000243

MUNICIPALIDAD PROVINCIAL DE ESPINAR
OFICINA DE TECNOLOGÍA DE LA INFORMACIÓN
"Año de la Recuperación y Consolidación de la Economía Peruana"

CUSCO – PERÚ

INFORME N.° 087–2025–JLCC–OTI–MPE/C

A: : LIC. ADM. JUAN L. CALLOHUANCA BURGOS
Director de la Oficina General de Administración

DE: :ING. JOSE LIZANDRO CONZA CCOLQUE
Jefe de la Oficina de Tecnología de la Información

ASUNTO : **Presentación del Plan de Contingencia de Tecnologías de la Información para su aprobación mediante resolución**

FECHA: Espinar, 31 de julio del 2025

Se presenta el Plan de Contingencia de Tecnologías de la Información de la Municipalidad Provincial de Espinar, elaborado por la Oficina de Tecnologías de la Información, con el objetivo de establecer procedimientos claros y organizados que permitan prevenir, enfrentar y superar cualquier eventualidad que pueda afectar el normal funcionamiento de los servicios tecnológicos de la institución.

El presente plan contempla acciones preventivas, de respuesta y recuperación orientadas a minimizar riesgos y asegurar la continuidad operativa ante situaciones imprevistas. Asimismo, contribuye al fortalecimiento de la infraestructura tecnológica y a una mejor capacidad de reacción institucional frente a posibles contingencias.

En ese contexto, y en concordancia con la normativa vigente en materia de gestión de riesgos y continuidad operativa, se requiere la aprobación del presente documento mediante resolución, a fin de formalizar su aplicación y garantizar su alineamiento a los lineamientos estratégicos institucionales.

La Oficina de Tecnologías de la Información queda a disposición para brindar las precisiones técnicas o complementarias que se consideren necesarias.

MUNICIPALIDAD PROVINCIAL DE ESPINAR
Ing. Jose L. Conza Ccolque
RESPONSABLE DE LA OFICINA DE TECNOLOGIAS DE LA INFORMACIÓN

RECIBIDO
FECHA 31 JUL. 2025
FOLIO: 24 N° DE REG. 12031
HORA 6:00 FIRMA:

000242

PLAN DE CONTINGENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN

1. INTRODUCCIÓN

Una organización es susceptible a encontrarse frente a una situación de emergencia que puede originar efectos adversos, ocasionando pérdidas de vidas humanas, ambientales, materiales, entre otros. El tiempo y la capacidad de respuesta con que cuenta la municipalidad son piezas claves para enfrentar y controlar cualquier situación de emergencia que se presente.

En tal sentido, se ha elaborado el Plan de Contingencia de Tecnologías de la Información de la Municipalidad Provincial de Espinar (MPE), dado que la Institución es vulnerable a diferentes hechos que pueden interrumpir los servicios informáticos y afectar el normal funcionamiento de las actividades. Esto no sólo afecta a usuarios internos sino también a los ciudadanos y usuarios externos. Asimismo, el Plan se encuentra alineado a los Objetivos Estratégicos Institucionales (OEI) establecidos en el Plan Estratégico Institucional (PEI) de la MPE, buscando fortalecer la capacidad operativa y reducir la vulnerabilidad ante riesgos de desastres.

El presente plan establece los objetivos, el alcance y la metodología a seguir, a fin de minimizar el impacto negativo de la interrupción de los servicios informáticos. Contribuye a que la Institución esté preparada ante cualquier contingencia a nivel de tecnología de información, considerando acciones preventivas (antes), de respuesta (durante) y de recuperación (después) de los incidentes.

2. MARCO TEÓRICO

2.1. PLAN DE CONTINGENCIA

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 ve afectado negativamente por una causa interna o externa. Este plan permite minimizar las consecuencias de un incidente con el fin de reanudar las operaciones en el menor tiempo posible de forma eficiente y oportuna.

Asimismo, establece acciones a realizarse en las siguientes etapas:

- **Antes de la eventualidad:** Contempla la evaluación de la situación actual de las tecnologías de información en la Institución para mitigar el nivel de riesgo. Su importancia radica en disminuir la probabilidad de ocurrencia de un evento que afecte los servicios.
- **Durante la eventualidad:** Contempla estrategias frente a las emergencias. Las acciones descritas permitirán recuperar la actividad normal.
- **Después de la eventualidad:** Contempla estrategias para la restauración o recuperación, incluyendo acciones para regresar al estado normal de los servicios informáticos.

2.2. IMPORTANCIA DEL PLAN DE CONTINGENCIA DE TI

La implementación de un plan de contingencia garantiza que, ante un fallo o emergencia, la organización pueda seguir funcionando o recupere su capacidad operativa en el menor tiempo posible.

Beneficios de contar con un Plan de Contingencia de TI:

- **Mitigación de riesgos:** Reduce el impacto negativo de interrupciones en las operaciones.
- **Protección de datos:** Asegura que la información crítica de la municipalidad y de los ciudadanos esté protegida.
- **Cumplimiento normativo:** Leyes como la Ley de Protección de Datos Personales (Ley N° 29733) exigen la implementación de planes de contingencia.
- **Garantía de continuidad operativa:** Permite que las funciones esenciales de la municipalidad sigan operativas durante y después de un incidente.

2.3. OBJETIVO DE TIEMPO DE RECUPERACIÓN (RTO)

El RTO indica el tiempo máximo tolerable que un sistema, aplicación o función crítica puede estar fuera de servicio antes de que su indisponibilidad afecte gravemente a la organización.

2.4 CÁLCULO DEL RTO

El cálculo del RTO no se basa en una fórmula matemática estricta, sino en un análisis de negocio y riesgo. Se determina a partir del juicio de experto del personal de la Oficina de Tecnologías de la Información (OTI) y otros responsables, considerando la criticidad del sistema y el impacto en las operaciones municipales. Bajo estos criterios se establecerán los RTO de los servicios o sistemas críticos de la MPE.

3. ANÁLISIS DE CONTEXTO INTERNO Y EXTERNO

Análisis Interno

Fortalezas	Debilidades
Compromiso de la Alta Dirección (Alcaldía, Gerencia Municipal) con la modernización y seguridad de la información.	Falta de presupuesto para proyectos de seguridad y renovación tecnológica.
Existencia de un Comité de Gobierno y Transformación Digital que impulsa iniciativas de TI.	Alta rotación de personal en áreas clave, lo que afecta la continuidad de los proyectos.
Personal de TI con conocimientos técnicos adecuados para la gestión de sistemas municipales.	Falta de capacitación continua en seguridad de la información para todo el personal.

Plataforma tecnológica en proceso de actualización, lo que mejora la seguridad y eficiencia.	Dependencia de la Oficina de Tecnologías de la Información (OTI) en otras gerencias, con posible conflicto de intereses.

Análisis Externo

Oportunidad	Amenazas
Disponibilidad de fondos de programas gubernamentales para la modernización de municipalidades.	Cambios en la gestión municipal (Alcalde, Gerentes) que puedan interrumpir proyectos de TI.
Posibilidad de convenios con universidades o institutos para prácticas profesionales y capacitación en seguridad.	Recortes presupuestales que afecten directamente los proyectos de TI y seguridad.
	Hackers que puedan vulnerar el Portal Institucional o sistemas críticos. Ataques de malware (ransomware, virus) a través de correos electrónicos o dispositivos USB.
	Sanciones por incumplimiento de la Ley de Protección de Datos Personales y otras normativas.

4. POLÍTICA DEL PLAN DE CONTINGENCIA DE TI

- **Desarrollo del Plan:** Se debe desarrollar y mantener un plan de contingencia de TI que identifique sistemas críticos, riesgos y procedimientos de recuperación, basado en un análisis de impacto al negocio municipal.
- **Gestión de Riesgos:** Se deben identificar y evaluar regularmente los riesgos que podrían afectar los servicios de TI (fallas de hardware, ciberataques, desastres naturales, errores humanos) e implementar controles para mitigarlos.
- **Respaldo y Recuperación:** Los datos críticos deben respaldarse regularmente y almacenarse en ubicaciones seguras. Los procedimientos de recuperación deben estar documentados y accesibles.
- **Pruebas y Simulacros:** El plan debe ser probado periódicamente mediante simulacros para asegurar su efectividad, y los resultados deben usarse para mejorarlo.
- **Capacitación del Personal:** El personal de TI y los usuarios clave deben recibir capacitación sobre sus roles y responsabilidades en el plan de contingencia.

- **Revisión y Actualización:** El plan debe revisarse y actualizarse anualmente o tras cambios significativos en la infraestructura o en los procesos de la municipalidad, con la aprobación de la alta dirección.
- **Cumplimiento:** Todos los empleados y contratistas de la MPE deben cumplir con esta política. El incumplimiento puede resultar en sanciones.

5. OBJETIVOS

5.1 Objetivo General

Establecer disposiciones para garantizar la continuidad de los servicios informáticos de la MPE en caso de una eventualidad, a fin de que su restablecimiento sea en el menor tiempo posible.

5.2 Objetivo Específicos

- Identificar, analizar y proteger los servicios informáticos críticos de la MPE.
- Establecer acciones para una restauración adecuada de los servicios informáticos en caso de interrupción, evitando la pérdida de información.
- Contar con personal capacitado y organizado para afrontar las contingencias.
- Evaluar los resultados de la ejecución del plan para su mejora continua.

6. CUMPLIMIENTO NORMATIVO

Este plan se alinea con el siguiente marco normativo aplicable al sector público peruano:

- Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado.
- Ley N° 28551, Ley que establece la obligación de elaborar y presentar planes de contingencia
- Ley N° 29664, Ley que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD).
- Ley N° 29733 - Ley de Protección de Datos Personales
- Decreto Supremo N° 018-2017 –PCM, Decreto Supremo que aprueba medidas para fortalecer la planificación y operatividad del Sistema Nacional de Gestión de Riesgos de Desastres mediante la adscripción y transferencia de funciones al Ministerio de Defensa a través del Instituto Nacional de Defensa Civil–INDECI y otras disposiciones.
- Decreto Supremo N° 034-2014-PCM, Decreto Supremo que aprueba el Plan Nacional de Gestión del Riesgos de Desastres - PLANAGERD 2014-2021.
- Decreto Supremo Nº 048-2011-PCM, Decreto Supremo que aprueba el Reglamento de la Ley Nº 29664, que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD).
- Decreto Supremo N° 083-2022-PCM - Reglamento de Seguridad Digital, Reglamento de Seguridad Digital, aprobado en 2022, establece que las entidades del sector público deben implementar políticas de seguridad digital, que incluyen la gestión de incidentes y contingencias.

- Directiva N° 003-2021-JUS/DGTAIPD - Directiva de Gestión de Riesgos de Seguridad de la Información.
- Directiva N° 001-2022-PCM/SEGDI - Gobierno Digital, que establece directivas para el Gobierno Digital, donde se enfatiza la necesidad de que las entidades públicas tengan un Plan de Contingencia para sus sistemas de TI, en línea con las normativas de gestión de la seguridad de la información.
- Resolución Ministerial N° 028-2015-PCM, aprobación de los Lineamientos para la Gestión de la Continuidad Operativa de las entidades públicas en los tres niveles de Gobierno.
- Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática.
- Resolución Contraloría General Nº 320-2006-GC que aprueba las Normas de Control Interno para el Sector Público.

7. ALCANCE

Las disposiciones contenidas en el presente Plan de Contingencia son de cumplimiento obligatorio para todas las unidades de organización de la Municipalidad Provincial de Espinar (MPE).

8. DEFINICIONES

- **Amenaza:** Causa potencial de un incidente no deseado que puede resultar en daño.
- **Malware:** Software malicioso que busca infiltrarse o dañar un sistema sin consentimiento.
- **Plan de Contingencia:** Plan con acciones para garantizar la continuidad de los servicios informáticos de la MPE ante una eventualidad.
- **Riesgo:** Posibilidad de que un evento adverso impacte los objetivos. Se mide en probabilidad y consecuencia.
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una amenaza

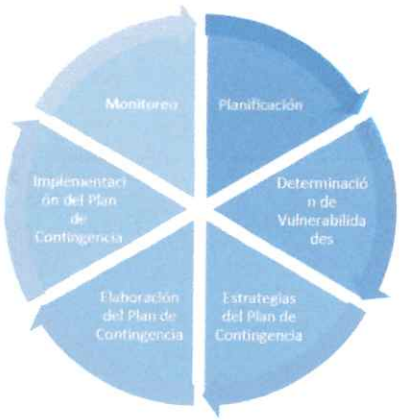
9. METODOLOGÍA DE TRABAJO

La metodología para desarrollar, implementar y mantener el plan sigue un ciclo de vida de seis fases para preservar la operatividad de TI en la MPE.

- **Fase 1: Planificación:** Organización de equipos y roles.
- **Fase 2: Determinación de Vulnerabilidades:** Identificación de activos críticos y amenazas.
- **Fase 3: Estrategias del Plan de Contingencia:** Definición de estrategias de prevención y recuperación.
- **Fase 4: Elaboración del Plan de Contingencia:** Documentación de procedimientos específicos.
- **Fase 5: Implementación del Plan de Contingencia:** Puesta en marcha del plan y pruebas.

- **Fase 6: Monitoreo:** Verificación, simulacros y mejora continua.

Metodología de implementación de un Plan de Contingencia de TI

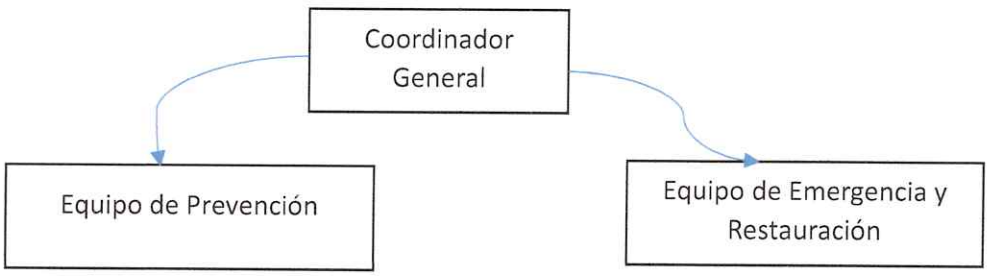


Elaboración propia

FASE 1: Planificación y Organización

La Oficina de Tecnologías de la Información (OTI) de la MPE, dependiente de la Oficina General de Administración, es responsable de administrar y brindar las soluciones informáticas y el soporte tecnológico a todas las áreas de la municipalidad. Para la mejor ejecución de funciones, así como, desarrollar el soporte tecnológico y soluciones informáticas para la operatividad de la red nacional de información científica e interconexión telemática.

Tiene dentro de sus funciones, elaborar y proponer lineamientos, directivas y la homologación de tecnologías informáticas y de comunicaciones para la MPE, sus órganos, proyectos y programas. Para el funcionamiento del Plan de Contingencias de Tecnologías de la Información se ha establecido, siguiente organigrama describiendo los roles y equipos que conforman el plan de contingencia de TI y esta conformado por el personal de la Oficina de Tecnologías de la Información (OTI) de MPE.



Descripción de Roles y Responsabilidades

- **Jefe de la OTI (Coordinador General)**
  - **Responsabilidades**:
    - Supervisar y coordinar todo el departamento de TI.
    - Activar y dirigir el plan de contingencia durante un incidente.
    - Tomar decisiones estratégicas sobre recursos y prioridades.
    - Comunicar el estado de la contingencia a la alta dirección.
  - **Interacción**: Supervisa directamente a todos los miembros del equipo.

- **Especialista Web (para actualización de gob.pe)**
  - **Responsabilidades**:
    - Mantener actualizado el contenido municipal en el sitio gob.pe.
    - Asegurar que el sitio web permanezca operativo durante una contingencia.
    - Preparar backups o versiones estáticas del contenido web como medida preventiva.
  - **Interacción**: Colabora con el Desarrollador Web y el Especialista en Mantenimiento Web, enfocándose en la gestión de contenido.

- **Equipo de Prevención**
  - **Liderado por**: Analista de Sistema
  - **Miembros**: Analista de Sistema, Especialista Web
  - **Funciones**:
    - Realizar copias de respaldo y pruebas de restauración.
    - Mantener actualizados los procedimientos de seguridad y el contenido web.

- **Equipo de Emergencia y Restauración**
  - **Liderado por**: Especialista en Soporte Técnico
  - **Miembros**: Especialista en Soporte Técnico, Desarrollador Web, Especialista en Mantenimiento Web
  - **Funciones**:
    - Mitigar impactos durante una contingencia.
    - Restaurar la infraestructura y servicios de TI, incluyendo el sitio web.

FASE 2: Determinación de Vulnerabilidades

La siguiente tabla presenta los procesos, aplicaciones y/o recursos críticos de la Municipalidad Provincial de Espinar, junto con sus respectivos tiempos de recuperación objetivo (RTO). Los RTO son estimaciones basadas en la importancia de cada aplicación para la continuidad operativa y los servicios al ciudadano.

Procesos y Recursos Críticos

Proceso	Aplicaciones y/o Recursos Críticos	Tiempo de Recuperación (RTO)
Gestión Documental	**TRAMIDOC** Sistema de trámite documental para la gestión de documentos internos y externos.	4 horas (Crítico para la comunicación y registro oficial).
Gestión Administrativa	**SIGA** Sistema Integrado de Gestión Administrativa.	6 horas (Esencial para la gestión de recursos internos).
Gestión Financiera	**SIAF** Sistema Integrado de Administración Financiera.	2 horas (Altamente crítico para la ejecución presupuestal y transparencia).
Gestión Tributaria	**RENTAS** Sistema para la recaudación y administración de tributos municipales.	4 horas (Clave para ingresos municipales y atención al ciudadano).
Gestión de Archivos	**ARCHIVO CENTRAL** Repositorio físico y/o digital de documentos históricos y administrativos.	12 horas (Importante, pero menos urgente que sistemas operativos).
Gestión de Servicios de Agua	**USAPAL** Sistema para la gestión de servicios de agua potable y alcantarillado.	4 horas (Crítico para servicios esenciales al ciudadano).
Gestión Catastral	**CATASTRO** Sistema para la gestión de información catastral y urbanística.	8 horas (Importante para planificación urbana, pero menos crítico en el corto plazo).
Gestión de Tesorería	**CAJA** Sistema para operaciones de caja y atención al público.	3 horas (Esencial para la atención directa al ciudadano).
Gestión de Inventarios	**OS-INVENTORY** Sistema para el control de inventarios municipales.	8 horas (Necesario para la gestión de activos, pero no de alta urgencia).
Gestión Patrimonial	**PATRIMONIO** Sistema para la gestión de bienes patrimoniales de la municipalidad.	12 horas (Importante para el control de activos, pero menos crítico en el corto plazo).
Gestión de Correos	**ZIMBRA**	3 horas (Esencial para la remisión y recepción de correos)

Infraestructura Tecnológica y Comunicaciones

Infraestructura Tecnológica y Comunicaciones	Equipos y/o Recursos Críticos	Tiempo de Recuperación (RTO)
Servidores dell R360	- **2 Servidores DC** (Controladores de Dominio): - **2 Servidores FS** (File Servers): Almacenamiento de archivos compartidos. - 1 **Servidor WSD** (Windows Server Deployment): Despliegue de servicios y actualizaciones. - 1 **Servidores SIGA**: Sistema Integrado de Gestión Administrativa para logística y abastecimiento - 1 **Servidores ZIMBRA**: Sistema para la emisión y recepción de correos	4 horas (Crítico para autenticación, almacenamiento y gestión administrativa).
Servidores de Aplicaciones Específicas	- **Catastro**: Gestión de información catastral y urbanística. - **SIAF**: Sistema Integrado de Administración Financiera para gestión presupuestal. - **Remuneraciones**: Gestión de planillas y pagos de personal. - **Aplicaciones**: Otras aplicaciones municipales críticas.	- **Catastro**: Gestión de información catastral y urbanística. - **SIAF**: Sistema Integrado de Administración Financiera para gestión presupuestal. - **Remuneraciones**: Gestión de planillas y pagos de personal. - **Aplicaciones**: Otras aplicaciones municipales críticas.
Sistema de Almacenamiento	NAS de 16 TB: Almacenamiento centralizado para datos críticos y respaldos.	12 horas (Esencial para recuperación de datos, pero con redundancia asumida).
Equipos de Comunicaciones	3 Switches Administrables: - **192.168.0.200** (Data Center OTI, núcleo de red). - **192.168.0.201** y	6 horas (Switch 0.200) 12 horas (Switches 0.201 y 0.202) (El switch núcleo es crítico para la conectividad; los

	192.168.0.202 (conectados al switch 0.200).	otros tienen menor impacto).
Enlaces de Internet y Datos	Conexiones de red que soportan los servicios municipales y acceso a sistemas críticos.	4 horas (Crítico para la continuidad de servicios digitales y atención al ciudadano).

Desarrollo, Mantenimiento y Soporte Técnico

Proceso	Aplicaciones y/o Recursos Críticos	Tiempo de Recuperación (RTO)
Desarrollo y Mantenimiento de Soluciones	**Sistema de Trámite Documentario (TRAMIDOC)** Sistema para la gestión de documentos internos y externos, esencial para la comunicación oficial.	48 horas (Crítico para la continuidad de los trámites administrativos).
	Sistema de Rentas y Tributación (RENTAS) Sistema para la recaudación y administración de tributos municipales, clave para los ingresos de la MPE	48 horas (Esencial para la sostenibilidad financiera y atención al ciudadano).
	Sistema de Gestión Administrativa (SIGA) Sistema para la gestión de logística y abastecimiento, soportado en servidores dedicados.	48 horas (Fundamental para la gestión interna de recursos).
	Bases de Datos de los Sistemas Críticos Bases de datos que soportan TRAMIDOC, RENTAS, SIGA y otros sistemas críticos, almacenadas en el NAS de 16 TB y servidores Dell R360.	48 horas (Vital para la integridad y disponibilidad de la información crítica).
Soporte Técnico	**Estaciones de Trabajo del Personal Crítico** Equipos de trabajo en gerencias clave, caja y otras áreas críticas para la operación municipal.	24 horas (Necesario para la continuidad de las operaciones de personal clave).

Jefatura de OTI	**Personal Crítico responsable de los Procesos de TI** Incluye al Oficial de Seguridad de la Información y otros responsables de la gestión de TI, esenciales para la coordinación y recuperación de sistemas.	12 horas (Crítico para la gestión y respuesta ante incidentes de TI).

Identificación de Amenazas

N°	Amenaza	Tipo	Probabilidad
01	Terremoto/Sismo	Natural	Muy Baja
02	Ataque Cibernético	Tecnológico	Media
03	Falla Eléctrica	Físico	Media
04	Incendio	Siniestro	Muy Baja
05	Falla de hardware y software	Tecnológico	Media
06	Ausencia del personal crítico de TI	Humano	Baja
07	Pandemia y/o Epidemia	Ambiental	Muy Baja

Listado de sistemas de información y portales clasificados por prioridad de atención

N°	Nombre	Descripción	Area Usuaria	Prioridad
01	**Sistemas Críticos (prioridad 1)**			
1.1	**Sistema de Trámite Documental (TRAMIDOC)**	Permite registrar y realizar seguimiento de documentos internos y externos, optimizando la gestión administrativa	Todas	1
1.2	**Sistema de Rentas y Tributación**	Gestión de Impuesto predial, arbitrios, tasas de servicios y tributos municipales específicos de Espinar	Gerencia de Administración Tributaria	1
1.3	**SIGA**	Sistema Integrado para la gestión administrativa, logística y presupuestal adaptado a las necesidades de la municipalidad	Todas	1
1.4	**Portal Web Institucional**	Principal canal de comunicación e información al ciudadano,	Oficina de Tecnología de la	1

		con énfasis en servicios y proyectos locales de Espinar.	Información (OTI)	
1.5	**Mesa de Partes Virtual**	Plataforma digital para que los ciudadanos de Espinar ingresen documentos de forma remota, agilizando trámites.	OTI y Oficina de Atención al ciudadano	1
1.6	**SIAF**	Sistema de Administración Financiera	Oficinas de Contabilidad, Abastecimientos, Presupuesto, Tesorería	1
1.7	**USAPAL**	Sistema de Gestión de Agua	USAPAL	1
1.8	**CAJA**	Sistema de Control de Caja	Caja	1
1.9	**ZIMBRA**	Sistema de Gestión de Correos	Todas	1
2	**Sistemas Importantes (Prioridad 2)**			
2.1	**Sistema de Registro Civil**	Gestión de actas de nacimiento, actas de defunción, actas de matrimonio	Registro Civil	2
2.2	**Locales**	Sistema de alquiler de locales	Gerencia de Desarrollo Social	2
2.3	**Archivos**	Sistema de gestión de archivos	Archivo Central	2
2.4	**Planillas**	Gestión de pagos y legajos del personal.	RRHH	2
2.5	**Catastro**	Sistema Catastral	Catastro	2
2.6	**Intranet Municipal**	Sistema Colaborativo interno para los trabajadores	Todas	2

10. Formatos de procedimientos de contingencia y restauración

a. Evento: Incendio en el Centro de Datos

Procedimiento de Prevención

Situación actual: La Municipalidad Provincial de Espinar (MPE) cuenta con un Centro de Datos equipado con servidores Dell R360 y un NAS de 16 TB. Existen extintores PQS y CO2 en las inmediaciones, con última inspección hace 6 meses. Hay detectores de humo, pero sin pruebas regulares. El personal de la Oficina de Tecnologías de la Información (OTI) tiene capacitación básica en prevención de incendios, pero no se realizan simulacros frecuentes. El cableado está parcialmente ordenado, con riesgo de acumulación de polvo. No hay centro de datos alterno, pero los respaldos se almacenan en el NAS.

Objetivo: Minimizar la interrupción de operaciones ante un incendio en el Centro de Datos. Acciones del Equipo de Prevención:

Acciones del Equipo de Prevención:

- Verificar la vigencia y operatividad de extintores PQS y CO2 cada 3 meses.
- Realizar mantenimiento preventivo mensual de servidores, UPS y NAS.
- Ejecutar y probar respaldos diarios de sistemas críticos (TRAMIDOC, SIGA, SIAF, RENTAS, ZIMBRA).
- Implementar limpieza regular para evitar acumulación de polvo en cableado.
- Capacitar al personal de OTI y brigadas en prevención de incendios, con simulacros anuales.

Procedimiento de Ejecución

Eventos que activan la contingencia: Incendio en el Centro de Datos o áreas adyacentes que afecten servidores, switches (192.168.0.200, 0.201, 0.202) o NAS.

Acciones a corto plazo:

- **¡Prioridad 1: Seguridad Humana!** Activar alarma y evacuar al personal.
- Desconectar el fluido eléctrico del área, si es seguro, con apoyo de mantenimiento.
- Notificar al Equipo de Emergencia y al Coordinador de Continuidad (Jefe de OTI).
- Contactar a bomberos y a la Oficina de Seguridad de la MPE.
- Restringir acceso al área hasta que sea declarada segura.

Procedimiento de Recuperación

Personal Encargado: Coordinador de Continuidad (Jefe de OTI) y Equipo de Restauración (Especialista en Soporte Técnico, Desarrollador Web, Especialista en Mantenimiento Web).

Descripción de actividades:

- Evaluar daños a infraestructura (servidores Dell R360, NAS, switches) tras autorización de bomberos.
- Restaurar desde respaldos en NAS o copias externas, priorizando SIAF (2 horas), TRAMIDOC, RENTAS, USAPAL, CAJA, ZIMBRA (4 horas), SIGA (6 horas).
- Contactar a proveedores (Dell, red) para reposición de hardware dañado.

- Verificar integridad de bases de datos y restaurar aplicaciones críticas.

b. Evento: Terremoto / Sismo

Procedimiento de Prevención

Situación actual: La MPE realiza simulacros anuales coordinados por Defensa Civil, con participación limitada de OTI. Los racks del Centro de Datos están parcialmente anclados, con riesgo en sismos fuertes. Hay brigadas de emergencia, pero no especializadas en TI. Las zonas seguras y rutas de evacuación están señalizadas, pero requieren actualización. Los respaldos se almacenan en el NAS, con pruebas mensuales.

Objetivo: Minimizar interrupciones tras un sismo, priorizando la seguridad del personal.

Acciones del Equipo de Prevención:

- Participar en simulacros de sismo bianuales, incluyendo a OTI.
- Asegurar anclaje de racks y servidores según normas antisísmicas.
- Actualizar señalización de zonas seguras y rutas de evacuación.
- Probar respaldos diarios y restauración semanal de sistemas críticos.
- Capacitar brigadas en protección de equipos tecnológicos.

Procedimiento de Ejecución

Eventos que activan la contingencia: Sismo que afecte la infraestructura tecnológica o las operaciones de la MPE.

Acciones a corto plazo:

- **Durante el sismo:** Mantener calma y ubicarse en zonas seguras.
- **Después del sismo:** Evacuar ordenadamente, dirigidos por brigadas.
- Verificar estado de salud del personal y reportar lesiones.
- Evaluar daños en infraestructura física y tecnológica con Defensa Civil.
- Restringir acceso al Centro de Datos hasta que sea seguro.

Procedimiento de Recuperación

Personal Encargado: Coordinador de Continuidad (Jefe de OTI) y Equipo de Restauración.

Descripción de actividades:

- Inspeccionar Centro de Datos tras cese de réplicas y autorización de Defensa Civil.
- Verificar operatividad de sistemas críticos (SIAF: 2 horas; TRAMIDOC, RENTAS, USAPAL, CAJA, ZIMBRA: 4 horas; SIGA: 6 horas).
- Restaurar servicios desde respaldos en NAS o copias externas.
- Contactar a proveedores para reposición de equipos dañados.
- Verificar aplicaciones críticas y documentar incidente.

c. Evento: Ataque Cibernético

Procedimiento de Prevención

Situación actual: La MPE utiliza sistemas críticos como TRAMIDOC, SIGA, SIAF, RENTAS y ZIMBRA, vulnerables a ciberataques (ransomware, phishing). El firewall y antivirus están implementados, pero no actualizados regularmente. No hay capacitación reciente en ciberseguridad para el personal. Los respaldos se realizan diariamente, pero las pruebas de restauración son esporádicas.

Objetivo: Prevenir y mitigar los impactos de un ataque cibernético en los sistemas de la MPE.

Acciones del Equipo de Prevención:

- Actualizar firewall y antivirus en servidores y estaciones de trabajo semanalmente.
- Implementar capacitación trimestral en ciberseguridad para todo el personal.
- Realizar auditorías mensuales de seguridad en sistemas críticos.
- Ejecutar y probar respaldos diarios de bases de datos y sistemas.
- Configurar políticas de acceso restringido a sistemas críticos (SIAF, ZIMBRA, SIGA, TRAMIDOC).

Procedimiento de Ejecución

Eventos que activan la contingencia: Detección de malware, ransomware, acceso no autorizado o interrupción de servicios críticos (SIAF, TRAMIDOC, ZIMBRA).

Acciones a corto plazo:

- Aislar sistemas comprometidos desconectándolos de la red (switches 192.168.0.200, 0.201, 0.202).
- Notificar al Coordinador de Continuidad y al Equipo de Emergencia.
- Ejecutar escaneos antivirus en servidores y estaciones de trabajo.
- Restringir accesos externos a sistemas críticos (ZIMBRA, Mesa de Partes Virtual).

- Informar al Oficial de Seguridad de la Información para análisis inicial.

Procedimiento de Recuperación

Personal Encargado: Coordinador de Continuidad (Jefe de OTI), Equipo de Restauración, Oficial de Seguridad de la Información.

Descripción de actividades:

- Identificar el alcance del ataque con herramientas de análisis forense.
- Restaurar sistemas desde respaldos seguros (NAS o copias externas), priorizando SIAF (2 horas), TRAMIDOC, RENTAS, USAPAL, CAJA, ZIMBRA (4 horas).
- Actualizar parches de seguridad y contraseñas de sistemas comprometidos.
- Verificar integridad de bases de datos y funcionalidad de aplicaciones.
- Documentar el incidente y reportar a la Autoridad Nacional de Protección de Datos Personales, si aplica.

d. Evento: Falla Eléctrica

Procedimiento de Prevención

Situación actual: El Centro de Datos cuenta con UPS, pero su capacidad no cubre interrupciones prolongadas. No hay generador eléctrico de respaldo. Los servidores Dell R360 y el NAS dependen de la red eléctrica local, con historial de cortes esporádicos. Los procedimientos de respaldo son diarios, pero las pruebas no son regulares.

Objetivo: Garantizar la continuidad de los servicios críticos ante una falla eléctrica prolongada.

Acciones del Equipo de Prevención:

- Realizar mantenimiento trimestral de UPS y verificar su capacidad.
- Gestionar la adquisición de un generador eléctrico para el Centro de Datos.
- Probar respaldos diarios y restauración semanal de sistemas críticos.
- Implementar políticas de apagado controlado para servidores durante cortes prolongados.
- Capacitar al personal de OTI en gestión de energía de emergencia.

Procedimiento de Ejecución

Eventos que activan la contingencia: Corte de energía que afecte el Centro de Datos o los servicios críticos por más de 30 minutos.

Acciones a corto plazo:

- Verificar el funcionamiento del UPS y estimar tiempo de autonomía.
- Notificar al Coordinador de Continuidad y al Equipo de Emergencia.
- Ejecutar apagado controlado de servidores no críticos para preservar energía.
- Contactar a la empresa eléctrica para estimar el tiempo de restablecimiento.
- Preparar la restauración desde respaldos en caso de daño por corte abrupto.

Procedimiento de Recuperación

Personal Encargado: Coordinador de Continuidad (Jefe de OTI) y Equipo de Restauración.

Descripción de actividades:

- Una vez restablecida la energía, verificar el estado de servidores, NAS y switches.
- Reiniciar sistemas críticos en orden de prioridad (SIAF: 2 horas; TRAMIDOC, RENTAS, USAPAL, CAJA, ZIMBRA: 4 horas; SIGA: 6 horas).
- Comprobar integridad de bases de datos y restaurar desde respaldos si es necesario.
- Documentar el incidente y evaluar la necesidad de mejoras en infraestructura eléctrica.
- Actualizar el inventario de equipos afectados

e. Evento: Falla de Hardware y Software

Procedimiento de Prevención

Situación actual: Los servidores Dell R360 y el NAS son críticos, pero no todos los equipos tienen mantenimiento regular. El software de sistemas críticos (SIAF, TRAMIDOC) tiene parches pendientes. No hay inventario actualizado de repuestos. Los respaldos son diarios, pero las pruebas de restauración son esporádicas.

Objetivo: Prevenir interrupciones por fallas de hardware o software en los sistemas críticos.

Acciones del Equipo de Prevención:

- Realizar mantenimiento preventivo trimestral de hardware (servidores, NAS, switches).
- Actualizar software crítico (SIAF, TRAMIDOC, ZIMBRA) con parches mensuales.
- Mantener un inventario de repuestos críticos (discos, fuentes de poder).
- Probar respaldos diarios y restauración semanal de sistemas críticos.
- Capacitar al personal de OTI en diagnóstico de fallas de hardware y software.

Procedimiento de Ejecución

Eventos que activan la contingencia: Falla de hardware (servidores, NAS, switches) o software que afecte sistemas críticos.

Acciones a corto plazo:

- Identificar el componente o software afectado (servidor, aplicación, base de datos).
- Notificar al Coordinador de Continuidad y al Equipo de Emergencia
- Aislar el equipo o sistema comprometido para evitar daños adicionales.
- Diagnosticar la falla con herramientas de monitoreo (logs, alertas).
- Preparar la restauración desde respaldos si el software está corrupto.

Procedimiento de Recuperación

Personal Encargado: Coordinador de Continuidad (Jefe de OTI) y Equipo de Restauración.

Descripción de actividades:

- Reemplazar hardware dañado usando repuestos del inventario o contactando a proveedores.
- Reinstalar o restaurar software crítico desde respaldos (SIAF: 2 horas; TRAMIDOC, RENTAS, USAPAL, CAJA, ZIMBRA: 4 horas).
- Verificar integridad de bases de datos y funcionalidad de aplicaciones.
- Actualizar parches de software para prevenir recurrencias.
- Documentar el incidente.

f. Evento: Ausencia del Personal Crítico de TI

Procedimiento de Prevención

Situación actual: La OTI depende de un equipo reducido, incluyendo al Jefe de OTI y especialistas clave. No hay un plan

formal de reemplazo para ausencias imprevistas. La documentación de procesos críticos está incompleta, lo que dificulta la continuidad.

Objetivo: Garantizar la operatividad de TI ante la ausencia de personal crítico.

Acciones del Equipo de Prevención:

- Documentar procedimientos operativos de sistemas críticos (SIAF, TRAMIDOC, ZIMBRA).
- Capacitar a personal alterno en tareas críticas de OTI.
- Establecer un plan de reemplazo para roles clave (Jefe de OTI, Especialista en Soporte Técnico).
- Mantener un repositorio accesible de contraseñas y configuraciones críticas.
- Realizar simulacros trimestrales con personal alterno.

Procedimiento de Ejecución

Eventos que activan la contingencia: Ausencia imprevista del Jefe de OTI, Especialista en Soporte Técnico u otros roles críticos por más de 24 horas.

Acciones a corto plazo:

- Notificar al director de la Oficina de Administración y designar un reemplazo temporal del personal ausente.
- Acceder a la documentación de procedimientos.
- Asignar tareas críticas al personal alterno capacitado.
- Priorizar el mantenimiento de sistemas críticos (SIAF, TRAMIDOC, ZIMBRA).
- Contactar a consultores externos si es necesario para soporte técnico.

Procedimiento de Recuperación

Personal Encargado: director de la Oficina de Administración, personal alterno de OTI, consultores externos (si aplica).

Descripción de actividades:

- Asegurar que el personal alterno mantenga la operatividad de sistemas críticos (SIAF: 2 horas; TRAMIDOC, RENTAS, USAPAL, CAJA, ZIMBRA: 4 horas).
- Actualizar la documentación de procedimientos con lecciones aprendidas.
- Planificar la reintegración del personal crítico ausente.
- Evaluar la necesidad de contratar personal adicional para OTI.
- Documentar el incidente

g. Evento: Pandemia y/o Epidemia

Procedimiento de Prevención

Situación actual: La MPE enfrentó limitaciones operativas durante la pandemia de COVID-19, con trabajo remoto parcial. Los sistemas ZIMBRA y Mesa de Partes Virtual soportan trabajo remoto, pero no todos los empleados tienen acceso a equipos adecuados. No hay un protocolo formal para operar TI en pandemias.

Objetivo: Garantizar la continuidad de los servicios de TI durante una pandemia o epidemia.

Acciones del Equipo de Prevención:

- Implementar políticas de trabajo remoto para personal de OTI, asegurando acceso a ZIMBRA y Mesa de Partes Virtual.
- Proveer equipos (laptops, VPN) a personal crítico de TI.
- Realizar respaldos diarios y almacenarlos en la nube o copias externas seguras.
- Capacitar al personal en herramientas de colaboración remota (ZIMBRA, Intranet).
- Establecer protocolos de bioseguridad para acceso al Centro de Datos.

Procedimiento de Ejecución

Eventos que activan la contingencia: Declaración de pandemia o epidemia que restrinja el acceso físico a las instalaciones de la MPE.

Acciones a corto plazo:

- Activar trabajo remoto para personal de OTI y áreas críticas.
- Asegurar acceso remoto a sistemas críticos (SIAF, TRAMIDOC, ZIMBRA) mediante VPN.
- Notificar al Coordinador de Continuidad y al Gerente Municipal.
- Implementar protocolos de bioseguridad para personal que acceda al Centro de Datos.
- Monitorear la operatividad de sistemas críticos desde ubicaciones remotas.

Procedimiento de Recuperación

Personal Encargado: Coordinador de Continuidad (Jefe de OTI), Equipo de Restauración, personal remoto.

Descripción de actividades:

- Mantener operatividad de sistemas críticos (SIAF: 2 horas; TRAMIDOC, RENTAS, USAPAL, CAJA, ZIMBRA: 4 horas) desde acceso remoto.
- Verificar integridad de respaldos y restaurar sistemas si hay interrupciones.
- Coordinar con proveedores para soporte técnico remoto, si es necesario.
- Actualizar protocolos de trabajo remoto con base en la experiencia.
- Documentar el incidente