesgos

De la evaluación de riesgos identificados en el proceso del alcance, los cuales se muestran en el punto “8.2. Fase 2: Análisis de la Organización” del presente documento y de otros escenarios supuestos que podrían darse, se establecen los siguientes escenarios de riesgos:

**Tabla. 8. Escenarios de Riesgo que se pueden perpetrar contemplados en el Plan de Continuidad TIC**

N°	ESCENARIO DE RIESGO	DESCRIPCIÓN
1	Indisponibilidad de Infraestructura Física, por causa de algún desastre natural u ocasionados por el hombre.	<p>Dicha infraestructura puede ser el lugar en donde se encuentra el personal que interactúa con los terminales o Pcs utilizando los sistemas de información y otros, que forman parte de los procesos del SALUDPOL, así como la infraestructura tecnológica de SALUDPOL u otro ambiente o entorno en donde se respalde recursos tecnológicos que soporten los procesos.</p> <p>En este escenario, se considera que los recursos informáticos alojados en estos lugares, no se encuentran disponibles a causa de la destrucción originada por un sismo, inundación, incendio incluso ocasionado por un corto circuito o con mala intención por parte de ente humano.</p>

N°	ESCENARIO DE RIESGO	DESCRIPCIÓN
2	Desastre pandémico	Por la posibilidad de que exista alguna infección viral crónica, grave o situación pandémica o fallecimiento del personal que se relacione o se encuentre inmerso en los procesos del SALUDPOL o se encarga del manejo de los activos tecnológicos, a causa de esta situación u otra similar, que ocasione paralización en la ejecución del proceso o procedimiento de forma presencial y/o por enfermedad o muerte de personal que realiza dichas funciones, incluso el personal que se encarga o es responsable de las funciones informáticas.
3	Indisponibilidad de los Servicios Web y/o Sistemas de Información.	Que soportan los principales procesos TIC de la entidad, en este escenario se considera la indisponibilidad de los servicios y/o sistemas de información en entorno web, causados por una falla física o lógica, lo cual trae como consecuencia la caída de servicios informáticos y pérdida de comunicación en los equipos que conforman la infraestructura tecnológica.
4	Indisponibilidad en los servicios por la ocurrencia de un delito informático.	En este escenario se considera la indisponibilidad de los servicios y/o sistemas de información del proceso del alcance y de la entidad, como resultado de un delito informático, o por un APT (amenaza persistente avanzada) o intento de denegación de servicios.
5	Caída de Suministro eléctrico.	Indisponibilidad en los servicios por falla o falta de energía eléctrica en la infraestructura tecnológica o en el lugar en donde se efectúa el proceso core o misional del alcance. Estas fallas del suministro, pueden ser causadas por la falta de ampliación de potencia en algunos casos u ocasionadas por alguna inadecuada conexión realizada o por la misma red eléctrica cuando no avisan que se realizarán los mantenimientos correspondientes.
6	Indisponibilidad de los servicios por ausencia o falta del personal crítico.	En este escenario se considera que no se encuentra disponible el personal necesario para la administración y gestión de la infraestructura tecnológica y servicios de tecnología, lo cual puede traer como consecuencia la indisponibilidad de estos servicios por no contar con procedimientos descritos de su interacción o manejo.
7	Indisponibilidad del servicio de internet	Esto a causa de que una inadecuada posición del Router que emite una señal débil, o porque las líneas de comunicación están saturadas, o porque el servicio del proveedor sufrió una caída masiva.

Fuente: Elaboración realizada por la OTI del SALUDPOL

#### 8.4.2. Estrategias de recuperación

A continuación, se presentan estrategias de recuperación, en caso ocurra un escenario de riesgo:

##### 1) 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.

## **2) Desastre pandémico**

- a) Ejecutar los procedimientos relacionados al teletrabajo en el SALUDPOL y solo ir a las instalaciones cuando sea requerido siempre y cuando el protocolo y/o normas vigentes lo permitan.
- b) Reportar muertes a causa de la endemia o pandemia y reemplazar al personal que ya no está, proporcionándole los procedimientos documentados para la realización de las tareas y/o actividades desde su hogar, monitoreando dichas actividades o tareas mediante las herramientas de reunión o virtuales que sirven para la comunicación.
- c) Proporcionar al nuevo personal el equipo informático y/o software correspondiente para la realización de labores.
- d) Llevar un control respecto al trabajo avanzado de forma semanal, así como las coordinaciones respectivas respecto a los recursos tecnológicos que pudieran faltar.
- e) Incentivar a la vacunación dentro de lo que es posible al personal a cargo por parte de los responsables de los grupos de trabajo.

## **3) 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

**4) 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

**5) 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.

**6) 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 indisponible.
- 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.

#### 7) **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.

#### 8.4.3. Ejecución de los procedimientos del Plan de Recuperación elaborados por OTI

Una vez identificados los eventos de contingencia y/o los escenarios de riesgo, se procede con el desarrollo de los procedimientos del Plan de Recuperación, los cuales se detallan en el “Anexo III: Procedimientos de Restauración de Servicios de TIC Según los Principales Escenarios de Riesgo”, agrupados por las categorías indicadas previamente, lo cual comprenderá los eventos de mayor impacto, identificado en la matriz de riesgos de contingencia y serán abordados tal como se indica en la siguiente tabla:

**Tabla. 9. Escenarios de Riesgo de mayor impacto definidos en el Plan de Continuidad TIC**

N°	ESCENARIO DE RIESGO	Nivel de Exposición al Riesgo	Formato de procedimientos de recuperación
1	Indisponibilidad de Infraestructura Física, por causa de algún desastre natural u ocasionados por el hombre.	EXTREMO	PR.01
2	Desastre pandémico	MEDIO	PR.07
3	Indisponibilidad del recurso o servicio Informático por falla en el Hardware y/o Software.	EXTREMO	PR.02
4	Indisponibilidad en los servicios por la ocurrencia de un delito informático.	EXTREMO	PR.03
5	Caída de Suministro eléctrico.	EXTREMO	PR.04

N°	ESCENARIO DE RIESGO	Nivel de Exposición al Riesgo	Formato de procedimientos de recuperación
6	Indisponibilidad de los servicios por ausencia o falta del personal crítico	MEDIO	PR.05
7	Indisponibilidad del servicio de internet	EXTREMO	PR.06

Fuente: Elaboración realizada por la OTI del SALUDPOL

#### 8.4.4. Coordinar el manejo de la crisis

Una vez detectado el incidente, se debe de reportar a la mesa de ayuda del SALUDPOL, siendo la primera instancia en comunicación y a los canales establecidos para la misma, los cuales son:

- Correo electrónico soporte@saludpol.gob.pe
- Teléfono: (6802710) Anexo: 703

Además, la mesa de ayuda deberá reportar al Equipo de Respuestas ante Incidentes de Seguridad Digital – CSIRT del SALUDPOL, para que proceda con las diligencias según su rol.

#### 8.4.5. Resolver el incidente para restituir la normalidad de los procesos misionales del SALUDPOL

Para resolver el incidente y restituir la normalidad del proceso misional del SALUDPOL denotado en el alcance se debe de tomar en cuenta el análisis de impacto correspondiente que se detalla a continuación:

##### a) Tiempo de recuperación (RTO): (Recovery Time Objective)

Es el tiempo que lleva solucionar el incidente antes de que todos los sistemas y/o el servicio informático vuelvan a su normalidad, es decir sea restaurado, en este caso, las personas que interactúan o usan los recursos tecnológicos que interviene en los diferentes procesos misionales del SALUDPOL, manifestaron que el tiempo promedio para dicha recuperación sería entre una (1) a diez (10) horas para que todo vuelva a la normalidad.

##### b) Tiempo máximo tolerable de caída (MTD)

Es el tiempo límite máximo de indisponibilidad (incluido el tiempo de recuperación (RTO), que se establece para señalar el momento en que se considera continuar con la actividad o restauración de productos y/o servicios de SALUDPOL, no puede exceder de veinticuatro (24) horas, en el supuesto caso, se produzca una caída del sistema o el servicio de internet u otro evento grave o extremo que implique falta a la integridad de la información o que paralice las operaciones de SALUDPOL.

##### c) Niveles mínimos de recuperación de servicio (ROL)

Siendo este el nivel mínimo de recuperación para que se considere como recuperados los procesos core, el nivel del servicio no será el óptimo; se considera, en cuanto al servicio informático en relación a sus Sistemas de información, restaurar la última copia generada como



backup, ante la contingencia establecida lo cual podrá operarse a un 60% hasta que se restablezcan todos los servicios.

**d) Dependencias de otros procesos o proveedores**

Con la Superintendencia Nacional de Salud (SUSALUD) de forma externa y de forma interna con las unidades orgánicas que se relacionan con los procesos estratégicos y los de apoyo, así como otros servicios internos que existen en el SALUDPOL.

**e) Grado de dependencia de la actualidad de los datos (RPO)**

SALUDPOL considera en su parte informática que la información junto con los activos conexos, tales como los sistemas de información (SGRA y otros) que soportan los principales procesos críticos de SALUDPOL, deben de recuperarse como prioridad.

#### **8.4.6 Plan de Crisis**

Después de lo anteriormente definido, el plan de crisis implementará los procedimientos según las iniciativas detalladas en las estrategias de continuidad del presente plan, en relación al proceso afectado, a partir de este punto, se tomará en cuenta los elementos más relacionados con la tecnología.

El plan de crisis se organizará en torno a los siguientes elementos que se detallan a continuación:

##### **8.4.6.1. Componentes del Plan de Crisis (o de incidentes)**

**a) Condiciones de disparo.**

Es decir, que situación límite debe darse para que declaremos una situación de crisis. En este caso tendremos en cuenta especialmente los MTD del proceso del alcance.

**b) Flujo de toma de decisiones.**

**c) Medios para la declaración de la situación de crisis.**

**d) Personal responsable de activar el Plan de Crisis y gestionarlo.**

**e) Celular y datos de contacto del personal implicado en la gestión de crisis.**

**f) Niveles de priorización en la recuperación de la infraestructura de la entidad.**

**g) Requisitos temporales de puesta en marcha.**

**h) Planes operativos existentes y personal responsable de su activación.**

#### **8.5. FASE 5: DEFINICIÓN Y EJECUCIÓN DEL PLAN DE PRUEBAS**

El plan de pruebas está enfocado principalmente a simular situaciones de contingencia en caso de incidencias producidas sobre equipos, información y procesos, manejados en situaciones reales y cuyos respaldos si pueden ser empleados y replicados en una hipotética situación de contingencia.

Con el fin de garantizar la ejecución integral de la prueba, se diseñará un conjunto de casos de pruebas según los escenarios de riesgos, que serán ejecutados por los equipos operativos de la OTI, los cuales probarán, verificarán y observarán cualquier incidencia que se origine durante dicha prueba, a fin de retroalimentar cualquier acción que pueda corregir el plan.

La información que se desarrollará como parte del Plan de Pruebas, tiene el siguiente esquema:

- ❖ Metodología (descripción de la prueba a efectuarse)
- ❖ Alcances (áreas afectadas / personal involucrado)
- ❖ Resultados

Las pruebas relacionadas a este plan se deberán ejecutar semestralmente, con el fin de evaluar la preparación de la entidad, ante la ocurrencia de un siniestro y realizar los ajustes necesarios y deberán ser registradas en el formato detallado en el Anexo N° 1.

## 8.6. FASE 6: MONITOREO

La fase de monitoreo, estará a cargo de la OTI y el Equipo de Continuidad, dicha fase permite tener la seguridad de que se podrá reaccionar en el tiempo preciso y con la acción correcta. Esta fase es primordialmente de mantenimiento. Cada vez que se da o realiza un cambio en la infraestructura, debemos de realizar la adaptación respectiva. A continuación, se enumeran las actividades principales a realizar:

- Revisión continua de las aplicaciones, sistemas de información y portales web.
- Revisión continua del sistema de copias de respaldo (backups).
- Revisión y mantenimiento de los sistemas de soporte eléctrico de la infraestructura tecnológica.

## IX.- APROBACIÓN Y ACTUALIZACIÓN

La aprobación del Plan, de acuerdo con la R.M. 158-2019-IN<sup>5</sup>, deberá ser efectuada por la Gerencia General.

El presente Plan de continuidad TIC, tiene un periodo de permanencia que va desde el año 2023 al 2026, lo cual no implica que, dentro de este periodo surjan situaciones internas y/o externas que ameriten su actualización, la misma se puede generar por los siguientes eventos:

- Cambios en la infraestructura o aplicativos y/sistemas de TI, que impliquen modificación en los escenarios de riesgos previstos.

---

<sup>5</sup> Artículo 10, literal j): "Aprobar los documentos de gestión formulados por los órganos".

- Resultados de la evaluación de riesgos que cambien los escenarios descritos para las contingencias de TIC.
- Auditorías en Informática y/o sistemas realizados en el SALUDPOL, que impliquen cambios en los escenarios de riesgos.

## ANEXO I: FORMATO DE CONTROL Y CERTIFICACIÓN DE LAS PRUEBAS DEL PLAN DE CONTINUIDAD TIC Y RECUPERACIÓN DE SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES EN SALUDPOL



ANEXO N.º1: Formato de control y certificación de las Pruebas del Plan de Contingencia y Recuperación de Servicios de Tecnologías de la Información y Comunicaciones en SALUDPOL

CONTROL Y CERTIFICACIÓN DE PRUEBAS DE CONTINGENCIA				
Prueba N°				
Escenario de prueba:	<i>(Descripción del escenario a probar/certificar)</i>			
Área responsable	<i>(Área responsable del escenario de prueba a probar/certificar)</i>			
INFORMACIÓN DEL PROCESO				
Metodología				
Alcance				
Condiciones de ejecución:	Equipo		Aplicación/software	
	Ubicación		Fecha de Backup	/ /
RESULTADO DE LA PRUEBA				
Resultado	Satisfactorio			
	Satisfactorio con observaciones			
	Deficiente			
Observaciones	(Se deberá anotar los motivos y resultados en el caso exista observaciones o la prueba haya sido deficiente)			
ACTUALIZACIÓN EN EL PLAN DE CONTINGENCIA				
Cambios o actualizaciones en el Plan de Contingencia TIC:	(Se indicará los cambios que se tienen que realizar al plan de contingencia TIC como consecuencia de las observaciones detectadas)			
ACTUALIZACIÓN PARTICIPANTES				
Participante	Cargo			Firma

## ANEXO II: INVENTARIO DE SISTEMAS DE INFORMACIÓN DEL SALUDPOL VIGENTE

Nro.	Aplicativo	Año Inicio	Prioridad	Funcionalidad
1	Sistema de Gestión de Registro de Asegurados	2016	Alta	Gestiona los datos de los asegurados de SALUDPOL
2	Sistema de Procedimientos Médicos (SPM)	2016	Alta	Gestiona el proceso de atención de solicitudes de procedimiento médico, y la emisión de Cartas Garantía, Autorizaciones por Convenio y Autorizaciones por Contrato.
3	Sistema de Gestión del Trámite Documentario (STD)	2017		Gestiona expedientes administrativos
4	Sistema de Gestión de Reembolsos (SGR)	2017	Alta	Gestiona el proceso de atención de solicitudes de reembolso económico hacia los beneficiarios de SALUDPOL.
5	Sistema de Gestión de Asistencia al Usuario y Libro de Reclamaciones (SGAU)	2017		Gestiona las asistencias y reclamaciones de asegurados.
6	Sistema de Gestión de Pasajes Aéreos (SGPA)	2016		Gestiona el proceso de solicitudes de pasajes aéreos
7	Intranet de SALUDPOL	2018		Plataforma para la comunicación interna de SALUDPOL
8	Sistemas de Transferencia de Información de Prestaciones de Salud (STIPS)	2018	Alta	Gestiona el proceso de remisión de la información de prestaciones de salud brindadas por las IPRESS PNP en el marco del convenio, que es usada para la transferencia económica de SALUDPOL hacia DIRSAPOL.
9	Sistema Integrado de Gestión Estratégica Financiera (SIGEF)	2018	Media	Gestiona el proceso de Administración, Tesorería, Contabilidad, Logística, Recursos Humanos, Presupuesto de SALUDPOL.
10	Sistema de Registro de Prestaciones de Salud (SRPS)	2018	Alta	Gestiona el proceso de remisión de la información de prestaciones de salud brindadas por las IPRESS NO PNP en el marco del convenio, que es usada para la transferencia económica de SALUDPOL hacia las IPRESS/UGIPRESS/GORE
11	Aplicativo Móvil Stock Farmacias PNP - SALUDPOL	2019		Permite la consulta de stock de medicamentos en IPRESS PNP
12	Aplicativo Móvil Salud Policial PNP	2019		Permite al asegurado gestionar su información ante SALUDPOL
13	Sistema de Gestión de Convocatorias CAS	2017		Permite gestionar las convocatorias y postulaciones a procesos CAS
14	Sistema de Interacción con Proveedores (SIP)	2019		Permite que las IPRESS no PNP realicen cotizaciones de solicitudes de procedimientos médicos. Además, pueden ingresar sus solicitudes de pago.
15	Sistema de Registro de Emergencia Prioridad I (SREP1)	2020		Permite a los asegurados reportar sus casos de Prioridad I
16	Sistema de Denuncias del Canal de Integridad	2020		Permite a los ciudadanos registrar denuncias ante SALUDPOL
17	Sistema Integrado de Monitoreo del Asegurado (SIMA)	2021		Contiene dashboards con principales datos de diversos sistemas
18	Marcaciones Web	2019	Media	Aplicativo para que el personal CAS que no la labora en la sede central realice la marcación de su ingreso y salida
19	Sistema de Gestión de Citas de IPRESS NO PNP	2019		Permite que las IPRESS no PNP propongan citas para los asegurados de SALUDPOL
20	Sistema de Gestión de Colas	2019		Permite gestionar el orden de atención de las personas que acuden a la UT Lima

Nro.	Aplicativo	Año Inicio	Prioridad	Funcionalidad
21	Módulo web de Consulta de Stock de Medicamentos.	2021		Permite la consulta de stock de medicamentos en IPRESS PNP
22	Módulo web de Consulta de Convenios y Contratos.	2021		Permite la consulta de convenios de SALUDPOL con IPRESS
23	Sistema de Gestión Documental	2022		Gestiona expedientes administrativos con firma digital
24	Servicios Web Modelo SITEDS (IAFAS)	2020		Permite que las IPRESS soliciten acreditaciones para asegurados de SALUDPOL
25	Interoperabilidad basada en SETIAF	2017	Alta	Servicio para la interoperabilidad de datos de asegurados entre SALUDPOL y SUSALUD basado en SETIAF

### ANEXO III: PROCEDIMIENTOS DE RESTAURACIÓN DE SERVICIOS DE TIC SEGÚN LOS PRINCIPALES ESCENARIOS DE RIESGO

ESCENARIO 01:	PR.01	INDISPONIBILIDAD DE INFRAESTRUCTURA FÍSICA, POR CAUSA DE ALGÚN DESASTRE NATURAL U OCASIONADOS POR EL HOMBRE.
---------------	-------	--

#### A) EVENTO: SISMO, MAREMOTO, HUAYCO O CUALQUIER DESASTRE NATURAL

##### 1. PLAN DE PREVENCIÓN

###### a) Descripción del escenario

Los sismos y los desastres naturales, son innatos a la naturaleza, que generan una liberación repentina de energía, movimientos, etc., que se propaga en forma de ondas provocando el movimiento del terreno y del mar.

Este evento incluye los siguientes elementos mínimos identificados por SALUDPOL, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia:

###### Infraestructura

- ✓ Oficinas o lugares en donde se llevan a cabo los procesos críticos de la entidad y/o infraestructura tecnológica ubicado en la sede central.

###### Recursos Humanos

- ✓ Personal de la entidad.

###### b) Objetivo

Establecer las acciones que se ejecutarán ante un sismo, maremoto u otro desastre natural a fin de minimizar el tiempo de interrupción de las operaciones del SALUDPOL, sin exponer la seguridad de las personas.

###### c) Entorno

Este evento puede afectar las instalaciones de la Sede Central y la infraestructura tecnológica, al ubicarse en la misma ciudad y distritos colindantes.

###### d) Personal Encargado

El Equipo de Continuidad del SALUDPOL, 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 de TIC debe realizar las acciones descritas en el literal f).

###### e) Condiciones de Prevención de Riesgo

- ✓ Inspecciones de seguridad realizadas periódicamente.
- ✓ Contar con un plan de evacuación de las instalaciones del SALUDPOL, el mismo que debe ser de conocimiento de todo el personal que labora en todas las sedes.

- ✓ Realización de simulacros de evacuación con la participación de todo el personal de las distintas sedes.
  - ✓ Conformación de las brigadas de emergencia, y capacitarlas semestralmente.
  - ✓ Mantenimiento de las salidas libres de obstáculos.
  - ✓ Señalización de las zonas seguras y las salidas de emergencia.
  - ✓ Funcionamiento de las luces de emergencia.
  - ✓ Definición de los puntos de reunión en caso de evacuación.
- f) Acciones del Equipo de Prevención de TIC
- ✓ Evaluar en coordinación con el Equipo de Continuidad operativa el ambiente para la infraestructura tecnológica, en el sitio alternativo o en el cloud de ser prudente y necesario.
  - ✓ Establecer, organizar, ejecutar y supervisar procedimientos de respaldo y restauración de información base de datos, código fuentes y ejecutables.
  - ✓ Programar, supervisar el mantenimiento preventivo a los equipos componentes de la infraestructura tecnológica.
  - ✓ Mantener actualizado el inventario hardware y software utilizado en la infraestructura tecnológica de la entidad.
  - ✓ Llevar un control de versiones de las fuentes de los sistemas de información y portales de la entidad.

## **2. PLAN DE EJECUCIÓN**

### a) Eventos que activan la contingencia:

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

### b) Procesos Relacionados antes del evento:

- ✓ Tener la lista actualizada de los servidores por Direcciones y/u Oficinas.
- ✓ Mantenimiento del orden y limpieza de los ambientes de la sede central y la infraestructura tecnológica.
- ✓ Inspecciones trimestrales de seguridad externa.
- ✓ Realización de simulacros internos en horarios que no afecten las actividades.

### c) Personal que autoriza la contingencia informática:

El/La 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 alternativo 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 alternativo 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 alternativo: 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 estén 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 estén funcionando según lo estimado tanto en el sitio alternativo, 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, EXPLOSIÓN 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 afectados 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 perpetrarse 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 alternativo 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.

## 1. PLAN DE PREVENCIÓN

### a) Descripción del escenario

La pandemia es un tema de gran interés en todo el mundo. Según la Organización Mundial de la Salud (OMS), una pandemia es una epidemia de una enfermedad infecciosa que se ha propagado en un área geográficamente extensa, por ejemplo, en varios continentes o en todo el mundo, afectando a un número considerable de personas. La pandemia de COVID-19, es un ejemplo reciente de una pandemia que ha afectado a todo el mundo.

El contemplar este escenario de riesgo, el cual tuvo como efecto el no permitir que se pudiera acceder al trabajo presencial en las oficinas y/o instalaciones de la entidad, y por ende, contar con la supervisión insitu de los servidores y equipos de SALUDPOL, siendo el servicio muy limitado. Por ello, es necesario establecer medidas con el fin que, mediante el teletrabajo, la funcionalidad de los servicios de SALUDPOL continúe sin retrasos considerables ni riesgos informáticos que impliquen no solo retrasos, también riesgos de pérdida de información o perjuicio sobre los trabajadores o derecho habientes.

#### Hardware

- ✓ Equipos electrónicos.
- ✓ Módems o Routers.
- ✓ Pcs y laptops.

#### Software

- ✓ Software Base y aplicaciones instaladas, con conexión a internet.
- ✓ Aplicativos y portales de SALUDPOL.

### b) Objetivos

- ✓ Implementar un sistema de teletrabajo en un contexto de pandemia.
- ✓ Usar los equipos y servicios TIC de SALUDPOL proporcionados al personal que laborará en remoto.
- ✓ Establecer un conjunto de medidas para garantizar la funcionalidad de los servicios.

### c) Entorno

Este evento puede darse a todo nivel e incluso involucrar a todos los ciudadanos.

d) Personal Encargado

El Equipo de Prevención de TIC es el responsable del correcto funcionamiento de los servidores, páginas web, Sistemas de información y servicios de TIC, de acuerdo con sus perfiles.

e) Condiciones de Prevención de Riesgo

- ✓ Tener los equipos de cómputo incluyendo laptops y demás activos de información listos con la instalación del software correspondiente, a fin de poder solventar dicho recurso.
- ✓ Contar con antivirus instalados en los dispositivos de los trabajadores, a fin de que no se transmita información envirada o con riesgo de pérdida.
- ✓ Implementar una VPN para que el trabajo remoto pueda ser efectuado sin riesgo externo, a lo que se realiza para la entidad.
- ✓ Contar con equipos de respaldo ante posibles fallas de servidores, para su reemplazo provisional hasta su desinfección y habilitación.
- ✓ Capacitación al personal de OTI, sobre el uso de software y de los riesgos del trabajo remoto aplicados a SALUDPOL, así como hacerles conocer los números de soporte para cualquier contingencia que se presente o requerimiento estando en esta modalidad de trabajo.
- ✓ Establecer, organizar, ejecutar y supervisar de forma remota, utilizando las herramientas apropiadas, los procedimientos de respaldo de información de la información procesada y almacenada en la infraestructura tecnológica.
- ✓ Llevar un control de versiones de las fuentes de los sistemas de información y portales de la entidad.
- ✓ Realizar un seguimiento del uso de la información brindada o requerida por los trabajadores.
- ✓ Implementar sistemas de autenticación, a fin de que solo el personal autorizado pueda acceder a las plataformas e información disponibles.
- ✓ Supervisar si se cumple con el trabajo colaborativo, de tal forma que se verifique si se están cumpliendo los requisitos de funcionalidad a través del trabajo remoto.

## **2. PLAN DE EJECUCIÓN**

a) Eventos que activan la contingencia

La contingencia se activará al ocurrir la alerta de pandemia declarada por el Estado Peruano mediante una Disposición a Nivel Nacional y por ende, tomada por SALUDPOL de



forma simultánea. 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

- ✓ El responsable de la continuidad informará y/o comunicará la decisión de la Alta Dirección en relación a la restricción de la asistencia física a las instalaciones del personal a menos que se requiera o se permita por parte del Gobierno Central.
- ✓ Establecer medidas que permitan garantizar que la continuidad de las operaciones se efectuará con total normalidad, pero del modo virtual.
- ✓ Asimismo, se tiene que garantizar que se realice las tareas programadas en la infraestructura tecnológica tales como la monitorización, el respaldo de información (backups), administración de servidores, entre otras; en lo que respecta a los respaldos realizados asegurar siempre de que 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 estado de emergencia y en cada área de responsabilidad y notificar y reunir a los demás integrantes del Equipo de Emergencia y Restauración a fin de verificar si se están tomando las acciones necesarias para la continuidad de las operaciones.

e) Duración

La duración total de la pandemia será hasta que dure la emergencia sanitaria y/o la entidad disponga otro tipo de modalidad de asistencia al trabajo en el SALUDPOL.

### **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 TIC del SALUDPOL.

b) Descripción de actividades

El plan de recuperación está orientado a recobrar o cambiar de modalidad en el menor tiempo posible las actividades afectadas durante la etapa de pandemia iniciando desde la atención a los procesos misionales o críticos de la entidad.

En caso, el evento haya sido de considerable magnitud como lo es una pandemia, se deberá:

- ✓ Verificar la disponibilidad de recursos para la contingencia como: manuales técnicos de instalación de los sistemas de información, almacenamiento de datos, sistemas comunicación, hardware y copias de respaldo.
- ✓ Realizar un cronograma de implementación si es que no lo hubiere para preparar a las Pcs o Laptops y trasladarlas a los inmuebles en donde se encuentra el personal crítico que interviene en los procesos misionales del SALUDPOL y las personas que corresponden a los gestores de Alta Dirección.
- ✓ Movilizar al Equipo de Restauración al sitio alternativo de recuperación según el cronograma realizado en el punto anterior.
- ✓ Si no se cuenta con disponibilidad de recursos informáticos, adaptar los recursos informáticos que el usuario tenga en casa a fin de no perjudicar las actividades laborales, si ambas cosas no se tienen, atender siempre con prioridad al personal que forma parte de los procesos misionales o críticos de la entidad y/o a los gestores de alta dirección.
- ✓ Establecer contacto con los proveedores clave y terceros para proporcionar instrucciones inmediatas y/o notificarles cualquier requisito de ayuda sobre la continuidad de las operaciones de los sitios o inmuebles que han sido adaptados para dicho propósito desde el modo remoto.

c) Mecanismos de Comprobación

El Equipo de Emergencia presentará un informe al/el coordinador de Continuidad, explicando qué actividades, como parte del cambio de modalidad de presencial a remoto que se han efectuado de forma progresiva en lo que respecta a la tecnología de la información y comunicaciones, tomando en cuenta de forma especial a los procesos críticos u otros y/u oficinas que aún no han sido atendidos y que han sido afectadas por la pandemia y cuáles son y/o serían 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.

ESCENARIO 03:	PR.02	INDISPONIBILIDAD DEL RECURSO O SERVICIO INFORMÁTICO POR FALLA EN EL HARDWARE Y/O SOFTWARE
---------------	-------	--

## 1. PLAN DE PREVENCIÓN

### a) Descripción del Escenario

- ✓ El cuarto de comunicaciones se encuentra conectado a una red eléctrica estabilizada y conectado a UPS.
- ✓ En ciertas ocasiones los equipos informáticos en general, han sido afectados por interrupciones del fluido eléctrico o apagados imprevistos, lo que afecta a los activos o recursos informáticos dañando progresivamente los componentes de las computadoras o que los mismos, queden en desuso o requieran una revisión técnica, consumiendo tiempo y/o presupuesto.
- ✓ Dependiendo del equipo, las fallas pueden ser atendidas o resueltas por el personal interno de la OTI, pero en otros casos es necesario sea remitido al servicio técnico del proveedor de las marcas adquiridas. En ambos casos es importante que se proporcione una atención rápida a las fallas que presenten los equipos.
- ✓ En los casos en que los sistemas de información están alojados en la nube, su disponibilidad está supeditada a la disponibilidad de la infraestructura de la empresa que brinda dicho servicio, así como de las actualizaciones que dicha empresa pudiese realizar. Esto, dado que dichas actualizaciones pueden generar un funcionamiento inadecuado de los servicios.

### b) Objetivo

Asegurar la continuidad de las operaciones, con los medios de respaldo adecuados, en relación a las imágenes de los servidores o máquinas virtuales en producción.

### c) Personal Encargado

El Equipo de Prevención.

### d) Condiciones de Prevención de Riesgo

- ✓ Revisión periódica de los registros (Logs) de los servidores, para prevenir mal funcionamiento de los mismos.
- ✓ Cumplir con el cronograma de back up establecido.
- ✓ Contar con servicios de soporte y mantenimiento que contemple actividades de prevención, revisión del sistema y mantenimiento general.
- ✓ Disponer de servidores de bases de datos de contingencia, con la instalación del motor de base de datos.

e) Acciones del Equipo de Prevención.

- ✓ Establecer, organizar, ejecutar y supervisar procedimientos de respaldo y restauración de información en los equipos (Pcs, laptops y demás recursos que se necesiten).
- ✓ Programar y supervisar el mantenimiento preventivo y correctivo a los equipos componentes de la infraestructura tecnológica.
- ✓ Mantener actualizado el inventario hardware y software (parque informático) del SALUDPOL.
- ✓ Realizar el monitoreo de los servicios publicados en nube a través del proveedor de servicio.
- ✓ Establecer con la empresa que brinda servicios de nube, mecanismos para una comunicación anticipada de las actualizaciones (u otras acciones) que vayan a realizar y que pudiese impactar en los servicios del SALUDPOL.
- ✓ Determinar la necesidad de adquisición de nuevos equipos considerando el tiempo de vida, y el impacto de un funcionamiento inadecuado de los mismos.

## 2. PLAN DE EJECUCIÓN

a) Eventos que activan la contingencia

- ✓ Fallas en la conexión, indisponibilidad del sistema de información y/o aplicativo, inoperatividad de la PC o Laptop o dispositivo electrónico que soporte los procesos críticos y/u otro proceso que demanda interés por el SALUDPOL.
- ✓ Identificación de falla en la pantalla de las estaciones de trabajo y/o servidores.

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

- ✓ Contar con la disponibilidad del personal para la reparación rápida de los equipos.
- ✓ Establecer con la empresa que brinda servicios de nube, o proveedor de servicios de mantenimiento de los equipos de cómputo, redes y comunicaciones, mecanismos para una comunicación anticipada de las actualizaciones (u otras acciones) que vayan a realizar y que pudiese impactar en los servicios del SALUDPOL, de forma tal que se puedan ejecutar simulacros y evaluar su impacto, previniendo una interrupción de los servicios.
- ✓ Acceder a las copias de respaldo para la restauración de la información en el servidor averiado.

- ✓ Verificar que el equipo se encuentre en garantía, de lo contrario se implementará un nuevo servidor virtual.

e) Duración

El tiempo máximo de la contingencia no debe exceder las tres (3) horas.

### **3. PLAN DE RECUPERACIÓN**

a) Personal Encargado

El Equipo de Restauración, después de validar la corrección del problema de los equipos informáticos, servidores, sistema de información u otros averiados, el/la Coordinador/a de Continuidad o responsable que él designe, informará al usuario y/o a los jefes de las áreas para la reanudación de las operaciones de los servicios afectados.

b) Descripción de actividades

- ✓ Instalación y configuración del sistema operativo, drivers y servicios necesarios para el funcionamiento de los equipos informáticos, servidores, sistema de información u otros a recuperar.
- ✓ Instalación y configuración del sistema de información y el motor de la base de datos, con sus respectivas librerías y niveles de seguridad.
- ✓ Proceder a la restauración de las copias de respaldo, de la información de los equipos informáticos, servidores, sistema de información u otros afectados.
- ✓ Verificar que la data y los aplicativos se hayan restaurado correctamente.
- ✓ Ejecutar pruebas de acceso a los sistemas y aplicaciones.
- ✓ Comunicar mediante correo electrónico a los usuarios la reanudación de los servicios.

c) Mecanismos de Comprobación

Se registrará el incidente en el Sistema de Gestión de Tickets utilizado por la Mesa de Ayuda y Soporte Técnico de la OTI, precisando las acciones realizadas.

El/La Especialista de infraestructura y Redes, presentará un informe a el/la jefe/a de OTI, informando que parte del servicio u operaciones se han visto afectadas, y cuáles son las acciones tomadas.

El/La Profesional o Técnico de Soporte Informático, presentará un informe a el/la jefe/a de OTI, informando sobre el equipamiento informático u otro que se hayan visto afectados, 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.

ESCENARIO 04:	PR.03	INDISPONIBILIDAD DE LOS SERVICIOS WEB Y/O SISTEMAS DE INFORMACIÓN POR LA OCURRENCIA DE UN DELITO INFORMÁTICO
---------------	-------	--

## 1. PLAN DE PREVENCIÓN

### a) Descripción del escenario

Alteración de datos de los portales y sistemas de información a través de ataque cibernético (hacking) y/o malware.

Los ataques cibernéticos o ciberataques, son intentos no deseados de robar, exponer, alterar, deshabilitar o destruir información mediante el acceso no autorizado a los sistemas informáticos, ejemplo de ellos están la inyección SQL<sup>6</sup>, Denegación de servicios, entre otros.

El malware es un software malicioso o software malintencionado, que tiene como objetivo infiltrarse y/o dañar una computadora y/o sistema de información y/o a la propia información, sin el consentimiento de su propietario, secuestrando y/o eliminando datos del equipo. Este tipo de malware Incluye virus, gusanos, troyanos, keyloggers, botnets, Ransomware o secuestradores, spyware, adware, hijackers, rootkits, bootkits, rogues, etc.

Este evento incluye los siguientes elementos mínimos identificados por SALUDPOL, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia, los cuales se muestran a continuación:

#### Hardware

- ✓ La infraestructura tecnológica.
- ✓ Estaciones de Trabajo, equipos de comunicación y otros.

#### Software

- ✓ Software Base
- ✓ Sistemas de información, aplicativos y portales del SALUDPOL.

### b) Objetivo

Restaurar la operatividad de los equipos y servicios después de eliminar las amenazas (malware, APTs entre otros ataques) y dejar operativos los sistemas de información core así como reinstalar las aplicaciones dañadas.

<sup>6</sup> La inyección de SQL es un tipo de ciberataque encubierto en el cual un hacker inserta código propio en un sitio web con el fin de quebrantar las medidas de seguridad y acceder a datos protegidos.

c) Entorno

d) Este evento puede darse en cualquiera de los servidores y estaciones ubicadas en la infraestructura tecnológica junto con la sede principal y/o otras sedes del SALUDPOL.

e) Personal Encargado

El Equipo de Prevención de TIC, es el responsable del correcto funcionamiento de los servidores, estaciones de trabajo, sistemas de información y servicios de TI de acuerdo a sus perfiles.

f) Condiciones de Prevención de Riesgo

- ✓ Instalación de parches de seguridad en los equipos.
- ✓ Establecimiento de políticas de seguridad para prevenir el uso de aplicaciones no autorizadas en las estaciones de trabajo.
- ✓ Aplicación de filtros para restricción de correo entrante, y revisión de archivos adjuntos en los correos y así prevenir la infección de los terminales de trabajo por virus.
- ✓ Contar con antivirus instalados en cada estación de trabajo, el mismo que debe estar actualizado permanentemente.
- ✓ Contar con equipos de respaldo ante posibles fallas de las estaciones y servidores, para su reemplazo provisional hasta su desinfección y habilitación.
- ✓ Restricción del acceso a Internet a las estaciones de trabajo que por su uso no lo requieran.
- ✓ Eliminación o restricción de USBs, en estaciones de trabajo que no lo requieran y/o no hayan sido autorizadas.
- ✓ Capacitación al personal de OTI, sobre Seguridad de la Información y/o ciberseguridad en relación a las Bases de Datos, Sistemas Operativos, Servidores, Sistemas de Información entre otros.
- ✓ Ejecución de ataques de Hacking Ético por terceros especializados.
- ✓ Establecer, organizar, ejecutar y supervisar procedimientos de respaldo de información de la información procesada y almacenada en los servidores (virtuales y físicos) que su hardware se encuentre alojado en la infraestructura tecnológica.
- ✓ Llevar un control de versiones de las fuentes de los sistemas de información y portales de la entidad.
- ✓ Realizar pruebas de restauración de la información almacenada en los repositorios y bases de datos, previa determinación de cronogramas establecidos.

- ✓ Documentar y validar los manuales de restauración de los sistemas de información en producción.

## **2. PLAN DE EJECUCIÓN**

### **a) Eventos que activan la Contingencia**

- ✓ Mensajes de error durante la ejecución de programas en red o en entorno Web.
- ✓ Lentitud en el acceso a las aplicaciones.
- ✓ Caída de los sistemas de información que sostienen los procesos críticos, de administración entre otros, independientemente del entorno que lo soporta.
- ✓ Páginas: web principal, de transparencia y otras, así como los Web Service que se tienen y que permiten la interoperabilidad entre las diversas instituciones del Estado Peruano con SALUDPOL.

### **b) Procesos relacionados antes del evento**

Cualquier proceso relacionado con el uso de las aplicaciones, las diversas páginas web y los sistemas informáticos independientemente del entorno.

### **c) Personal que autoriza la contingencia**

El/La Coordinador/a de Continuidad de TIC y el/la Oficial de Seguridad y Confianza Digital, pueden activar la contingencia.

### **d) Personal Encargado**

Equipo de Emergencia de TIC.

### **e) Descripción de las actividades después de activar la contingencia**

- ✓ Desconectar el cable de red de datos o retirar de la red de datos del SALUDPOL, el servidor o la estación infectada o vulnerada.
- ✓ Verificar si el equipo se encuentra infectado, utilizando un detector de malware/virus actualizado. En el caso de aplicaciones, verificar si el código o la información de las bases de datos ha sido alterada.
- ✓ Rastrear de ser necesario el origen de la infección u ataque (archivo infectado, correo electrónico, hacking, etc.)
- ✓ Guardar el nombre del virus detectado y remitirlo al proveedor del antivirus utilizado. En el caso de hacking a aplicaciones, se debe guardar el archivo modificado, a nivel de software y base de datos.
- ✓ Eliminar el agente causante de la infección, es decir, remover el malware/virus del sistema, en el supuesto caso de que la amenaza viniera por un ataque perpetrado de



forma externa, revisar en el firewall el tráfico de paquetes, el cual permitirá analizar los logs que se tienen para determinar en el caso corresponda de donde proviene el determinado ataque y de ser posible revisar las direcciones lógicas a fin de que se pueda proteger a futuro de las mismas mejorando las políticas establecidas.

- ✓ Probar el sistema.
- ✓ En caso no solucionarse el problema, formatear el equipo servidor y restaurar copia de respaldo hasta analizar las causas que fomentaron dicho ataque o perpetración del malware tomando en cuenta la red y la seguridad perimetral correspondiente.

f) Duración

La duración del evento no debe de exceder de los tiempos límites de caída analizada por cada servicio afectado.

### **3. PLAN DE RECUPERACIÓN**

a) Personal Encargado

El Equipo de Restauración de TIC, luego de restaurar el correcto funcionamiento del servidor, estación de trabajo (PC, laptop), sistemas de información y portales web, coordinará con el usuario responsable del mismo y/o Director del área para reanudar las labores de trabajo con el equipo o sistema que fue afectado.

b) Descripción de actividades

Se informará a el/la Director/a de OTIC del SALUDPOL el tipo de malware/virus, o tipo de ataque encontrado y el procedimiento usado para removerlo.

Estas actividades deben contemplar como mínimo:

- ✓ Para terminales de usuarios:
  - Rescate de archivos de usuario y proceder al formateo del equipo.
  - Instalar un antivirus con antimalware
- ✓ Para Servidores
  - Eliminar la máquina virtual y realizar un rescate con la última copia de seguridad en nube
  - En caso que sea físico, proceder con el rescate reinstalando el servidor con la última copia de seguridad.
  - Coordinar con los operadores de base de datos y sistemas para la restauración de los servicios.
- ✓ Reinicio del servicio, prueba y afinamiento del sistema de información.

- ✓ Conectar el servidor o la estación a la red del SALUDPOL.
- ✓ Efectuar las pruebas necesarias con el usuario final de los equipos y/o sistemas de información afectados y luego solicitar la conformidad de la restauración realizada.
- ✓ Comunicar el restablecimiento del servicio.

En función a esto, el/la Oficial de Seguridad y Confianza Digital, tomará las medidas preventivas del caso enviando una alerta vía correo al personal del SALUDPOL.

El evento será evaluado y registrado de ser necesario en el formato de ocurrencia de incidentes de seguridad de la información.

c) Mecanismos de Comprobación

- ✓ Se llenará el formato de incidentes de seguridad de la información y se informará al Comité de Gobierno y Transformación Digital.
- ✓ El personal de Técnico de Soporte y/o Especialista en Redes y Comunicaciones, según sea el caso, presentará un informe a el/la Director/a de OTIC, explicando que parte del servicio u operaciones se han visto afectadas, y cuáles son las acciones tomadas.

d) Desactivación del Plan de Contingencia

Con el aviso de el/la Coordinador/a de Continuidad de TIC del SALUDPOL, se desactivará el presente Plan.

e) Proceso de Actualización

El problema de infección o alteración presentado en la estación de trabajo y/o servidor de red, en base al informe que describe los problemas presentados, se determinarán las acciones de prevención a tomar.

## 1. PLAN DE PREVENCIÓN

### a) Descripción del escenario

- ✓ El inmueble cuenta con luces de emergencia que cuenta con revisiones y cambios periódicos.
- ✓ La continuidad del fluido eléctrico de la infraestructura tecnológica está soportada en un (1) UPS que dan un promedio de dos (2) horas para el apagado progresivo de los equipos, dichos UPS emiten sonidos de advertencia al ponerse en funcionamiento, lo que alerta a los especialistas de la OTI, para que ejecuten las acciones correspondientes para un apagado adecuado.
- ✓ Es importante que el personal responsable, se concientice sobre la importancia de usar adecuadamente sobre el tiempo que brindan los UPS, para el apagado de los servicios alojados en los servidores de la infraestructura tecnológica, a fin de realizar adecuadamente dicho apagado de los equipos y evitar que queden defectuosos y/o dañar la información.
- ✓ Realizar simulacros de interrupciones de fluido eléctrico en la infraestructura tecnológica, y no existen procedimientos formales de apagado y encendido del mismo.

### b) Objetivo

Restaurar las funciones consideradas como críticas para el servicio.

### c) Personal Encargado

- ✓ El/la Coordinador/a de Continuidad, es el responsable de atender y supervisar las respuestas ante el incidente.
- ✓ El/La jefe/a de la Oficina de Logística de la OGA, es el responsable de realizar las coordinaciones para restablecer el suministro de energía eléctrica con los proveedores de energía.
- ✓ El Equipo de Prevención debe realizar las acciones descritas en el punto e).

### d) Condiciones de Prevención de Riesgo

- ✓ Se cuenta con un equipo UPS que en situaciones de corte mantendrá las operaciones por 2 horas.
- ✓ Realización de pruebas periódicas del equipo UPS para asegurar su correcto funcionamiento.

e) Acciones del Equipo de Prevención.

- ✓ Revisar periódicamente y de forma conjunta con Servicios Generales del SALUDPOL, las instalaciones eléctricas de la infraestructura tecnológica y programar y supervisar el mantenimiento preventivo y correctivo de los equipos componentes de la infraestructura tecnológica.
- ✓ Coordinar el mantenimiento preventivo de pozos a tierra, climatización, UPS, gabinetes y sistema eléctrico del cuarto de comunicaciones con periodo mínimo a 1 año.

## **2. PLAN DE EJECUCIÓN**

a) Eventos que activan la contingencia

- ✓ Fallas en la conexión. Indisponibilidad del sistema de información y/o aplicativo.
- ✓ Identificación de falla en la pantalla de las estaciones de trabajo y/o servidores de aplicaciones.

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

- ✓ Contar con la disponibilidad del personal para la reparación rápida de los equipos.
- ✓ Establecer con la empresa que brinda servicios de nube, mecanismos para una comunicación anticipada de las actualizaciones (u otras acciones) que vayan a realizar y que pudiese impactar en los servicios del SALUDPOL, de forma tal que se puedan ejecutar simulacros y evaluar su impacto, previniendo una interrupción de los servicios.
- ✓ Acceder a las cintas de respaldo para la restauración de la información en el servidor averiado
- ✓ Verificar que el equipo se encuentre en garantía, de lo contrario de implementará un nuevo servidor virtual.

e) Duración

El tiempo máximo de la contingencia no debe sobrepasar las seis (6) horas.

## **3. PLAN DE RECUPERACIÓN**

a) Personal Encargado

El Equipo de Restauración, quienes se encargarán de realizar las acciones de recuperación necesarias.

b) Descripción de actividades

- ✓ Al retorno de la energía comercial se verificará por el lapso de media hora que no haya interrupciones o fluctuaciones de energía
- ✓ Proceder a encender la plataforma tecnológica ordenadamente de acuerdo con el siguiente detalle: - Equipos de Comunicaciones (router, switches core, switches de acceso)
- ✓ Equipos de almacenamiento (storage)
- ✓ Servidores físicos por orden de prioridad.
- ✓ Servidores virtuales por orden de prioridad.
- ✓ La contingencia finaliza cuando retorna la energía eléctrica y todos los equipos se encuentran operativos brindando servicio.

c) Mecanismos de Comprobación

El/La Especialista de infraestructura y Redes, presentará un informe a el/la jefe/a de OTI, informando que parte del servicio y equipos han fallado, y cuáles son las acciones correctivas que realizar.

d) Desactivación del Plan de Continuidad TIC

El/La Coordinador/a de Continuidad desactivará el Plan de Continuidad TIC, una vez que se recupere la funcionalidad del suministro eléctrico y la operatividad de los sistemas y servicios de tecnología de la información.

ESCENARIO 06:	PR.05	<u>INDISPONIBILIDAD DE LOS SERVICIOS POR AUSENCIA O FALTA DEL PERSONAL CRÍTICO</u>
---------------	-------	--

## 1. PLAN DE PREVENCIÓN

### a) Descripción del escenario

- ✓ En los procesos críticos el personal clave, a veces no cuenta con otra persona que reemplace o alterne con las tareas encomendadas en referencia al tratamiento de gran volumen de información, por ende, es importante que se tenga o genere los reemplazos correspondientes a fin de que, si sucede algo en referencia a la persona principal que atiende, los procesos no queden sin la continuidad que exige su formulación.

#### Infraestructura:

- ✓ Lugares en donde se atiende a los derechos habientes y demás centros de atención de SALUDPOL.

#### Recursos Humanos:

- ✓ Personal de la entidad bajo vínculo contractual o proveedores de servicio.

### b) Objetivo

Establecer las acciones que se ejecutarán ante la falta de personal principal en la atención de los procesos.

### 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

- ✓ Considerar que las atenciones fuera del horario laboral sean atendidas oportunamente previa coordinación con los operadores de soporte de aplicaciones e infraestructura tecnológica.
- ✓ Asegurarse que los procedimientos que son para la atención para los procesos críticos, así como los procedimientos referidos a los procesos de apoyo de la OTI, estén disponibles, a fin de que si surge una eventualidad puedan responderse de forma inmediata siguiendo los procedimientos correspondientes.
- ✓ Si surge la atención o el tratamiento del volumen de datos, considerar a personal adicional a fin de que se pueda atender toda la información para tratar en los diferentes procesos que tiene SALUDPOL.

e) Acciones del Equipo de Prevención

- ✓ Evaluar con el coordinador de Continuidad, que se cuenten con los procedimientos requeridos para la atención de los procesos misionales del SALUDPOL, así como tener de forma alterna, algún proceso para salvaguardar el proceso misional que se esté llevando a cabo de corresponder de la entidad.
- ✓ Prever con la OTI, el desarrollo de procedimientos que responden a los procesos de apoyo, alineados con las buenas prácticas y normativa vigente, en referencia a los activos o recurso informático de la infraestructura tecnológica y sus componentes relacionados, que denoten incluso el encendido y apagado de los mismos, a fin de que ante una contingencia se pueda restablecer los mismos de forma adecuada (pcs, laptops, servidores, entre otros).

## 2. PLAN DE EJECUCIÓN

a) Eventos que activan la contingencia

- ✓ La contingencia se activará al ocurrir alguna falta de personal crítico de los procesos, de forma fortuita o por deceso. 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

- ✓ Establecer medidas que permitan garantizar que se tendrá un proceso alterno que garantice la atención a los derechos habientes siempre, incluso mediante plataformas en entorno web.
- ✓ Tener el compromiso de los dueños o responsables de los procesos críticos de la presencia de personal para el abastecimiento en la atención y que también se pueda gestionar el contar con el mismo en horario fuera de oficina.
- ✓ Tener en un lugar de respaldo los documentos de los procedimientos tanto de la infraestructura tecnológica y de los procedimientos de los procesos críticos a fin de que se encuentren disponibles ante cualquier contingencia.
- ✓ Tener un lugar en donde el jefe de la OTI pueda custodiar las claves de identificación y autenticación de emergencia, para la administración de los servidores y servicios correspondientes incluido la llave de acceso al espacio físico de la infraestructura tecnológica a fin de poder manejar los equipos de cómputo, los servidores tanto físicos como virtuales entre otros dispositivos conexos, por parte del personal suplente, las

mismas que deberán ser proporcionadas como identificación de contingencia para el propósito requerido, luego tener un procedimiento de desechar las mismas cuando el personal principal vuelva a la administración y/o se restablezca su permanencia.

e) Duración

- ✓ La duración máxima para colocar a otra persona en ese rol según la carga de trabajo, será de 3 horas a fin de que se restablezca la continuidad de las operaciones.

### **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:

Para restablecer el servicio de internet en una entidad, se pueden seguir los siguientes pasos:

- ✓ Verificar la disponibilidad de recursos humanos para la contingencia.
- ✓ Realizar el seguimiento para asegurar de que se maneje con facilidad los manuales técnicos de instalación del sistema de información, almacenamiento de datos, sistemas comunicación, hardware, y copias de respaldo, así como los procedimientos del proceso, a fin de que se restablezca la continuidad de las operaciones.
- ✓ 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/La Coordinador de continuidad, presentará un informe a el/la jefe/a de OTI, informando si el recurso humano estuvo y fue el necesario al presentarse esta contingencia, y/o cuáles serían las acciones correctivas que realizar.

d) Desactivación del Plan de Continuidad TIC

El/La Coordinador/a de Continuidad desactivará el Plan de Continuidad TIC, una vez que se recupere la funcionalidad del proceso u o procesos junto con el manejo óptimo de los sistemas y servicios de tecnología de la información.



ESCENARIO 07:	PR.06	<u>INDISPONIBILIDAD DEL SERVICIO DE INTERNET</u>
------------------	-------	--

## 1. PLAN DE PREVENCIÓN

### a) Descripción del escenario

- ✓ Actualmente en SALUDPOL se cuenta con el servicio de internet brindada por un proveedor de servicios, los equipos en su mayoría incluso a nivel nacional lo proveen la entidad contratista, se cuenta con equipos alternos que permiten la continuidad del servicio, así como los enlaces correspondientes, tanto de modo principal como contingente, sin embargo, a pesar de eso, durante el presente año sucedió una caída del servicio, que se restableció en dos (2) horas.

#### Infraestructura:

- ✓ Equipos de red y comunicaciones de la infraestructura tecnológica del SALUDPOL.

#### Recursos Humanos:

- ✓ Especialista en redes y comunicaciones y Proveedor de servicios.

### b) Objetivo

Establecer las acciones que se ejecutarán ante la indisponibilidad del internet, en la atención de los procesos.

### 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

- ✓ Tener una lista de números telefónicos a fin de poder contactarse con el proveedor de servicios.
- ✓ Tener a la mano la llave del espacio físico de la infraestructura tecnológica, para poder realizar o examinar los enlaces y la disposición de los equipos de red y comunicaciones y verificar que estén en buen estado.

### e) Acciones del Equipo de Prevención

- ✓ Evaluar en coordinación con el coordinador de Continuidad, que se cuenten con los procedimientos de manejo o manuales de los equipos de red y comunicaciones para restablecer la continuidad del servicio de internet, si es que se notara de que existe un desperfecto en dichos equipos.

- ✓ Prever con la OTI y el proveedor de servicios, que se tengan equipos de respaldo o de modo contingente dentro de la infraestructura tecnológica o en sitios alternos a fin de que se pueda restablecer el servicio de internet de forma óptima.

## **2. PLAN DE EJECUCIÓN**

### **a) Eventos que activan la contingencia**

La contingencia se activará al ocurrir alguna falta de la continuidad del internet, es decir, que se denote que en las Pcs o laptops del personal y/o en los servicios, no se tiene el acceso a internet correspondiente.

### **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**

- ✓ Si perdemos la conexión a internet, empezar por el propio computador, es necesario revisar si el equipo se encuentra correctamente conectado, enviando y recibiendo paquetes al router (si estás conectado a uno) y si la tarjeta de red está funcionando sin problemas.
- ✓ Si el incidente se detecta en la Sede Central, el personal de soporte deberá de realizar las revisiones necesarias para determinar la causa de la desconexión, de es necesario elevar el incidente al equipo de redes, si el incidente requiere de elevación de nivel se deberá contactar con los proveedores de servicio hasta restablecer el servicio, se deberá realizar un informe conjunto para describir el problema y la solución.

### **e) Duración**

- ✓ Para un incidente considerado leve o de menor complejidad la duración de la solución no debe de exceder de tres (3) horas a fin de que se restablezca la continuidad del servicio de internet, más la tendencia es realizarlo en el menor tiempo posible.

## **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 tecnológicos en referencia a los equipos de comunicaciones por parte del proveedor y/o la OTI de SALUDPOL.
- ✓ Realizar el monitoreo y seguimiento para asegurar de que se verifique la continuidad del servicio de internet en todo el recurso informático del SALUDPOL.

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