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

Mayo 2022

INDICE

INTRODUCCIÓN

El presente documento define el Plan de Contingencia Informático y Recuperación de Servicios de Tecnología de la Información y Comunicaciones como un proceso continuo de planeación, desarrollo, prueba e implantación de procesos y procedimientos de recuperación en caso de una posible contingencia que pueda presentarse en el SENARA. Estas acciones buscan asegurar la reanudación eficiente y efectiva de los servicios y operaciones de Tecnologías de la Información y Comunicaciones en el menor tiempo e impacto posible.

El Plan de Contingencia Informático y Recuperación de Servicios de Tecnologías de la Información y Comunicaciones cuenta con procesos que en conjunto permiten la gestión, ejecución, pruebas y mantenimiento, esta disgregación permiten una fácil y ágil operación por los responsables autorizados, ante situaciones de desastres.

1. FINALIDAD

Garantizar la continuidad de los servicios de tecnología de información y comunicaciones del Servicio Nacional de Aguas Subterráneas, Riego y Avenamiento (SENARA), 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

Establecer los principios básicos y el marco necesario para garantizar la operatividad de los servicios y/o procesos de tecnologías de la información y comunicaciones de mayor urgencia del SENARA, ante la eventual presencia de siniestros que los pueda paralizar parcial o totalmente y garantizar que se continúen prestando de una manera razonable.

2.2 Objetivos Específicos

- Identificar y analizar los riesgos posibles que pueden afectar las operaciones, procesos y servicios de tecnologías de la información y comunicaciones de la Entidad.

- Definir las actividades de planeamiento, preparación, entrenamiento y ejecución de tareas destinadas a proteger la información contra los daños y perjuicios producidos por corte de servicios, fenómenos naturales o humanos.

- Organizar y disponer al personal técnico debidamente capacitado para afrontar adecuadamente las contingencias que puedan presentarse.

- Establecer actividades que permitan evaluar los resultados y retroalimentación del presente plan.

3. ALCANCE

El Plan de Contingencia Informático y Recuperación de Servicios de Tecnología de la Información y Comunicaciones, incluye los elementos referidos a los sistemas de información, aplicaciones informáticas, bases de datos, equipos e instalaciones tecnológicas, servicios y otros administrados por la Unidad de Gestión Informática (UGI) direccionado a minimizar eventuales riesgos ante situaciones adversas que atentan contra el normal funcionamiento de los servicios informáticos de la entidad.

4. BASE LEGAL

- Directriz No 31681 MICIT, Promoción del Desarrollo Científico y tecnológico.
- Decreto Nº 33147MP, Comisión Intersectorial de Gobierno Digital.
- Políticas y Normas Generales de Tecnología de Información, SENARA.

5. MARCO TEORICO

5.1 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.

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

5.3 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. En el Anexo 1, se detalla la metodología utilizada en el presente plan basada en COBIT 5.

5.4 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.

5.5 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.

5.6 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.

5.7 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.

6. METODOLOGIA

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 cada fase:

6.1 Fase 1: Planificación

6.1.1. Organización

La Unidad de Gestión Informática depende directamente de la Gerencia General y tiene dentro de sus funciones administrar la integridad, confiabilidad, y seguridad de la plataforma institucional, además de diseñar, implantar y mantener la infraestructura tecnológica necesaria para el cumplimiento de los objetivos de la Institución, así como asegurar la disponibilidad y brindar soporte a los mismos.

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.

6.1.2. Roles, funciones y responsabilidades dentro del plan

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 TIC

Está representado por el titular de la Unidad de Gestión Informática 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 del Centro de Datos y Comunicaciones.

- 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 del Centro de Datos y Comunicaciones hayan sido restablecidas.

B. Equipo de seguridad, Redes y Comunicaciones

Es el equipo (funcionarios) de la Unidad de Gestión Informática de SENARA, 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 componentes del Centro de Datos y Comunicaciones.

- Verificar las tareas de copias de respaldo (backup).

- Mantener actualizado el inventario hardware y software utilizado en el Centro de Datos y Comunicaciones 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 y Comunicaciones.

- Elaborar informes técnicos de conformidad, luego de cada mantenimiento efectuado, así como elaborar informes periódicos del funcionamiento del Centro de Datos y Comunicaciones.

- 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.

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

- Llevar un control de versiones de las fuentes de los sistemas de información y portales de la entidad.

- Coordinar y verificar que se realicen las copias de respaldo de las fuentes de las aplicaciones informáticas existentes en un ambiente adecuado.

- Realizar copias de respaldo de las bases de datos de las aplicaciones y sistemas de la entidad.

- Acopiar las copias de respaldo y clasificarlas por tipo de motor de base de datos, aplicaciones y sistemas.

A continuación, se citan las acciones que se realizarán durante la contingencia:

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

- Ejecutar las acciones de emergencia en los equipos informáticos y componentes instalados Centro de Datos y Comunicaciones del SENARA.

- Realizar la evaluación de condiciones de los equipos de comunicaciones y los componentes del Centro de Datos y Comunicaciones del SENARA, durante la emergencia.

- 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.
- 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.
- 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.

A continuación, se citan las acciones de restauración 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 SENARA:

- Iniciar el proceso de recuperación de los servicios de tecnología de la información, realizando las pruebas de funcionamiento en los equipos afectados de la infraestructura informática y los equipos componentes del Centro de Datos y Comunicaciones del SENARA.
- 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 y Comunicaciones del SENARA.
- 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 y los equipos componentes del Centro de Datos y Comunicaciones.
- Coordinar acciones para la verificación de estado de los sistemas de información alojados en los servidores de aplicaciones.
- Verificar el estado de las aplicaciones alojados en los servidores de aplicaciones del SENARA.
- En caso se quiera desplegar y/o reinstalar las aplicaciones informáticas y sistemas de información, de lo contrario verificar que se encuentren funcionando correctamente.
- Elaborar un informe técnico que incluya la evaluación de condiciones de las aplicaciones informáticas y sistemas de información del SENARA.
- Verificar el funcionamiento de las bases de datos institucionales.

- Realizar las pruebas de funcionamiento.
- Elaborar un informe técnico que incluya la evaluación de condiciones de los datos e información del SENARA luego de efectuado el proceso de recuperación.
- Solucionar los problemas de conexión y funcionamiento de los equipos asignados al personal, impresoras, escáner entre otros.
- Elaborar un informe técnico que incluya la evaluación de condiciones de los equipos asignados al personal luego de efectuado el proceso de recuperación.

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	Tiempo de Recuperación (RTO *)
Gestión de redes e infraestructura de TI	Equipos de comunicaciones.	**12 h**
	Equipos de protección eléctrica del Centro de Datos y Comunicaciones (Batería UPS).	**48 h**
	Sistema de aire acondicionado del Centro de Datos y Comunicaciones.	**48 h**
	Infraestructura del Centro de Datos y Comunicaciones.	**72 h**
	Cableado de red de datos.	**24 h**
	Enlaces de cobre y fibra.	**24 h**
	Sistema de almacenamiento (WD storage).	**24 h**
	Servidores de red críticos: Directorio Activo, File Server, Base de Datos.	**96h**
Gestión de sistemas de información y bases de datos	Sistemas de información y portales.	**48 h**
	Base de datos y repositorios utilizados por los sistemas y aplicativos.	**48 h**
Soporte Técnico	Estaciones de trabajo del personal crítico (computadoras personales y portátiles).	**48 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 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 el Centro de Datos y Comunicaciones.	
03	Incendio en el Centro de Datos y Comunicaciones.	
04	Falla en telecomunicaciones.	**Tecnológicos**
05	Delito informático.	
06	Falla de hardware y software.	
07	Falla del suministro eléctrico en el Centro de Datos y Comunicaciones.	**Físico y ambiental**
08	Ausencia o no disponibilidad del personal crítico de TI.	**Humanos**
09	Pandemia y/o Epidemia.	**Ambiental**

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 el Centro de Datos y Comunicaciones	**1**	Puede ocurrir al menos una vez en periodos superiores a cinco años
03	Incendio en el Centro de Datos y Comunicaciones	**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 el Centro de Datos y Comunicaciones	**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

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.

a) Acuerdos de niveles de servicio con proveedor de enlace de comunicación ubicado el Centro de Datos y Comunicaciones.

b) Cámaras de vigilancia en el interior del Centro de Datos y Comunicaciones.

c) Grupo electrógeno para el Centro de Datos y Comunicaciones.

d) Mantenimiento de UPS. El mantenimiento de UPS está a cargo de la Unidad de Gestión Informática.

e) Mantenimiento para equipos de aire acondicionado del Centro de Datos y Comunicaciones.

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

g) Redundancia en los equipos de del Sistema de almacenamiento (WD storage).

h) Respaldo en equipo redundante del servidor de Red LAN.

i) 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.

j) Solución antivirus instalada en los servidores de red y computadoras.

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

l) Respaldo de equipos de comunicaciones (router, switch, access point).

m) Esquema MESH de interconexión de Access Point.

n) 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 el Centro de Datos y Comunicaciones y equipos portátiles de usuario.	5
2	Cámaras de vigilancia en el interior del Centro de Datos y Comunicaciones.	4
3	Grupo electrógeno para el Centro de Datos y Comunicaciones.	4
4	Mantenimiento de UPS. El mantenimiento de UPS está a cargo de la Unidad de Gestión Informática.	3
5	Mantenimiento para equipos de aire acondicionado del Centro de Datos y Comunicaciones.	4
6	Redundancia en los enlaces de comunicaciones (fibra óptica para ERP) con el mismo proveedor	4
7	Redundancia de equipos de aire acondicionado en la Oficina de Gestión Informática	4
8	Redundancia en los equipos de del Sistema de almacenamiento (WD storage).	4
9	Respaldo en equipo redundante del servidor de Red LAN.	4
10	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
11	Solución antivirus instalada en los servidores de red y computadoras.	5
12	Solución de protección de portales y aplicaciones web publicadas en internet a través de solución en la nube.	5
13	Respaldo de equipos de comunicaciones (router, switch, access point).	4
14	Esquema MESH de interconexión de Access Point.	4

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 a la aplicación de la metodología de riesgos descrita en los anexos del 1 al 5, se obtuvo el siguiente resultado:

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

MAPA DE CALOR										
N°	Recursos Críticos / Amenazas (Eventos)	Terremoto	Inundación y aniego en el Centro de Datos y Comunicaciones	Incendio en el Centro de Datos y Comunicaciones	Falla en telecomunicaciones	Delito informático	Falla de hardware y software	Falla del suministro eléctrico en el Centro de Datos y Comunicaciones	Ausencia o no disponibilidad del personal crítico de TI	Pandemia y/o Epidemia
1	Equipos de comunicaciones.	Alto	Bajo	Bajo	Moderado	Alto	Alto	Alto	Bajo	Bajo
2	Equipos de protección eléctrica del Centro de Datos y Comunicaciones(UPS)	Alto	Bajo	Bajo	Bajo	Bajo	Moderado	Alto	Bajo	Bajo
3	Aire acondicionado de precisión del Centro de Datos	Moderado	Bajo	Bajo	Bajo	Bajo	Bajo	Moderado	Bajo	Bajo
4	Infraestructura del Centro de Datos y Comunicaciones	Alto	Bajo	Bajo	Bajo	Moderado	Moderado	Bajo	Bajo	Bajo
5	Cableado de red de datos.	Alto	Bajo	Bajo	Bajo	Bajo	Bajo	Bajo	Bajo	Bajo
6	Enlaces de cobre y fibra óptica para interconexión entre proveedor y el Centro de Datos y Comunicaciones	Alto	Bajo	Bajo	Bajo	Bajo	Moderado	Bajo	Bajo	Bajo
7	Sistema de almacenamiento (WD storage)	Moderado	Bajo	Bajo	Bajo	Moderado	Alto	Moderado	Bajo	Bajo
8	Servidores de red	Medio	Bajo	Bajo	Bajo	Alto	Alto	Moderado	Bajo	Bajo
9	Medios de respaldo internos	Medio	Bajo	Bajo	Bajo	Alto	Alto	Bajo	Bajo	Bajo
10	Sistemas de información y portales web	Bajo	Bajo	Bajo	Bajo	Bajo	Bajo	Bajo	Bajo	Bajo
11	Base de datos utilizados por los sistemas operativos	Moderado	Bajo	Bajo	Bajo	Bajo	Alto	Bajo	Bajo	Bajo
12	Estaciones de trabajo del personal crítico	Alto	Bajo	Bajo	Bajo	Alto	Alto	Moderado	Bajo	Bajo
13	Personal crítico responsable de los procesos de TIC.	Bajo	Bajo	Bajo	Bajo	Alto	Bajo	Bajo	Bajo	Bajo

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 el Centro de Datos y Comunicaciones	Incendio en el Centro de Datos y Comunicaciones	Falla en telecomunicaciones	Delito informático	Falla de hardware y software	Falla del suministro eléctrico en el Centro de Datos y Comunicaciones	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	Equipos de protección eléctrica del Centro de Datos y Comunicaciones(UPS)	Medio	Bajo	Bajo	Bajo	Bajo	Moderado	Medio	Bajo	Bajo
3	Aire acondicionado de precisión del Centro de Datos.	Moderado	Bajo	Bajo	Bajo	Bajo	Bajo	Bajo	Bajo	Bajo
4	Infraestructura del Centro de Datos y Comunicaciones.	Medio	Bajo	Bajo	Bajo	Moderado	Moderado	Bajo	Bajo	Bajo
5	Cableado de red de datos.	Alto	Bajo	Bajo	Bajo	Bajo	Bajo	Bajo	Bajo	Bajo
6	Enlaces de cobre y fibra óptica para interconexión entre proveedor y el Centro de Datos y Comunicaciones.	Alto	Bajo	Bajo	Bajo	Bajo	Moderado	Bajo	Bajo	Bajo
7	Sistema de almacenamiento (WD storage).	Moderado	Bajo	Bajo	Bajo	Moderado	Moderado	Bajo	Bajo	Bajo
8	Servidores de red.	Medio	Bajo	Bajo	Bajo	Medio	Medio	Moderado	Bajo	Bajo
9	Medios de respaldo internos.	Medio	Bajo	Bajo	Bajo	Medio	Medio	Bajo	Bajo	Bajo
10	Sistemas de información y portales web.	Bajo	Bajo	Bajo	Bajo	Bajo	Bajo	Bajo	Bajo	Bajo
11	Base de datos utilizados por los sistemas operativos.	Moderado	Bajo	Bajo	Bajo	Moderado	Bajo	Bajo	Bajo	Bajo
12	Estaciones de trabajo del personal crítico (computadoras personales y portátiles)	Alto	Bajo	Bajo	Bajo	Medio	Bajo	Moderado	Bajo	Bajo
13	Personal crítico responsable de los procesos de TIC.	Bajo	Bajo	Bajo	Bajo	Moderado	Bajo	Bajo	Bajo	Bajo

6.2.5. Escenarios de riesgo

- Destrucción e indisponibilidad del Centro de Datos y Comunicaciones por terremoto.
- Falla en el funcionamiento de los sistemas de información y portales web por delito informático (ataque cibernético, virus, etc.).
- Indisponibilidad de los servidores de red por falla de hardware y software.
- Interrupción de comunicaciones por fallas en el suministro eléctrico del Centro de Datos y Comunicaciones.
- Datos y Comunicaciones.

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

Tabla N° 7 - Escenarios de Riesgos

Escenario de Riesgo	Descripción	Impacto
Destrucción e indisponibilidad del Centro de Datos y Comunicaciones	Este escenario consiste en que el Centro de Datos y Comunicaciones deje de funcionar o se destruya, como resultado de un terremoto o incendio, lo cual podría ocasionar caídas de servicios y destrucción de los equipos informáticos alojados en el Centro de Datos y	**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**
Indisponibilidad de los servidores de red por falla de 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.	**Medio**
Interrupción de comunicaciones por fallas en el suministro eléctrico del Centro de Datos y Comunicaciones.	Este escenario consiste en el corte o interrupción de las comunicaciones entre el Centro de Datos y Comunicaciones 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.	**Moderado**

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)

- Gestión de copias de respaldo (Backup) de la información almacenada y procesada en el Centro de Datos y Comunicaciones, de acuerdo a lo establecido en las Políticas relativas a bases de datos, apartado N°4 y Políticas relativas a la seguridad, apartado N°9 del Manual de Políticas de Tecnologías de Información considerando la criticidad de los datos, así como los criterios de identificación de los medios, la frecuencia de rotación y transporte al sitio externo.

- Realización de copias de instaladores de las aplicaciones, de software base, sistema operativo, utilitarios, etc.

- Verificar la ejecución periódica de las tareas programadas de respaldo de información y comprobación de los medios de respaldo.

b) 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.

- Si es necesario, adquirir o habilitar hardware y software; las estrategias básicas para disponer de equipo de reemplazo serán:

  - **Acuerdos con proveedores:** Establecer acuerdos de nivel de servicios con los proveedores de software, hardware y medios de soporte; se debe especificar el tiempo de respuesta requerido.

  - **Equipos de respaldo:** Los equipos requeridos se compran o alquilan y se almacenan en una instalación segura (*)**.**

(*) Comprar los equipos cuando se necesitan puede ser mejor financieramente, pero puede incrementar de manera significativa el tiempo de recuperación. Asimismo, almacenar un equipo sin ser usado es costoso, pero permite que la recuperación comience más rápidamente.

c) Entrenamiento y personal de reemplazo

- Todo el personal de la Unidad de Gestión Informática, 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 la Unidad de Gestión Informática.

d) Renovación tecnológica

- Programación de dos revisiones anuales 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 contingencia.

e) 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.

- Activación del desvío de las llamadas telefónicas a los usuarios asignados encarados de la atención de la central telefónica.

- Verificación de los accesos seguros de los proveedores a cualquier elemento de la plataforma e infraestructura de servicios TICs, a cargo de la Unidad de Gestión Informática en el Centro de Datos y Comunicaciones.

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 SENARA 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:

a) Acciones durante la contingencia

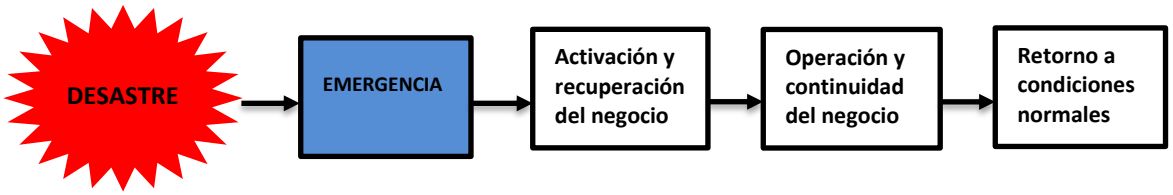
- Estudiar y evaluar el alcance del desastre en cada área de responsabilidad.
- Notificar y reunir a los integrantes de la Unidad de Gestión Informática.
- Informar al Coordinador de Continuidad de TIC sobre la situación presentada, para decidir la realización de la Declaración de Contingencia.
- Determinar 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 SENARA para estabilizar la infraestructura tecnológica luego del evento suscitado. Para lo cual se definen las pautas que permitan al personal de la Unidad de Gestión Informática 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:

Figura N° 1 - Ciclo de la estrategia de recuperación de TI



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

Tabla N° 8 - 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), Servidores de bases de datos de red LAN, 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: Intranet, 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.

Acciones después de la contingencia:

- Evaluar el trabajo de los funcionarios encargados durante el proceso de recuperación.
- Evaluar la efectividad del Plan de Contingencia.

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°7-, los cuales serán abordados en formatos independientes, tal como se indica en el siguiente cuadro:

Tabla N° 9 - 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 el Centro de Datos y Comunicaciones	Alto	FPC - 04

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 N° 05.

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 Oficial de Seguridad de la Información, realiza 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:

- Realizar mantenimiento de la documentación técnica de operación de los servicios de TI.
- Revisión continúa de las aplicaciones, sistemas de información y portales web.
- Revisión continúa del sistema de copias de respaldo (backups).
- Revisión y mantenimiento de los sistemas de soporte eléctrico del Centro de Datos y Comunicaciones.

7. 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 del Centro de Datos y Comunicaciones 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 1

METODOLOGÍA APLICADA A LA GESTIÓN DE RIESGOS

1. Cálculo de la Probabilidad de Ocurrencia 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 utilizara la escala indicada en la Tabla N°8 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.

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 "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.	

3. 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.	

4. 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

5. 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.

6. 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 utilizara 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**

ANEXO 2

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	Servidor de red LAN – Primary Domain - Windows Server 2008 R2	Es un sistema operativo comercial para servidores desarrollado por Microsoft. Está basado en tecnología NT y su versión del núcleo NT es la 6.0. Administra y gestiona las operaciones de la Red LAN en esquema Domain Server (Dominio de Servidor).	Unidad de Gestión Informática	MS Windows SQL	Cliente /Servidor	**1**
2	Servidor de red LAN – BackUp Domain - Windows Server 2008 R2	Es un sistema operativo comercial para servidores desarrollado por Microsoft. Está basado en tecnología NT y su versión del núcleo NT es la 6.0. Funcionar como respaldo del equipo Primary Domain de la red LAN esquema Domain Server (Dominio de Servidor).	Unidad de Gestión Informática	MS Windows SQL	Cliente /Servidor	**1**
3	WatchGuard Dimension	Es una solución de visibilidad y administración virtual que puede utilizar para capturar los datos de registro de sus Firebox, FireCluster y servidores WatchGuard, así como gestionar sus Firebox y FireCluste.	Unidad de Gestión Informática	Data Base Management System - Progress	Cliente /Servidor	**1**
4	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	Cliente /Servidor	**1**
4	Sistema Integrado de administración Financiera (SIA) - Consulta	Es un sistema de administración financiera utilizado como consulta para datos de periodo 2000 al 2020.	Unidades y Áreas	ORACLE 8	Cliente /Servidor	**1**

ANEXO 3

LISTADO DE EQUIPOS DEL CENTRO DE DATOS Y COMUNICACIONESY COMUNICACIÓN CLASIFICADOS POR PRIORIDAD DE ATENCIÓN PARA LA RECUPERACIÓN DE TIC

N°	Tipo de equipo	Rol	Descripción Prioridad	Prioridad
1	Equipo de almacenamiento	Almacenamiento	Equipo de almacenamiento de información de usuarios, donde se almacena las carpetas de datos de usuarios y se replican en equipo redundante. Y almacenamiento de copias de sistemas de Servidores de Red LAN.	**1**
2	Servidor	Controlador de Dominio	Servidor de dominio de red. (Directorio Activo, DNS).	**1**
3	Servidor	Backup	Servidor donde se encuentra instalado el software de respaldo, para respaldo y restauración de información.	**1**
4	Servidor	Aplicaciones	Servidor para publicación de portales web mediante agente de publicación.	**2**
5	Servidor	Aplicaciones	Servidor virtual de control de detección de violaciones a la seguridad, el robo de datos y los ciberataques	**2**
6	Switch	Comunicaciones	Switches Core, swicthes de acceso y DMZ.	**1**
7	UPS	Energía	Equipo de suministro eléctrico para servidores y equipos	**1**
8	Aire acondicionado	Acondicionamiento	Aire acondicionado de precisión para el Centro de Datos y Comunicaciones.	**1**
9	Switch	Telefonía	Switch controlador de telefonía IP.	**1**
10	Router –RACSA	Internet-ERP	Redundancia en los enlaces de comunicaciones (fibra óptica para ERP) con RACSA.	**1**
11	Router-ICE	Internet	Enlace de comunicaciones INPUT/OUTPUT SENARA-ICE.	**1**

ANEXO 4

FORMATOS DEL PLAN DE CONTINGENCIA INFORMÁTICO Y RESTAURACIÓN DE SERVICIOS DE TIC

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 del Centro de Datos y Comunicaciones, 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.

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 para el Centro de Datos y Comunicaciones.
- 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 y Comunicaciones.
- Mantener actualizado el inventario hardware y software utilizado en el Centro de Datos y Comunicaciones de la entidad.
- Llevar un control de versiones de las fuentes de los sistemas de información.

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 Unidades.
- Mantenimiento del orden y limpieza de los ambientes de la Oficinas Centrales y Centro de Datos y Comunicaciones.
- 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, Redes y Comunicaciones.

e) Descripción de las actividades después de activar la contingencia

- Desconectar el fluido eléctrico y cerrar las llaves de gas u otros líquidos inflamables si corresponde.

- Evacuar las oficinas de acuerdo a las disposiciones de los Brigadistas de Evacuación, utilizando las rutas establecidas durante los simulacros. Considerar las escaleras de emergencia, señalización de rutas, zonas de agrupamiento del personal, etc. Por ningún motivo utilizar los ascensores.

- Verificar que todo el personal del 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 los mismos.
- 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, Redes 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, Redes 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, Redes 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.

SENARA	Evento: Delito Informático	FPC - 02

1. 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

- Servidores
- Estaciones de Trabajo

Software

- Software Base
- Sistemas de información, aplicativos y portales del SENARA

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 y Comunicaciones en Oficinas Centrales del SENARA.

d) Personal Encargado

El Equipo de seguridad, Redes y Comunicaciones, 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.

- 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 Equipo de seguridad, Redes y Comunicaciones, 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.
- 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 Coordinador de Continuidad de TIC puede activar la contingencia.

g) Personal Encargado

Equipo de seguridad, Redes y Comunicaciones.

d) Descripción de las actividades después de activar la contingencia

- Desconectar o retirar de la red de datos del SENARA, 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.

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 servidores de red. Esperar la indicación del Equipo de seguridad, Redes y Comunicaciones para reanudar el trabajo.

3. PLAN DE RECUPERACIÓN

a) Personal Encargado

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

b) Descripción de actividades

Se informará 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 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 EL SENARA.
- 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 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 ell 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 servidor de red, en base al informe que describe los problemas presentados, se determinarán las acciones de prevención a tomar.

SENARA	Evento: Falla de hardware y software	FPC-03

1. PLAN DE PREVENCIÓN

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 SENARA 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 SENARA.

d) Personal Encargado

Equipo de seguridad, Redes y Comunicaciones.

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, jboss, wildfly.

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 y Comunicaciones.

- Mantener actualizado el inventario hardware y software utilizado en el Centro de Datos y Comunicaciones del SENARA.

- Realizar monitoreo del funcionamiento de los servidores instalados en el Centro de Datos y Comunicaciones 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 Coordinador 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.

e) Duración

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

3. PLAN DE RECUPERACIÓN

a) Personal Encargado

El Equipo de seguridad, Redes y Comunicaciones, luego de validar la corrección del problema de acceso a los servidores, y el Coordinador 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 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, Redes 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, Redes y Comunicaciones, quienes identifican 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 personal encargado deberá iniciar las labores de actualización de los procedimientos o guías de recuperación de servidores.

SENARA	Evento: : Falla del suministro eléctrico en el Centro de Datos y Comunicación	FPC-04

1. PLAN DE PREVENCIÓN

a) Descripción del evento

Falla general del suministro de energía eléctrica en el Centro de Datos y Comunicaciones de la entidad.

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

- 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

Este evento puede darse en las Oficinas Centrales donde se ubica el Centro de Datos y Comunicaciones, por tener los equipos de comunicación que brinda servicios informáticos a los usuarios a nivel interno y externo.

d) Personal Encargado

Equipo de seguridad, Redes y Comunicaciones, es el responsable de realizar las coordinaciones para restablecer el suministro de energía eléctrica.

e) Condiciones de Prevención de Riesgo

- Durante las operaciones diarias del servicio u operaciones del SENARA se contará con los UPS necesarios para asegurar el suministro eléctrico en los equipos consideradas como críticos.

- Equipos UPS cuentan con mantenimiento preventivo y con suficiente energía para soportar una operación continua de 30 minutos como mínimo. El tiempo variará de acuerdo a la función que cumplan los equipos UPS.

- Realización de pruebas periódicas de los equipos UPS para asegurar su correcto funcionamiento.

- 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.

- Disponibilidad de UPS para proteger los equipos de vigilancia (cámaras, sistemas de grabación) y de control de acceso a las instalaciones del SENARA puertas, contactos magnéticos, etc.)

- Coordinar la verificación del cableado eléctrico de Oficinas Centrales, una vez por año.

- Coordinar la instalación de luces de emergencia con tolerancia de 15 minutos, accionados automáticamente al producirse el corte de fluido eléctrico, los cuales deben estar instalados en los ambientes críticos.

f) Acciones del Equipo de seguridad, Redes y Comunicaciones

- Revisar periódicamente y de forma conjunta con la Unidad de Servicios Administrativos las instalaciones eléctricas del Centro de Datos y Comunicaciones de la entidad.

- Coordinar y supervisar el mantenimiento preventivo de cableado a tierra, aire acondicionado de precisión del Centro de Datos y Comunicaciones y UPS, trimestralmente.

- Verificar que la red eléctrica utilizada en el Centro de Datos y Comunicaciones y la red de cómputo 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 el Centro de Datos y Comunicaciones del SENARA.

2. 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 el/la Director/a de la unidad o área el problema presentado.
- Comunicar a la empresa 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 el caso de los equipos que entren en funcionamiento automático con UPS´s, se deberá monitorear el tiempo de autonomía del equipo y no exceder el indicado anteriormente.

En caso de que la interrupción de energía en el Centro de Datos y Comunicaciones sea mayor a dos (2) horas, se deberán apagar los equipos en forma ordenada mientras funcione el UPS y hasta que regrese el fluido eléctrico.

3. PLAN DE RECUPERACIÓN

a) Personal Encargado

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

c) Mecanismos de Comprobación

El Equipo de seguridad, Redes 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 CERTIFICACION DE LAS PRUEBAS

CONTROL Y CERTIFICACIÓN DE PRUEBAS DE CONTINGENCIA

PRUEBA N° _____

Escenario de Prueba: (Descripción del escenario a probar/certificar)

Área Responsable: (Área responsable del escenario de prueba a probar/certificar)

INFORMACION DEL PROCESO

Metodología: (Detallar lo que se va a hacer en la prueba)

Alcance: (Definir hasta donde va a abarcar)

Condiciones de Ejecución

Equipo: Nombre Servidor/PC de prueba

Aplicación/Software: _____

Ubicación: Lugar de prueba

Fecha de Backup: / /

RESULTADO DE LA PRUEBA

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

Observaciones: (En el caso de haber observaciones o que la prueba haya sido deficiente, se indicarán los motivos, y resultados

ACTUALIZACION EN EL PLAN DE CONTINGENCIA

Cambios o actualizaciones en el Plan de Contingencia: (Se indicarán los cambios que se deben realizar al Plan de Contingencia como consecuencia de las observaciones detectadas en las pruebas correspondientes)

ACTUALIZACION PARTICIPANTES

Participante	Cargo	Firma