



SERVICIO NACIONAL DE CERTIFICACIÓN AMBIENTAL  
PARA LAS INVERSIONES SOSTENIBLES

# PLAN DE CONTINGENCIA PARA LA PRODUCCIÓN DE MICROFORMAS DIGITALES EN EL SENACE



## ÍNDICE

1. OBJETO
2. ALCANCE
3. BASE NORMATIVA
4. RESPONSABILIDAD
5. DEFINICIONES
6. ABREVIATURAS
7. DESCRIPCIÓN
  - 7.1 Plan de reducción de riesgos
    - 7.1.1 Análisis de riesgos
      - 7.1.1.1 Riesgos por intervención humana
        - 7.1.1.1.1 Acceso no autorizado
        - 7.1.1.1.2 Error humano
        - 7.1.1.1.3 Robo
        - 7.1.1.1.4 Vandalismo
      - 7.1.1.2 Riesgos tecnológicos
        - 7.1.1.2.1 Falla técnica
      - 7.1.1.3 Riesgos por siniestro
        - 7.1.1.3.1 Sismo
        - 7.1.1.3.2 Fuego
        - 7.1.1.3.3 Inundación
    - 7.1.2 Medidas para reducir los riesgos
      - 7.1.2.1 Para reducir los riesgos en general
      - 7.1.2.2 Para reducir los riesgos por intervención humana
      - 7.1.2.3 Para reducir los riesgos tecnológicos
      - 7.1.2.4 Para reducir los riesgos por siniestro
    - 7.1.3 Estrategias
  - 7.2 Plan de recuperación de una situación de contingencia
    - 7.2.1 Actividades previas a la situación de contingencia
      - 7.2.1.1 Plan de acción
      - 7.2.1.2 Formación de equipo operativo
      - 7.2.1.3 Formación de equipo de evaluación
    - 7.2.2 Actividades durante a la situación de contingencia
      - 7.2.2.1 Plan de emergencias
      - 7.2.2.2 Formación de equipo para afrontar la emergencia
      - 7.2.2.3 Entrenamiento
      - 7.2.2.4 Acciones específicas para contingencias en caso de fallas tecnológicas
    - 7.2.3 Actividades posteriores a la situación de contingencia
      - 7.2.3.1 Informe
      - 7.2.3.2 Caso en que haya habido evacuación o daño de las microformas
      - 7.2.3.3 Caso en que haya habido daño a la infraestructura de la línea de producción
      - 7.2.3.4 Priorización de actividades del Plan de Acción
      - 7.2.3.5 Ejecución de actividades
      - 7.2.3.6 Evaluación de resultados
      - 7.2.3.7 Retroalimentación del Plan de Acción
8. DIAGRAMA DE FLUJO
9. CAMBIOS A LA VERSIÓN ANTERIOR

## 1. OBJETO

Describir de forma concreta las acciones, tareas, responsables, plazos y controles, entre otros elementos, para la implementación del plan de contingencia para la producción de microformas digitales en el Sistema de Producción de Microformas Digitales - SPMD del Servicio Nacional de Certificación Ambiental para las Inversiones Sostenibles - Senace.

## 2. ALCANCE

Lo dispuesto en el presente documento es de obligatorio cumplimiento para la Oficina de Atención a la Ciudadanía y Gestión Documentaria - OAC y demás órganos y/o unidades orgánicas del Senace involucrados en la evaluación del SPMD, incluyendo a los evaluadores.

## 3. BASE NORMATIVA

- 3.1 Decreto Legislativo N° 681, que legisla sobre el uso de tecnologías de avanzada en materia de archivo.
- 3.2 Resolución Directoral N° 016-2015-INACAL/DN, que aprueba la Norma Técnica Peruana NTP 392.030-2:2015 Microformas. Requisitos para las organizaciones que administran sistemas de producción y almacenamiento. Parte 2: Medios de archivo electrónico.

En lo no previsto por el presente documento se aplica lo establecido en los documentos normativos internos que Senace aplique para regular la evaluación de sus procesos y de sus aspectos tecnológicos en general.

## 4. RESPONSABILIDAD

- 4.1 La OAC es responsable de velar por el cumplimiento de lo dispuesto en el presente documento.
- 4.2 El Supervisor de la Línea de Producción de Microforma es responsable de gestionar para la implementación del presente documento.
- 4.3 Los órganos del Senace involucrados son responsables de cumplir lo dispuesto en el presente documento.

## 5. DEFINICIONES

- 5.1 **Comité de Evaluación de Documentos:** Comité conformado en aplicación de la legislación archivística, responsable de asesorar legal y técnicamente sobre el funcionamiento del sistema de producción de microformas y de designar a las personas que ejecutan la evaluación del SPMD y la auditoría informática, según lo establece el Manual del Sistema de Producción de Microformas Digitales.
- 5.2 **Contingencia:** Situación en que se suspende o inhabilita la operatividad del sistema. Por sus características y consecuencias, impide el normal desarrollo de las actividades durante un plazo estimado como no aceptable para los objetivos de disponibilidad del servicio.
- 5.3 **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Efecto de la incertidumbre en los objetivos.

- 5.4 **Supervisor:** El responsable de la administración del sistema de producción de microformas, según lo establece el Manual del Sistema de Producción de Microformas Digitales.

## 6. ABREVIATURAS

CED:	Comité de Evaluación de Documentos del Senace.
NTP:	Norma Técnica Peruana.
OAC:	Oficina de Atención a la Ciudadanía y Gestión Documentaria.
Senace:	Servicio Nacional de Certificación Ambiental para las Inversiones Sostenibles.
SPMD:	Sistema de Producción de Microformas Digitales.

## 7. DESCRIPCIÓN

La elaboración del plan de contingencia se ha realizado considerando la planificación, identificación de riesgos, identificación de soluciones y la determinación de la estrategia a adoptar.

### 7.1 Plan de Reducción de Riesgos

Ante la necesidad de disponibilidad continua de los recursos para la línea de producción de microformas digitales y para asegurar la continuidad del negocio, se cuenta con un Plan de Reducción de Riesgos que contempla el análisis y mitigación de los mismos.

#### 7.1.1 Análisis de riesgos

El entorno en que se presentan los riesgos es el local donde funciona la línea de producción de microformas digitales del Senace, situado en Av. Ernesto Diez Canseco N° 351, distrito de Miraflores, ciudad de Lima.

El objetivo del análisis de cada riesgo es establecer las acciones que se ejecutarán ante la correspondiente situación de contingencia, con el fin de minimizar el tiempo de interrupción de las operaciones del SPMD, sin exponer la seguridad de las personas.

Atendiendo a la naturaleza del servicio de la línea de producción y a las particularidades que presenta su implementación en los ambientes de la entidad, se han identificado diversos riesgos y se ha estimado la probabilidad de que originen un incidente de seguridad con determinado impacto, asignándosele un factor de riesgo. Al efecto se usa una escala de 5 niveles que funciona de la siguiente manera:

Amenaza	Probabilidad (1 a 5)	Impacto (1 a 5)	Medición del riesgo	Factor de riesgo (1 a 25)
AAA	3	5	3x5=15	Medio
BBB	1	4	1x4=4	Muy bajo
CCC	4	2	4x2=8	Bajo

Donde el factor de riesgo sigue la siguiente escala:

Muy bajo	1 a 5
Bajo	6 a 10

Medio	11 a 15
Alto	16 a 20
Muy alto	21 a 25

La descripción de los riesgos identificados se aborda a continuación.

#### 7.1.1.1 Riesgos por intervención humana

##### a) Acceso no autorizado

- Probabilidad: 2, considerando la ubicación en el segundo piso del inmueble, el acceso al área de la línea de producción de microformas, mediante cerradura biométrica, los controles de ingreso y la vigilancia externa e interna (vigilantes, recepcionista, cámaras de seguridad).
- Impacto: 4, considerando que los equipos de cómputo o los documentos en papel pueden contener información protegida por la legislación de protección de datos personales.
- Factor de riesgo:  $2 \times 4 = 8$  (bajo).

##### b) Error humano

- Probabilidad: 1, considerando que el personal responsable directo de la operación de la línea de producción de microformas consiste en varias personas debidamente capacitadas que incluyen controladores de calidad y que las aplicaciones informáticas están instaladas en servidores de aplicaciones de acceso controlado.
- Impacto: 2, considerando que los eventuales errores son relativamente fáciles de detectar y corregir revisando los registros de actividad.
- Factor de riesgo:  $1 \times 2 = 2$  (muy bajo).

##### c) Robo

- Probabilidad: 1, considerando las barreras físicas y vigilancia existentes (vigilante, recepcionista, cámaras de seguridad).
- Impacto: 5, considerando que la desaparición de un equipo informático puede implicar la pérdida de las microformas que contiene.
- Factor de riesgo:  $1 \times 5 = 5$  (muy bajo).

##### d) Vandalismo

- Probabilidad: 1, considerando las barreras físicas y vigilancia existentes.
- Impacto: 5, considerando que la destrucción de un equipo informático implica la pérdida de las microformas que contiene.
- Factor de riesgo:  $1 \times 5 = 5$  (muy bajo).

#### 7.1.1.2 Riesgos tecnológicos

- a) Falla técnica
- Probabilidad: 3, considerando que los equipos informáticos (servidores, terminales, escáneres, impresoras y equipos de conmutación de red, etc.) pueden tener fallas de fábrica y tienen una vida útil limitada.
  - Impacto: 5, considerando que el daño a un equipo informático puede volver irrecuperables la información y documentos contenidos en él.
  - Factor de riesgo:  $3 \times 5 = 15$  (medio).

### 7.1.1.3 Riesgos por siniestro

- a) Sismo
- Probabilidad: 4, considerando que Lima es zona sísmica.
  - Impacto: 2, considerando que la construcción cumple estándares de resistencia sísmica.
  - Factor de riesgo:  $4 \times 2 = 8$  (bajo).
- b) Fuego
- Probabilidad: 2, considerando que la línea de producción de microformas está destinada a digitalizar cantidades significativas de documentos en papel.
  - Impacto: 3, considerando que la habitación de la línea de producción y de las oficinas contiguas poseen alguna infraestructura combustible.
  - Factor de riesgo:  $2 \times 3 = 6$  (bajo).
- c) Inundación
- Probabilidad: 1, considerando que no hay fuentes cercanas de agua y la ubicación de la línea de producción en el segundo piso del inmueble.
  - Impacto: 2, considerando que no hay desniveles que permitan que el agua se empoce y que los equipos informáticos están elevados sobre el piso.
  - Factor de riesgo:  $1 \times 2 = 2$  (muy bajo).

A modo de resumen, tenemos el siguiente resultado de la evaluación de riesgos:

Riesgo	Factor de riesgo
Falla técnica	Medio
Acceso no autorizado	Bajo
Fuego	Bajo
Sismo	Bajo
Robo	Muy bajo
Vandalismo	Muy bajo
Error humano	Muy bajo
Inundación	Muy bajo

## 7.1.2 Medidas para reducir los riesgos

Con el fin de reducir los riesgos identificados, el Supervisor toma las medidas que se indican a continuación:

### 7.1.2.1 Para reducir los riesgos en general:

- Se realizan copias de respaldo (backups) con regularidad.
- Se mantienen despejadas las vías de evacuación.
- Se mantienen en buen estado las señalizaciones de salida.
- Se gestiona la evaluación al menos anualmente del funcionamiento de la línea de producción de microformas digitales, según lo establecido en el correspondiente manual del SPAMD.

### 7.1.2.2 Para reducir los riesgos por intervención humana:

- Se realizan capacitaciones de inducción y evaluaciones del personal operario de manera constante en lo que se refiere a conocimiento del software aplicativo, uso de sistemas operativos y aplicaciones de oficina que se requieran para el manejo de la línea de producción. Asimismo, se capacita y evalúa a todo el personal involucrado en lo referente a acciones a tomar en caso de robos y/o vandalismo.
- Se realizan capacitaciones programadas periódicas de manera anual y/o cada vez que se implementen modificaciones al sistema, tomando en cuenta puntos de actualización de hardware, software y repaso de medidas de seguridad física.

### 7.1.2.3 Para reducir los riesgos tecnológicos:

- Se realiza mantenimiento del hardware y software según las recomendaciones de los fabricantes.
- Se evalúa anualmente la necesidad de actualización tecnológica.
- Se revisa a diario el buen estado de las instalaciones eléctricas.

### 7.1.2.4 Para reducir los riesgos por siniestro:

- Se mantienen operativos y en buen estado las instalaciones eléctricas y el equipamiento contra incendio (extintor, sensores de humo, alarma).
- Se realizan rondas por el personal de vigilancia.
- Se reciben inspecciones periódicas por parte de la autoridad competente en defensa civil para la revisión de instalaciones y procedimientos en caso de siniestros.

## 7.1.3 Estrategias

La estrategia aplicada para el presente plan de contingencia es contar con lo siguiente:

- Plan de reducción de riesgos y plan de recuperación de una situación de contingencia, desarrollados en el presente documento.
- Se propone una organización para la gestión del Plan de Contingencia, el mismo que está desarrollado en el presente documento (formación de equipos, según se describe en la sección Plan de Recuperación de una situación de contingencia).
- Tener desarrolladas y documentadas las principales situaciones de contingencia susceptibles planteadas en el presente Plan de Contingencia (se tratan en la sección Plan de Reducción de Riesgos).

## **7.2 Plan de recuperación de una situación de contingencia**

Con el fin de poder afrontar una situación de contingencia, se contemplan actividades previas, durante y después de la misma.

### **7.2.1 Actividades previas a la situación de contingencia**

#### 7.2.1.1 Plan de acción

- Se mantiene un inventario actualizado de los equipos informáticos.
- Se mantiene control adecuado de la ubicación de las copias de respaldo de la información y del software.
- Se ejecutan las medidas para reducir riesgos descritas en el numeral 9.1

#### 7.2.1.2 Formación de equipo operativo

El Jefe de la OAC y el Supervisor son responsables de la seguridad de la información en la línea de producción. En tal sentido:

- Velan por el cumplimiento del plan de contingencia.
- Solicitan y coordinan el soporte técnico para los equipos, hardware y software correspondientes.
- Participan en las pruebas y simulacros de desastres.

#### 7.2.1.3 Formación de equipo de evaluación

De conformidad con lo establecido en el manual del SPMD, se realiza al menos una evaluación anual a cargo de un evaluador que no pertenece a dicho sistema y que es designado por el CED. Su evaluación incluye los aspectos pertinentes de seguridad de la información.

### **7.2.2 Actividades durante la situación de contingencia**

#### 7.2.2.1. Plan de emergencias

- Una vez detectada la emergencia, quien se percate de ella dará aviso inmediato a las siguientes personas, observando la siguiente prioridad en la medida de lo posible:
  - a) La persona que tenga acceso a las llaves del ambiente de la línea de producción.
  - b) Los contactos de emergencia (bomberos, policía, Defensa Civil, etc.).
  - c) Los miembros del comité de emergencia o de otros grupos o responsables que la entidad hubiese designado para casos de emergencias en general.
  - d) El Supervisor.
  - e) El Jefe de la OAC.
  - f) El Gerente General.
  - g) El depositario de la fe pública.
  
- Asimismo, en caso de riesgo de incendio el Supervisor dispondrá que se corte inmediatamente el suministro de electricidad y se desconecte los aparatos eléctricos.
  
- En caso se haga necesaria la evacuación de las microformas que temporalmente se encuentren en el ambiente de la línea de producción y no en un microarchivo se realizará lo siguiente:
  - a) El Supervisor autoriza la evacuación de las microformas. De no ser posible comunicarse con él, la decisión corresponde a la persona que tenga acceso a las llaves del mueble de custodia temporal.
  - b) Esta última persona se hará cargo de la evacuación de los soportes que contienen las microformas. Todo el personal está obligado a colaborar con ella.
  - c) Durante la evacuación de los soportes:
    - i. Se les manipulará cuidadosamente para impedir que sufran cualquier daño.
    - ii. Se guardarán en recipientes idóneos sobre los cuales se ejercerá vigilancia constante.
    - iii. Se trasladarán a un lugar seguro.
    - iv. En la medida en que las circunstancias lo permitan, se registrará la cantidad de soportes y sus datos esenciales de identificación.
  
- Para asegurar la continuidad de la producción, el Supervisor dispone la recuperación de la información a partir de las copias de respaldo.

#### 7.2.2.2. Formación de equipo para afrontar la emergencia:

- El Jefe de la OAC y el Supervisor conforman el equipo para afrontar de inmediato la emergencia.

#### 7.2.2.3. Entrenamiento

- El Jefe de la OAC y el Supervisor participan en los programas de prácticas periódicas dispuestos por la entidad para afrontar los diferentes tipos de siniestros.

#### 7.2.2.4. Acciones específicas para contingencias en caso de fallas tecnológicas

- Escenario 1: Corrupción del sistema operativo en el servidor.
  - Acción a tomar: Reparación del sistema operativo en un tiempo máximo de 60 minutos. En caso no se solucione el problema se recurre al uso de un servidor de contingencia.
- Escenario 2: Corrupción de datos en base de datos (data file) o software de aplicación.
  - Acción a tomar: Se recurre al apoyo de la Oficina de Tecnologías de la Información para la reparación o recuperación de información de base de datos. En caso no se pueda recuperar la información perdida se recurre al levantamiento del Back up de la Base de datos. Para la continuidad del negocio se recurre a los servidores de contingencia que ponga a disposición la Oficina de Tecnologías de la Información. Asimismo, se solicita el servicio de asistencia técnica del proveedor del software.
- Escenario 3: Mal funcionamiento de hardware de la línea de producción de microformas.
  - Se recurrirá a los equipos de respaldo, como son los escáneres de producción, computadoras adicionales y servidor de contingencia. Al efecto estos equipos cuentan con réplicas de las aplicaciones utilizadas en la línea de producción. Asimismo, se solicita el servicio de asistencia técnica del proveedor del hardware.
- Escenario 4: Incorrecta operación del sistema de producción de microformas que imposibilite el normal acceso de los usuarios al servicio.
  - Reinstalación de la aplicación en el equipo que presenta la falla, previa evaluación del código y de los perfiles de usuario. Asimismo, se solicita el servicio de asistencia técnica del proveedor del software.

### 7.2.2 Actividades posteriores a la situación de contingencia

Tan pronto pase la emergencia, se procederá a realizar y registrar las acciones que se mencionan a continuación:

#### 7.2.2.2 Informe

- En todos los casos, el Supervisor elaborará un informe detallado de las acciones tomadas durante la emergencia y las acciones posteriores previstas. Dicho informe estará dirigido al Jefe de la OAC y un ejemplar firmado del mismo

será entregado al depositario de la fe pública encargado de la línea de producción.

#### 7.2.2.3 Caso en que haya habido evacuación o daño de las microformas

- Si la emergencia ocasionó la evacuación de las microformas que permanecían temporalmente en los ambientes de la línea de producción y/o se presume razonablemente que éstas sufrieron daños, el Supervisor dispondrá que se ejecuten las siguientes acciones:
  - a) Realizar el inventario detallado de los soportes de las microformas.
  - b) Evaluar el estado de conservación de los soportes de las microformas.
  - c) Trasladar y depositar en un microarchivo, de ser necesario.

#### 7.2.2.4 Caso en que haya habido daño a la infraestructura de la línea de producción

- Si la emergencia ocasionó daños a la habitación y/o a los equipos, y/o se presume razonablemente que dichos daños se produjeron, el Supervisor realizará una evaluación integral de la línea de producción, con especial atención en el estado de su infraestructura y equipamiento.

#### 7.2.2.5 Priorización de actividades del Plan de Acción

- Se compara la evaluación de los daños reales contra el Plan de Acción para obtener una lista de actividades a realizar, ordenándolas por prioridades atendiendo a las actividades estratégicas y urgentes de la entidad.

#### 7.2.2.6 Ejecución de actividades

- Se reparten las actividades previstas en el Plan de Acción, destinadas primero a restaurar los servicios y luego a contar con los recursos en las cantidades y lugares normales.
- En caso de imposibilidad de acceder al contenido de los equipos informáticos, se recurre al personal informático de apoyo para la reparación o recuperación de información. En caso de que no se pueda recuperar la información perdida, se recurre a las copias de respaldo.

#### 7.2.2.7 Evaluación de resultados

- Una vez finalizada la recuperación, se evalúan las actividades realizadas (su eficacia, duración, circunstancias favorables y desfavorables, etc.). Esto da lugar a la retroalimentación del

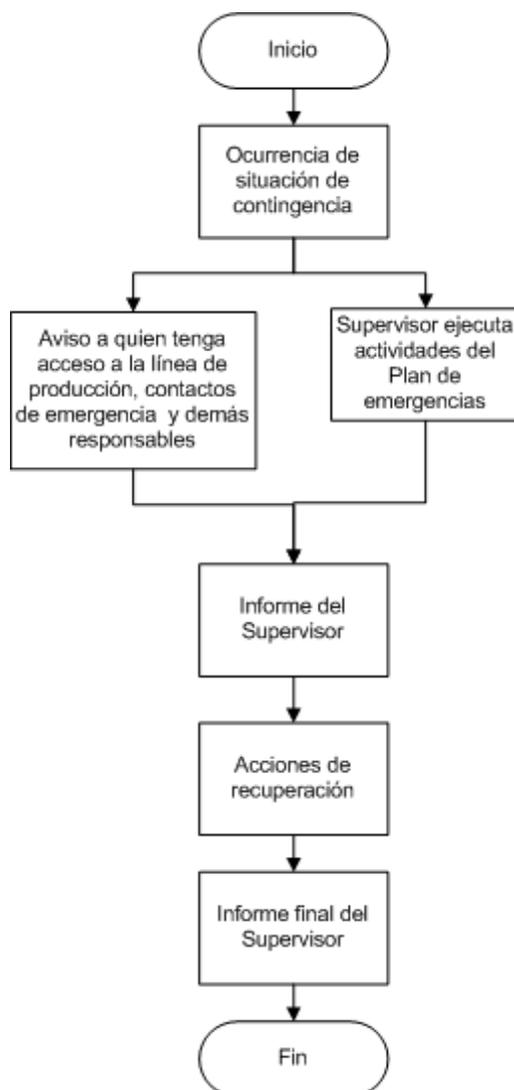
Plan de Contingencia y una lista de recomendaciones para reducir los riesgos y pérdidas del tipo de siniestro ocurrido.

#### 7.2.2.8 Retroalimentación del Plan de Acción

- La evaluación de resultados mejora el Plan de acción original, perfeccionando los aciertos y corrigiendo los errores.

## 8 DIAGRAMA DE FLUJO

En caso de ocurrencia de una situación de contingencia, se procede de la siguiente manera:



## 9 CAMBIOS A LA VERSIÓN ANTERIOR

VERSIÓN ANTERIOR	VERSIÓN ACTUAL
------------------	----------------

Número, capítulo o ítem del párrafo	Descripción del número, capítulo o ítem del párrafo	Descripción del cambio efectuado	Motivo del cambio efectuado
No aplica.			