Firma Digital Senamhi
Firmado digitalmente por TAKAHASHI GUEVARA Ken FAU 20131366028 soft
Motivo: Doy V° B°
Fecha: 18.01.2021 20:29:22 -05:00

REPÚBLICA DEL PERÚ

RESOLUCIÓN DE PRESIDENCIA EJECUTIVA
N° 003-2021-SENAMHI/PREJ

Lima, 18 de enero de 2021

Firma Digital Senamhi
Firmado digitalmente por GONZALES QUISPE Luz Marina FAU 20131366028 soft
Motivo: Doy V° B°
Fecha: 18.01.2021 19:05:57 -05:00

VISTA:

La Nota de Elevación N° D000004-2021-SENAMHI-OPP de fecha 7 de enero de 2021, de la Oficina de Planeamiento y Presupuesto, y;

CONSIDERANDO:

Que, la Ley N° 24031, Ley del Servicio Nacional de Meteorología e Hidrología - SENAMHI, modificada por la Ley N° 27188, establece que el SENAMHI es un organismo público descentralizado, con personería jurídica de derecho público interno y autonomía técnica, administrativa y económica, dentro de los límites del ordenamiento legal del Sector Público;

Firma Digital Senamhi
Firmado digitalmente por GARCIA TUEROS Laiter Luis FAU 20131366028 hard
Motivo: Doy V° B°
Fecha: 18.01.2021 12:29:16 -05:00

Que, de conformidad con el acápite 07 del numeral 3.10 de la Resolución de Contraloría Nº 320-2006-CG, que aprueba las Normas de Control Interno, señala que *"Para el adecuado ambiente de control en los sistemas informáticos, se requiere que éstos sean preparados y programados con anticipación para mantener la continuidad del servicio. Para ello se debe elaborar, mantener y actualizar periódicamente un plan de contingencia debidamente autorizado y aprobado por el titular o funcionario designado donde se estipule procedimientos previstos para la recuperación de datos con el fin de afrontar situaciones de emergencia";*

Firma Digital Senamhi
Firmado digitalmente por CHACON CALDERON Jose Antonio FAU 20131366028 soft
Motivo: Doy V° B°
Fecha: 18.01.2021 15:27:40 -05:00

Que, el numeral 4.1 de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2a. Edición" en todas las entidades integrantes del Sistema Nacional de Informática, aprobada mediante Resolución Ministerial Nº 246-2007-PCM, señala que *"La evaluación de riesgos debe identificar, cuantificar y priorizar riesgos contra el criterio para la aceptación del riesgo y los objetivos relevantes para la organización. Los resultados deben guiar y determinar la apropiada acción de gestión y las prioridades para manejar la información de los riesgos de seguridad y para implementar controles seleccionados para proteger estos riesgos. El proceso de evaluación de riesgos y de seleccionar controles puede requerir que sea realizado un número de veces con el fin de cubrir diferentes partes de la organización o sistemas de información individuales";*

Firma Digital Senamhi
Firmado digitalmente por BARRON LOPEZ Jose Percy FAU 20131366028 soft
Motivo: Doy V° B°
Fecha: 18.01.2021 19:30:52 -05:00

Que, la Estrategia 4 del "Plan de Desarrollo de la Sociedad de la Información en el Perú - La Agenda Digital Peruana 2.0", aprobado mediante Decreto Supremo Nº 066-2011-PCM, precisa que en la actualidad existe el aumento de las amenazas cibernéticas sobre infraestructuras de tecnologías de la información y la comunicación del ámbito público y privado, lo que hace necesario contar con una Estrategia Nacional de Ciberseguridad con el objetivo de minimizar los riesgos de sufrir algún tipo de incidente en las infraestructuras criticas;

Que, a través de la Resolución Ministerial Nº 028-2015-PCM, se aprueban los Lineamientos para la Gestión de la Continuidad Operativa de las entidades públicas en los tres niveles de Gobierno, con el objetivo de lograr el desarrollo de los procedimientos técnicos, administrativos y legales que permitan garantizar la adecuada y oportuna gestión de la continuidad operativa de las Entidades Públicas en los tres niveles de gobierno;

Que, mediante documento del Visto, la Oficina de Planeamiento y Presupuesto remite el Informe N° D000001-2021-SENAMHI-UM, mediante el cual la Unidad de Modernización y Gestión de la

Firma Digital

Firmado digitalmente por BARRON LOPEZ Jose Percy FAU 20131366028 soft
Motivo: Doy V° B°
Fecha: 18.01.2021 19:31:34 -05:00

Calidad, señala que la Oficina de Tecnologías de la Información y la Comunicación ha elaborado el Plan de Contingencia Informático del Servicio Nacional de Meteorología e Hidrología del Perú – SENAMHI, en el marco de la función atribuida a dicho órgano a través del Reglamento de Organización y Funciones del SENAMHI, aprobado mediante Decreto Supremo N° 003-2016-MINAM, que precisa que es función de la referida dependencia elaborar, proponer e implementar el Plan de Contingencia de Sistemas de Información; por lo cual recomienda la aprobación del Plan en mención;

Firma Digital

Firmado digitalmente por GONZALES QUISPE Luz Marina FAU 20131366028 soft
Motivo: Doy V° B°
Fecha: 18.01.2021 19:06:57 -05:00

Que, por su parte el literal m) del artículo 11 del Reglamento de Organización y Funciones del SENAMHI, aprobado mediante Decreto Supremo N° 003-2016-MINAM, precisa que es función del Presidente Ejecutivo *"Aprobar las normas que regulen el Plan de Seguridad de la Información de la Entidad";*

Que, conforme a lo expuesto, resulta pertinente emitir el acto mediante el cual se aprueba el Plan de Contingencia Informático del Servicio Nacional de Meteorología e Hidrología del Perú – SENAMHI;

Firma Digital

Firmado digitalmente por GARCIA TUEROS Laiter Luis FAU 20131366028 hard
Motivo: Doy V° B°
Fecha: 18.01.2021 12:29:34 -05:00

Con el visado del Gerente General, de la Directora de la Oficina de Planeamiento y Presupuesto, del Director de la Oficina de Tecnologías de la Información y la Comunicación, y del Director de la Oficina de Asesoría Jurídica; y,

De conformidad con lo dispuesto por la Ley N° 24031, Ley del Servicio Nacional de Meteorología e Hidrología del Perú – SENAMHI, su modificatoria Ley N° 27188; y su Reglamento de Organización y Funciones, aprobado mediante Decreto Supremo N° 003-2016-MINAM.

SE RESUELVE:

Firma Digital

Firmado digitalmente por CHACON CALDERON Jose Antonio FAU 20131366028 soft
Motivo: Doy V° B°
Fecha: 18.01.2021 15:28:28 -05:00

Artículo 1.- Aprobar el Plan de Contingencia Informático del Servicio Nacional de Meteorología e Hidrología del Perú – SENAMHI, que como Anexo se encuentra adjunto a la presente.

Artículo 2.- Disponer la publicación de la presente Resolución en el Portal Web Institucional del SENAMHI (www.senamhi.gob.pe).

Regístrese y comuníquese

Firma Digital

Firmado digitalmente por TAKAHASHI GUEVARA Ken FAU 20131366028 soft
Motivo: Soy el autor del documento
Fecha: 18.01.2021 21:30:14 -05:00

KEN TAKAHASHI GUEVARA
Presidente Ejecutivo
Servicio Nacional de Meteorología e Hidrología
del Perú – SENAMHI

PLAN DE CONTINGENCIA INFORMÁTICO

Firma Digital
Senamhi
SERVICIO NACIONAL DE METEOROLOGÍA E HIDROLOGÍA DEL PERÚ

Firmado digitalmente por GONZALES QUISPE Luz Marina FAU 20131366028 soft
Motivo: Soy el autor del documento
Fecha: 15.01.2021 19:11:38 -05:00

Firma Digital
Senamhi
SERVICIO NACIONAL DE METEOROLOGÍA E HIDROLOGÍA DEL PERÚ

Firmado digitalmente por CHACON CALDERON Jose Antonio FAU 20131366028 soft
Motivo: Soy el autor del documento
Fecha: 11.01.2021 10:42:21 -05:00

Firma Digital
Senamhi
SERVICIO NACIONAL DE METEOROLOGÍA E HIDROLOGÍA DEL PERÚ

Firmado digitalmente por HERR GARCIA Carlos Alejandro FAU 20131366028 hard
Motivo: Doy V° B°
Fecha: 11.01.2021 10:07:31 -05:00

OFICINA DE TECNOLOGIAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

ÍNDICE

INTRODUCCION

Que, mediante Resolución de Contraloría General N° 320-2006-CG se aprobaron las "Normas de Control Interno", de aplicación a las entidades del Estado conforme a lo establecido por la ley N° 28716, Ley de Control Interno de las Entidades del Estado, con la finalidad de propiciar el fortalecimiento de los sistemas de control interno y mejorar la gestión pública, en relación a la protección del patrimonio público y al logro de los objetivos y metas institucionales

Que, en el séptimo comentario de la Norma Básica "3.10 Controles para las Tecnologías de la Información y Comunicaciones" de las Normas de Control Interno antes señaladas, se establece que el adecuado ambiente de control en los sistemas informáticos requiere que estos sean preparados y programados con anticipación para mantener la continuidad del servicio, para lo cual se debe elaborar, mantener y actualizar periódicamente un plan de contingencia debidamente autorizado y aprobado por el titular o funcionario designado donde se estipule procedimientos previstos para la recuperación de datos con el fin de afrontar situaciones de emergencia.

En atención a lo expuesto, se indica que “Un plan de contingencia es un instrumento de gestión para el buen gobierno de las Tecnología de la Información y las comunicaciones en el dominio del soporte y desempeño. Estos planes de contingencia contienen las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad del negocio y las operaciones de un proyecto. Es un caso particular de plan de continuidad del negocio, pero dada la importancia actual de las tecnologías modernas, el plan de contingencia es el más relevante”.

El presente documento es administrado por la Oficina de Tecnologías de la Información y la Comunicación del SENAMHI, siendo fuente de consulta y aplicación para atender situaciones de contingencia, permitiendo restaurar los sistemas o servicios por algún inconveniente que pudiera presentarse con los mismos. A través de este plan se busca definir:

- Las situaciones y escenarios que pudieran preverse con la finalidad de permitir la operación de los sistemas de la institución a través de las acciones de contingencia.
- La formación del equipo humano y sus roles en casos de contingencia, el procedimiento de activación del plan de contingencia.

- El procedimiento general de recuperación necesario para restaurar el normal funcionamiento de los sistemas y servicios, que deben estar operando ya sea en el mismo computador al momento del suceso o en un computador alterno.

Que mediante Decreto Supremo N° 003-2016-MINAM, se aprobó el Reglamento de Organización y Funciones (ROF) del Servicio Nacional de Meteorología e Hidrología del Perú - SENAMHI, donde señala que es función de la Oficina de Tecnologías de la Información y la Comunicación, elaborar, proponer e implementar el Plan de Contingencia Informático.

El presente Plan se constituye en un instrumento que da el marco de actuación para garantizar en el SENAMHI la continuidad de los servicios que brinda, por lo que deberá ser incluido como parte del Gestión de la Continuidad Operativa del SENAMHI,

1. FINALIDAD

Garantizar la continuidad de los servicios de tecnología de información y comunicaciones del Servicio Nacional de Meteorología e Hidrología del Perú - SENAMHI, a fin de que se restablezcan en el menor tiempo posible, en caso de la ocurrencia de alguna eventualidad que interrumpa su funcionamiento.

2. OBJETIVOS

2.1. Objetivo General.

Contar con un Plan de Contingencia Informático, que permita gestionar la continuidad operativa informática del Servicio Nacional de Meteorología e Hidrología del Perú, así como disminuir las fallas y eventos inesperados; con el propósito de asegurar y restaurar los equipos e información con las menores perdidas posibles en forma rápida, eficiente y oportuna.

2.2. Objetivo Específico

- Identificar los riesgos a los que se encuentra expuestos los activos informáticos de la Institución a Nivel Nacional y establecer un Plan de tratamiento para su mitigación.
- Identificar los controles existentes para la mitigación o reducción de ocurrencia y/o impacto de los riesgos identificados
- Reducir la incertidumbre en el cumplimiento de la misión, objetivos y metas del SENAMHI frente la ocurrencia de eventos que puedan alterar el normal funcionamiento de los sistemas de la información considerados críticos en la entidad.
- Definir las estrategias de respaldo, emergencia y recuperación para salvaguardar la infraestructura tecnológica y la información del SENAMHI.

3. ALCANCE

El Plan de Contingencia Informático, incluye los elementos referidos a los sistemas de información, aplicativos informáticos, bases de datos, equipos e instalaciones tecnológicas, personal, servicios y otros administrados por la Oficina de Tecnologías de la Información y la Comunicación, direccionado a minimizar eventuales riesgos ante situaciones adversas que atentan contra el normal funcionamiento de los servicios informáticos de la entidad

4. BASE LEGAL

4.1. Decreto Supremo Nº 004-2019-JUS, que aprueba el Texto Único Ordenado de la Ley N° 27444, Ley del Procedimiento Administrativo General.

4.2. Ley Nº 29664 Ley que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD).

4.3. Resolución Ministerial N° 188-2015-PCM, Aprobación de los Lineamientos para la Formulación y Aprobación de Planes de Contingencia.

4.4. Resolución Ministerial N° 028-2015-PCM, Aprueba los lineamientos para la gestión de la continuidad operativa de las Entidades Públicas en los tres niveles de gobierno.

4.5. Ley N° 24031, Ley del Servicio Nacional de Meteorología e Hidrología del Perú, modificado por la Ley Nº 27188.

4.6. Decreto Supremo N° 003-2016-MINAM, Aprueba Reglamento de Organización y Funciones (ROF) del Servicio Nacional de Meteorología e Hidrología del Perú – SENAMHI.

4.7. Resolución Ministerial N° 004-2016-PCM, Aprueba 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.

4.8. Decreto Supremo N° 066-2011-PCM que aprueba el "Plan de Desarrollo de la Sociedad de la información en el Perú - La Agenda Digital Peruana 2.0", y que en su Objetivo N° 7, establece la necesidad de promover una Administración Pública de calidad orientada a la población, y la necesidad de contar con una Estrategia Nacional de Ciberseguridad, con el objetivo de minimizar los riesgos en caso de sufrir algún tipo de incidente en los recursos Informáticos del Estado, así como, la disuasión del crimen cibernético, que se producen mediante el uso de redes teleinformáticas, entre otros.

4.9. Resolución Ministerial N° 246-2007-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana NTP-ISO/IEC 17799:2007 EDI Tecnologías de la Información, Código de Buenas Prácticas para la Gestión de Seguridad de la Información 2da edición en todas las entidades integrantes del Sistema Nacional de Informática.

5. DEFINICIONES Y SIGLAS

5.1. DEFINICIONES

5.1.1. **Plan de Contingencia Informático.** 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 con el fin de reanudar las operaciones en el menor tiempo posible en forma eficiente y oportuna. Asimismo, establece las acciones a realizarse en las siguientes etapas: Antes, como un plan de prevención para mitigar los incidentes. Durante, como un plan de emergencia y/o ejecución en el momento de presentarse el incidente. Después, como un plan de recuperación una vez superado el incidente para regresar al estado previo a la contingencia.

5.1.2. **Incidente**. Circunstancia o suceso que sucede de manera inesperada y que puede afectar al desarrollo de una actividad, aunque no forme parte de él. En nuestro contexto, es una interrupción de las condiciones normales de operación en cualquier proceso informático en el SENAMHI.

5.1.3. **Método 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.

5.1.4. **Plan de Prevención.** Es el conjunto de acciones, decisiones y comprobaciones orientadas a prevenir la presencia de un evento no deseado, con el propósito de disminuir y mitigar la probabilidad de ocurrencia del mismo en las categorías identificadas en el presente plan. El

plan de prevención es la parte principal del Plan de Contingencia porque permite aminorar y atenuar la probabilidad de ocurrencia de un estado de contingencia.

5.1.5. **Plan de Ejecución.** Es el conjunto detallado de acciones 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. Las acciones descritas dentro del plan de ejecución deben ser completamente claras y definidas de forma tal que sean de conocimiento y entendimiento inequívoco del personal involucrado en atender la contingencia.

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

5.1.7. **Plan de Pruebas**. Está constituido por un conjunto de pruebas. Cada prueba debe dejar claro qué tipo de propiedades se quieren probar, cómo se mide el resultado, especificar en qué consiste la prueba y definir cuál es el resultado que se espera.

5.2. SIGLAS

5.2.1. OTI. Oficina de Tecnologías de la Información y la Comunicación.

5.2.2. UFN. Unidad Funcional Operativa de Infraestructura Tecnológica

5.2.3. **UFI. Unidad** Funcional Operativa de Sistemas de Información

6. METODOLOGÍA

El desarrollo del presente Plan seguirá la siguiente metodología basada en siete (7) fases:

- Fase 1: Planificación.
- Fase 2: Determinación de vulnerabilidades y escenarios de contingencia.
- Fase 3: Estrategias.
- Fase 4: Elaboración del Plan de Contingencia informático.
- Fase 5: Definición y Ejecución del Plan de Pruebas.
- Fase 6: Implementación del Plan de Contingencia.
- Fase 7: Monitoreo

A continuación, se detalla casa fase:

6.1. FASE 1: PLANIFICACIÓN.

6.1.1. Diagnóstico

Efectuada la revisión de la documentación existente de Tecnologías de Información del SENAMHI, se ha identificado la existencia de normas, procedimientos y controles que cubren algunos aspectos de la seguridad de la información, tales como: Procedimiento de Gestión de Backup (PR-OTI-002), Procedimiento de Gestión de Restauración (PR-OTI-004), Procedimiento de Gestión de mantenimiento preventivo y correctivo de equipos informáticos y redes de comunicaciones de datos (PR-OTI-003), , Procedimiento de Gestión de la seguridad perimetral (PR-OTI-007), Procedimiento de Gestión de Control Accesos a los sistemas informáticos y recursos tecnológicos (PR-OTI-006) Procedimiento de Auditoria de Seguridad (PR-OTI-005).

Sin embargo, aún está pendiente realizar una identificación de los controles que obedescan a una definición previa de una política de Seguridad y a una evaluación de riesgos de seguridad de la información a nivel de todo el SENAMHI.

6.1.2. Marco Institucional

El Servicio Nacional de Meteorología e Hidrología del Perú (SENAMHI), es una entidad técnica especializada del Estado Peruano que provee información y conocimiento meteorológico, hidrológico y climático para la sociedad peruana de manera oportuna y confiable, para la toma de decisiones de las autoridades y público en general.

SENAMHI como entidad pública busca modernizar los sistemas de información y servicios mediante las TICs lo que llevará a un incremento en la eficiencia y eficacia de la difusión de información obtenida de los estudios del tiempo.

Su rol principal es planificar, organizar, coordinar, normar, dirigir y supervisar las actividades meteorológicas, hidrológicas, agrometeorológicas y ambiental atmosféricas con fines de monitoreo, pronóstico y desarrollo de estudios e investigaciones en materia de su competencia hidrometeorológica y ambiental teniendo en cuenta el conocimiento del clima del Perú, como sus recursos naturales y como factor esencial las actividades económico sociales obteniendo predicciones meteorológicas en diversas escalas de tiempo. Para el apoyo en las estrategias de reducción de los efectos perjudiciales de los fenómenos hidrometeorológicos. Logrando una evaluación cuantitativa y cualitativa de los recursos hídricos para su aprovechamiento óptimo de los sectores.

Las funciones del SENAMHI conforme lo establecido en el Reglamento de Organización y Funciones son:

- Desarrollar, evaluar y actualizar el planeamiento estratégico de Tecnologías de la Información y la Comunicación (TIC), de la entidad en concordancia con los objetivos institucionales y necesidades de los Órganos de la entidad.
- Formular, proponer y evaluar las políticas y planes en materia de Tecnologías de la Información y la Comunicación (TIC), en le entidad, en concordancia con lineamientos de política establecidos.
- Proponer y ejecutar proyectos tecnológicos de desarrollo de sistema de información.

- Programar, desarrollar y administrar los sistemas de información y comunicaciones que sirvan de apoyo a las actividades operativas de gestión de la entidad.
- Administrar los procesos de la seguridad de la información y las comunicaciones.
- Abastecer el soporte de recursos tecnológicos a los sistemas de información y las comunicaciones institucionales.
- Asistir al sistema de archivo, trámite, procedimientos y directivas para la regulación de los procesos de atención a los ciudadanos.
- Formular y proponer los estándares, procedimientos y directivas para la regulación de los procesos de atención a los ciudadanos.
- Organizar, conducir y ejecutar la provisión de información y orientación al ciudadano de acuerdo a la normatividad vigente.
- Cumplir con las normas, estándares y directivas emitidas por el Ente Rector del Sistema Nacional de Informática.
- Promover el gobierno electrónico a través del uso intensivo de las tecnologías de la información y la comunicación (TIC).
- Formular, proponer e implementar los lineamientos de políticas y normas sobre recursos informáticos, comunicaciones y la administración del soporte para las bases de datos o similares y la transmisión de las observaciones meteorológicas, hidrológicas, agro meteorológicas y ambientales.
- Elaborar, proponer e implementar el Plan de Contingencia de Sistemas de Información.
- Elaborar, desarrollar, ejecutar, evaluar y mantener el Plan Operativo Informático en armonía con las políticas trazadas por la Alta Dirección.
- Efectuar el soporte tecnológico Informático para el portal web institucional, portal de transparencia, y otros medios de comunicación.
- Planificar y ejecutar el mantenimiento preventivo y correctivo del parque informático e inventario de hardware y software en coordinación con la Unidad de Logística.
- Otras funciones que le sean asignadas por la Secretaria General, en el ámbito de su competencia.

6.1.3. Organización del SENAMHI.

La estructura orgánica del Servicio Nacional de Meteorología e Hidrología del Perú – SENAMHI, aprobada mediante Decreto Supremo N° 003-2016-MINAM, es la siguiente:

- Órganos de la Alta Dirección:
  - Consejo Directivo
  - Presidencia Ejecutiva
  - Gerencia General

- Órgano de Control Institucional
  - Órgano de Control Institucional

- Órganos de Asesoramiento
  - Oficina de Planeamiento y Presupuesto
    - Unidad de Planeamiento e Inversión Pública
    - Unidad de Presupuesto
    - Unidad de Modernización y Gestión de la Calidad
    - Unidad de Cooperación Técnica
  - Oficina de Asesoría Jurídica

- Órganos de Apoyo
  - Oficina de Administración
    - Unidad de Abastecimiento
    - Unidad de Tesorería
    - Unidad de Contabilidad
    - Oficina de Recursos Humanos
  - Oficina de Tecnologías de la Información y la Comunicación

- Órganos de Línea
  - Dirección de Redes de Observación y Datos
    - Subdirección de Gestión de Redes de Observación
    - Subdirección de Gestión de Datos
  - Dirección de Meteorología y Evaluación Ambiental Atmosférica
    - Subdirección de Predicción Meteorológica

Subdirección de Predicción Climática

Subdirección de Modelamiento Numérico de la Atmósfera

Subdirección de Evaluación del Ambiente Atmosférico

- Dirección de Hidrología

  Subdirección de Predicción Hidrológica

  Subdirección de Estudios e Investigaciones Hidrológicas

- Dirección de Agrometeorología

  Subdirección de Predicción Agrometeorológica

  Subdirección de Estudios e investigaciones Agrometeorológicas

- Órganos Desconcentrados
  - Direcciones Zonales

6.1.4. Organigrama del Servicio Nacional de Meteorología e Hidrología del Perú – SENAMHI:

Se muestra los órganos de dirección y coordinación entre la Presidencia Ejecutiva, Gerencia General, Órganos de Línea y Direcciones Zonales.

Gráfico 01: Organigrama de SENAMHI.

6.1.5. Rol de la Oficina de Tecnologías de la Información y la Comunicación (OTI) de la institución.

La OTI, según el ROF del SENAMHI, tiene las siguientes funciones:

- Desarrollar, evaluar y actualizar el planeamiento estratégico de Tecnologías de la Información y la Comunicación (TIC), de la entidad en concordancia con los objetivos institucionales y necesidades de los Órganos de la entidad.
- Formular, proponer y evaluar las políticas y planes en materia de Tecnologías de la Información y la Comunicación (TIC), en le entidad, en concordancia con lineamientos de política establecidos.
- Proponer y ejecutar proyectos tecnológicos de desarrollo de sistema de información.
- Programar, desarrollar y administrar los sistemas de información y comunicaciones que sirvan de apoyo a las actividades operativas de gestión de la entidad.
- Administrar los procesos de la seguridad de la información y las comunicaciones.
- Abastecer el soporte de recursos tecnológicos a los sistemas de información y las comunicaciones institucionales.
- Asistir al sistema de archivo, trámite, procedimientos y directivas para la regulación de los procesos de atención a los ciudadanos.
- Formular y proponer los estándares, procedimientos y directivas para la regulación de los procesos de atención a los ciudadanos.
- Organizar, conducir y ejecutar la provisión de información y orientación al ciudadano de acuerdo a la normatividad vigente.
- Cumplir con las normas, estándares y directivas emitidas por el Ente Rector del Sistema Nacional de Informática.
- Promover el gobierno electrónico a través del uso intensivo de las tecnologías de la información y la comunicación (TIC).
- Formular, proponer e implementar los lineamientos de políticas y normas sobre recursos informáticos, comunicaciones y la administración del soporte para las bases de datos o similares y la transmisión de las observaciones meteorológicas, hidrológicas, agro meteorológicas y ambientales.
- Elaborar, proponer e implementar el Plan de Contingencia de Sistemas de Información.

- Elaborar, desarrollar, ejecutar, evaluar y mantener el Plan Operativo Informático en armonía con las políticas trazadas por la Alta Dirección.
- Efectuar el soporte tecnológico Informático para el portal web institucional, portal de transparencia, y otros medios de comunicación.
- Planificar y ejecutar el mantenimiento preventivo y correctivo del parque informático e inventario de hardware y software en coordinación con la Unidad de Logística.
- Otras funciones que le sean asignadas por la Secretaria General, en el ámbito de su competencia.

Para un mejor manejo operacional en cumplimiento al Decreto Supremo N° 054-2018-PCM, mediante Resolución Presidencial Ejecutiva N° 0171–2016/SENAMHI-PREJ-SG-OTI del 15 de agosto del 2016, establece la creación de las siguientes unidades funcionales operativas para la OTI:Unidad Funcional Operativa de Sistemas de Información (UFI) y Unidad Funcional Operativa de Infraestructura Tecnológica (UFN).

Las Unidades Funcionales Operativas de la OTI, según la Resolución Presidencial Ejecutiva Nro. 0171–2016/SENAMHI-PREJ-SG-OTI, tienen las siguientes funciones:

Unidad Funcional Operativa de Sistemas de Información (UFI):

- Brindar asistencia técnica a los usuarios de sistemas desarrollados en el SENAMHI, y asegurar el registro, análisis, gestión de incidentes y problemas con el fin de incrementar los niveles de confiabilidad.
- Gestionar el análisis, diseño, construcción, implementación, y mantenimiento de los sistemas de información institucionales, en concordancia con las metodologías de desarrollo aprobadas y las políticas de seguridad establecidas.
- Planificar, ejecutar, monitorear y evaluar los proyectos de desarrollo propio de software, así como participar, evaluar y aprobar los que sean realizados por terceros, dentro del ámbito de su competencia.
- Garantizar una adecuada gestión de los requerimientos referidos al desarrollo y mantenimiento de sistemas de información, así como el

apoyo técnico para registrar y publicar la información del SENAMHI en el portal institucional.

- Desplegar los productos de software desarrollados y realizar el entrenamiento y/o capacitación respectiva.
- Definir las arquitecturas de procesos, información y aplicaciones que sirvan como base para los sistemas a ser implementados, conjuntamente con las áreas usuarias.
- Formular y mantener las metodologías y estándares de desarrollo de software para el SENAMHI, supervisando su cumplimiento en las diversas fases del ciclo de vida del software.
- Realizar labores de aseguramiento de la calidad de los sistemas de información que desarrolle y que garantice el cumplimiento de los requerimientos funcionales, el cumplimiento de estándares y la optimización de los recursos informáticos.
- Desarrollar el análisis, modelamiento y administración de datos relevantes relacionados con las actividades institucionales, a fin de generar el conocimiento necesario para facilitar la toma de decisiones a nivel estratégico.
- Desarrollar los mecanismos para la integración de información interna o externa que requiera el SENAMHI, necesaria para la toma de decisiones;
- Instalación del motor de base de datos, en colaboración y coordinación con el administrador de redes, que consiste en realizar tareas de instalación y configuración del motor de la Base de Datos, actualizaciones, herramientas administrativas, cambios de hardware, planificación de capacidad, etc.
- Controlar la seguridad de la Base de Datos que incluye la altas y bajas de usuarios, creación de roles y auditorias de seguridad.
- Monitorear y optimizar del rendimiento de la Base de Datos.
- Realizar las copias de seguridad (Backups) y participar en la política de copias de seguridad y recuperación de datos.
- Prevención de riesgos a través de la información de los cambios de hardware y software en el servidor, programar mantenimientos, probar copias de seguridad, etc.

- Apoyar a los desarrolladores que incluye el diseño del modelo de datos, la optimización (TUNING), construcción de procedimientos almacenados y triggers, definición de estándares de diseño y nomenclatura.
- Documentar todo lo relativo a la Base de Datos.
- Análisis, desarrollo e implementación de sistemas de datos espaciales del SENAMHI.
- Mantenimiento de los sistemas GIS interoperable.
- Desarrollar servicios GIS interoperables - Web y Móvil.
- Mejora continua del sistema de catálogo de metadatos del SENAMHI.
- Elaborar directivas de procedimientos y estándares para la producción cartográfica en el SENAMHI; y,
- Las demás tareas que le asigne el director de la Oficina de Tecnologías de la Información y la Comunicación.

Unidad Funcional Operativa De Infraestructura Tecnológica (UFN)

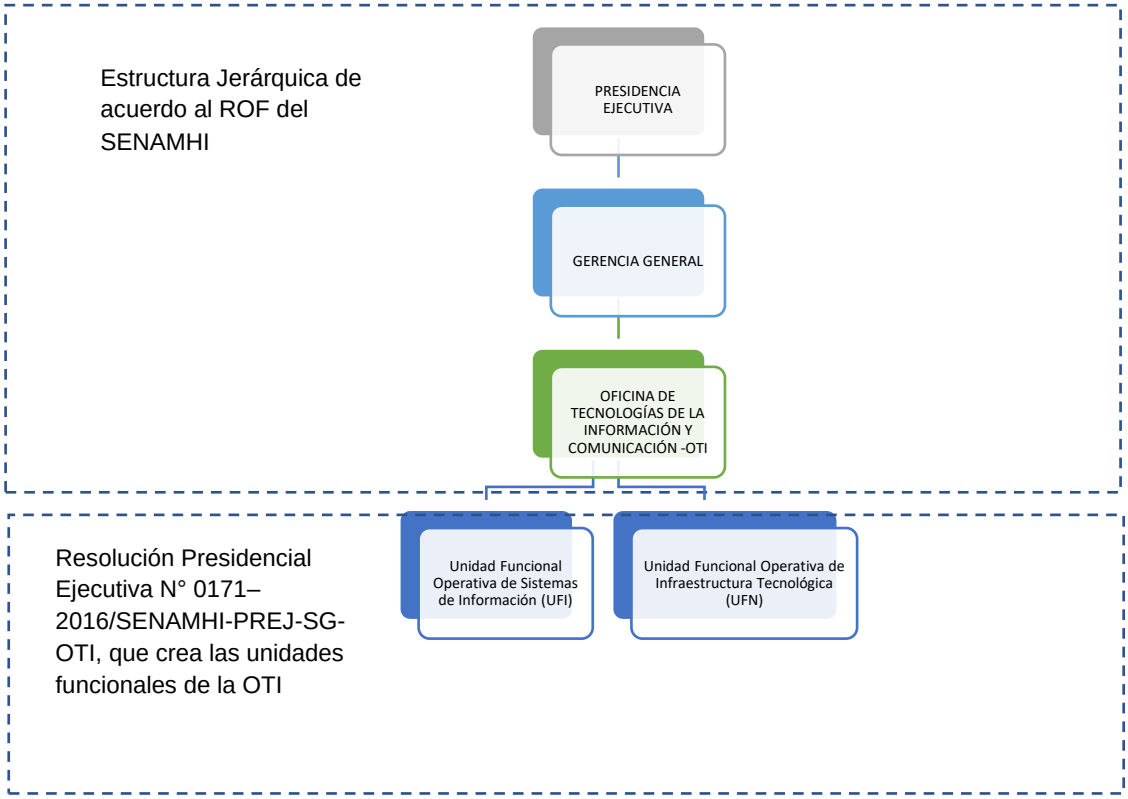
- Brindar apoyo a los usuarios cuando se presenta problemas de software y/o hardware.
- Realizar servicios técnicos a los equipos, de acuerdo a la solicitud del usuario, o en caso de presentar falla.
- Apoyar a usuarios en operaciones de implementación o adecuación de servicios informáticos.
- Instalación y mantenimiento de software propio.
- Configuración de dispositivos de hardware y otros periféricos.
- Inventario y control de hardware y software.
- Informar las condiciones de uso, status y vigencia de todo el software que maneja la institución, de manera que esta información pueda ser manejada como soporte para la toma de decisiones.
- Presentar propuestas de políticas de uso de equipos informáticos.
- Formación y capacitación de los usuarios.
- Desarrollo de planes de mantenimiento de equipos informáticos.
- Asesorar en la elaboración de especificaciones técnicas para la adquisición de productos y/o servicios.

- Mantener niveles adecuados del desempeño, capacidad operativa y seguridad de la infraestructura informática, redes de comunicaciones, servicios de tecnologías de información y la plataforma tecnológica;
- Diseñar, implementar y gestionar el plan de contingencia informático y el plan de continuidad de negocios de la institución en el ámbito de su competencia.
- Administrar y asegurar la disponibilidad y el acceso a los aplicativos, base de datos y redes corporativas en producción, teniendo en cuenta las necesidades de los órganos.
- Diseñar, implementar y mantener la infraestructura tecnológica, los sistemas de seguridad informática y la arquitectura tecnológica de nuevos sistemas de información, considerando los requerimientos del Plan Estratégico de Tecnologías de Información (PETI) y las necesidades de las Direcciones del SENAMHI.
- Definir e implementar el proceso de atención de los requerimientos de tecnologías de la información de las direcciones del SENAMHI, así como el registro, clasificación y gestión de incidentes y problemas que permita mejorar el desempeño de los servicios brindados.
- Proponer proyectos y alternativas de solución que permitan el mejoramiento de los servicios, sistemas e infraestructura de tecnologías de información del SENAMHI.
- Gestionar y verificar los trabajos encargados a terceros relacionados con la instalación y mantenimiento de la infraestructura tecnológica y aplicativa del SENAMHI.
- Proveer la información, los mecanismos y herramientas para la actualización del inventario de activos informáticos.
- Definir y dar mantenimiento de las políticas y planes de seguridad informático para el SENAMHI.
- Coordinar la implementación de la infraestructura de seguridad.
- Proponer la implementación de nuevas tecnologías de seguridad informática.
- Estudiar los incidentes de seguridad informática en el SENAMHI, coordinando con las áreas que correspondan, las actividades necesarias para su solución.
- Proponer proyectos relacionados con la seguridad física y lógica para el SENAMHI, y.

- Las demás tareas que le asigne el director de la Oficina de Tecnologías de la Información y la Comunicación.

6.1.6. Ubicación de la OTI en la organización.

Gráfico 02: Ubicación de la OTI

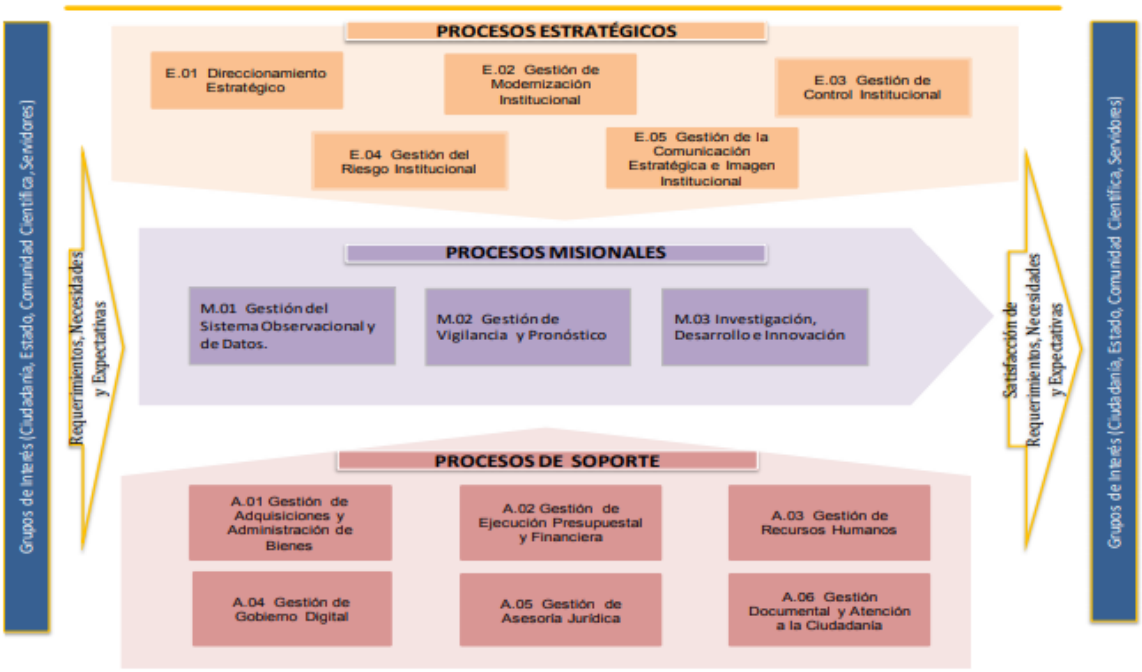


6.1.7. Procesos de la Entidad

Mediante la resolución de Gerencia General N°035-2020-SENAMHI/GG, de fecha 31 de diciembre del 2020 se aprueba:

- Modificar el Mapa de Procesos del Servicio Nacional de Meteorología e Hidrología del Perú – SENAMHI.
- Manual de Procedimientos - MAPRO del Servicio Nacional de Meteorología e Hidrología del Perú - SENAMHI

Gráfico 03: Mapa de procesos del SENAMHI



- Procesos de nivel 0
  - E.01. Direccionamiento Estratégico.
  - E.02. Gestión de Modernización institucional.
  - E.03. Gestión de Control Institucional.
  - E.04. Gestión de Riesgo Institucional.
  - E.05. Gestión de la Comunicación Estratégica e Imagen Institucional.
  - M.01. Gestión del Sistema Observacional y de datos.
  - M.02. Gestión de vigilancia y pronósticos.
  - M.03. Investigación, Desarrollo e Innovación
  - A.01. Gestión de Adquisiciones y Administración de Bienes.

- A.02. Gestión de Ejecución Presupuestal y Financiera.
- A.03. Gestión de Recursos Humanos.
- A.04. Gestión de Gobierno Digital.
- A.05. Gestión de Asesoría Jurídica.
- A.06. Gestión Documental y Atención a la Ciudadanía.

En el marco de lo expuesto, la dirección de la Oficina de Tecnologías de la Información y la Comunicación es dueña del proceso A.04 Gestión del Gobierno digital, siendo los procesos de último nivel que la comprenden y sobre los cuales se realizará el análisis de riesgos, los que se listan a continuación:

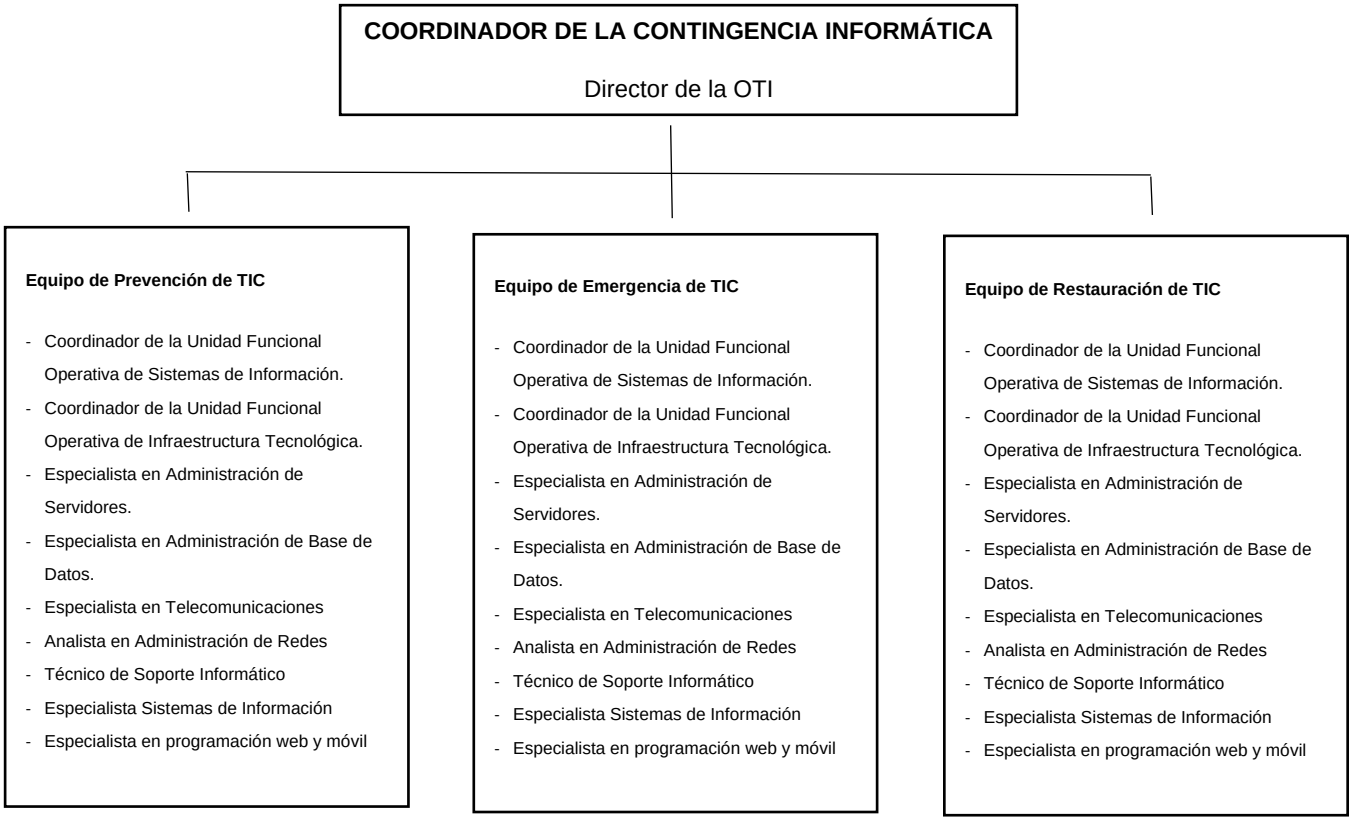
Tabla N° 01: Inventario aprobado de procesos Gestión del Gobierno Digital

A.04	Gestión de Gobierno Digital	A.04.01	Gestión de la Seguridad de la Información	A.04.01.01	Gestión de Control de accesos a los Sistemas Informáticos y recursos tecnológicos
				A.04.01.02	Gestión de la seguridad perimetral.
				A.04.01.03	Gestión de backups
				A.04.01.04	Gestión de restauración
				A.04.01.05	Auditoria a la seguridad de la información
		A.04.02	Gestión de Operación del Servicio de TI	A.04.02.01	Gestión de la atención de requerimientos de soporte técnico informático
				A.04.02.02	Gestión preventivo y correctivo de equipos informáticos y redes de comunicaciones de datos
				A.04.02.03	Administración de los Servicios de Telefonía Fija, Internet y Cable
				A.04.02.04	Gestión de Cambios
				A.04.02.05	Gestión de licencias de software
				A.04.02.06	Gestión de telefonía móvil
				A.04.02.07	Gestión de recursos tecnológicos
		A.04.03	Gestión de Sistemas de Información	A.04.03.01	Gestión de la adquisición de sistemas informáticos
				A.04.03.02	Gestión de desarrollo y mantenimiento de sistemas informáticos
		A.04.04	Gestión Normativa de TI	A.04.04.01	Gestión de Planes y Documentos Normativos de TI
				A.04.04.02	Gestión de Proyectos de TI
				A.04.04.03	Gestión de Mejora Continua de los Servicios de TI

6.1.8. Organización del Plan de Contingencia Informático

Para el funcionamiento del Plan de Contingencia Informático, se ha establecido la siguiente organización operativa, conformado exclusivamente por personal de la OTI.

Gráfico N° 04: Organización Operativa del Plan de Contingencia Informático y Recuperación de Servicios de Tecnología de la Información y Comunicaciones (TIC)



La relación del personal de la OTI que forma parte del Plan de contingencia debe ser actualizada de manera permanente y socializada al siguiente personal:

- Personal de la OTI.
- Personal de la Alta Dirección.
- Caseta de vigilancia de cada una de las sedes de la entidad.

Las actividades planificadas como parte del presente plan podrán ejecutarse en forma presencial, semipresencial o en remoto, conforme a los escenarios de prueba que pudieran desprenderse ante los diversos eventos de mayor

impacto considerados para el presente Plan de Contingencia Informático; así como, conforme a las disposiciones vigentes.

6.1.9. Roles, funciones y responsabilidades dentro del Plan de Contingencia Informático.

A continuación, se describe los roles, responsabilidades y funciones que deben desarrollar los distintos equipos del Plan de Contingencia Informático.

a. Coordinador de Continuidad de TIC

Está representado por el/la Director/a de la OTI y tiene las siguientes funciones:

- Coordinar, dirigir y decidir respecto a acciones o estrategias a seguir en un escenario de contingencia dado.
- Tomar la decisión de activar el Plan de Contingencia Informático y Recuperación de Servicios de Tecnologías de la Información y Comunicaciones.
- Guiar y supervisar a los equipos operativos de contingencia informática, 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.
- Monitorear, supervisar y vigilar la recuperación de infraestructura de Tecnologías de la Información (TI) en el Centro de Datos.
- Contactar a los proveedores 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 Contingencia Informático y Recuperación de Servicios de Tecnologías de la Información y Comunicaciones, cuando las operaciones del Centro de Datos hayan sido restablecidas.

b. Equipo de Prevención de TIC

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

Los responsables del Equipo de Prevención de TIC serán los coordinadores de la Unidad Funcional Operativa de Sistemas de Información y la Unidad Funcional Operativa de Infraestructura Tecnológica. A continuación, se detallan las funciones por cada integrante del equipo de prevención:

Coordinadores de la de la Unidad Funcional Operativa de Sistemas de Información y la Unidad Funcional Operativa de Infraestructura Tecnológica

- Establecer y supervisar los procedimientos de seguridad de los servicios de TIC.
- Coordinar la realización de las pruebas de restauración de hardware y software.
- Participar en las pruebas y simulacros de desastres.
- Verificar la realización del mantenimiento preventivo a los equipos componentes del Centro de Datos. Verificar las tareas de copias de respaldo (backup).

Especialista en Administración de Servidores.

- Monitorear el funcionamiento de los servidores existentes en el centro de datos.
- Mantener actualizado el inventario de los servidores existentes en el centro de datos.
- Verificar el estado de las garantías y/o licencias soportes de los servidores ubicados en el centro de datos.
- Coordinar oportunamente los upgrade de los servidores

Especialista en Administración de Base de Datos.

- Realizar copias de respaldo de las bases de datos de los aplicativos y sistemas de la entidad.
- Acopiar las copias de respaldo y clasificarlas por tipo de motor de base de datos, aplicativos y sistemas.
- Realizar las pruebas de restauración de bases de datos en coordinación con el Especialista en Seguridad de la Información.

Especialista en Telecomunicaciones

- Monitorear el funcionamiento de la Central Telefónica
- Verificar que la central telefónica cuenta con las garantías requeridas.
- Mantener actualizada la lista de anexos y teléfonos.
- Actualizar el software que utiliza la central telefónica.

Analista en Administración de Redes

- Mantener actualizado el inventario hardware y software utilizado en el Centro de Datos de la entidad.
- Ejecutar y verificar las tareas de copias de respaldo (backup).
- Programar y/o realizar el mantenimiento preventivo de los equipos de comunicaciones y de los equipos componentes del Centro de Datos, considerando el tiempo de vida útil y garantía de los mismos.
- Llevar un control detallado del mantenimiento realizado a cada equipo y componentes del Centro de Datos.
- Elaborar informes técnicos de conformidad, luego de cada mantenimiento efectuado, así como elaborar informes periódicos del funcionamiento del Centro de Datos.
- Verificar que se mantiene actualizado los diagramas de servidores, los diagramas de red, la documentación de las configuraciones de equipos de comunicaciones, el inventario de software de gestión y otros.

- Monitorear la red y definir medidas preventivas para minimizar o evitar las contingencias.
- Realizar las pruebas previas de recuperación.

Técnico de Soporte Informático

- Mantener actualizado el inventario hardware y software de usuario final.
- Verificar el estado de las garantías y/o vigencias tecnológicas de los equipos informáticos de usuario final

Especialista Sistemas de Información

- Soporte y mantenimiento de los sistemas y aplicativos instalados en la entidad.
- Documentación, consolidación y validación de los manuales de los sistemas en producción.
- Realizar periódicamente las pruebas de restauración de las fuentes de los sistemas de información en producción de la entidad.

Especialista en programación web y móvil

- Soporte y mantenimiento al portal web y de los sistemas móviles en producción.
- En coordinación con el especialista en administración de servidores habilitar un servidor de contingencia que contenga el portal web institucional y las configuraciones respectivas.

c. <u>Equipo de Emergencia de TIC</u>

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

A continuación, se citan las acciones que se realizarán durante la contingencia, según los miembros del equipo:

Coordinadores de la de la Unidad Funcional Operativa de Sistemas de Información y la Unidad Funcional Operativa de Infraestructura Tecnológica

- Apoyar en las labores de verificación y validación de operación de los servicios de TIC.
- Coordinar acciones para la verificación de estado de los sistemas de información alojados en los servidores de aplicaciones.
- Coordinar acciones para verificar el estado de las bases de datos de los sistemas de información.

Especialista en Administración de Servidores.

- Notificar el desastre o incidencia al Coordinador de Continuidad de TIC.
- Ejecutar las acciones de emergencia en los servidores instalados en el Centro de Datos del SENAMHI.
- Realizar la evaluación de condiciones de los servidores del Centro de Datos del SENAMHI, durante la emergencia.
- Comunicar al Coordinador de Continuidad de TIC las acciones de emergencia ejecutadas.

Especialista en Administración de Base de Datos.

- Realizar la evaluación de las condiciones de los datos y la información almacenada en las diferentes bases de datos, durante la emergencia.

Especialista en Telecomunicaciones

- Ejecutar las acciones de emergencia en la central telefónica instalada en el SENAMHI.
- Realizar la evaluación de condiciones de los equipos de telecomunicaciones, durante la emergencia.

- Comunicar al Coordinador de Continuidad de TIC las acciones de emergencia ejecutadas.

Analista en Administración de Redes

- Notificar el desastre o incidencia al Coordinador de Continuidad de TIC.
- Ejecutar las acciones de emergencia en los equipos de comunicación y componentes instalados Centro de Datos del SENAMHI.
- Realizar la evaluación de condiciones de los equipos de comunicaciones y los componentes del Centro de Datos del SENAMHI, durante la emergencia.
- Comunicar al Coordinador de Continuidad de TIC las acciones de emergencia ejecutadas.

Técnico de Soporte Informático

- Realizar la evaluación de la afectación a los equipos informáticos de usuario final (computadoras, teléfonos, impresoras, entre otros).
- Notificar los casos críticos en cuanto a equipos de usuario final, que afecte la continuidad de operaciones y/o la pérdida de información de los usuarios del SENAMHI.

Especialista Sistemas de Información

- Realizar la evaluación de las condiciones de los aplicativos informáticos y sistemas de información durante la emergencia.
- Solicitar los logs de los aplicativos informáticos afectados durante la emergencia.

Especialista en programación web y móvil

- En coordinación con el especialista en administración de servidores, poner en operatividad el servidor que contiene el portal web de contingencia.

- Realizar la evaluación de las condiciones del portal web y sus componentes durante la emergencia.
- Solicitar los logs de las conexiones al portal web durante la emergencia.

d. <u>Equipo de Restauración de TIC</u>

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 SENAMHI.

Coordinadores de la de la Unidad Funcional Operativa de Sistemas de Información y la Unidad Funcional Operativa de Infraestructura Tecnológica

- Coordinar acciones para la verificación de estado de los sistemas de información alojados en los servidores de aplicaciones.
- Coordinar el estado de las bases de datos de los sistemas de información.
- Coordinar y monitorear la restauración de aplicativos y ejecución de pruebas para verificación de funcionalidad.
- Supervisar la restauración de los servicios de TI.
- Validar la información documentada de los procedimientos de restauración utilizados.

Especialista en Administración de Servidores y Analista en Administración de Redes

- Inician 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 componentes del Centro de Datos del SENAMHI.
- Restaurar la información de los equipos afectados de la infraestructura informática que afecten los servicios de TI y los equipos componentes del Centro de Datos del SENAMHI.

- Notificar al Coordinador de Continuidad de TIC, las acciones de recuperación ejecutadas.
- Elaborar un informe técnico, que incluya las acciones de recuperación de los equipos de comunicaciones, los servidores y los equipos componentes del Centro de Datos.

Especialista en Administración de Base de Datos.

- Verificar el funcionamiento de las bases de datos institucionales.
- Realizar la creación de bases de datos en servidores alternos, en caso sea requerido.
- Restaurar las copias de respaldo correspondientes respetando la prioridad establecida para cada escenario.
- Realizar las pruebas de funcionamiento.
- Elaborar un informe técnico que incluya la evaluación de condiciones de los datos e información del SENAMHI luego de efectuado el proceso de recuperación.

Especialista en Telecomunicaciones

- Iniciar el proceso de recuperación de los servicios relacionados a la central telefónica instalada en el SENAMHI.
- Realizar la evaluación de condiciones de los equipos de telecomunicaciones, durante la emergencia.
- Elaborar un informe técnico, que incluya las acciones de recuperación de los equipos móviles y la central telefónica ubicada del Centro de Datos.

Técnico de Soporte Informático

- Verificar el funcionamiento de los equipos personales en las sedes afectadas del SENAMHI, distribuyendo el trabajo entre los técnicos de soporte.
- Solucionar los problemas de conexión y funcionamiento de los equipos personales, impresoras, escáner entre otros.
- Elaborar un informe técnico que incluya la evaluación de condiciones de los equipos personales e información del

personal del SENAMHI, luego de efectuado el proceso de recuperación.

Especialista Sistemas de Información

- Verificar el estado de Los sistemas alojados en los servidores de aplicaciones del SENAMHI, en caso se quiera desplegar y/o reinstalar los sistemas de información, de lo contrario verificar que se encuentren funcionando correctamente.
- Elaborar un informe técnico que incluya la evaluación de condiciones de los sistemas de información del SENAMHI.

Especialista en programación web y móvil

- Verificar que el portal web y los sistemas móviles institucional se encuentre funcionando correctamente.
- Elaborar un informe técnico que incluya la evaluación de condiciones del portal web y los sistemas móviles del SENAMHI

6.2. FASE 2: DETERMINACIÓN DE VULNERABILIDADES Y ESCENARIOS DE CONTINGENCIA.

En esta fase se ha procedido a la identificación de las aplicaciones críticas, los recursos y el periodo máximo de recuperación de los servicios de tecnologías de la información y comunicaciones, para los cuales se consideraron todos los elementos susceptibles de provocar eventos que conlleven a activar la contingencia.

6.2.1. Procesos y recursos críticos

A continuación, se detalla los procesos, aplicaciones y recursos críticos, con su respectiva expectativa del tiempo de recuperación:

Tabla N° 02: Procesos y recursos críticos

PROCESO	APLICACIONES Y/O RECURSOS CRITICOS	TIEMPO DE RECUPERACION (RTO)
Gestión de Operación del Servicio	Grupo electrógeno	6 h
	Sistema de aire acondicionado del Centro de Datos	6 h
	Sistema de alarmas contraincendio	6 h
	Sistema de cámaras de videovigilancia	6 h
	Equipos de protección eléctrica del centro de datos (UPS)	6 h
	Infraestructura del Centro de Datos	24 h
	Equipos de comunicaciones.	6 h
	Cableado de red de datos	6 h
	Estaciones de trabajo del personal crítico (computadoras personales y portátiles)	6 h
	Central Telefónica	6 h
	Personal crítico responsable de los procesos de TIC.	2 h
Gestión de la Seguridad de la Información	Equipo de seguridad perimetral	6 h
	Servidores de aplicaciones críticas	24 h
	Servidores de aplicaciones en general	6 h
	Medios de respaldo (cintas de backup)	6 h
	Base de datos y repositorios utilizados por los sistemas y aplicativos.	24 h
Gestión de Sistemas de Información	Sistemas de información y portales core	24 h
	Sistemas de información administrativos	6 h

*El RTO: Tiempo de Recuperación Objetivo, es determinado por Juicio de Expertos.

6.2.2. Identificación de amenazas

Este paso, permite identificar aquellas amenazas que pudieran vulnerar los servicios TIC del SENAMHI, considerando la ubicación geográfica, el contexto actual de la sede central y centro de datos, así como la percepción del juicio experto.

Tabla N° 03: Identificación de Amenaza

N°	AMENAZA (EVENTO)	TIPO
1	Terremoto/Sismo	Siniestros Naturales
2	Inundación y aniego en el Centro de Datos.	
3	Incendio en el centro de datos	
4	Falla en telecomunicaciones.	Tecnológicos
	Falla en el servicio de internet principal	
5	Delito informático.	
6	Falla de hardware y software.	
7	Falla del suministro eléctrico en el Centro de Datos y gabinetes de comunicación.	Físico y ambiental
8	Ausencia o no disponibilidad del personal crítico de TI.	Humanos
9	Pandemia y/o Epidemia	Ambiental

Determinadas las amenazas que pueden afectar los recursos críticos de TI, se ha calculado el nivel de probabilidad estimada, a fin de identificar las amenazas que serán consideradas en la evaluación de los riesgos.

A continuación, se detalla el resultado obtenido:

Tabla N° 04: Nivel de probabilidad estimada

N°	AMENAZA (EVENTO)	OCURRENCIA	PERCEPCIÓN	NIVEL PROBABILIDAD ESTIMADA
1	Terremoto/Sismo	2	5	Extremo
2	Inundación y aniego en el centro de datos.	1	2	Menor
3	Incendio en el centro de datos	2	5	Extremo
4	Falla en telecomunicaciones.	1	1	Insignificante
5	Falla en el servicio de internet principal	2	2	Menor
6	Delito informático.	3	4	Extremo
7	Falla de hardware y software.	4	4	Extremo
8	Falla del suministro eléctrico en el Centro de Datos y gabinetes de comunicación.	4	4	Extremo
9	Ausencia o no disponibilidad del personal crítico de TI.	1	3	Menor
10	Pandemia y/o Epidemia	1	2	Menor

6.2.3. Identificación de Controles Existentes

La identificación de controles existentes, permiten conocer que tan protegidos están los recursos de TI del SENAMHI frente a cada amenaza.

- Cámaras de vigilancia en el interior exterior del Centro de Datos.
- Instalación reciente de un grupo electrógeno para el centro de datos.
- Equipo informático de seguridad perimetral.
- Mantenimiento de generadores eléctricos y UPS. El mantenimiento de generadores (grupo electrógeno está a cargo de Servicios Generales de la Oficina de Abastecimiento) y el mantenimiento de UPS está a cargo de la OTI).
- Mantenimiento para equipos de aire acondicionado del Centro de Datos.
- Redundancia en los enlaces de comunicaciones (fibra óptica) y de internet, pero con el mismo proveedor.
- Sistema contra incendios en el centro de datos.
- Respaldo de información y custodia externa de medios de respaldo.
- Solución antivirus instalada en los servidores de red y computadoras.
- Solución de correo electrónico en la nube.

6.2.4. Evaluación del Nivel de Riesgo

Para determinar el Nivel de Riesgo de un recurso de TI crítico del SENAMHI, se consideraron los controles existentes que mitigan la afectación de la amenaza descritos en el numeral 5 de acuerdo a la aplicación de la metodología de riesgos descrita en el Anexo N°1, se obtuvo el siguiente resultado:

Tabla N° 05: Resultado de la evaluación de riesgos de los servicios de TI

NRO	RECURSOS CRÍTICOS / AMENAZAS (EVENTOS)	Terremoto/Sismo (4)	Inundación y aniego en el Centro de Datos (2)	Incendio en el centro de datos(4)	Falla en telecomunicaciones (1)	Falla en el servicio de internet principal (2)	Delito informático (4)	Falla de hardware y software (4)	Falla del suministro eléctrico en el Centro de Datos y gabinetes de comunicación (4)	Ausencia o no disponibilidad del personal crítico de TI (2)	Pandemia y/o Epidemia (2)
1	Grupo electrógeno (2)										
2	Sistema de aire acondicionado del Centro de Datos (2)										
3	Sistema de alarmas contraincendio (2)										
4	Sistema de cámaras de videovigilancia (2)										
5	Equipos de protección eléctrica del centro de datos (UPS) (2)										
6	Infraestructura del Centro de Datos (3)										
7	Equipos de comunicaciones. (2)										
8	Cableado de red de datos (2)										
9	Estaciones de trabajo del personal crítico (computadoras personales y portátiles) (2)										
10	Central Telefónica (2)										
11	Personal crítico responsable de los procesos de TIC. (1)										
12	Equipo de seguridad perimetral (2)										
13	Servidores de aplicaciones críticas (3)										
14	Servidores de aplicaciones en general (2)										
15	Medios de respaldo (cintas de backup) (2)										
16	Base de datos y repositorios utilizados por los sistemas y aplicativos. (3)										
17	Sistemas de información y portales core (3)										
18	Sistemas de información administrativos (2)										

6.2.5. Escenarios de riesgo

Los escenarios de riesgos identificados para el presente Plan son los que se detallan a continuación

- Destrucción e indisponibilidad del centro de datos, servidores que contienen aplicaciones críticas, sistemas de información y portales core, base de datos y repositorios utilizados por los sistemas y aplicativos, por un terremoto o incendio.
- Falla en el funcionamiento del centro de datos, servidores que contienen aplicaciones críticas, sistemas de información y portales core, base de datos y repositorios utilizados por los sistemas y aplicativos, por ataque informático (virus, ataque cibernético, etc)
- Indisponibilidad del centro de datos, servidores que contienen aplicaciones críticas, sistemas de información y portales core, base de datos y repositorios utilizados por los sistemas y aplicativos, por fallas en el hardware y software.
- Interrupción en el funcionamiento del centro de datos, servidores que contienen aplicaciones críticas, sistemas de información y portales core, base de datos y repositorios utilizados por los sistemas y aplicativos, por fallas en el suministro eléctrico de la sede central.

A continuación, se presenta el consolidado de los escenarios de riesgo y su impacto, para activar el Plan de Contingencia Informático.

Tabla N° 06: Escenario de Riesgos

ITEM	ESCENARIO DE RIESGO	DESCRIPCION	IMPACTO
1	Destrucción e indisponibilidad del centro de datos, servidores que contienen aplicaciones críticas, sistemas de información y portales core, base de datos y repositorios utilizados por los sistemas y aplicativos	Este escenario consiste en que el Centro de Datos deje de funcionar o se destruya, como resultado de un terremoto, lo cual podría ocasionar caídas de servicios y destrucción de los equipos informáticos alojados en el centro datos, como también los componentes del mismo.	Extremo

2	Destrucción e indisponibilidad del centro de datos, servidores que contienen aplicaciones críticas, sistemas de información y portales core, base de datos y repositorios utilizados por los sistemas y aplicativos	Este escenario consiste en que el Centro de Datos deje de funcionar o se destruya, como resultado de un incendio, lo cual podría ocasionar caídas de servicios y destrucción de los equipos informáticos alojados en el centro datos, como también los componentes del mismo.	Extremo
3	Falla en el funcionamiento del centro de datos, servidores que contienen aplicaciones críticas, sistemas de información y portales core, base de datos y repositorios utilizados por los sistemas y aplicativos	Se refiere a la falla lógica o caída de aplicaciones, sistemas de información, portales core, base de datos y repositorios que no estén disponibles por ataques informáticos.	Extremo
4	Indisponibilidad del centro de datos, servidores que contienen aplicaciones críticas, sistemas de información y portales core, base de datos y repositorios utilizados por los sistemas y aplicativos, por fallas en el hardware y software.	Se refiere al fallo físico o lógico de los servidores físicos y virtuales, lo cual produce que la información o servicios brindados por ellos no estén disponibles.	Extremo
5	Interrupción en el funcionamiento del centro de datos, servidores que contienen aplicaciones críticas, sistemas de información y portales core, base de datos y repositorios utilizados por los sistemas y aplicativos	Este escenario consiste en el corte o interrupción de los servicios informáticos como resultado de fallas del sistema eléctrico o equipos de suministro eléctrico, así como el corte de energía eléctrica, lo cual ocasionar caídas de servicios informáticos y pérdidas de comunicación en los equipos de infraestructura tecnológica.	Extremo

6.3. FASE 3: ESTRATEGIAS DEL PLAN DE CONTINGENCIA

A continuación, se presentan estrategias para la contingencia operativa en caso de un desastre.

6.3.1. Estrategias de prevención de tecnologías de la información

a. Almacenamiento y respaldo de la información (BACKUPS)

- La Gestión de Backup, de la data almacenada y procesada, firewall y servicios, así como la frecuencia con las que se lleva a cabo las tareas

de backup y el servicio de resguardo externo, se encuentran detallados en el Procedimiento PR-OTI-002 Gestión de Backup.

- Verificar la ejecución periódica de las tareas programadas de respaldo de información y comprobación de los medios de respaldo utilizando el procedimiento de PR-OTI-004 Gestión de Restauración.

b. Sitios Alternos para el Centro de Datos El plan incluye una estrategia para recuperar y ejecutar operaciones de sistemas en instalaciones alternativas por un periodo extendido; los sitios alternativos podrán ser:

- Propios de la entidad.

Para tal efecto, se debe identificar un ambiente adecuado como lugar alterno para la recuperación de equipos y servicios de tecnologías de la información del Centro de Datos.

c. Evaluación y gestión de proveedores

- Listado de proveedores claves de servicios y recursos de TI, con sus datos de contacto actualizados.
- Mantener listas detalladas de necesidades de equipos y sus especificaciones técnicas.

d. Entrenamiento y personal de reemplazo

- Todo el personal de la OTI, debe entrenarse en el proceso de recuperación de los servicios de TI. La capacitación debe ser planificada, estructurada y acorde con las exigencias de recuperación. El entrenamiento se debe evaluar para verificar que ha logrado sus objetivos.
- Se debe elaborar un programa de vacaciones que garantice la presencia permanente del personal crítico de las diferentes áreas y procesos de OTI, tales como soporte técnico, servidores, redes y comunicaciones, sistemas de información y bases de datos.

e. Renovación tecnológica

- Programación de una revisión anual de obsolescencia tecnológica de las partes internas de los servidores informáticos, para realizar la renovación de las mismas, en caso se requiera.
- Registrar las incidencias de deterioro de los equipos de almacenamiento, procesamiento y comunicaciones, para en base a las

estadísticas de este registro adquirir equipos de reemplazo y de contingencia.

f. Activación de trabajo remoto

- Verificación y validación de acceso seguro, en remoto, a los sistemas y servicios TICs.
- Activación de redes virtuales VPN, siempre y cuando el equipo a conectarse cuente con los mecanismos de seguridad informáticos necesarios.
- En caso el usuario no cuente con un equipo para realizar su trabajo remoto, se le pueda habilitar el equipo asignado, que se encuentra en la sede del SENAMHI, para entregársela en su domicilio a fin de que cuente con las herramientas necesarias, siguiendo los protocolos dados por la Oficina de Administración
- Realizar el Trámite Certificados digitales, para instalarlos en los equipos de los usuarios, fuera de la institución.
- Activación del desvío de las llamadas telefónicas a los usuarios asignados encarados de la atención de la central telefónica.

6.3.2. Estrategia frente a emergencias en tecnologías de la información

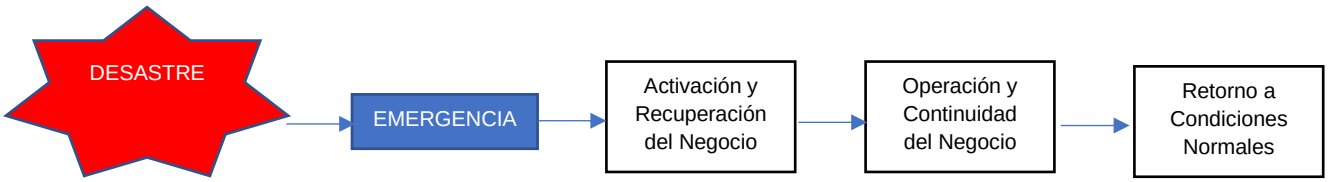
El alcance de las estrategias frente a emergencias involucra las acciones que deben realizarse durante una emergencia o desastre, a fin de salvaguardar la información del SENAMHI y garantizar la continuidad de los servicios informáticos para lo cual se definen las acciones para mitigar las pérdidas que puedan producirse en una emergencia o desastre. A continuación, se citan las acciones que se realizarán durante y después de una contingencia:

- Estudiar y evaluar el alcance del desastre en cada área de responsabilidad.
- Notificar y reunir a los demás integrantes del equipo de Emergencia y Restauración de TIC.
- Informar al responsable del Grupo de Comando de Continuidad Operativa sobre la situación presentada, para decidir la realización de la Declaración de Contingencia y activación del sitio alterno o de respaldo.
- Determinar si el área afectada es segura para el personal (en caso de catástrofe).
- Estudiar y evaluar la dimensión de los daños a los equipos y sus facilidades, y elaborar un informe de los daños producidos.
- Proveer facilidades al personal encargado de la recuperación, con la finalidad de asegurar que se realicen las tareas asignadas en los procedimientos que forman parte de este plan.

6.3.3. Estrategia para la restauración de tecnologías de la información

El alcance de las estrategias para la restauración o recuperación involucra las acciones que deben realizarse luego de suscitada una emergencia o desastre, a fin de recuperar la información y los servicios informáticos del SENAMHI para estabilizar la infraestructura tecnológica luego del evento suscitado. Para lo cual se definen las pautas que permitan al personal de la OTI garantizar la continuidad de las operaciones en la entidad. El ciclo considerado para la estrategia de recuperación de tecnologías de la información es el siguiente:

Gráfico 05: Ciclo de la estrategia de recuperación de TI



La priorización de la restauración de los servicios de tecnologías de información del SENAMHI se ejecutará de acuerdo a lo indicado en la siguiente Tabla de información:

Tabla 07: Prioridad de atención durante la restauración de TIC

PRIORIDAD DE ATENCION	DESCRIPCIÓN
1	Atención prioritaria: Sistemas de información y equipos que requieran alta disponibilidad de atención a los usuarios externos y manejen alto volumen de información. Ejemplo: Portal web institucional, sistemas de ingresos de información de datos hidrometeorológicos, sistemas que realizan el control de calidad de los datos hidrometeorológico, sistema integrado de gestión de administrativa, etc.
2	Atención normal: Sistemas de información y equipos no relacionados con la atención a los usuarios y manejen bajo volumen de información. Ejemplo: Sistemas que no requirieran conectividad y/o que cuenten con mayor plazo para la consulta y disponibilidad de información, etc.
3	Atención baja: Sistemas de información de uso interno, uso poco frecuente y/o que manejan bajo volumen de información. Asimismo, equipos de apoyo. Ejemplo: Sistema de Gestión de Transporte.

En el Anexo 2 y Anexo 3 se detallan los sistemas de información y equipos informáticos, con la respectiva prioridad de atención, en caso de activarse la contingencia informática. Acciones después de la contingencia - Evaluar el trabajo de los equipos durante el proceso de recuperación. - Evaluar la efectividad del Plan de Contingencia. - Evaluar la efectividad del sitio alterno de contingencia y sus facilidades.

6.4. FASE 4: ELABORACIÓN DEL PLAN DE CONTINGENCIA Y RECUPERACIÓN DE SERVICIOS DE TIC

Una vez identificados los eventos de contingencia y los escenarios de riesgos, se desarrollan los Planes de Contingencia agrupados por las categorías indicadas previamente. El Plan de Contingencia y Recuperación de los Servicios de Tecnología de la Información y Comunicaciones comprenderá los eventos de mayor impacto, identificados en la Matriz de Riesgo de Contingencia, los cuales serán abordados en formatos independientes, tal como se indica en el siguiente cuadro:

Tabla N° 08: Eventos de mayor impacto para el Plan de Contingencia Informático

N°	EVENTO	EXPOSICION AL RIESGO	FORMATO PLAN DE CONTINGENCIA
1	Terremoto /Sismo	Extremo	FPC - 01
2	Incendio en el Centro de Datos	Extremo	FPC - 02
2	Delito informático (ataque)	Extremo	FPC - 03
3	Falla de hardware y software	Extremo	FPC - 04
4	Falla del suministro eléctrico en el Centro de Datos y gabinetes de comunicación.	Extremo	FPC - 05

En el Anexo 4 se presenta el desarrollo de cada formato.

6.5. 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 funcionales, 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, en los meses de junio y diciembre, 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° 05.

6.6. FASE 6: IMPLEMENTACIÓN DEL PLAN DE CONTINGENCIA

La implementación del presente plan se realizará a partir del segundo mes de su aprobación.

Para tal efecto, los/las Coordinadores de la Unidad Funcional Operativa de Infraestructura Tecnológica y Unidad Funcional Operativa de Sistemas de Información, realizan las siguientes funciones:

- Supervisar las actividades de copias de respaldo y restauración.
- Establecer procedimientos de seguridad en los sitios de recuperación.
- Organizar las pruebas de restauración de hardware, software y servicios de Tecnologías de Información (TI).
- Participar en las pruebas y simulacros de desastres.

6.7. FASE 7: MONITOREO

La fase de Monitoreo 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 del Centro de Datos.

7. ANEXOS

- Anexo 1: Metodología aplicada a la gestión de riesgos
- Anexo 2: Listado de sistemas de información clasificados por prioridad de atención para la recuperación de tic
- Anexo 3: Listado de equipos del centro de datos ubicados por gabinetes y clasificados por prioridad de atención para la recuperación de TIC
- Anexo 4: Formatos del Plan de Contingencia Informático y Recuperación de Servicios de Tecnologías de la Información y Comunicaciones por evento de riesgo
- Anexo 5: Formato de Control y certificación de las Pruebas del Plan de Contingencia y Recuperación de Servicios de Tecnologías de la Información y Comunicaciones

ANEXO N° 1: METODOLOGÍA APLICADA A LA GESTIÓN DE RIESGOS

METODOLOGÍA APLICADA A LA GESTION DE RIESGOS

1. **Cálculo de la Probabilidad de Ocurrencia de la Amenaza.** Para realizar este cálculo, se toman en cuenta dos variables: “Ocurrencia” y “Percepción”.

Se considera “ocurrencia” a la frecuencia en que se presentan los eventos a evaluar, sobre la base de los registros históricos de incidentes que hayan afectado al SENAMHI directamente. Se consideró la siguiente tabla de valores para el “cálculo”.

N°	OCURRENCIA	DESCRIPCION
1	Rara Vez	Se presentó al menos una vez en los últimos 20 años / Nunca se presentó
2	No Frecuente	Se presentó al menos una vez en los últimos 10 años
3	Moderada	Se presentó más de una vez en los últimos 5 años
4	Frecuente	Se presentó por lo menos una vez al año en los últimos 5 años
5	Muy frecuente	Se presentó más de una vez al mes en el último año

La “Percepción” está basada netamente en la sensación de los expertos, de que la amenaza en cuestión podría ocurrir, se consideró la siguiente tabla de valores para el cálculo:

N°	PERCEPCION	DESCRIPCION
1	Muy Difícil	• <= 1% probabilidad, o • El acontecimiento requiere de circunstancias excepcionales, o • La probabilidad es nula, incluso en un futuro a largo plazo
2	Difícil	• >1% ó <=10% de probabilidad, o • Puede ocurrir pero no será anticipada
3	Mediana	• >10% ó <=50% de probabilidad, o • Puede ocurrir en el mediano plazo
4	Posible	• >50% ó <=75% de probabilidad, o • Podría ocurrir anualmente
5	Muy Posible	• >75% ó 100% de probabilidad, o • El impacto está ocurriendo ahora, o • Podría ocurrir dentro de unos meses

Los valores definidos para la Ocurrencia y Percepción son promediados y consolidados a fin de obtener una Probabilidad de Ocurrencia consensuada, asociada a cada amenaza en evaluación.

2. **Identificación de las amenazas que se tomarán en cuenta para la evaluación**. De la combinación de las variables descritas se obtiene la Probabilidad Estimada, que sirve como valor discriminatorio para seleccionar que amenazas se deberían evaluar para el alcance. Aquellas que resultan en un nivel de probabilidad estimada insignificante, según la tabla siguiente, no son tomados en cuenta.

NIVEL DE PROBABILIDAD ESTIMADA	INTERPRETACIÓN
Extremo	Probabilidad de ocurrencia alta (Evaluación de prioridad alta – Valor entre 4 a 5)
Moderado	Probabilidad de ocurrencia intermedia (Evaluación. de prioridad baja – Valor 3)
Menor	Probabilidad de ocurrencia muy baja (Evaluación sin prioridad – Valor 2)
Insignificante	No se cree que ocurra (Desestimar evaluación – Valor 1)

3. **Cálculo de la Probabilidad de Afectación del Recurso.** Se utiliza la siguiente tabla de valores para el cálculo:

N°	PROBABILIDAD	DESCRIPCIÓN
1	Improbable	Se cuenta con controles razonablemente suficientes que responden a un programa de mantenimiento (evaluados y mejorados), se evidencia que han respondido a acontecimientos ocurridos y ejercicios realizados
2	Baja	Se cuenta con controles razonablemente suficientes que responden a un programa de mantenimiento y responden a los ejercicios y pruebas realizadas
3	Moderada	Se cuenta con controles que responden a un programa de mantenimiento y responden a los ejercicios y pruebas realizadas, pero no son suficientes.
4	Alta	Algunos controles se prueban esporádicamente, debido a que no cuentan con un programa definido o de existir no se cumple con el mismo
5	Muy Alta	Bajo nivel de controles o los controles existentes no son efectivos o eficientes

4. **Cálculo del Impacto del Recurso.** Se utiliza la siguiente tabla de valores para el cálculo:

N°	IMPACTO	DESCRIPCIÓN
1	No significativo	Tiene un efecto nulo o muy pequeño en las operaciones de la sede evaluada
2	Menor	Afecta hasta en 6 horas las operaciones de la sede evaluada.
3	Moderado	Afecta hasta en 24 horas las operaciones de la sede evaluada.
4	Mayor	Afecta hasta en 48 horas las operaciones de la sede evaluada.
5	Catastrófico	Afecta por más de una semana las operaciones de la sede evaluada

5. **Cálculo del Nivel de Riesgo.** Se calcula considerando el mayor Nivel de Riesgo del recurso afectado por la amenaza que se está analizando. Para la identificación del Nivel de Riesgo se considera la siguiente matriz:

PROBABILIDAD DE AFECTACION	IMPACTO				
	NO SIGNIFICATIVO (1)	MENOR (2)	MODERADO (3)	MAYOR (4)	CATATRÓFICO (5)
MUY ALTA (5)	Alto	Alto	Extremo	Extremo	Extremo
ALTA (4)	Moderado	Alto	Alto	Extremo	Extremo
MODERADA (3)	Bajo	Moderado	Alto	Extremo	Extremo
BAJA (2)	Bajo	Bajo	Moderado	Alto	Extremo
IMPROBABLE (1)	Bajo	Bajo	Moderado	Alto	Alto

Interpretación de cada cuadrante de calor o Nivel de Riesgo de la amenaza en evaluación

NIVEL DE RIESGO	INTERPRETACION
EXTREMO	Riesgo no deseable, se requiere acción correctiva inmediata
ALTO	Riesgo no deseable que requiere de una acción correctiva, pero se permite alguna discreción de la gerencia sobre los plazos y compromisos
MODERADO	Riesgo aceptable con revisión de la dirección
BAJO	Riesgo aceptable sin revisión

ANEXO N° 2: LISTADO DE SISTEMAS DE INFORMACIÓN CLASIFICADOS POR PRIORIDAD DE ATENCIÓN PARA LA RECUPERACIÓN DE TIC

N°	Sistema	DESCRIPCION	PRIORIDAD
1	Sistema de intranet	Sistema que permite la consulta y carga de información hidrometereológica y ambiental	1
2	Sistema de gestión de contenidos de los sitios web (admin)	Sistema que permite a los usuarios internos gestionar el contenido de todos los sitios web	1
3	Sistema control de calidad	Consultar información con control de calidad de variables meteorológicas.	1
4	Sistema integrado de gestión administrativa	Sistema para gestión administrativa	1
5	Sistema de migración	Migración de Datos - Estaciones Convencionales - al Control de Calidad	1
6	Sistema de recepción y monitoreo de datos (claro)	Permite visualizar los datos recibidos a través de celular vía Voz y Data para el monitoreo	1
7	App de registro de datos hidrometeorológicos. (claro)	App que permite al observador registrar los datos de ciertas variables de las estaciones convencionales.	1
8	Sistema de automáticas	Sistema de registro y visualización de datos de estaciones automáticas.	1
9	Sistema de descarga automática de datos	Sistema para descarga, decodificación de los datos de estaciones automáticas, tipo SUTRON y OTT.	1
10	Sistema de registro de datos meteorológicos e hidrometeorológico	Sistema de ingreso para información de las estaciones convencionales	1
11	Sistema de gestión hidrológica (versión 1.0)	Ingreso, procesamiento y difusión de datos de variables hidrológicas	1
12	Sistema de vigilancia de datos meteorológicos v1	Es un sistema que consulta de datos de estaciones automáticas y convencionales por periodos, muestra imágenes de satélite, datos climáticos, entre otros.	1
13	Sistema de gestión documental	Sistema inicial para tramites, registro, consulta de documentos.	1
14	Sistema de monitoreo de datos de estaciones automáticas	Sistema de monitoreo de datos descargados de estaciones automáticas.	1
15	Página web antigua del senamhi		1
16	Sistema de calidad control de datos y visor de imágenes satelitales	Sistema de control de calidad de los datos y visor de imágenes; que permite un control de calidad de los datos e imágenes de las estaciones automáticas.	1
17	Sistema de gestión de datos de estaciones (voz y data web) v.2	Sistema web de monitoreo de datos medidos por el instrumental de estaciones convencionales a nivel nacional, registrados por el aplicativo móvil de voz y data por parte del personal observador o reportados al área de monitoreo de datos del SENAMHI.	1
18	Aplicativo móvil de registro de datos de estaciones (voz y data móvil) v.2	Aplicativo móvil y web que facilite el registro de datos e incidentes generados por los instrumentos de medición que se encuentran en las estaciones convencionales a nivel nacional, por parte del personal observador.	1
19	Sistema integrado de gestión de avisos meteorológicos del senamhi – sigamet	Sistema que integra información datos de avisos meteorológicos, generados en el SENAMHI; por la web institucional, permitiendo la visualización, consulta y descarga de información de mapas multi-fenómeno, para una cantidad de días de atención.	1
20	Sistema de aviso de corto plazo ante posible activación de quebrada	Sistema que pone a disposición de todos los ciudadanos, empresas privadas e instituciones públicas, los avisos que indican la posibilidad de activación de quebradas asociada a las lluvias pronosticadas para las siguientes 24 horas (aviso de corto plazo), considerando la lluvia de los 7 días antecedentes y la susceptibilidad a movimientos en masa.	1

21	Sistema de aviso de corto plazo ante lluvias intensas 24 horas	Sistema que integra información de datos espaciales de Avisos de Lluvias a Corto Plazo, generados en el SENAMHI; en forma dinámica por la página web institucional, permitiendo la visualización, consulta y descarga de información de los mapas en forma diaria.	1
22	Sistema de registro de aforos	El módulo de Aforos, de la Plataforma Hidrológica de Información Sistematizada e Integrada del SENAMHI permite la recolección de datos de campo de aforos y datos de reservorios, así como el registro y asignación de equipos de medición; también el control de calidad y procesamiento de datos para obtener los procesados de aforos, curvas de descarga e índices de reservorios; todo ello para la toma de decisiones del usuario final.	1
23	Migración de portal institucional	El GOB.PE es una plataforma digital única del Estado peruano para orientación a la ciudadanía, según el Decreto Supremo 033-2018-PCM y su objetivo principal es brindar una experiencia sencilla, consistente e intuitiva de acceso a información institucional, trámites y servicios públicos digitales. Se realizó la migración total de todo el contenido informativo y de orientación, como también la independización de los servicios que ofrece la institución.	1
24	Sistema de pronóstico inmediato (nowcasting)	Sistema que gestiona información de datos espaciales de Avisos de Lluvias a Muy Corto Plazo, generados en el SENAMHI; en forma dinámica por la página web institucional, a fin de poner a disposición de todos los ciudadanos, empresas privadas e instituciones públicas; la visualización, consulta y descarga de información de los mapas en forma horaria.	1
25	Sistema integrado de administración financiera	Sistema para gestión Financiera	2
26	Sistema de facturación y registro de clientes	Proceso de registro de clientes y emisión de facturas. Factura las ventas y lleva el control de los clientes.	2
27	Sistema estadístico meteorológico	Proceso de consulta de reportes estadísticos. Consultar información estadística calculada de datos de variables meteorológicas.	2
28	Sistema de remuneraciones	Proceso de transacciones en remuneraciones. Administra la información de remuneraciones del personal.	2
29	Sistema de legajos	Proceso de registro y consulta de legajos. Registra información del legajo de los trabajadores.	2
30	Sistema de control de asistencia	Proceso de consulta y reportes de asistencia. Registra y consulta la asistencia del personal a través de marcadores digitales	2
31	Infraestructura de datos espaciales	Procesamiento de datos cartográficos y diseño de mapas. Administra la información cartográfica vectorial y satelital. Se compone de: visor cartográfico, catalogo de metadatos y geoportal web.	2
32	Sistema de gestión de imágenes satelitales	Sistema de Gestión de Solicitudes y almacenamiento de Imágenes Satelitales al CONIDA.	2
33	Sistema de visualización de planillas	Sistema de registro y visualización de Imágenes de planillas meteorológicas escaneada.	2
34	Portal del estado peruano	Portal del Estado Peruano	2
35	Mesa de partes virtual	Aplicativo que sirve para el envió y recepción de documentos (escaneados) a todas las direcciones zonales del país, así como a instituciones externas como OEFA, etc.	2

36	Sistema integrado de gestion presupuestal	herramienta para realizar el seguimiento y evaluación del presupuesto, control de la programación y ejecución presupuestal	2
37	Tambos/buffer	Scripts que decodifican tramas por FTP y registran la data de las Estaciones pertenecientes al proyecto Tambos	2
38	Plataforma de interoperabilidad de servicios del senamhi	Plataforma – Interface que muestra el listado de diferentes servicios interoperables que se desarrollan en el SENAMHI; disponible para su consumo a través de consultas y descargas de información, por diversos medios y/o plataformas.	2
39	Sistema integral de gestión presupuestal	Sistema integrado de alcance nacional a nivel estratégico, programático y operativo; lo cual facilite el planeamiento institucional y la gestión presupuestal.	2
40	Intranet	Sistema que permite visualizar información institucional a todos los empleados del SENAMHI	3
41	Sistema de actualización del portal de servicios al ciudadano mediante el sistema de la pcm	Sistema que permite la actualización de información orientada al ciudadano, elaborado por la ONGEI	3
42	Sistema de control de visitas	Sistema que permite el registro de visitas a la institución, Elaborado por la ONGEI	3
43	Sistema de digitalización y procesamiento de bandas hidrometeorológicas	Permite aplicar el proceso de digitalización y captura de datos de bandas hidrometeorológicas.	3
44	Sistema de análisis agrometeorológico	Ingreso y consulta de datos y funciones aplicadas a la agrometeorología	3
45	Sistema de gestión de educación a distancia (campus virtual)	Proceso de administración de cursos de capacitación. Lleva a cabo cursos de capacitación a distancia.	3
46	Sistema fenológico	Consulta de datos del monitoreo fenológico de cultivos agrícolas.(Proceso de ingreso y consulta de datos fenológicos. Ingreso y consulta de datos del monitoreo fenológico de cultivos agrícolas.)	3
47	Sistema fenológico web	Proceso de ingreso y consulta de datos fenológicos. Ingreso y consulta de datos del monitoreo fenológico de cultivos agrícolas.	3
48	Sistema de gestión de transporte	Permite gestionar la logística de distribución y asignación vehicular y de choferes a comisiones de servicios, tiempos y gastos de traslado, insumos y mantenimiento vehicular.	3
49	Sistema de control de asistencia tempus	Sistema para el control de asistencia a nivel nacional	3
50	Sistema de tramite documental	Sistema para tramites, registro, consulta de documentos.	3
51	Sistema de convenios	Sistema para el registro, consulta y evaluación de convenios interinstitucionales.	2
52	Sistema integrado de recursos humanos - modulo de legajo	Sistema para la gestión de las convocatorias, legajos y nominas.	3
53	Sistema de procesos administrativos	Sistema de gestión de expedientes de procesos administrativos generados dentro del SENAMHI.	3
54	Sistema de procesos judiciales para el senamhi	Mejoras del sistema en el módulo de expedientes del SISPROJ a fin de fortalecer los procesos de gestión de expedientes.	3
55	Catalogo institucional del senamhi	Aplicativo donde se almacena los libros, revistas, apuntes, compendios de datos meteorológicos e hidrológicos relacionados a SENAMHI	3
56	Módulo de administración del portal de transparencia estándar	Módulo de Administración del Portal de Transparencia Estándar	3
57	Sigamef	Aplicativo que genera y gestiona códigos QR* para el inventario de bienes muebles e inmuebles del SENAMHI	3
58	Sistema de monitoreo de servidores	Sistema que permite controla y evitar fallos en los sistemas tecnológicos	3

59	Sistema de migracion	MODULO INCORPORADO EN EL SISMETHA WEB / Forma parte	3
60	Sistema de control de versiones gitlab	Sistema de control de versiones y desarrollo de software colaborativo basado en Git	3
61	Sistema de patrimonio (2004)	Sistema que permite la gestión de los bienes patrimoniales del SENAMHI	3
62	Sistema de inventario de planillas	Sistema que sirve para controlar todas las planillas y registradores (bandas) de todas las direcciones zonales	3
63	Sistema de emisión de boletas	Genera y emite las boletas de pago de los empleados del SENAMHI(No crea ni tiene usuarios)	3
64	Sistema rtps	Sistema que permite la generación de reportes relacionados a la Planilla y AFP, SUNAT, etc.	3
65	Sistema de datos agrometeorológico - modulo vista de datos	Aplicativo web para el área de datos Agrometeorológico, con el fin de poner a disposición la información de las estaciones para su respectivo análisis.	3
66	Repositorio institucional de la biblioteca de servicio nacional de meteorología e hidrología del perú	Sistema repositorio institucional para incorporar contenidos en el portal de ALICIA (CONCYTEC) y otros recolectores nacionales e internacional para la cual se implementaran protocolos que permitan el intercambio de información con repositorios locales e internacional.	3
67	Sistema de registro de incidentes laborales	El Sistema de Registro de Incidencias Laborales es una plataforma para el reporte de incidencias presenciadas en el SENAMHI por parte de personal interno o externo, además cuando con módulos de trámite del reporte y estado, reportes estadísticos, gestión de tablas de mantenimiento y gestión de usuarios.	3
68	Sistema de registro de denuncias anticorrupción	Sistema para automatizar funciones y procesos relacionados a denuncias de actos de corrupción dentro de la institución, el cual registra información de que será de ayuda para cumplir con el Decreto Legislativo N°1327, Decreto supremo N°010 – 2017 – JUS y la Directiva N°01 – 2019 – SENAMHI/GG.	3
69	Sistema de registro de denuncias de hostigamiento sexual	Sistema que permite automatizar funciones y procesos de las denuncias de hostigamiento sexual dentro de la entidad, cumpliendo con la Ley N°27942, Ley de Prevención y Sanción del Hostigamiento Sexual, Decreto Supremo N°014 - 2019 MIMP y la Resolución de Presidencia Ejecutiva N°144 - 2019 - SERVIR-PE.	3
70	Sistema de prestamos cafae	Sistema que automatiza el proceso de gestión de préstamos, control y seguimiento con reportes, gestión de ventas de productos y afiliación de servidores SENAMHI al CAFAE. También se da interoperabilidad con el sistema de Planillas, brindado la gestión de los descuentos de una forma automática y flexible para el personal de CAFAE	3
71	Página web de biblioteca	La Biblioteca es una página web que fue diseñada para que tenga una interacción amigable ya sea en versión móvil, tablet y PC, donde se pueden realizar búsquedas de recursos bibliográficos impresos y digitales, a través de la página web se puede redireccionar a los servicios esenciales de la Biblioteca como el Repositorio, Catalogo y Base de Datos.	3

72	Sistema de procesos judiciales - modulo de visualización de reportes.	Sistema enfocado en la gestión de los expedientes (principales o cuadernos) que administra la oficina de asesoría jurídica (OAJ), dando una distribución del expediente en datos del expediente, ubicación judicial, partes procesales, documentos, montos y reposición. el sistema también brinda información estadística con gráficos y cuadros de los expedientes registrados.	3
73	Encuesta de transición al régimen de servir.	Sistema de registro, administración y seguimientos de las encuestas brindadas a los servidores de sedes a nivel nacional y servidores de estación meteorológicas o hidrológicas (observadores/ operadores). el sistema también cuenta con un modelo administrador el cual facilita conocer los intereses y las carencias que el personal presenta para la transición al régimen SERVIR.	3
74	Sistema de gestión de usuarios.	Sistema que gestiona la información de usuarios y sistemas del SENAMHI, a fin de mantener una única instancia de autentificación para los servidores dentro de la entidad, así mismo contando con reportes y servicios que son de utilidad para cada uno de los sistemas a implementarse en la institución.	3
75	Sistema de tendencias históricas del senamhi (thendis)	Brinda información sobre “Tendencias históricas de precipitación y temperatura” para formuladores de fichas de Servicios Ecosistémicos de Regulación Hídrica de proyectos de inversión de los gobiernos regionales y locales.	3
76	Sistema de descarga automática de datos – módulo de consulta de datos	Aplicativo web de consulta de datos de las estaciones automáticas a nivel nacional que permita seleccionar la información por diferentes filtros, de esta manera obtener cuadros y gráficos para su respectivo análisis.	3

ANEXO N° 3: LISTADO DE EQUIPOS DEL CENTRO DE DATOS UBICADOS POR GABINETES Y CLASIFICADOS POR PRIORIDAD DE ATENCIÓN PARA LA RECUPERACIÓN DE TIC

N°	GABINETE	TIPO	MARCA	MODELO	NOMBRE SERVIDOR	IP	FUNCIÓN	ANTIGÜEDAD	CAPACIDAD DE PROCESAMIENTO	CAPACIDAD DE ALMACENAMIENTO	CAPACIDAD DE MEMORIA	PRIORIDAD
1	2	Servidor virtualizador	DELL	Power Edge R730	DBPRUEBA	10.10.20.38	Servidor Virtual pruebas DB ORACLE - Ambiente desarrollo de la base de datos	27-Jun-16	24 CPUs x Intel(R) Xeon(R) CPU E5-2687W v4 @ 3.00GHz	6,5 TB	64 GB	3
						172.25.0.188	Máquina Virtual DB prueba - Ambiente desarrollo de la base de datos	27-Jun-16	8 vCPUs	2 TB	32 GB	3
2	2	Servidor Dedicado	HP	Proliant DL 380	SRV-SIGA	10.10.20.15	Servidor SIGA y SIAF	19-Oct-15	Intel(R) Xeon(R) CPU E5-2667w v2 @ 3.2GHz	600GB	32GB	1
3	2	Servidor Virtualizador	SGI	C2108-RP2	VMSGD	172.25.0.30	Servidor Virtualizador	21-Ago-13	16 CPUs x Intel(R) Xeon(R) CPU E5-2670 0 @ 2.60GHz	2,5 TB	128 GB	1
						172.25.0.97	Dominio W2012R2	21-Ago-13	4 vCPUs	400 GB	8 GB	1
						172.25.0.98	DHCP W2012R2	21-Ago-13	2 vCPUs	200 GB	4 GB	2
						10.10.20.6	IDE-SP - Servidor de prueba de IDESEP	21-Ago-13	4 vCPUs	450 GB	24 GB	3
						10.10.20.7	SENAMHI-WSUS - Servidor de actualizaciones de Windows	21-Ago-13	8 vCPUs	550 GB	32 GB	3

						172.25.50.60	SENAMHI-RENIEC - Servidor de Gestión de Certificados Digitales	21-Ago-13	8 vCPUs	250 GB	4 GB	2
						172.25.0.18	SENAMHI-Servidor antivirus	21-Ago-13	4 vCPUs	120 GB	8 GB	2
						172.25,0,250	SENAMHI-PIDE	21-Ago-13	1 vCPUS	75 GB	8 GB	3
						10.10.20.40	SENAMHI-COMISIONES	21-Ago-13	8 vCPUs	100 GB	16 GB	3
						172.25.0.66	SENAMHI-ORH	21-Ago-13	4 vCPUs	500 GB	8 GB	2
						172.25.0.175	SENAMHI-OCR - Servidor Therefore	21-Ago-13	4 vCPUs	195 GB	8 GB	3
4	2	Servidor Dedicado	DELL	Power Edge R820	CPN-WRF SEDAPAL	10.10.30.245	Administrado por SMN CPN-WRF SEDAPAL	15-Ene-15	4x Intel(R) Xeon(R) CPU E5-4650L 0 @ 2.60GHz	1TB	128GB	3
5	2	Servidor Dedicado	DELL	Power Edge R530	SRV02	172.25.212.187	SMARTMET 1	24-Feb-15	Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz	2TB	64GB	2
6	2	Servidor Dedicado	DELL	Power Edge R530	SMARTNET	172.25.0.210	SMARTMET 2	24-Feb-15	Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz	2TB	64GB	2
7	2	Servidor Dedicado	HP	Proliant DL 360	APP-JAVA-DV	10.10.20.4	Sistema de VOZ y DATOS - Servicio de Transmisión de Voz y Data	Sin dato	Intel(R) Xeon(R) CPU E5-2640 v3 @ 2.60GHz	2TB	64GB	1
8	2	Servidor Dedicado	SGI	UV20	SRV CPN/respaldo	10.10.30.35	Administrado por SMN - SRV CPN/respaldo	2015	4x Intel(R) Xeon(R) CPU E5-4650 0 @ 2.60GHz	1.5TB	128GB	3
9	2	Servidor Dedicado	IBM	System X3650 M4	SERVER WRFCHEM	172.25.0.44	SERVER WRFCHEM Control Aire	2012	Intel(R) Xeon(R) CPU E5-2630 0 @ 2.30GHz	2TB	32GB	3

10	2	Servidor Dedicado	DELL	Power Edge R740	Proyecto Libelula	10.10.30.0	Proyecto Libelula	1-Ago-19	Intel Xeon Bronze 3106 1.7G	8TB	16GB	3
11	2	Servidor Dedicado	DELL	Power Edge R440	ANTI-SPAN	10.10.20.9	ANTI-SPAN	8-Mar-18	Intel(R) @2.2GHZ	1TB	16GB	2
12	2	Chasis Blade Servidor Dedicado	DELL	Power Edge M1000E	SMN	10.10.30.21	Administrado por SMN	5-Ene-15	No aplica – Chasis Server	No aplica – Chasis Server	No aplica – Chasis Server	2
13	2	Servers Blade	DELL	Power Edge M620	SMN	10.10.30.0	Administrado por SMN	24-Nov-14	Intel(R) Xeon(R) CPU E5-2680 v4 @ 2.80GHz	1TB	256GB	2
												2
												2
			DELL	Power Edge M620	SMN	10.10.30.0	Administrado por SMN	24-Nov-14	Intel(R) Xeon(R) CPU E5-2680 v4 @ 2.80GHz	1TB	256GB	2
												2
			DELL	Power Edge M620	SMN	10.10.30.0	Administrado por SMN	24-Nov-14	Intel(R) Xeon(R) CPU E5-2680 v4 @ 2.80GHz	1TB	256GB	2
												2
			DELL	Power Edge M620	SMN	10.10.30.0	Administrado por SMN	24-Nov-14	Intel(R) Xeon(R) CPU E5-2680 v4 @ 2.80GHz	1TB	256GB	2
14	2	Servers Blade	DELL	Power Edge M630	SMN	10.10.30.0	Administrado por SMN	2-Set-16	Intel(R) Xeon(R) CPU E5-2680 v4 @ 2.80GHz	1TB	256GB	2
15	2	Servers Blade	DELL	Power Edge R530	SMN	10.10.30.0	Administrado por SMN	30-Oct-19	Intel Xeon E5-2640 v3 2.6GHz	2TB	16GB	2
			DELL	Power Edge R530	SMN	10.10.30.0	Administrado por SMN	30-Oct-19	Intel Xeon E5-2640 v3 2.6GHz	2TB	16GB	2
16	2	Servers Blade	DELL	Power Edge R730	SMN	10.10.30.0	Administrado por SMN	30-Oct-19	Intel Xeon E5-2687W v4 3.0GHz	1.2TB	64GB	2
17	2	Servers Blade	DELL	Power Edge R820	SMN	10.10.30.0	Administrado por SMN	30-Oct-19	Intel Xeon E5-4650L 2.60GHz	900GB	128GB	2
18	3	Servidor Dedicado	SGI	C2108-RP2	OGIP	172.25.13.188	Base de Datos OGIEP	2013	INTEL® XEON CPU E5-2640 2.5GHZ	4TB	64GB	1

19	3	Servidor Dedicado	Boxx	Workstation Box 3DBOX	USER01-PC	172.25.13.149	Servidor Bandas	2010	Intel Core i7 960 - 3.20 GHz	1 TB	6 GB	3
20	4	Servidor virtualizador	SuperMicro	SSG-6047R-E1R36N	VMPOSTGRES	10.10.20.38	Servidor Virtual DB POSTGRES	1-Jul-13	12 CPUs x Intel(R) Xeon(R) CPU E5-2640 0 @ 2.50GHz	2,17 TB	24 GB	1
						10.10.20.17	Máquina Virtual DB POSTGRES	1-Jul-13	8 vCPUs	1 TB	16 GB	1
21	4	Servidor Dedicado	SGI	C2108-TY11	senamhi-ftp	172.25.0.9	Servidor FTP	2012	INTEL® XEON CPU E5-2640 2.5GHZ	1TB	16GB	2
22	4	Servidor Dedicado	SGI	AltixXE270	STORAGE	172.25.0.52	STORAGE BANDAS	2010	INTEL® XEON CPU E5-2640 2.5GHZ	4TB	16GB	3
23	5	Servidor Dedicado	HP	Proliant DL 360	STORAGE	172.25.0.53	CONFIGURACION DE STORAGE	28-Nov-17	Intel(R) Xeon(R) CPU E5-5645 @ 2.60GHz	300GB	8 BG	1
24	5	Servidor Dedicado	HP	Proliant DL 120	DPSENAMHI	172.25.3.11	Data Protector Backup Cintas	23-Nov-17	Intel(R) Xeon(R) CPU E5-2630 V 4 @ 2.2GHz	3TB	16 GB	2
25	5	Servidor Dedicado	HP	Proliant DL 380	-	172.25.0.54	CONFIGURACION DE STORAGE	28-Nov-17	Intel(R) Xeon(R) CPU E5-2630 V 4 @ 2.2GHz	300GB	8 BG	1
26	5	Servidor virtualizador	HP	C7000	Plataforma Virtual-Principal	172.25.2.106	Plataforma Virtual-Principal	23-Nov-17	-	150 TB	640 GB	1
						172.25.0.44	SENAMHI-CTRL-AIRE	1-Oct-19	4 vCPUs	1 TB	16 GB	3
						172.25.0.158	SENAMHI-DSPACE	23-Nov-17	4 vCPUs	500 GB	20 GB	3
						172.25.0.69	SENAMHI-DSRRLLO-OGEIP	23-Nov-17	16 vCPUs	1 TB	15 GB	3
						172.25.0.70	SENAMHI-FTP-IDESEP	23-Nov-17	16 vCPUs	80 GB	16 GB	3
						172.25.0.137	SENAMHI-GITLAB	23-Nov-17	8 vCPUs	500 GB	16 GB	3
						10.10.20.3	SENAMHI-GLASSFISH	23-Nov-17	2 vCPUs	500 GB	8 GB	1

						172.25.0.121	SENAMHI-GLPI	23-Nov-17	4 vCPUs	100 GB	6 GB	2
						10.10.20.20	SENAMHI-IDESEP	23-Nov-17	8 vCPUs	2,5 TB	133 GB	3
						172.25.0.6	SENAMHI-MNTVCENT-A	23-Nov-17	1 vCPUs	16 GB	2 GB	3
						10.10.20.125	SENAMHI-MOODLE	23-Nov-17	16 vCPUs	9,5 TB	32 GB	3
						10.10.20.28	SENAMHI-MP-VIRTUAL	23-Nov-17	4 vCPUs	1 TB	32 GB	3
						172.25.0.56	SENAMHI-NAS	23-Nov-17	4 vCPUs	19 TB	16 GB	3
						172.25.0.169	SENAMHI-NAS-GOES	23-Nov-17	4 vCPUs	24 TB	20 GB	1
						172.25.0.155	SENAMHI-NAS-SMN	23-Nov-17	8 vCPUs	10 TB	16 GB	3
						172.25.0.7	SENAMHI-ORH-TEMPUS	23-Nov-17	24 vCPUs	500 GB	12 GB	2
						172.25.0.68	SENAMHI-PANDORA	23-Nov-17	2 vCPUs	100 GB	8 GB	3
						172.25.0.122	SENAMHI-REG-INCIDENTES	23-Nov-17	4 vCPUs	100 GB	8 GB	3
						10.10.20.10	SENAMHI-REPOSITORIO	23-Nov-17	16 vCPUs	1 TB	8 GB	2
						10.10.30.220	SENAMHI-RESPALDO-SMN	23-Nov-17	2 vCPUs	5 TB	4 GB	3
						10.10.20.47	SENAMHI-SERV-ORH	23-Nov-17	4 vCPUs	1 TB	8 GB	2
						10.10.20.34	SENAMHI-SIGAWEB	23-Nov-17	4 vCPUs	500 GB	16 GB	3
						172.25.0.249	SENAMHI-SIGP	23-Nov-17	4 vCPUs	200 GB	16 GB	1
						172.25.0.5	SENAMHI-SISDAD	23-Nov-17	8 vCPUs	200 GB	16 GB	1
						-	SENAMHI-SPIJ	23-Nov-17	8 vCPUs	136 GB	8 GB	3
						10.10.20.29	SENAMHI-STD	23-Nov-17	8 vCPUs	580 GB	16 GB	1
						172.25.50.55	SENAMHI-TEMPUS	23-Nov-17	8 vCPUs	200 GB	20 GB	3

						172.25.0.165	SENAMHI-THEREFORE	23-Nov-17	4 vCPUs	1 TB	8 GB	3
						10.10.20.2	SENAMHI-WEB	23-Nov-17	8 vCPUs	2 TB	82 GB	1
						10.10.20.45	SENAMHI-WEB2	23-Nov-17	4 vCPUs	5 TB	8 GB	1
						172.25.0.248	SENAMHI-WEBSERVICES	23-Nov-17	4 vCPUs	200 GB	16 GB	2
						172.25.0.247	SENAMHI-WEB-SERVICES_2	23-Nov-17	4 vCPUs	200 GB	8 GB	2
						172.25.0.251	SENAMHI-AD	23-Nov-17	16 vCPUs	1,5 TB	16 GB	3
						10.10.20.35	SIGAP-SENAMHI-P	23-Nov-17	8 vCPUs	250 GB	16 GB	3
						172.25.0.126	SISPAD-DES	23-Nov-17	4 vCPUs	500 GB	16 GB	3
27	6	Servidor virtualizador	SGI	3500	VMWARE	10.10.20.8	SERVIDOR VIRTUALIZADOR	1-Oct-12	8 CPUs x Intel(R) Xeon(R) CPU E5620 @ 2.40GHz	10 TB	32 GB	1
						172.25.0.40	SENAMHI-PROPALMS	1-Oct-12	8 vCPUs	250 GB	8 GB	2
						10.10.20.185	SENAMHI-BV	1-Oct-12	8 vCPUs	500 GB	16 GB	3
28	6	Servidor Dedicado	SGI	c2108-ty11	VPN	172.25.0.16	Servidor VPN Envío Argentina / Brasil	2012	Intel(R) Xeon(R) CPU E5-5645 2.4GHz	550GB	24GB	3
29	6	Servidor Dedicado	SGI	c2108-ty11	BUFFER	125.25.0.20	Servidor Buffer	2012	Intel(R) Xeon(R) CPU E5645 @ 2.40GHz	600 GB	12 GB	3
30	6	Servidor Dedicado	HP	Proliant DL 380	SRV_SIAPMICROS	172.25.0.48	Servidor SIAP+MICROS	2012	Intel(R) Xeon(R) CPU E5-2650 2.0GHz	1TB	32GB	1
31	6	Servidor Dedicado	HP	Proliant DL 380	TRUENO	172.25.0.8	TRUENO-Servidor de procesamiento	2012	Intel(R) Xeon(R) CPU E5-2470 2.2GHz	1.5TB	14GB	1
32	6	Servidor virtualizador	SGI	C1208-RP2	VMHOST03.SENMAHI.GOB.PE	172.25.0.31	Servidor Virtualizador	1-Feb-14	12 CPUs x Intel(R) Xeon(R) CPU	500 GB	64 GB	1

									E5-2640 0 @ 2.50GHz			
							senamhi-ocolegiados	1-Feb-14	4 vCPUs	100 GB	8 GB	3
33	8	Servidor Dedicado	HP	Prolian DL380	SENAMHI-ANA	172.25.1.115	Servidor de ANA	21-Feb-19	Intel(R) Xeon(R) GOLD 6136 3.0GHz	2 TB	48 GB	3
34	9	Servidor Dedicado	DELL	R740 XD	J0119-awsg	10.10.20.60	GOES1 Modelamiento	23-Set-18	Intel(R) Xeon(R) Platinum 8168 2.7GHz	10 TB	190 GB	1
35	9	Servidor Dedicado	DELL	R740 XD	J0119-dpsg	10.10.20.61	GOES2	22-Set-18	Intel(R) Xeon(R) Platinum 8168 2.7GHz	10 TB	45 GB	1

Anexo 4: Formatos del Plan de Contingencia Informático y Recuperación de Servicios de Tecnologías de la Información y Comunicaciones por evento de riesgo

SENAMHI	EVENTO: TERREMOTO	FPC - 01

1. PLAN DE PREVENCION

a) Descripción del evento

Los sismos son movimientos en el interior de la tierra, que generan una liberación repentina de energía, que se propaga en forma de ondas provocando el movimiento del terreno.

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

Infraestructura:

- Oficinas y/o Centro de Datos de la sede Central.

Recursos Humanos

- Personal de la entidad.

b) Objetivo

Establecer las acciones que se ejecutarán ante un sismo a fin de minimizar el tiempo de interrupción de las operaciones del SENAMHI, sin exponer la seguridad de las personas.

c) Entorno

Este evento puede afectar las instalaciones de la Sede Central.

d) Personal Encargado

La Alta Dirección del SENAMHI, 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 punto f).

e) Condiciones de Prevención de Riesgo

- Inspecciones de seguridad realizadas periódicamente.
- Contar con un plan de evacuación de las instalaciones del SENAMHI, 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.
- Definición de los puntos de reunión en caso de evacuación.

f) Acciones del Equipo de Prevención de TIC

- Evaluar en coordinación con la Alta Dirección el ambiente para el Centro de Datos, en el sitio alterno.
- 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 del Centro de datos.
- Mantener actualizado el inventario hardware y software utilizado en el Centro de Datos de la entidad.
- Llevar un control de versiones de las fuentes de los sistemas de información y portal web 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 Centro de Datos. - 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.
- 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.
- Verificar que todo el personal del SENAMHI 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 SENAMHI, para las acciones que deban ser efectuadas por ellos.

En caso se requiera la habilitación del ambiente provisional alterno para restablecer la función de los ambientes afectados, el/la Director/a de la OTI deberá coordinar con la Alta Dirección.

f) Duración
Los procesos de evacuación del personal del SENAMHI 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 SENAMHI.

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 los equipos de respaldo al sitio alterno de recuperación.
- Establecer contacto con los proveedores clave y terceros para proporcionar instrucciones inmediatas y/o notificarles cualquier requisito de ayuda sobre la recuperación de negocio.
- Supervisar el progreso de las operaciones de recuperación y de servicios de TI y mantener informado al Grupo de Comando de Continuidad Operativa.
- Restauración de los servicios y operaciones de TI en el sitio alterno. El Equipo de restauración de TIC restaurarán el espacio de trabajo para permitir que el personal crítico de la oficina pueda operar, para lo cual deberán:
  - Ejecutar los procedimientos de recuperación de la plataforma tecnológica.
  - Verificar que las aplicaciones críticas se hayan recuperado y estén funcionando correctamente.

- Confirmar los puntos de recuperación de datos de las aplicaciones.
- Verificar que las funcionalidades de comunicación están funcionando correctamente.
- Verificar que equipos básicos como escáner, impresora estén disponibles y operacionales para dar soporte a los requisitos de la entidad.
- Asegurar que el ambiente del área de trabajo, las aplicaciones y las telecomunicaciones están funcionando según lo estimado tanto en el sitio alterno, como al retornar al sitio original, una vez concluida la emergencia o siniestro.

- Registrar todos los gastos operacionales relacionados con la continuidad del negocio.

c) Mecanismos de Comprobación
El/La Coordinador/a de Continuidad de TIC, presentará un informe a la alta dirección, 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 Contingencia
El/La Coordinador/a de Continuidad de TIC desactivará el Plan de Contingencia Informático una vez que se haya tomado las acciones descritas en el presente Plan de Recuperación, mediante una comunicación electrónica a la Alta Dirección.

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.

SENAMHI	EVENTO: INCENDIO EN EL CENTRO DE DATOS	FPC - 02

4. PLAN DE PREVENCION

a) Descripción del evento
Fuego de grandes proporciones que se desarrolla sin control, el cual puede presentarse de manera instantánea o gradual, pudiendo provocar daños materiales, interrupción de los procesos de producción, pérdida de vidas humanas y afectación al ambiente.

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

Infraestructura:
- Oficinas y/o Centro de Datos de la sede Central.

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 del SENAMHI, sin exponer la seguridad de las personas.

c) Entorno
Este evento puede afectar las instalaciones de la Sede Central.

d) Personal Encargado
La Alta Dirección del SENAMHI, 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 punto f).

e) Condiciones de Prevención de Riesgo
- Inspecciones de seguridad realizadas periódicamente.
- Revisión anual de las alarmas contraincendios, extintores.
- Contar con un plan de evacuación de las instalaciones del SENAMHI, 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 salidas de emergencia.
- Definición de los puntos de reunión en caso de evacuación.

f) Acciones del Equipo de Prevención de TIC
- Evaluar en coordinación con la Alta Dirección el ambiente para el Centro de Datos, en el sitio alterno.
- 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 del Centro de datos, alarmas contraincendios, extintores ubicados en el centro de datos.
- Mantener actualizado el inventario hardware y software utilizado en el Centro de Datos de la entidad.
- Llevar un control de versiones de las fuentes de los sistemas de información y portal web de la entidad.

5. **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) Procesos Relacionados antes del evento
- Mantenimiento del orden y limpieza de los ambientes en el Centro de Datos.
- 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
- Llamar a la comandancia de bomberos.
- Desconectar el fluido eléctrico.
- Utilización de extintores.
- Evacuar las oficinas cercanas al centro de datos 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.
- Verificar que todo el personal de las oficinas cercanas al centro de datos del SENAMHI se encuentre bien.
- Brindar los primeros auxilios al personal afectado si fuese necesario.
- 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 SENAMHI, para las acciones que deban ser efectuadas por ellos.

En caso se requiera la habilitación del ambiente provisional alterno para restablecer la función de los ambientes afectados, el/la Director/a de la OTI deberá coordinar con la Alta Dirección.

f) Duración
La duración total del evento dependerá de la magnitud del incendio y los daños a la infraestructura.

6. 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 SENAMHI.

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 los equipos de respaldo al sitio alterno de recuperación.
- Establecer contacto con los proveedores clave y terceros para proporcionar instrucciones inmediatas y/o notificarles cualquier requisito de ayuda sobre la recuperación de negocio.
- Supervisar el progreso de las operaciones de recuperación y de servicios de TI y mantener informado a la alta dirección.
- Restauración de los servicios y operaciones de TI en el sitio alterno. El Equipo de restauración de TIC restaurarán el espacio de trabajo para permitir que el personal crítico de la oficina pueda operar, para lo cual deberán:
  - Ejecutar los procedimientos de recuperación de la plataforma tecnológica.

- Verificar que las aplicaciones críticas se hayan recuperado y estén funcionando correctamente.

- Confirmar los puntos de recuperación de datos de las aplicaciones.
- Verificar que las funcionalidades de comunicación están funcionando correctamente.
- Verificar que equipos básicos como escáner, impresora estén disponibles y operacionales para dar soporte a los requisitos de la entidad.
- Asegurar que el ambiente del área de trabajo, las aplicaciones y las telecomunicaciones están funcionando según lo estimado tanto en el sitio alterno, como al retornar al sitio original, una vez concluida la emergencia o siniestro.

- Registrar todos los gastos operacionales relacionados con la continuidad del negocio.

c) Mecanismos de Comprobación
El/La Coordinador/a de Continuidad de TIC, presentará un informe a la alta dirección, 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 Contingencia
El/La Coordinador/a de Continuidad de TIC desactivará el Plan de Contingencia Informático una vez que se haya tomado las acciones descritas en el presente Plan de Recuperación, mediante una comunicación electrónica a la Alta Dirección.

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.

SENAMHI	EVENTO: DELITO INFORMATICO	FPC - 03

1. PLAN DE PREVENCION

a) Descripción del evento

Alteración de datos de los portales y sistemas de información a través de ataque cibernético (hacking) y/o malware. El malware es un software malicioso o software malintencionado, que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario, eliminando datos del equipo. Incluye virus, gusanos, troyanos, keyloggers, botnets, ransomwares o secuestradores, spyware, adware, hijackers, keyloggers, rootkits, bootkits, rogues, etc. Este evento incluye los siguientes elementos mínimos identificados por SENAMHI, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia, los cuales se muestran a continuación:

Hardware
- Servidores
- Estaciones de Trabajo

Software
- Software Base
- Sistemas de información, aplicativos y portal del SENAMHI

b) Objetivo

Restaurar la operatividad de los equipos y servicios después de eliminar los malware o reinstalar las aplicaciones dañadas.

c) Entorno

Este evento se puede darse en cualquiera de los servidores y estaciones ubicadas en el Centro de Datos de la sede principal del SENAMHI.

d) 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.

e) 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 lectoras y/o quemadores de CD en estaciones de trabajo que no lo requieran.
- Deshabilitación de los puertos de comunicación USB en las estaciones de trabajo que no los requieran habilitados, para prevenir la conexión de unidades de almacenamiento externo.
- Capacitación al personal de OTI, sobre Ethical Hacking a las Bases de Datos, Sistemas Operativos, Servidores y Sistemas Informáticos.
- Ejecución de ataques de Hacking Ético por terceros especializados.

f) Acciones del Equipo de Prevención de TIC
- Establecer, organizar, ejecutar y supervisar procedimientos de respaldo de información de la información procesada y almacenada en el Centro de Datos.

- Llevar un control de versiones de las fuentes de los sistemas de información y portal de la entidad.
- Realizar pruebas de restauración de la información almacenada en los repositorios y bases de datos.
- 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.
- Lentitud en el acceso a las aplicaciones.
- Falla general en el equipo (sistema operativo, aplicaciones).

b) Procesos relacionados antes del evento
Cualquier proceso relacionado con el uso de las aplicaciones en los servidores y en las estaciones de trabajo.

c) Personal que autoriza la contingencia
El/La Coordinador/a de Continuidad de TIC, los Coordinadores de la UFN o UFI pueden activar la contingencia.

d) Personal Encargado
Equipo de Emergencia de TIC.

e) Descripción de las actividades después de activar la contingencia
- Desconectar o retirar de la red de datos del SENAMHI, 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 la muestra 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.
- Probar el sistema.
- En caso no solucionarse el problema, formatear el equipo y restaurar copia de respaldo.

f) Duración
La duración del evento no deberá ser mayor dos horas en caso se confirme la presencia de un virus en estaciones de trabajo y de cuatro horas en servidores de red. Esperar la indicación del personal de soporte técnico para reanudar el trabajo.

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 portal 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 OTI del SENAMHI el tipo de malware/virus, o tipo de ataque encontrado y el procedimiento usado para removerlo.

Estas actividades deben contemplar como mínimo:
- Instalación y puesta a punto de un cómputo compatible y hardware necesarios para la instalación del sistema de información con las características mínimas exigidas.

- Instalación y configuración del sistema operativo, drivers y servicios necesarios para el funcionamiento del sistema de información 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.
- Instalación de aplicaciones adicionales necesarias para el funcionamiento del sistema de información.
- Realización de la restauración de la base de datos con la última copia de seguridad disponible (Restore).
- Reinicio del servicio, prueba y afinamiento del sistema de información.
- Conectar el servidor o la estación a la red del SENAMHI.
- Efectuar las pruebas necesarias con el usuario final de los equipos y/o sistemas de información afectados.
- Solicitar la conformidad de la restauración realizada del equipo y o sistema de información afectado.
- Comunicar el restablecimiento del servicio

En función a esto, el/la Coordinadores de la Unidad Funcional Operativa de la UFN o UFI, tomará las medidas preventivas del caso enviando una alerta vía correo al personal del SENAMHI.

El evento será evaluado.

c) Mecanismos de Comprobación
Se informará del incidente a la alta dirección
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 OTI, 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 SENAMHI, 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.

SENAMHI	EVENTO: FALLA DE HARDWARE Y SOFTWARE	FPC - 04

1. PLAN DE PREVENCION

a) Descripción del evento

El hardware de servidores es el recurso principal para almacenar, procesar y proteger los datos, permitiendo acceso controlado y procesamiento de transacciones rápido para cumplir con los requisitos de las aplicaciones de la entidad.

El software

En ausencia del mismo, los sistemas de información que dependen del mismo no pueden funcionar, siendo la parte afectada o causa de la contingencia, los cuales se muestran a continuación:

Hardware

- Servidores de Base de Datos, Aplicaciones, Archivos
- Storage

Software

- Aplicativos usados por el SENAMHI y de servicio al ciudadano

Información

- Información contenida en base de datos.
- Información contenida en repositorios de información

b) Objetivo

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

c) Entorno

Se puede producir durante el servicio, afectando a las aplicaciones usadas para dar soporte a las operaciones del SENAMHI.

d) Personal Encargado

Equipo de Prevención de TIC.

e) Condiciones de Prevención de Riesgo

- Revisión periódica de los registros (logs) de los servidores, para prevenir mal funcionamiento de los mismos.
- Contar con los backups diarios de datos de las aplicaciones en desarrollo/producción de la entidad, así como de las imágenes de los servidores.
- 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.
- Disponer de servidores de Aplicaciones de contingencia, con software de instalación tomcat, glassfish.

f) Acciones del Equipo de Prevención de TIC

- Establecer, organizar, ejecutar y supervisar procedimientos de respaldo y restauración de información.
- Programar, supervisar el mantenimiento preventivo a los equipos componentes del Centro de Datos.
- Mantener actualizado el inventario hardware y software utilizado en el Centro de Datos de la entidad.
- Realizar monitoreo del funcionamiento de los servidores instalados en el Centro de Datos para su correcto funcionamiento.

- Realizar revisiones de obsolescencia tecnológica de los servidores y componentes internos de forma anual.

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) Procesos Relacionados antes del evento
   - Disponibilidad de las copias de respaldo.
   - Disponibilidad de instaladores de sistemas operativos y motor de base de datos.

c) Personal que autoriza la contingencia
   El/La Coordinador/a de Continuidad de TIC debe activar la contingencia.

d) Descripción de las actividades después de activar la contingencia
   - Realizar la revisión del servidor averiado, buscando un recurso de reemplazo
   - verificando que dicho equipo cuente con garantía, de lo contrario se implementará un nuevo servidor virtual configurado de acuerdo a lo requerido.
   - Solicitar las cintas de respaldo para poder proceder a la restauración de la información almacenada en el servidor averiado.

f) Duración
   El tiempo máximo de la contingencia no debe sobrepasar las cuatro (4) horas.

3. PLAN DE RECUPERACIÓN

a) Personal Encargado
   El Equipo de Restauración de TIC, luego de validar la corrección del problema de acceso a los servidores, y el/la Coordinador/a de Continuidad de TIC informará a los Directores y/o Directores de áreas para la reanudación de las operaciones de los servicios afectados en el servidor averiado.

b) Descripción de actividades
   El plan de recuperación estará orientado a recuperar en el menor tiempo posible las actividades afectadas durante la interrupción del servicio afectado por falla de los servidores.

   Se debe realizar como mínimo las siguientes actividades:
   - Instalación y puesta a punto de un cómputo compatible y hardware necesarios para la instalación del sistema de información con las características mínimas exigidas.
   - Instalación y configuración del sistema operativo, drivers y servicios necesarios para el funcionamiento del sistema de información 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 servidores afectados
   - Verificar que la data y los aplicativos se hayan restaurado correctamente.
   - Ejecutar pruebas de acceso a los sistemas y aplicaciones.
   - Brindar los permisos de acceso a los usuarios finales.
   - Remitir un mensaje electrónico a los usuarios del SENAMHI informando la reanudación de los servicios.

   En función a esto, se tomarán las medidas preventivas del caso y se revisará el plan de contingencia para actualizarlo en caso sea necesario.

c) Mecanismos de Comprobación

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

El/La Especialista en Redes y Comunicaciones, presentará un informe a el/la Director/a de OTI, 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, se desactivará el presente Plan.

e) Proceso de Actualización
En base al informe presentado por el/la Técnico en Redes y Comunicaciones, quien identifica las causas de la pérdida o fallas de la base de datos institucional, se determinará las acciones preventivas necesarias que deberían incluirse en el presente plan.
En caso existiese información pendiente de actualización, el/la Técnico en Redes y Comunicaciones deberá iniciar las labores de actualización de los procedimientos o guías de recuperación de servidores.

SENAMHI	EVENTO: FALLA DEL SUMINISTRO ELECTRICO EN EL CENTRO DE DATOS Y GABINETES DE COMUNICACION	FPC - 05

1. PLAN DE PREVENCION

a) Descripción del evento

Falla general del suministro de energía eléctrica en el Centro de Datos de la sede principal de la entidad.

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

Servicios Públicos:
- Suministro de Energía Eléctrica

Hardware
- Servidores y sistema de almacenamiento de información (storage)
- Estaciones de Trabajo
- Equipos de Comunicaciones

Equipos Diversos
- UPS y generador eléctrico
- Aire acondicionado

b) Objetivo

Restaurar las funciones consideradas como críticas para el servicio.

c) Entorno

Sede Central y Centro de Datos del SENAMHI, por tener los gabinetes de comunicación y equipos que brinda servicios informáticos a los usuarios a nivel interno y externo.

d) Personal Encargado

El/La Director/a de la Oficina de Abastecimiento de la OA y el/la Coordinador/a de Continuidad de TIC son los responsables de realizar las coordinaciones para restablecer el suministro de energía eléctrica. El Equipo de Prevención de TIC debe realizar las acciones descritas en el punto f).

e) Condiciones de Prevención de Riesgo
- Durante las operaciones diarias del servicio u operaciones del SENAMHI se contará con los UPS necesarios para asegurar el suministro eléctrico en los equipos consideradas como críticos.
- Equipos UPS cuentan con mantenimiento preventivo para soportar una operación continua de 30 minutos como mínimo.
- Capacidad de los UPS para proteger los servidores de archivos, base de datos y aplicaciones, previniendo la pérdida de datos durante las labores. La autonomía del equipo UPS no deberá ser menor a 30 minutos.
- Verificación del cableado eléctrico del SENAMHI, recomendando una vez por año.

f) Acciones del Equipo de Prevención de TIC
- Revisar periódicamente y de forma conjunta con el área de Servicios Generales las instalaciones eléctricas del Centro de Datos y Sede principal de la entidad.
- Coordinar y supervisar el mantenimiento preventivo de pozos a tierra, aire acondicionado de precisión del Centro de Datos, UPS, transformador y del gabinete de baterías, generador eléctrico anualmente.
- Verificar que la red eléctrica utilizada en el Centro de Datos y la red de cómputo de la sede principal sea estabilizada. En caso no existan se debe gestionar la implementación de lo requerido con el área respectiva.
- Revisar la presencia de exceso de humedad en la sala de energía del centro de datos del SENAMHI.

2. PLAN DE EJECUCIÓN

a) Eventos que activan la contingencia
Corte de suministro de energía eléctrica en los ambientes de la sede central de SENAMHI.

b) Procesos Relacionados antes del evento
Cualquier actividad de servicio dentro de las instalaciones.

c) Personal que autoriza la contingencia
El/La Director/a de OA y/o Coordinador de Continuidad de TIC pueden activar la contingencia.

d) Descripción de las actividades después de activar la contingencia
- El generador eléctrico se activará para brindar energía a los equipos ubicados en el centro de datos
- Informar a el/la Director/a de la Oficina de Abastecimiento del problema presentado.
- Comunicar a la empresa prestadora de servicios de energía eléctrica la falta de energía.
- Las actividades afectadas por la falta de uso de aplicaciones, deberán iniciar sus procesos de contingencia a fin de no afectar las operaciones en curso.

e) Duración
El tiempo máximo de duración de la contingencia dependerá del proveedor externo de energía eléctrica.

3. PLAN DE RECUPERACIÓN

a) Personal Encargado
El Equipo de Restauración de TIC, quienes se encargarán de realizar las acciones de recuperación necesarias.

b) Descripción de actividades
El evento será evaluado

Se debe realizar como mínimo las siguientes actividades:
- Al retorno de la energía comercial se verificará por el lapso de media hora que no haya interrupciones o fluctuaciones de energía.
- La contingencia finaliza cuando retorna la energía eléctrica y todos los equipos se encuentran operativos brindando servicio.

c) Mecanismos de Comprobación
El/La Técnico en Redes y Comunicaciones presentará un informe a el/la Director/a de la OTI, explicando cuales han sido los efectos ocasionados por la falla del suministro eléctrico.

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

e) Proceso de Actualización
En base al informe que describe los problemas presentados, se determinarán las acciones de prevención a tomar.

ANEXO 5

FORMATO DE CONTROL Y CERTIFICACION DE LAS PRUEBAS

CONTROL Y CERTIFICACION DE PRUEBAS DE CONTIGENCIA

PRUEBA N°

Escenario de Prueba	
Área Responsable	

INFORMACION DEL PROCESO

Metodología ----------

Alcance ----------

Condición de Ejecución

Equipo [ ] Aplicación/ Software [ ]

Ubicación [ ] Fecha de Backup [ ]

RESULTADO DE PRUEBA

Resultado Satisfactoria [ ] Satisfactorio Con [ ] Observ. [ ]
Deficiente

Observaciones: ----------

ACTUALIZACION EN EL PLAN DE CONTINGENCIA

Cambio o actualización en el Plan de contingencia ----------

Actualización de Participantes

Participante	Cargo	Firma

Firma Digital Senamhi
Firmado digitalmente por HERR GARCIA Carlos Alejandro FAU 20131366028 hard
Motivo: Doy V° B°
Fecha: 11.01.2021 10:08:25 -05:00

Firma Digital Senamhi
Firmado digitalmente por CHACON CALDERON Jose Antonio FAU 20131366028 soft
Motivo: Soy el autor del documento
Fecha: 11.01.2021 10:43:02 -05:00