SERVICIO NACIONAL DE AGUAS SUBTERRÁNEAS, RIEGO Y AVENAMIENTO (SENARA)

Plan de Atención de Contingencia Informática y Recuperación de Servicios de Tecnología de la Información y Comunicaciones del Servicio Nacional de Aguas Subterráneas, Riego y Avenamiento (PCRTIC)

UNIDAD DE GESTIÓN INFORMÁTICA

ENERO 2026

El documento fue:

Actualizado por

Ingeniero Jorge Muñoz Muñoz
Coordinador General
Unidad de Gestión Informática

Firmado digitalmente por JORGE GERARDO MUÑOZ MUÑOZ (FIRMA)
Fecha:2026.02.11 14:35:06 -06’00’

Revisado por:

MBA Katia Hidalgo Hernández
Coordinadora
Dirección de Planificación

KATTIA HIDALGO HERNANDEZ (FIRMA)
Firmado digitalmente por KATTIA HIDALGO HERNANDEZ (FIRMA)
Fecha: 2026.02.13 12:07:28 -06'00'

Ing. Rocío Méndez Araya
Profesional Especialista en Gestión
Dirección de Planificación

ROCIO MENDEZ ARAYA (FIRMA)
Firmado digitalmente por ROCIO MENDEZ ARAYA (FIRMA)
Fecha: 2026.02.12 07:51:12 -06'00'

Autorizado por:

Ing, Osvaldo Quirós Arias
Gerente General de Senara


Firmado digitalmente por OSVALDO QUIROS ARIAS (FIRMA)
Fecha: 2026.02.17 09:26:46 -06'00'

ÍNDICE

1. INTRODUCCIÓN

Desde el año 2024, las oficinas del Servicio Nacional de Aguas Subterráneas, Riego y Avenamiento (SENARA) forman parte de las instalaciones del Ministerio de Agricultura y Ganadería, lo cual ha implicado adaptaciones institucionales a nuevas condiciones en materia de tecnologías de información y comunicación. En este contexto, y como parte del fortalecimiento continuo de la gestión de riesgos y la resiliencia tecnológica, se determinó la necesidad de actualizar el Plan de Contingencia Informático y Recuperación de Servicios de Tecnología de la Información y Comunicaciones (PCRTIC), cuya primera versión fue aprobada por la Gerencia General en el año 2023.

Para la elaboración de esta segunda versión del PCRTIC, se aplicó la metodología de análisis de riesgos basada en el marco COBIT 5.0, desarrollado por la Information Systems Audit and Control Association (ISACA), ampliamente reconocido por sus buenas prácticas internacionales en auditoría, gestión y control de tecnologías de la información.

Esta metodología fue seleccionada por su mayor robustez técnica y su capacidad para identificar amenazas específicas y escenarios de contingencia en entornos tecnológicos complejos, los cuales no se encontraban suficientemente contemplados en la estructura de riesgos definida por el Sistema de Valoración de Riesgo del Senara Componentes del Sistema (SEVRI institucional) aprobado mediante Acuerdo Nº 6073 de la sesión de Junta Directiva Nº 771-19 de fecha 18 del mes de noviembre del año 2019.

Aunque la Unidad de Gestión Informática aplica regularmente la metodología SEVRI indicada para la evaluación de riesgos en sus procesos operativos, se evidenció que en la Estructura de Riesgos Institucional vigente y descrita en el documento Sistema de Valoración de Riesgos-Componentes SEVRI, no se incorporan ciertos factores críticos relacionados con la continuidad tecnológica, tales como: la destrucción o indisponibilidad de la Oficina de Tecnologías de Información (TI), fallas en los sistemas de información y portales web institucionales, e interrupciones de comunicación causadas por eventos eléctricos o físicos.

Por esta razón, se optó por complementar el análisis institucional con la metodología COBIT 5.0, permitiendo así un abordaje más integral, técnico y alineado con estándares internacionales.

El uso de COBIT 5.0 permitió una identificación más precisa de los riesgos inherentes y residuales que enfrenta la infraestructura tecnológica del SENARA, también facilitará la actualización y el fortalecimiento de la estructura de riesgos y factores críticos considerados en el SEVRI institucional, promoviendo así su alineamiento con los requerimientos específicos en materia de tecnologías de la información.

Para asegurar y garantizar el adecuado alineamiento entre ambas metodologías de valoración de riesgo el Plan Contingencia dispone realizar las siguientes pertinentes para alcanzar la adecuada vinculación y alineamiento entre ambas metodologías, en la fase de implementación del Plan.

Por lo anterior, este Plan establece un proceso continuo de planificación, desarrollo, prueba e implementación de procedimientos orientados a garantizar la recuperación oportuna, eficiente y efectiva de los servicios de tecnología de información y comunicaciones ante cualquier eventualidad. De esta forma, se contribuye a asegurar la continuidad operativa de la institución, minimizando el impacto sobre los procesos sustantivos y administrativos del SENARA.

2. OBJETIVOS

2.1 Objetivo General

Establecer e implementar un conjunto integral de lineamientos, estrategias y procedimientos técnicos, basados en el marco COBIT 5.0, que permitan a la Unidad de Gestión Informática (UGI) del SENARA prevenir, responder y recuperar los servicios de tecnología de información y comunicaciones institucionales ante eventos disruptivos, con el fin de garantizar la continuidad operativa y minimizar el impacto sobre los procesos críticos de la Institución, en el momento en que se presenten contingencias que afecten la disponibilidad, integridad o confidencialidad de los activos tecnológicos.

2.2 Objetivos Específicos

a) Reducir el nivel de exposición al riesgo de interrupción de los servicios tecnológicos críticos del SENARA, mediante la implementación de un sistema de evaluación y priorización de amenazas, que permita establecer escenarios de contingencia medibles.

b) Incrementar la capacidad institucional de respuesta ante incidentes tecnológicos, mediante la formalización de estrategias de continuidad operativa orientadas a la restauración de sistemas, datos y servicios en un tiempo máximo definido según su criticidad.

c) Asegurar la disponibilidad de la información institucional esencial, mediante la implementación y mantenimiento de mecanismos de respaldo y recuperación, con tiempos de recuperación (RTO) definidos y medibles por cada tipo de activo.

d) Fortalecer la coordinación y toma de decisiones ante situaciones de contingencia, mediante un esquema de comunicación interfuncional con roles definidos y tiempos de respuesta establecidos para cada grupo de interés.

e) Garantizar que el personal técnico responsable esté preparado para la ejecución del plan, mediante la capacitación anual y la realización de simulacros con evaluación de desempeño basada en indicadores de tiempo de reacción y efectividad.

f) Mantener vigente y alineado el Plan de Contingencia con los cambios tecnológicos e institucionales, mediante revisiones documentadas al menos una vez por año o tras la ocurrencia de una contingencia real.

3. ALCANCE

El presente Plan de Contingencia Informático y Recuperación de Servicios de Tecnología de la Información y Comunicaciones (PCRTIC) del SENARA aplica a todo el personal técnico y administrativo vinculado con la operación, soporte, mantenimiento y uso de los servicios tecnológicos institucionales, así como a las unidades que dependan de estos servicios para el desarrollo de sus funciones sustantivas.

Este plan será activado por la Unidad de Gestión Informática (UGI) cuando se presente una interrupción o amenaza inminente que afecte significativamente la continuidad de los sistemas de información, aplicaciones críticas, infraestructura tecnológica, bases de datos, redes, servicios de comunicaciones o recursos digitales alojados en la Oficina de Tecnologías de Información del SENARA, ubicada en las instalaciones centrales del Ministerio de Agricultura y Ganadería.

El plan entra en vigor desde el momento en que se emite una alerta de contingencia, ya sea por detección automática del sistema, comunicación formal del personal responsable, o evidencia verificable de una afectación real a la infraestructura TIC. La ejecución del plan concluye una vez que los servicios hayan sido restaurados de forma estable y se minimicen los riesgos residuales, conforme al protocolo establecido en este documento.

Asimismo, el plan cubre tanto las instalaciones físicas de la Unidad de Gestión Informática como los entornos digitales en la nube y servicios externos contratados, siempre que se encuentren bajo la responsabilidad directa de esta Unidad. En escenarios donde la afectación se extienda a otras dependencias o sitios remotos, el plan podrá aplicarse de forma escalonada o simultánea, según el análisis de impacto y prioridad de los servicios comprometidos.

4. BASE LEGAL

- Ministerio de Ciencia y Tecnología. (2004). Directriz Nº 31681-MICIT sobre la Promoción del Desarrollo Científico y Tecnológico. La Gaceta Nº 54.
- Ministerio de la Presidencia. (2006). Decreto Ejecutivo Nº 33147-MP que crea la Comisión Intersectorial de Gobierno Digital. La Gaceta Nº 95.
- SENARA. (2019). Manual de Políticas y Normas Generales de Tecnología de Información. Unidad de Gestión Informática

5. DEFINICIONES

A continuación, se describen las definiciones técnicas que se utilizaran en el desarrollo del PCRTIC.

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.

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 este contexto, es una interrupción de las condiciones normales de operación en cualquier proceso informático en SENARA.

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 contra peligros potenciales o reducir su impacto. En el Anexo 1, se detalla la metodología utilizada en el presente plan basada en COBIT 5 de Information Systems Audit and Control Association - ISACA (Asociación de Auditoría y Control de Sistemas de Información), una asociación internacional que apoya y patrocina el desarrollo de metodologías y certificaciones para la realización de actividades de auditoría y control en sistemas de información.

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 de este 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.

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.

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.

Plan de Pruebas: Está constituido por un conjunto de pruebas. Cada prueba debe dejar claro qué 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.

6. METODOLOGÍA PARA ELABORACIÓN DEL PLAN DE CONTINGENCIA

La elaboración del presente Plan de Contingencia Informático y Recuperación de Servicios de Tecnología de la Información y Comunicaciones (PCRTIC) del SENARA se desarrolló siguiendo una metodología estructurada en siete fases secuenciales, basada en las buenas prácticas definidas por el marco COBIT 5.0 (Control Objectives for Information and Related Technology), desarrollado por la Information Systems Audit and Control Association (ISACA), así como en lineamientos de gestión de continuidad de servicios TIC propuestos por el Instituto Nacional de Estándares y Tecnología de los Estados Unidos (NIST), guía SP 800-34 Rev. 1 y complementada por directrices propias de la Unidad de Gestión Informática del SENARA.

Este enfoque metodológico fue seleccionado por su adecuación al entorno tecnológico institucional, su enfoque en la gestión de riesgos y su alineación con marcos internacionales ampliamente aceptados en el ámbito de continuidad operativa, recuperación ante desastres y gobierno de tecnologías de la información.

En la ilustración N○1 se presentan las fases que conforman esta metodología.

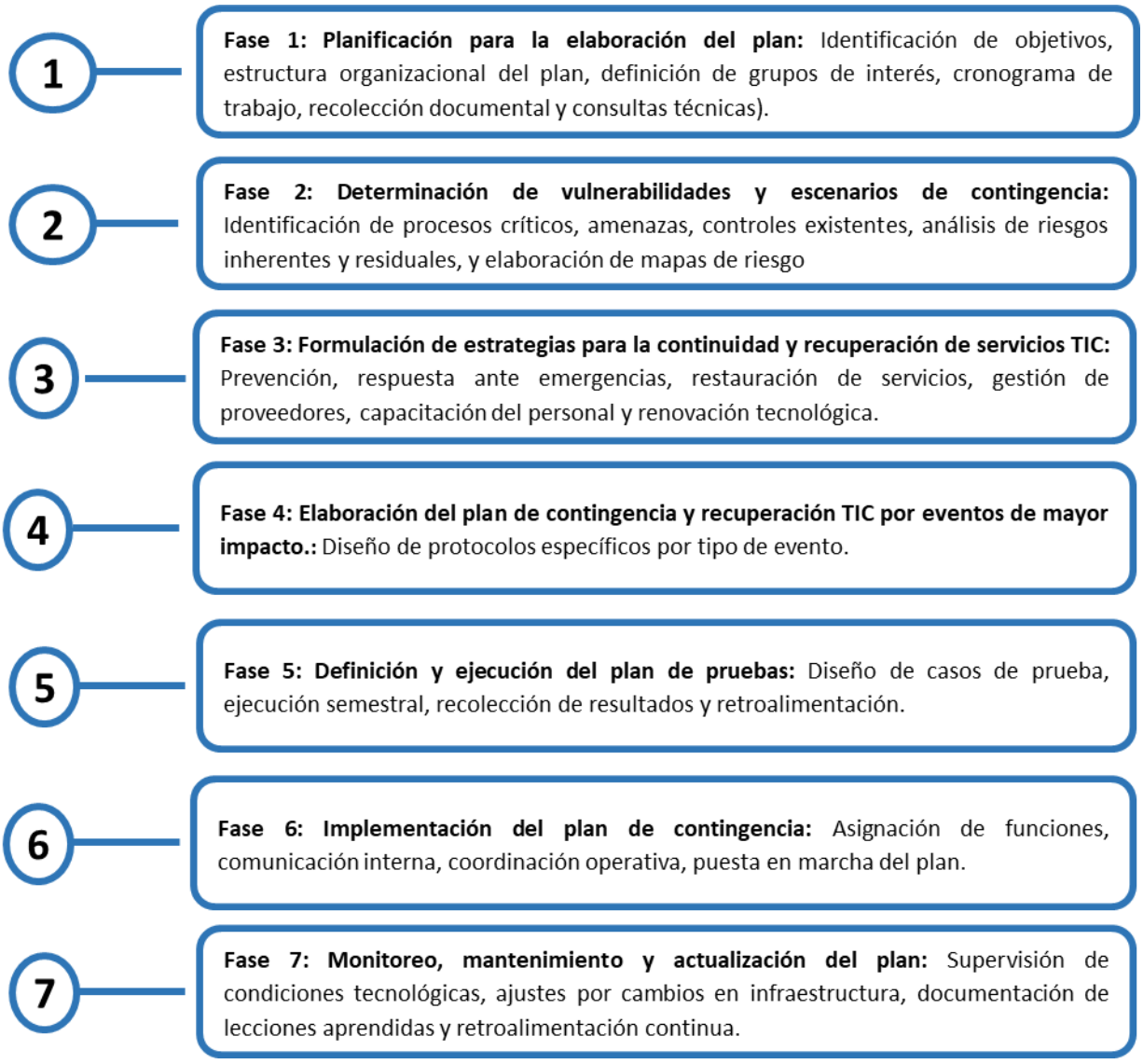

Ilustración N°1: Fases para la elaboración del Plan de Contingencia Informático y Recuperación de Servicios de Tecnología de la Información y Comunicaciones (PCRTIC) del SENARA con base en las buenas prácticas definidas por el marco COBIT 5.0.

6.1 Fase 1: Planificación

6.1.1 Organización del PCRTIC

La elaboración del Plan PCRTIC fue organizada y coordinada por la Unidad de Gestión Informática (UGI) del SENARA, bajo la supervisión directa de la Gerencia General. Este proceso se estructuró en función de los siguientes elementos organizativos:

Equipo técnico de formulación: Integrado por personal especializado de la Unidad de Gestión Informática, con experiencia en continuidad operativa, gestión de infraestructura tecnológica y análisis de riesgos. Este equipo fue responsable de compilar insumos, aplicar la metodología de análisis COBIT 5.0, redactar el contenido del plan y proponer los escenarios de contingencia.

Cronograma de trabajo: Se estableció un calendario de actividades que incluyó la recolección de información técnica, análisis de procesos críticos, identificación de amenazas, formulación de estrategias, validación institucional y revisión final. El cronograma fue adaptado conforme al avance técnico y la disponibilidad de actores clave.

Revisión documental y técnica: Se consultaron versiones anteriores del plan, normativas nacionales e institucionales vigentes, políticas de TIC del SENARA, y marcos metodológicos internacionales como COBIT 5.0 e ISO 22301 para continuidad de negocio.

Asesoría especializada: Para reforzar la validez del análisis de riesgos y escenarios de impacto, se contó con el criterio de personal experto en gestión de tecnologías de información y metodologías de auditoría de sistemas.

Identificación de partes interesadas: Se definieron los grupos clave involucrados directa o indirectamente en la ejecución del plan, incluyendo: Gerencia General, Direcciones funcionales, usuarios críticos de servicios TIC y proveedores estratégicos.

Definición de objetivos y alineamiento institucional: Se establecieron los objetivos generales y específicos del PCRTIC, asegurando su alineación con las políticas internas del SENARA, los lineamientos de gobierno digital y las necesidades reales de continuidad operativa de los servicios tecnológicos.

6.1.2. Roles, funciones y responsabilidades dentro del PCRTIC

A continuación, se describe los roles, responsabilidades y funciones que deben desarrollar los funcionarios de la Unidad de Gestión Informática respecto al Plan de Contingencia Informático y Recuperación de Servicios de Tecnologías de la Información y Comunicaciones.

a. Coordinador de Continuidad de Tecnologías de Información y Comunicaciones (TIC)

Está representado por el coordinador de la Unidad de Gestión Informática (UGI) de SENARA 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.

- Evaluar la extensión de la contingencia y sus consecuencias potenciales sobre la infraestructura tecnológica.

- Notificar y mantener informados, a los miembros del Comité de Tecnologías de Información 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 las instalaciones de la Unidad de Gestión Informática.

- Contactar a los proveedores para el reemplazo de hardware, software y/o activación de servicios para los sistemas 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 en la Unidad de Gestión Informática hayan sido restablecidas.

b. Equipo de seguridad, Intranet y Comunicaciones

Es el equipo (funcionarios) de la Unidad de Gestión Informática de SENARA, los cuales son los encargados 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. A continuación, se detallan las funciones de este equipo:

- 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 y componentes informáticos en la Unidad de Gestión Informática.
- Mantener actualizado el inventario hardware y software utilizado en la Unidad de Gestión Informática de SENARA.
- Programar y/o realizar el mantenimiento preventivo de los equipos de comunicaciones y de los equipos componentes de la Unidad de Gestión Informática, considerando el tiempo de vida útil y garantía de estos.
- Llevar un control detallado del mantenimiento realizado a cada equipo y componentes en la Unidad de Gestión Informática.
- Elaborar informes técnicos de conformidad, luego de cada mantenimiento efectuado, así como elaborar informes periódicos del funcionamiento de los equipos en la Unidad de Gestión Informática.
- Verificar que se mantiene actualizado, la documentación de las configuraciones de equipos de comunicaciones, el inventario de software de gestión y otros.
- Monitorear la intranet y definir medidas preventivas para minimizar o evitar las contingencias.

- Realizar las pruebas previas de recuperación.

- Coordinar acciones de mantenimiento de sistemas de información existentes asegurando el cumplimiento del ciclo de vida de software.

El protocolo de actuación que deberá ser activado por el Equipo de Seguridad, Intranet y Comunicaciones ante la ocurrencia de un evento de contingencia que afecte los servicios tecnológicos institucionales, es el siguiente:

- Notificar el desastre o incidencia al Coordinador de Continuidad de TIC.

- Ejecutar las acciones de emergencia en los equipos informáticos y componentes instalados en la oficina de la Unidad de Gestión Informática.

- Realizar la evaluación de condiciones de los equipos de comunicaciones y los componentes durante la emergencia en la Unidad de Gestión Informática.

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

- 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.

- Realizar la evaluación de la afectación a los equipos informáticos de usuario final (computadoras, 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 SENARA.

Una vez que el evento de contingencia haya sido controlado y se haya declarado su cierre operativo, se procederá con la fase de restauración de los servicios informáticos

6.2 Fase 2: Determinación de vulnerabilidades y escenarios de contingencia

Esta fase consiste en identificar, analizar y evaluar los elementos críticos de la infraestructura tecnológica institucional que podrían verse afectados ante la ocurrencia de eventos disruptivos, con el fin de establecer los escenarios de riesgo prioritarios que justifiquen la activación del Plan de Contingencia (PCRTIC).

En esta etapa se identifican los procesos, recursos y activos tecnológicos esenciales, se analizan las amenazas más probables que podrían afectar dichos activos, y se determina el nivel de exposición al riesgo mediante una evaluación sistemática. A partir de esta información, se definen los escenarios de contingencia más relevantes, sobre los cuales se construyen las estrategias de respuesta y restauración.
La ejecución de esta fase se realizó con base en:

- La metodología de gestión de riesgos COBIT 5.0, desarrollada por ISACA, que permite establecer niveles de riesgo inherente y residual a partir del análisis de probabilidad, impacto y efectividad de los controles existentes.
- El criterio técnico de expertos institucionales en gestión de TIC.
- El contexto operativo y geográfico de la Oficina de Tecnologías de Información del SENARA.
- La infraestructura tecnológica disponible, los acuerdos de servicio con proveedores y la experiencia en incidentes pasados.

Los resultados de esta fase permitieron definir:

- Los procesos y recursos tecnológicos críticos con sus respectivos tiempos objetivo de recuperación (RTO).
- Las amenazas internas y externas más relevantes, clasificadas por tipo (natural, tecnológica, humana, ambiental).
- La valoración de controles existentes, su efectividad y cobertura.
- El nivel de riesgo (inherente y residual) de cada activo frente a cada amenaza.
- Los escenarios de riesgo con mayor impacto operativo, los cuales sirven como base para las estrategias y protocolos del plan.

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° 1 – Procesos críticos de TI

Proceso crítico	Aplicaciones y/o recursos críticos	(RTO)
Gestión de redes e infraestructura de TI	Equipos de comunicaciones.	**12 h**
	Infraestructura en la Unidad de Gestión Informática.	**72 h**
	Enlaces de fibra óptica (intranet/Wifi).	**24 h**
Gestión de sistemas de información y bases de datos	Sistemas de información y portales.	**48 h**
	Repositorios utilizados por los sistemas y aplicativos.	**48 h**
Soporte Técnico	Estaciones de trabajo del personal crítico (computadoras portátiles).	**48 h**

*El RTO: Tiempo de Recuperación Objetivo, es determinado por Juicio de Expertos.
Fuente: Criterio Experto- COBIT 5.0 –Framework 2012

6.2.2. Identificación de amenazas

Este paso, permite identificar aquellas amenazas que pudieran vulnerar los servicios TIC del SENARA, considerando la ubicación geográfica, el contexto actual de la Oficinas Centrales y Centro de Datos y Comunicaciones, así como la percepción del Juicio Experto.

Tabla N° 2 - Amenazas a los servicios de TI

N°	Amenaza (Evento)	Tipo
01	Terremoto/Sismo.	Siniestros Naturales
02	Inundación y aniego en la Unidad de Gestión	
03	Incendio en la Unidad de Gestión Informática.	
04	Falla en telecomunicaciones.	Tecnológicos
05	Delito informático.	
06	Falla de hardware y software.	
07	Falla del suministro eléctrico en la Unidad de Gestión Informática.	Físico y ambiental
08	Ausencia o no disponibilidad del personal crítico de	Humanos
09	Pandemia y/o Epidemia.	Ambiental

Fuente: Criterio Experto- COBIT 5.0 –Framework 2012

Una vez determinadas las amenazas que pueden afectar los recursos críticos de TI, se calcula el nivel de probabilidad estimada (por Juicio de Expertos), a fin de identificar las amenazas que serán consideradas en la evaluación de los riesgos. A continuación, se detalla el resultado obtenido.

Tabla N° 3 - Probabilidad estimada de las amenazas a los servicios de TI

N°	Probabilidad	Calificación Cuantitativa	Nivel de probabilidad estimada
01	Terremoto	2	Puede ocurrir alguna vez entre uno y cinco años.
02	Inundación y aniego en la Unidad de Gestión Informática	1	Puede ocurrir al menos una vez en periodos superiores a cinco años
03	Incendio en la Unidad de Gestión Informática	1	Puede ocurrir al menos una vez en periodos superiores a cinco años
04	Falla en telecomunicaciones	1	Puede ocurrir al menos una vez en periodos superiores a cinco años
05	Delitos informáticos	3	Puede ocurrir al menos una vez al año
06	Falla del suministro eléctrico en la Unidad de Gestión	4	Puede ocurrir varias veces en un mes
07	Falla del hardware y software	3	Puede ocurrir al menos una vez al año
08	Ausencia o no disponibilidad del personal crítico de TI	1	Puede ocurrir alguna vez entre uno y cinco años
09	Pandemia y/o Epidemia	1	Puede ocurrir al menos una vez en periodos superiores a cinco años

Fuente: Criterio Experto- COBIT 5.0 –Framework 2012

6.2.3. Identificación de Controles Existentes

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

- Acuerdos de niveles de servicio con proveedor de enlace de comunicación ubicado la Unidad de Gestión Informática.

- Redundancia en los enlaces de comunicaciones (fibra óptica para ERP y Wifi) con el mismo proveedor.

- Respaldo de información (OneDrive y discos duros externos de usuario) y custodia externa de información para el ERP y aplicaciones de Bases de Datos en la Nube.

- Solución antivirus instalada en la Nube.

- Solución de protección de portales y aplicaciones web publicadas en internet a través de solución en la nube.

- Respaldo de equipos de comunicaciones (router, switch, Access Point).

- Esquema MESH de interconexión de Access Point.

- Acuerdos de niveles de servicio con proveedor de estaciones de trabajo del personal crítico

Una vez que se han identificado los controles, se expresar la valoración de cada control en términos numéricos. Para ello, se utiliza la escala de efectividad presentada en la Tabla N°4 Valorización de controles.

Tabla N° 4 – Escala de valoración de los controles

N°	Descripción del Control	Valor
1	Acuerdos de niveles de servicio con proveedor de enlace de comunicación ubicado la Unidad de Gestión Informática.	**5**
2	Redundancia en los enlaces de comunicaciones (fibra óptica para ERP y Wifi) con el mismo proveedor	**4**
3	Respaldo de información (OneDrive y discos duros externos de usuario) y custodia externa de información para el ERP y aplicaciones de Bases de Datos en la Nube.	**3**
4	Solución antivirus instalada en la Nube.	**5**
5	Solución de protección de portales y aplicaciones web publicadas en internet a través de solución en la Nube.	**5**
6	Respaldo de equipos de comunicaciones (router, switch, Access Point).	**4**
7	Esquema MESH de interconexión de Access Point.	**4**

Fuente: Criterio Experto- COBIT 5.0 –Framework 2012

6.2.4. Evaluación del Nivel de Riesgo

Para determinar el Nivel de Riesgo de un recurso de TI crítico del SENARA, se consideraron los controles existentes que mitigan la afectación de la amenaza descritos en el punto 6.2.3 y de acuerdo con la aplicación de la metodología de riesgos descrita en los anexos del 1 al 5, se obtuvo el siguiente resultado. A continuación, se presentan los resultados obtenidos:

- Tabla N° 5 - Riesgo inherente (Probabilidad x Impacto)

- Tabla N° 6 - Riesgo residual ((Probabilidad x Impacto) – Valor de la efectividad de los controles)

Tabla N° 5 - Riesgo inherente (Probabilidad x Impacto)										
MAPA DE CALOR										
N°	Recursos Críticos / Amenazas (Eventos)	Terremoto	Inundación y aniego en la Unidad de Gestión Informática	Incendio en la Unidad de Gestión Informática	Falla en telecomunicaciones	Delito informático	Falla de hardware y software	Falla del suministro eléctrico en la Unidad de Gestión Informática	Ausencia o no disponibilidad del personal crít de TI	Pandemia y/o Epidemia
1	Equipos de comunicaciones.	Alto	Bajo	Bajo	Moderado	Alto	Alto	Alto	Bajo	Bajo
2	Infraestructura de la Unidad de Gestión Informática	Alto	Bajo	Bajo	Bajo	Moderado	Moderado	Bajo	Bajo	Bajo
3	Cableado de red de Access Point	Alto	Bajo	Bajo	Bajo	Bajo	Bajo	Bajo	Bajo	Bajo
4	Enlaces de fibra óptica para interconexión entre proveedor y la Unidad de Gestión Informática	Alto	Bajo	Bajo	Bajo	Bajo	Moderado	Bajo	Bajo	Bajo
5	Sistemas de información y portales web	Bajo	Bajo	Bajo	Bajo	Bajo	Bajo	Bajo	Bajo	Bajo
6	Estaciones de trabajo del personal crítico	Alto	Bajo	Bajo	Bajo	Alto	Alto	Moderado	Bajo	Bajo
7	Personal crítico responsable de los procesos de TIC.	Bajo	Bajo	Bajo	Bajo	Alto	Bajo	Bajo	Bajo	Bajo

Fuente: Criterio Experto- COBIT 5.0 –Framework 2012

Tabla N° 6 - Riesgo residual ((Probabilidad x Impacto) – Valor de la efectividad de los controles)										
MAPA DE CALOR										
N°	Recursos Críticos / Amenazas (Eventos)	Terremoto	Inundación y aniego en la Unidad de Gestión Informática	Incendio en la Unidad de Gestión Informática	Falla en telecomunicaciones	Delito informático	Falla de hardware y software	Falla del suministro eléctrico en la Unidad de Informática Gestión	Ausencia o no disponibilidad del personal crítico de TI	Pandemia y/o Epidemia
1	Equipos de comunicaciones.	Medio	Bajo	Bajo	Bajo	Medio	Medio	Medio	Bajo	Bajo
2	Infraestructura de la Unidad de Gestión Informática.	Medio	Bajo	Bajo	Bajo	Moderado	Moderado	Bajo	Bajo	Bajo
3	Cableado de red de Access Point	Alto	Bajo	Bajo	Bajo	Bajo	Bajo	Bajo	Bajo	Bajo
5	Enlaces de fibra óptica para interconexión entre proveedor y la Unidad de Gestión Informática	Alto	Bajo	Bajo	Bajo	Bajo	Moderado	Bajo	Bajo	Bajo
6	Sistemas de información y portales web.	Bajo	Bajo	Bajo	Bajo	Bajo	Bajo	Bajo	Bajo	Bajo
7	Estaciones de trabajo del personal crítico (computadoras portátiles)	Alto	Bajo	Bajo	Bajo	Medio	Bajo	Moderado	Bajo	Bajo
8	Personal crítico responsable de los procesos de TIC.	Bajo	Bajo	Bajo	Bajo	Moderado	Bajo	Bajo	Bajo	Bajo

Fuente: Criterio Experto- COBIT 5.0 –Framework 2012

6.2.5. Escenarios de riesgo

A continuación, se indican los posibles escenarios de riesgo que se deben de tomar en cuenta en esta metodología:

- Destrucción e indisponibilidad de la Unidad de Gestión Informática por terremoto.
- Falla en el funcionamiento de los sistemas de información y portales web por delito informático (ataque cibernético, virus, etc.).
- Indisponibilidad de los equipos de Wifi por falla de hardware y software.
- Interrupción de comunicaciones por fallas en los equipos en la Unidad de Gestión Informática.
- Datos y Comunicaciones.

El nivel de impacto asignado a cada escenario de riesgo considera las consecuencias operativas en caso de materialización del evento, independientemente de su probabilidad de ocurrencia. La severidad del riesgo se determina posteriormente mediante la combinación de impacto y probabilidad, conforme a la metodología COBIT 5.

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

Tabla N° 7 - Escenarios de Riesgos

Escenario de Riesgo	Descripción	Impacto
Destrucción e indisponibilidad de la Unidad de Gestión Informática	Este escenario consiste en que la infraestructura tecnológica de la Unidad de Gestión Informática deje de funcionar parcial o totalmente como resultado de un terremoto o incendio, lo cual puede ocasionar caídas de servicios críticos, indisponibilidad de sistemas institucionales y daños a equipos e instalaciones.	Alto
Falla en el funcionamiento de los sistemas de información alojados en los portales web	Se refiere a la falla lógica o caída de los sistemas de información, aplicativos y portales web, lo cual produce que la información o servicios brindados por ellos no estén disponibles.	Bajo
Interrupción de comunicaciones por fallas en el suministro eléctrico en las instalaciones de la Unidad de Gestión Informática.	Este escenario consiste en el corte o interrupción de las comunicaciones entre en la Unidad de Gestión Informática y los servicios hospedados en Internet, 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.	Bajo

Fuente: Criterio Experto- COBIT 5.0 –Framework 2012

Los escenarios descritos representan eventos de alto impacto operativo, cuya materialización puede afectar significativamente la continuidad de los servicios TIC institucionales.

6.3 Fase 3: Estrategias PCRTIC

Una vez concluidas las fases de identificación de vulnerabilidades, evaluación de riesgos y análisis de escenarios de contingencia, se definió un conjunto de estrategias institucionales orientadas a garantizar la continuidad y recuperación de los servicios tecnológicos ante la ocurrencia de eventos disruptivos. Estas estrategias constituyen el marco de referencia sobre el cual se diseñan los procedimientos específicos de actuación del Plan de Contingencia Informático y Recuperación de Servicios de TIC (PCRTIC).

Desde una perspectiva metodológica, las estrategias fueron estructuradas en función del ciclo de la contingencia tecnológica, considerando tres momentos clave: prevención, respuesta y recuperación. Cada una de estas dimensiones responde a una lógica de gestión integral del riesgo tecnológico y permite establecer lineamientos de acción adaptados al nivel de impacto, criticidad del recurso afectado y prioridades operativas de la institución.

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 siguiente Matriz de Riesgo de Contingencia Tabla N°8, los cuales serán abordados en formatos independientes, tal como se indica en el siguiente cuadro:

Tabla N° 8 - Eventos de mayor impacto para el Plan de Contingencia Informático

N°	Evento	Exposición al Riesgo	Formato Plan de Contingencia
1	Terremoto	Alto	FPC - 01
2	Delito informático (ataque)	Alto	FPCI - 02
3	Falla de hardware y software	Alto	FPC - 03
4	Falla del suministro eléctrico en la Unidad de Gestión Informática	Alto	FPC - 04

La exposición al riesgo indicada en la anterior tabla se determina con base en la severidad del impacto y el nivel de riesgo inherente identificado en la fase de análisis, conforme a la metodología COBIT 5.

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 OTIC, 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 5.

6.6 Fase 6: Implementación del Plan de Contingencia

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

- Para tal efecto, el/la Coordinador de Continuidad de Tecnologías de Información y Comunicaciones (Coordinador de la UGI), realizará 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.

- El Coordinador de la UGI deberá considerar e incluir en los formatos vigentes, establecidos por el Senara para realizar la aplicación del SEVRI, los resultados de la valoración de riesgo identificados al aplicar la metodología COBIT 5.0, de forma tal que se logre asegurar y garantizar adecuada vinculación y alineamiento entre ambas metodologías y procesos de aplicación.
- Adicional a lo anterior como parte de la responsabilidad como Coordinador de la UGI, deberá aplicar los procedimientos establecidos en el Sistema de Valoración de Riesgo-Componentes SEVRI del Senara para actualizar de manera periódica la Estructura de Valoración de Riesgos.

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:

- Realizar mantenimiento de la documentación técnica de operación de los servicios de TI.

- Revisión continúa de las aplicaciones, sistemas de información y portales web.

- Implementar Políticas de Firewall para garantizar conexiones seguras (VPN, Wifi seguro).

- Supervisión activa de antivirus en dispositivos portátiles.

7. PROTOCOLO DE ACTIVACIÓN, RESPUESTA Y RESTAURACIÓN DEL PCRTIC

Este apartado define las acciones que deberán ejecutarse antes, durante y después de un evento que active el Plan de Contingencia Informático y Recuperación de Servicios TIC del

SENARA (PCRTIC). Su aplicación está a cargo de la Unidad de Gestión Informática y de los equipos designados en este plan.

7.1 Activación del Plan de Contingencia

Los escenarios clasificados como de impacto alto o riesgo alto, conforme a la metodología de análisis aplicada en el presente plan, constituyen criterios suficientes para la activación inmediata del Plan de Contingencia Informático y Recuperación de Servicios de TIC (PCRTIC). El Coordinador de Continuidad de TIC será responsable de declarar formalmente la activación del plan, con base en una o varias de las siguientes condiciones:

- Alerta emitida por los sistemas de monitoreo o personal técnico.
- Verificación de falla total o parcial en los servicios críticos TIC.
- Determinación de amenaza inminente a la infraestructura tecnológica.

Una vez activado el plan:

- Se notifica a los equipos designados.
- Se ejecutan las acciones inmediatas de control, aislamiento o contención del evento.
- Se activa el protocolo de comunicación institucional, según el tipo de evento.

7.2 Ejecución de la respuesta durante la contingencia

Durante la contingencia, el Equipo de Seguridad, Intranet y Comunicaciones deberá:

- Evaluar la afectación a los servicios tecnológicos.
- Asegurar las condiciones mínimas para continuidad operativa parcial si es posible.
- Implementar medidas provisionales de acceso, respaldo o redireccionamiento.
- Comunicar las acciones realizadas al Coordinador TIC y a los usuarios críticos.

7.3 Fase de restauración de servicios

Una vez que el siniestro haya sido contenido y controlado, se ejecutarán las siguientes acciones:

- Iniciar el proceso de recuperación de los servicios de tecnología de la información, incluyendo la infraestructura informática, los equipos de comunicaciones y los componentes alojados en la Unidad de Gestión Informática del SENARA.
- Ejecutar pruebas de funcionamiento en los equipos afectados, tanto de infraestructura como de estaciones de trabajo del personal crítico.
- Restaurar la información desde las copias de respaldo disponibles, validando su integridad, y verificar que los puntos de recuperación cumplan con los objetivos establecidos (RTO y RPO).
- Verificar el correcto funcionamiento de las aplicaciones informáticas, sistemas de información, bases de datos y servicios institucionales, realizando las pruebas necesarias y reinstalando componentes críticos si fuera necesario.
- Solucionar los problemas de conexión y funcionamiento de los equipos asignados al personal (computadoras, impresoras, escáneres u otros periféricos esenciales).
- Validar, en coordinación con los usuarios responsables, la operatividad de los sistemas recuperados y confirmar la reactivación de los servicios afectados.
- Elaborar informes técnicos detallados que incluyan:
    - Acciones de recuperación ejecutadas.
    - Evaluación del estado de los equipos y componentes restaurados.
    - Estado de las aplicaciones, bases de datos y sistemas de información.
    - Evaluación de los dispositivos de usuario final.
- Notificar formalmente al Coordinador de Continuidad de TIC la finalización del proceso de recuperación y entregar los informes correspondientes.
- Comunicar oficialmente la reactivación total de los servicios tecnológicos, una vez validada la restauración integral.

7.4 Estrategias operativas de prevención

Las siguientes acciones deben ejecutarse de forma permanente como parte del plan de prevención institucional frente a posibles eventos que afecten la continuidad de los servicios de tecnología de la información:

- Mantener actualizados y verificados los respaldos de información crítica institucional, tanto en la nube (OneDrive, servicios externos) como en dispositivos físicos protegidos.
- Aplicar políticas de almacenamiento con criterios de rotación, identificación y transporte seguro de medios de respaldo.
- Supervisar la renovación tecnológica mediante evaluaciones semestrales de obsolescencia, con base en estadísticas de fallas o deterioro de equipos.

- Implementar controles de seguridad perimetral, antivirus actualizado, protección de portales web y monitoreo de amenazas.
- Mantener inventarios actualizados de hardware, software y configuraciones críticas de red.
- Establecer y actualizar contratos con proveedores clave (software, enlaces, hardware), incluyendo niveles de servicio y tiempos de respuesta ante emergencias.
- Asegurar la capacitación anual del personal técnico en procedimientos de recuperación y restauración, incluyendo simulacros internos documentados.
- Garantizar la disponibilidad de personal crítico mediante una programación de vacaciones rotativa o mecanismos de reemplazo.
- Verificar periódicamente los accesos remotos seguros para garantizar la continuidad operativa fuera de sitio (VPN, autenticación, cifrado).
- Activar la opción de trabajo remoto y desvío de llamadas para personal de soporte y atención a usuarios cuando la contingencia lo amerite.

7.5 Estrategias operativas de respuesta inmediata ante contingencias

Una vez activado el PCRTIC por parte del Coordinador de Continuidad de TIC, se ejecutarán las siguientes acciones inmediatas:

- Notificar al equipo técnico responsable y convocar la activación del plan según el tipo de evento.
- Evaluar el alcance del incidente y definir la zona afectada (Unidad de Gestión Informática, red, sistema, comunicaciones, estaciones de trabajo).
- Aislar los equipos o sistemas comprometidos para contener daños (desconexión de red, suspensión de servicios, restricción de accesos).
- Activar canales alternos de comunicación y coordinación institucional.
- Verificar la seguridad del área para permitir la intervención técnica (en caso de siniestro físico).
- Elaborar un informe preliminar del evento, posibles causas y riesgos inmediatos, para notificación a la Gerencia y partes interesadas.
- Aplicar medidas transitorias de continuidad como: activación de respaldos secundarios, acceso limitado a sistemas o atención en modo contingencia.

7.6 Estrategias operativas de recuperación de servicios

El ciclo considerado para la estrategia de recuperación de tecnologías de la información es el siguiente:

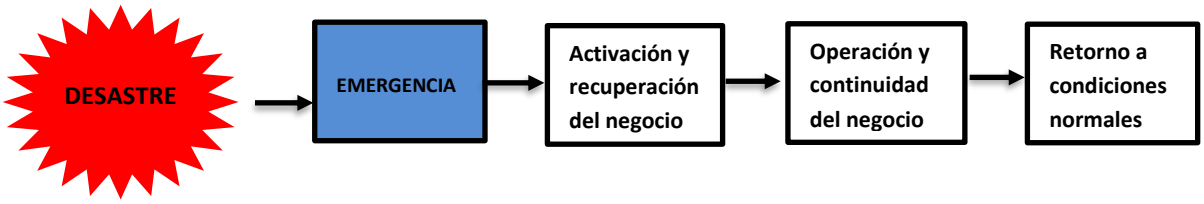

Ilustración N° 2 - Ciclo de la estrategia de recuperación de TI

Una vez que el evento de contingencia haya sido controlado y se declare su cierre operativo, se procederá con las siguientes acciones para restaurar los servicios TIC institucionales:

- Iniciar el proceso de recuperación de los servicios de tecnología de la información, incluyendo la infraestructura afectada y los equipos críticos de la Unidad de Gestión Informática.
- Ejecutar pruebas de funcionamiento en los equipos restaurados y estaciones de trabajo del personal crítico.
- Restaurar la información desde copias de respaldo, validando su integridad y cumplimiento de los puntos de recuperación establecidos.
- Verificar el estado de las aplicaciones institucionales, bases de datos y sistemas de gestión, reinstalando los componentes que lo requieran.
- Solucionar los problemas de conectividad y funcionamiento de los equipos de usuario final (computadoras, impresoras, escáneres, etc.).
- Validar la operatividad de los servicios restaurados con los usuarios responsables y unidades solicitantes.
- Elaborar informes técnicos documentados que incluyan:

    - Acciones de recuperación realizadas
    - Estado de los equipos de red, servidores y estaciones
    - Funcionamiento de aplicaciones y bases de datos,
    - Evaluación del servicio recibido por los usuarios finales.

- Notificar formalmente al Coordinador de Continuidad TIC la finalización del proceso de recuperación.
- Comunicar oficialmente a nivel institucional la reactivación total o parcial de los servicios tecnológicos.

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

Tabla N° 9 - Prioridad de atención durante la restauración de TIC

Prioridad de Atención	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: Atención a público, comunicación con el Sistema Administrativo Financiero (ERP), equipos de comunicación (intranet) entre otros.
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: impresoras, escáneres, sistemas de ofimática, etc.

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.

8. ANEXOS

- **Anexo 1:** Metodología aplicada a la gestión de riesgos.

- **Anexo 2:** Listado de aplicaciones y sistemas de información clasificados por prioridad de atención para la recuperación de TIC.

- **Anexo 3:** Listado de equipos den la Unidad de Gestión Informática 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.

9. ANEXO 1: METODOLOGÍA APLICADA A LA GESTIÓN DE RIESGOS

9.1.1 **Cálculo de la probabilidad de 0currencia de la amenaza**.

Para realizar este cálculo, se toman en cuenta dos variables: “Frecuencia” y “Factibilidad de Ocurrencia”.

- **Frecuencia**:
  Número de veces que sucede un evento. Por ejemplo, número de veces que se descompone el equipo, número de veces que no hay información disponible o número de veces que hubo ataques de virus.

- **Factibilidad**:
  Se refiere a la presencia de factores internos y externos que pueden propiciar la aparición u ocurrencia del riesgo, aunque este no se haya materializado anteriormente.

Para establecer el nivel de probabilidad de los riesgos, se utilizará la escala indicada en la Tabla N°1 que contempla la calificación cuantitativa y la cualitativa. Esto, con el objetivo de que los participantes puedan ubicar el riesgo en una de las calificaciones y que dicha calificación sea útil en la determinación del nivel de riesgo.

10. 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 “Improbable”, según la tabla siguiente no son tomados en cuenta.

Tabla N°10 Escala de probabilidad

Probabilidad	Calificación Cuantitativa	Calificación Cualitativa	Código de Colores
Altamente probable (AP)	5	Puede ocurrir diariamente.	
Muy probable (MP)	4	Puede ocurrir varias veces en un mes.	
Probable (P)	3	Puede ocurrir al menos una vez al año.	
Poco Probable (PP)	2	Puede ocurrir alguna vez entre uno y cinco años.	
Improbable (IP)	1	Puede ocurrir al menos una vez en periodos superiores a cinco años.	

11. Cálculo del Impacto:

Se refiere a las consecuencias que podría ocasionar el riesgo en el logro del objetivo de TI y de SENARA si llega a materializarse. Se utiliza la siguiente tabla:

Tabla N°11 – Escala de Impacto

Impacto	Calificación Cuantitativa	Calificación Cualitativa	Código de Colores
Impacto Catastrófico	5	Puede ocasionar daños muy considerables y una interrupción completa de los servicios.	
Impacto Alto	4	Puede ocasionar daños muy considerables o una interrupción de los servicios.	
Impacto Medio	3	Puede ocasionar algunos daños y una interrupción parcial de los servicios.	
Impacto Moderado	2	Puede ocurrir una interrupción parcial de los servicios.	
Impacto Bajo	1	Existe una alerta, pero no hay interrupción de los servicios ni daños ocasionados.	

12. Nivel de riesgo y mapa de calor

El nivel de riesgo, también conocido como severidad, representa el grado de exposición al riesgo. Este valor se determina a partir del análisis de la probabilidad de ocurrencia del evento y de la magnitud de sus consecuencias potenciales sobre el cumplimiento de los objetivos; se utiliza las siguientes tablas:

Tabla N° 12 - Nivel de riesgo

Nivel de Riesgo	Probabilidad x Impacto
Muy Alto	Mayor o igual que 20
Alto	Mayor o igual que 10 y menor que 20
Medio	Mayor o igual que 5 y menor que 10
Moderado	Mayor o igual que 3 y menor que 5
Bajo	Menor que 3

Tabla N° 13 - Mapa de calor

Mapa de calor		Impacto				
Probabilidad	Valor	Bajo	Moderado	Medio	Alto	Catastrófico
Altamente probable	5	Medio	Alto	Alto	Catastrófico	Catastrófico
Muy probable	4	Moderado	Medio	Alto	Alto	Catastrófico
Probable	3	Moderado	Medio	Medio	Alto	Alto
Poco probable	2	Bajo	Moderado	Medio	Medio	Alto
Improbable	1	Bajo	Bajo	Moderado	Moderado	Medio

13. Riesgo Inherente y riesgo residual

El valor del riesgo obtenido de multiplicar los valores de probabilidad e impacto se conoce como riesgo inherente. Este valor representa el nivel de riesgo antes de considerar cualquier método de control que se haya implementado en SENARA para gestionar el riesgo.

Posteriormente, se debe calcular el riesgo residual que se refiere al nivel de riesgo que permanece al considerar los controles que SENARA haya definido con anterioridad.

14. Valorización de Controles

Una vez que se han identificado los controles existentes, se debe expresar la valoración de cada control en términos numéricos. Para ello, se utilizará la escala de efectividad presentada en la siguiente tabla.

Tabla N°14 - Valorización de controles

Descripción del control	Valor
Documentado y sujeto a revisión periódica	5
Se realiza formalmente y está documentado	4
Se realiza informalmente en forma total	3
Se realiza parcial e informalmente	2
No se realiza	1

Nota: Metodología de Control Objectives for Information and Related Technology-COBIT 5.0 (Objetivos de control para tecnologías de la información y tecnologías relacionadas), el cual fue desarrollado por Information Systems Audit and Control Association (Asociación de Auditoría y Control de Sistemas de Información).

15. ANEXO 2: TABLA N°15 LISTADO DE APLICACIONES Y SISTEMAS DE INFORMACIÓN CLASIFICADOS POR PRIORIDAD DE ATENCIÓN PARA LA RECUPERACIÓN DE TIC

N°	Sistema / Aplicativo	Breve descripción	Área Usuaria	Motor de BD	Tipo	Prioridad
1	WatchGuard - Dimension	Es una solución de visibilidad y administración virtual que puede utilizar para capturar los datos de registro de sus Firebox, FireCluster y equipo WatchGuard, así como gestionar sus Firebox y FireCluste.	Unidad de Gestión Informática	Data Base Management System -Progress	NUBE	2
2	Hermes 7.0.0.575 Administrador de Sitios	Es un agente de comunicación remota con la aplicación Hermes 7.0.0575, para publicación de contenido en la página Web de Senara.	Unidades y Áreas	HERMES Hash-DB	NUBE	2

16. ANEXO 3: TABLA N°16 LISTADO DE EQUIPOS DE LA UNIDAD DE GESTIÓN INFORMÁTICA CLASIFICADOS POR PRIORIDAD DE ATENCIÓN PARA LA RECUPERACIÓN DE TIC

N°	Tipo de equipo	Rol	Descripción Prioridad	Prioridad
1	Router WatchGuard	Comunicaciones	Equipo de control de detección de violaciones a la seguridad, el robo de datos y los ciberataques	1
2	Switch	Comunicaciones	Equipo de control de entradas/ salidas para la intranet (Access Point)	1
3	Router-ICE	Internet	Enlace de comunicaciones INPUT/OUTPUT SENARA-ICE.	1
4	Access Point	Intranet	Equipo de soporte para Intranet tipo MESH	1

17. ANEXO 4: FORMATOS DEL PLAN DE CONTINGENCIA INFORMÁTICO Y RESTAURACIÓN DE SERVICIOS DE TIC

8.4.1 Evento: Terremoto

SENARA	Evento: Terremoto /Sismo	FPC - 01

1.PLAN DE PREVENCIÓN

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 SENARA, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia:

Infraestructura

- Oficinas y/o Centro de Datos y Comunicaciones.
- 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 SENARA, sin exponer la seguridad de las personas.

c) Entorno

Este evento puede afectar las instalaciones de la Oficinas Centrales y den la Unidad de Gestión Informática, al ubicarse en la misma ciudad.

d) Personal Encargado

Equipo de seguridad, Redes y Comunicaciones, son quienes deben dar los lineamientos y dar cumplimiento a las Condiciones de Prevención de Riesgo del presente Plan y 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 SENARA, el mismo que debe ser de conocimiento de todo el personal que labora en todas las sedes.

f) Realización de simulacros de evacuación con la participación de todo el personal.

- Conformación de las brigadas de emergencia, y capacitarlas semestralmente.
- Mantenimiento de las salidas libres de obstáculos.
- Señalización de las zonas seguras y las salidas de emergencia.
- Funcionamiento de las luces de emergencia.
- Definición de los puntos de reunión en caso de evacuación.

f) Acciones preventivas

- Evaluar el ambiente en la Unidad de Gestión Informática.
- Establecer, organizar, ejecutar y supervisar procedimientos reconfiguración de equipos de comunicaciones.
- Programar, supervisar el mantenimiento preventivo a los equipos y componentes de la intranet en la Unidad de Gestión Informática.
- Mantener actualizado el inventario hardware y software utilizado en la Unidad de Gestión Informática.

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

- Mantenimiento del orden y limpieza de los ambientes de la Oficinas Centrales y Unidad de Gestión Informática.
- Inspecciones trimestrales de seguridad externa.
- Realización de simulacros internos en horarios que no afecten las actividades.

c) Personal que autoriza la contingencia informática: Coordinador de Continuidad de TIC.

d) Personal Encargado: Equipo de seguridad, Intranet y Comunicaciones.

e) Descripción de las actividades después de activar la contingencia

- Evacuar las oficinas de acuerdo con las disposiciones de los Brigadistas de Evacuación, utilizando las rutas establecidas durante los simulacros. Considerar las escaleras de emergencia, señalización de rutas, zonas de agrupamiento del personal, etc. Por ningún motivo utilizar los ascensores.
- Verificar que todo el personal del SENARA 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 estos.
- Limpieza de las áreas afectadas por el sismo. En todo momento se coordinará con personal de mantenimiento del SENARA, para las acciones que deban ser efectuadas por ellos.

f) Duración

- Los procesos de evacuación del personal del SENARA 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

Equipo de seguridad, Intranet y Comunicaciones, cuyo rol principal es asegurar el normal desarrollo de los servicios y operaciones de TI del SENARA.

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.

- 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.

- Restauración de los servicios y operaciones de TI. El equipo de seguridad, Intranet y Comunicaciones 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, una vez concluida la emergencia o siniestro.
    - Registrar todos los gastos operacionales relacionados con la continuidad del negocio.

c) Mecanismos de Comprobación
El equipo de seguridad, Intranet y Comunicaciones presentará un informe al Coordinador de Continuidad de TIC 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 Coordinador 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.

e) Proceso de Actualización
El proceso de actualización será con base en el informe presentado por el Equipo de seguridad, Redes y Comunicaciones, luego del cual se determinará las acciones a tomar.

8.4.2 Evento: Delito Informático

SENARA	Evento: Delito Informático	FPC - 02

PLAN DE PREVENCIÓN

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 el SENARA, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia, los cuales se muestran a continuación:

- Hardware: Estaciones de Trabajo
- Software: Software Base, Sistemas de información, aplicativos y portales del SENARA
- Supervisión activa de antivirus en dispositivos portátiles

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 las estaciones ubicadas en la Unidad de Gestión Informática en Oficinas Centrales del SENARA.

d) Personal Encargado

- El Equipo de seguridad, Intranet y Comunicaciones, es el responsable del correcto funcionamiento de las estaciones de trabajo, sistemas de información y servicios de TI de acuerdo con sus perfiles
- Eliminación o restricción de lectoras y/o quemadores de CD en estaciones de trabajo que no lo requieran.

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.
- Contar con antivirus instalados en cada estación de trabajo, el mismo que debe estar actualizado permanentemente
- 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 equipos de respaldo ante posibles fallas de las estaciones de trabajo, 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.
- Des habilitación 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 Equipo de seguridad, Intranet y Comunicaciones, sobre Ethical Hacking a las Bases de Datos, Sistemas Operativos y Sistemas Informáticos.
- Ejecución de ataques de Hacking Ético por terceros especializados.

f) Acciones del Equipo de Prevención de TIC:

- Llevar un control de versiones de las fuentes de los sistemas de información.
- Realizar pruebas de restauración de la información en estaciones de trabajo.

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 las estaciones de trabajo.

c) Personal que autoriza la contingencia

- El Coordinador de Continuidad de TIC puede activar la contingencia.

g) Personal Encargado

- Equipo de seguridad, Intranet y Comunicaciones.

d) Descripción de las actividades después de activar la contingencia

- Desconectar o retirar de la intranet de SENARA 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 configuración 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.

e) 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 la intranet. Esperar la indicación del Equipo de seguridad, Intranet y Comunicaciones para reanudar el trabajo

PLAN DE RECUPERACIÓN

a) Personal Encargado

El Equipo de seguridad, Intranet y Comunicaciones, luego de restaurar el correcto funcionamiento de la estación de trabajo (laptop) y portales web, coordinará con el usuario responsable del mismo y/o director del área para reanudar las labores de trabajo con el equipo o sistema que fue afectado.

b) Descripción de actividades

Se informará al Coordinador de Continuidad de TIC 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.
- Reinicio del servicio.
- Conectar la estación a la Intranet del SENARA.
- Efectuar las pruebas necesarias con el usuario final de los equipos y/o sistemas afectados.
- Solicitar la conformidad de la restauración realizada del equipo y o sistema afectado.
- Comunicar el restablecimiento del servicio.
- Conectar la estación a la Intranet del SENARA.
- Efectuar las pruebas necesarias con el usuario final de los equipos y/o sistemas afectados.
- Solicitar la conformidad de la restauración realizada del equipo y o sistema afectado.
- Comunicar el restablecimiento del servicio.

En función a esto, el Coordinador de Continuidad de TIC, tomará las medidas preventivas del caso enviando una alerta vía correo al personal del SENARA.
El evento será evaluado y registrado de ser necesario en el formato de ocurrencia de incidentes de seguridad de la información.

c) Mecanismos de Comprobación

Se llenará el formato de incidentes de seguridad de la información y se informará al Coordinador de Continuidad de TIC.

El personal del Equipo de seguridad, Redes y Comunicaciones presentará un informe al Coordinador de Continuidad de TI, 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 indicado anteriormente el Coordinador de Continuidad de TIC desactivará el presente Plan.

e) Proceso de Actualización

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

8.4.3 Evento: Falla de hardware y software

SENARA	Evento: Falla de hardware y software	FPC-03

PLAN DE PREVENCIÓN

a) Descripción del evento
El hardware de procesamiento y comunicaciones 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
Intranet, Archivos.
Storage.

Software
Aplicativos usados por el SENARA y de servicio al ciudadano.

Información
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 equipos en producción.

c) Entorno
Se puede producir durante el servicio, afectando a las aplicaciones usadas para dar soporte a las operaciones del SENARA.

d) Personal Encargado
Equipo de seguridad, Intranet y Comunicaciones.

e) Condiciones de Prevención de Riesgo
Contar con servicios de soporte y mantenimiento que contemple actividades de prevención, revisión del sistema y mantenimiento general.

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 den la Unidad de Gestión Informática.
- Mantener actualizado el inventario hardware y software utilizado en la Unidad de Gestión Informática del SENARA.
- Realizar revisiones de obsolescencia tecnológica de los equipos de procesamiento general y comunicaciones de forma anual.

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 equipos de comunicación.

b) Procesos Relacionados antes del evento

Disponibilidad de instaladores de sistemas operativos.

c) Personal que autoriza la contingencia

El Coordinador de Continuidad de TIC debe activar la contingencia.

d) Descripción de las actividades después de activar la contingencia

Realizar la revisión del equipo averiado, buscando un recurso de reemplazo verificando que dicho equipo cuente con garantía.

e) Duración

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

PLAN DE RECUPERACIÓN

a) Personal Encargado

El Equipo de seguridad, Intranet y Comunicaciones, luego de validar magnitud de los daños en los equipos y el Coordinador de Continuidad de TIC informará a los directores de áreas para la reanudación de las operaciones de los servicios afectados en el equipo 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 equipos.

Se debe realizar como mínimo las siguientes actividades:

- Instalación y puesta a punto del hardware necesario para la operación de los servicios.
  Instalación y configuración del sistema operativo, drivers y servicios necesarios para el funcionamiento del sistema de información a recuperar.
- 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.

Activación de redundancia en la red Intranet (Wifi) mediante redes vecinas implementadas en las instalaciones física de SENARA.

Remitir un mensaje electrónico a los usuarios del SENARA 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 los dispositivos definidos por la Unidad de Gestión Informática, precisando las acciones realizadas.

El Equipo de seguridad, Intranet y Comunicaciones, presentará un informe al Coordinador de Continuidad de TIC, 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 el Coordinador de Continuidad de TIC desactivará el presente Plan.

e) Proceso de Actualización
En base al informe presentado por el Equipo de seguridad, Intranet y Comunicaciones, quienes identifican las causas de la pérdida o fallas en equipos institucionales, se determinará las acciones preventivas necesarias que deberían incluirse en el presente plan.

En caso existiese información pendiente de actualización, el personal encargado deberá iniciar las labores de actualización de los procedimientos.

8.4.4 Evento: Falla del suministro eléctrico en la Unidad de Gestión Informática

SENARA	Evento: Falla del suministro eléctrico en la Unidad de Gestión Informática	FPC-04

PLAN DE PREVENCIÓN

a) Descripción del evento
Falla general del suministro de energía eléctrica en la Unidad de Gestión Informática de SENARA.

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

Servicios Públicos:
Suministro de Energía Eléctrica.

Hardware
Estaciones de Trabajo e Intranet.
Equipos de Comunicaciones.

b) Objetivo
Restaurar las funciones consideradas como críticas para el servicio.

c) Entorno
Este evento puede darse en las Oficinas Centrales donde se ubica en la Unidad de Gestión Informática, por tener los equipos de comunicación que brinda servicios informáticos a los usuarios a nivel interno y externo.

d) Personal Encargado
Equipo de seguridad, Intranet y Comunicaciones, es el responsable de realizar las coordinaciones para restablecer el suministro de energía eléctrica.

e) Condiciones de Prevención de Riesgo
Coordinar la verificación del cableado eléctrico de Oficinas Centrales, una vez por año.
Configuración y monitoreo avanzado de los puntos de acceso (Access Point) para garantizar cobertura y estabilidad.

f) Acciones del Equipo de seguridad, Redes y Comunicaciones
Revisar periódicamente y de forma conjunta con la Unidad de Servicios Administrativos las instalaciones eléctricas den la Unidad de Gestión Informática de la entidad.

- Verificar que la red eléctrica utilizada en la Unidad de Gestión Informática y la intranet de Oficinas Centrales 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 Unidad de Gestión Informática del SENARA.
- Supervisión continua del enlace de fibra óptica contratado.

PLAN DE EJECUCIÓN

Eventos que activan la contingencia

Corte de suministro de energía eléctrica en los ambientes del SENARA.

b) Procesos Relacionados antes del evento

Cualquier actividad de servicio dentro de las instalaciones.

c) Personal que autoriza la contingencia

El Coordinador de Continuidad de TIC puede activar la contingencia.

d) Descripción de las actividades después de activar la contingencia

- Informar a él/la director/a de la unidad o área el problema presentado.
- Comunicar a la entidad prestadora de servicios de energía eléctrica la falta de energía.
- Dar aviso del corte de energía eléctrica en forma oportuna a todas las áreas del SENARA y coordinar las acciones necesarias.
- 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.

En caso de que la interrupción de energía en la Unidad de Gestión Informática sea mayor a dos (2) horas, se deberán apagar los equipos en forma ordenada hasta que regrese el fluido eléctrico.

PLAN DE RECUPERACIÓN

Personal Encargado

Equipo de seguridad, Intranet y Comunicaciones, quienes se encargarán de realizar las acciones de recuperación necesarias.

b) Descripción de actividades

El evento será evaluado y registrado de ser necesario en el formato de incidentes de seguridad de la información. Se debe realizar como mínimo las siguientes actividades:

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

c) Mecanismos de Comprobación

El Equipo de seguridad, Intranet y Comunicaciones presentará un informe Coordinador de Continuidad de TIC, explicando que parte del servicio, equipos u operaciones de tecnología de la información han fallado y cuáles son las acciones correctivas y/o preventivas a realizar.

d) Desactivación del Plan de Contingencia

El 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 CERTIFICACIÓN DE LAS PRUEBAS
CONTROL Y CERTIFICACIÓN DE PRUEBAS DE CONTINGENCIA

PRUEBA. N° _____

Escenario de Prueba: _____

Área Responsable: _____

INFORMACIÓN DEL PROCESO

Metodología: _____

Alcance: _____

Condiciones de Ejecución

Equipo: _____ **Aplicaciones/Software:** _____

Ubicación: _____ **Fecha:** _____

RESULTADO DE LA PRUEBA

Resultado: **Satisfactorio:** ☐ **Satisfactorio con Observaciones:** ☐ **Deficiente:** ☐

Observaciones: _____

ACTUALIZACIÓN EN EL PLAN DE CONTINGENCIA

Cambios o actualizaciones en el Plan de Contingencia: _____

ACTUALIZACIÓN PARTICIPANTES

Participante	Cargo	Firma

18. BITÁCORA DE ACTUALIZACIONES.

Versión Modificada	Fecha de Versión Modificada	Fecha de actualización	Descripción del cambio	Responsable
01	2023	30-10-25	Actualización con base en la metodología de análisis de riesgos basada en el marco COBIT 5.0, desarrollado por la Information Systems Audit and Control Association (ISACA),	Ing. Jorge Muñoz Muñoz, coordinador de UGI