RESOLUCIÓN DE GERENCIA MUNICIPAL N° 246-2024-MPC/G.M.

Cajamarca, 27 de agosto de 2024.

EL GERENTE MUNICIPAL DE LA MUNICIPALIDAD PROVINCIAL DE CAJAMARCA.

VISTO:

El Expediente N° 55322-2024; Informe N° 021-2024-JCSC-OTI-OGAF-MPC, de fecha 14 de agosto de 2024; Informe N° 128-2024-OTI-OGAyF-MPC, de fecha 15 de agosto de 2024; Informe Legal Nº 334-2024-OGAJ-MPC, emitido por la Oficina General de Asesoría Jurídica de la Municipalidad Provincial de Cajamarca y;

Firmado digitalmente por NARRO MARTOS Wilder Max FAU 20143623042 soft
Motivo: Doy V° B°
Fecha: 28.08.2024 15:52:15 -05:00

CONSIDERANDO:

Que, la Constitución Política del Perú en su artículo 194º modificada por la Ley de Reforma Constitucional Nº 28607, concordante con el artículo II del Título Preliminar de la Ley Nº 27972, establece que los Gobiernos Locales gozan de autonomía política, económica y administrativa en los asuntos de su competencia, precisando la última norma indicada que la autonomía que la Constitución Política del Perú establece para las Municipalidades, radica en la facultad de ejercer actos de gobierno, actos administrativos y de administración, con sujeción al Ordenamiento Jurídico.

Que, la Ley N° 28551, en su artículo 2, establece que: *"Los planes de contingencia son instrumentos de gestión que definen los objetivos, estrategias y programas que orientan las actividades institucionales para la prevención, la reducción de riesgos, la atención de emergencias y la rehabilitación en casos de desastres permitiendo disminuir o minimizar los daños, víctimas y pérdidas que podrían ocurrir a consecuencia de fenómenos naturales, tecnológicos o de la producción industrial, potencialmente dañinos".* De igual manera, el artículo 3, estipula: *"Todas las personas naturales y jurídicas de derecho privado o público que conducen y/o administran empresas, instalaciones, edificaciones y recintos tienen la obligación de elaborar y presentar, para su aprobación ante la autoridad competente, planes de contingencia para cada una de las operaciones que desarrolle".*

Firmado digitalmente por HUAMAN ROJAS Victor Alberto FAU 20143623042 soft
Motivo: Doy V° B°
Fecha: 28.08.2024 12:16:33 -05:00

Que, la Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado, en su artículo 1, menciona que: *"Declárase al Estado peruano en proceso de modernización en sus diferentes instancias, dependencias, entidades, organizaciones y procedimientos, con la finalidad de mejorar la gestión pública y construir un Estado democrático, descentralizado y al servicio del ciudadano".*

Que, el Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, en su artículo 6, señala: *"El gobierno digital es el uso estratégico de las tecnologías digitales y datos en la Administración Pública para la creación de valor público. Se sustenta en un ecosistema compuesto por actores del sector público, ciudadanos y otros interesados, quienes apoyan en la implementación de iniciativas y acciones de diseño, creación de servicios digitales y contenidos, asegurando el pleno respeto de los derechos de los ciudadanos y personas en general en el entorno digital. 6.2. Comprende el conjunto de principios, políticas, normas, procedimientos, técnicas e instrumentos utilizados por las entidades de la Administración Pública en la gobernanza, gestión e implementación de tecnologías digitales para la digitalización de procesos, datos, contenidos y servicios digitales de valor para los ciudadanos".*

De igual manera, el artículo 30 del mencionado texto normativo, estipula lo siguiente: *"La seguridad digital es el estado de confianza en el entorno digital que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales en*

dicho entorno. Se sustenta en la articulación con actores del sector público, sector privado y otros quienes apoyan en la implementación de controles, acciones y medidas".

En ese sentido, se advierte que mediante Informe N° 021-2024-JCSC-OTI-OGAF-MPC, de fecha 14 de agosto de 2024, emitido por el Sr. Juan Carlos Sánchez Chunque, oficial de seguridad y confianza digital, presenta Propuesta del Plan de Contingencias Informático de la Municipalidad Provincial de Cajamarca 2024-2026, el cual tiene como objetivo general: *"Garantizar la continuidad operativa de los sistemas de información y la infraestructura tecnológica para el normal desarrollo de actividades de la Municipalidad Provincial de Cajamarca".* Señalándose que dicho Plan de Contingencia Informático es el documento que: *"Compila una serie de procedimientos alternativos diseñados para asegurar la continuidad de los servicios de Tecnologías de Información cuando estos se vean afectados por incidentes internos o externos a la organización. El Plan de Contingencia busca minimizar el impacto de dichos incidentes, permitiendo reanudar las operaciones de manera eficiente y oportuna*".

Finalmente, mediante Informe Legal Nº 334-2024-OGAJ-MPC, emitido por la Oficina General de Asesoría Jurídica, existe en primer lugar la necesidad de contar con un documento de contingencia informático en la entidad, el cual tiene como finalidad la protección de la información tecnológica de la entidad evitando lo más posible la pérdida de dicha información, tanto más que tiene congruencia con las normas legales citadas encaminadas al cumplimiento de la Ley de Gobierno Digital, por lo cual, resulta VIABLE la aprobación del **PLAN DE CONTINGENCIAS INFORMÁTICO 2024-2026.**

Estando a lo expuesto y de conformidad con la parte in fine del Art. 39º de la Ley Orgánica de Municipalidades, Ley N° 27972;

SE RESUELVE:

ARTÍCULO PRIMERO. – APROBAR el Plan de Contingencias Informático de la Municipalidad Provincial de Cajamarca mismo que como anexo forma parte de la presente resolución, en mérito a los considerandos de la presente resolución.

ARTÍCULO SEGUNDO. – DELEGAR al jefe de la Oficina de Tecnologías de la Información de la Municipalidad Provincial de Cajamarca, el desarrollo, ejecución y cumplimiento del Plan de Contingencias Informático, el cual deberá ejecutarse en cumplimiento estricto de la normatividad legal vigente, todo ello bajo su expresa responsabilidad.

ARTÍCULO TERCERO. – DEVOLVER el presente expediente a la Oficina de Tecnologías de la Información de la Municipalidad Provincial de Cajamarca a fin de que proceda conforme lo resuelto en la presente resolución.

ARTÍCULO CUARTO. – DISPONER, la publicación de la presente Resolución en el Portal web de la Municipalidad Provincial de Cajamarca.

REGÍSTRESE, COMUNÍQUESE, CÚMPLASE Y ARCHÍVESE.

MUNICIPALIDAD PROVINCIAL DE CAJAMARCA ... renace.

Firmado digitalmente por NARRO MARTOS Wilder Max FAU 20143623042 soft
Motivo: Soy el autor del documento
Fecha: 28.08.2024 15:53:21 -05:00

Distribución:
- **Alcaldía.**
- **Oficina General de Administración y Finanzas.**
- **Oficina de Tecnologías de la Información.**
- **Interesado.**
- **Archivo.**

PLAN DE CONTINGENCIAS INFORMÁTICO DE LA MUNICIPALIDAD PROVINCIAL DE CAJAMARCA 2024-2026

Firmado digitalmente por LEZAMA BAZAN Jorge Rodrigo FAU 20143623042 soft
Motivo: Doy V° B°
Fecha: 28.08.2024 15:10:06 -05:00

Cajamarca, 2024

Firmado digitalmente por NARRO MARTOS Wilder Max FAU 20143623042 soft
Motivo: Doy V° B°
Fecha: 28.08.2024 15:54:43 -05:00

APROBACIONES

#	Nombres y Apellidos	Cargo
Elaborado por:		
1	Juan Carlos Sánchez Chunque	Miembro del Equipo de CSIRT-MUNICAJ
2	Carlos Alfonso Perez Cerna	Miembro del Equipo de CSIRT-MUNICAJ
3	Cesar Martín Barrantes Guzmán	Miembro del Equipo de CSIRT-MUNICAJ
4	Omar Enrique Toribio Cueva	Miembro del Equipo de CSIRT-MUNICAJ
5	Wilson Becerra Pérez	Miembro del Equipo de CSIRT-MUNICAJ
Revisado por:		
1	Ing. Jorge Rodrigo Lezama Bazán	Jefe de la Oficina de Tecnologías de la Información

Av. Alameda de los Incas
Cajamarca - Perú
076 602660 - 076 602661
contactenos@municaj.gob.pe

Índice

Av. Alameda de los Incas
Cajamarca - Perú
076 602660 - 076 602661
contactenos@municaj.gob.pe

1. FINALIDAD

El presente Plan de Contingencia Informático describe las acciones a seguir para prepararse o responder eficientemente a eventos que afecten o interrumpan el funcionamiento los sistemas de información y la infraestructura tecnológica que son gestionados por la Oficina de Tecnologías de la Información de la Municipalidad Provincial de Cajamarca, asegurando finalmente la confidencialidad, integridad y disponibilidad de la información.

2. OBJETIVOS

2.1. Objetivo General

- Garantizar la continuidad operativa de los sistemas de información y la infraestructura tecnológica para el normal desarrollo de actividades de la Municipalidad Provincial de Cajamarca.

2.2. Objetivos Específicos

- Identificar amenazas a los sistemas de información y la infraestructura tecnológica.
- Identificar escenarios de riesgos.
- Establecer planes de contingencia por amenaza o evento.
- Proteger la infraestructura tecnológica y los sistemas de información de la organización.
- Establecer el RTO (Recovery Time Objective), periodo de tiempo dentro del cual se va a restaurar los servicios después de una interrupción.
- Establecer RPO (Recovery Point Objective) tiempo al que una organización está dispuesta a aceptar la pérdida de datos durante una interrupción.

3. ALCANCE

El presente Plan de Contingencias Informático es de cumplimiento obligatorio de todos los trabajadores de la Municipalidad Provincial de Cajamarca.

4. BASE LEGAL

- Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado.
- Ley N° 29733, Ley de Protección de Datos Personales.
- Ley N° 31572, Ley del Teletrabajo.
- Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital.

Av. Alameda de los Incas
Cajamarca - Perú
076 602660 - 076 602661
contactenos@municaj.gob.pe

- Decreto de Urgencia N° 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital.
- Decreto de Urgencia N° 007-2020-PCM, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.
- Decreto Supremo N° 118-2018-PCM, que declara de interés nacional las estrategias, acciones, actividades e iniciativas para el desarrollo del gobierno digital, la innovación y la economía digital en el Perú con enfoque territorial.
- Decreto Supremo N° 029-2021-PCM, Decreto Supremo que aprueba el Reglamento del Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo.
- Decreto Supremo N° 157-2021-PCM, Reglamento del Decreto de Urgencia N° 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital. Decreto Supremo que aprueba el Reglamento del Decreto de Emergencia N° 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital, Decreto Supremo N° 157-2021-PCM.
- Decreto Supremo N° 103-2022-PCM, Decreto Supremo que aprueba la Política Nacional de Modernización de la Gestión Pública al 2030.
- Decreto Supremo N° 003-2013-JUS, que aprueba el Reglamento de la Ley Nº 29733, Ley de Protección de Datos Personales.
- Decreto Supremo N° 002-2023-TR, Decreto Supremo que aprueba el Reglamento de la Ley N° 31572, Ley del Teletrabajo.
- Decreto Supremo N° 026-2016-PCM que aprueba medidas para el fortalecimiento de la infraestructura oficial de firma electrónica y la implementación progresiva de la firma digital en el Sector Público y Privado.
- Decreto Supremo N° 052-2008-PCM, que aprueba el Reglamento de la Ley de Firmas y Certificados Digitales.
- Resolución Ministerial N° 004-2016-PCM, Aprueba el uso obligatorio de la Norma Técnica Peruana “NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición”, en todas las entidades integrantes del Sistema Nacional de Informática.
- Resolución Ministerial Nº 119-2018-PCM, que dispone la creación de un Comité de Gobierno Digital en cada entidad de la Administración Pública.

Av. Alameda de los Incas
Cajamarca - Perú
076 602660 - 076 602661
contactenos@municaj.gob.pe

- Resolución Ministerial Nº 087-2019-PCM, que aprueba disposiciones sobre la conformación y funciones del Comité de Gobierno Digital.
- Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD, que establece la implementación y mantenimiento del Sistema de Seguridad de la Información en las Entidades Públicas.
- Resolución Directoral N° 022-2022-INACAL/DN, que aprueba, entre otras, la Norma Técnica Peruana NTP-ISO/IEC 27001:2022 Seguridad de la Información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información. Requisitos. 3ra. Edición. Reemplaza a la NTP-ISO/IEC 27001:2014.
- Ordenanza Municipal N° 842-CMPC, que aprueba el Reglamento de Organización y Funciones (ROF) de la Municipalidad Provincial de Cajamarca.
- Resolución de Alcaldía N.° 128-2024, que aprueba el Plan Estratégico Institucional 2024-2027 de la Municipalidad Provincial de Cajamarca.
- Resolución de Alcaldía N° 410-2023-A, que aprueba el Plan de Gobierno y Transformación Digital 2023 – 2026 de la Municipalidad Provincial de Cajamarca.
- Resolución de Alcaldía N° 408-2023-A, que designa el Oficial de Seguridad y Confianza Digital de la Municipalidad Provincial de Cajamarca 2023.

5. ABREVIATURAS Y DEFINICIONES

5.1. Abreviaturas

MPC: Municipalidad Provincial de Cajamarca.

OTI: Oficina de Tecnologías de la Información.

WAF: Web Application Firewall

5.2. Definiciones

Amenaza:

Cualquier cosa que pueda interferir con el funcionamiento adecuado de una equipo informático, o causar la difusión no autorizada de información. Ejemplo: Fallas de suministro eléctrico, virus, saboteadores o usuarios descuidados.

Av. Alameda de los Incas
Cajamarca - Perú
076 602660 - 076 602661
contactenos@municaj.gob.pe

Ataque de Denegación de Servicio:

Acción o evento que busca interrumpir el funcionamiento normal de un sistema informático o la conectividad de una red, o que intenta acceder de manera no autorizada a información confidencial.

Base de Datos:

Conjunto de datos organizados y relacionados entre sí, almacenados de forma independiente de los programas que los utilizan. Una base de datos también se define como un conjunto de archivos interrelacionados gestionados por un Sistema de Gestión de Bases de Datos (DBMS).

Contingencia:

Interrupción de la continuidad de las operaciones de la entidad que afecta significativamente el desarrollo normal de un servicio crítico. Esto puede deberse a la falla de uno o varios componentes o a la interrupción no planificada de una tarea.

Datos:

Hechos y cifras que, al ser procesados, se convierten en información. Aunque a menudo se utilizan como sinónimos, "datos" se refiere a la forma más básica de información. Los datos pueden presentarse en diversas formas: campos, registros, archivos, bases de datos, textos, hojas de cálculo, imágenes, videos, entre otros

Fallo de Suministro Eléctrico:

Se refiere al corte de energía eléctrica o entrega intermitente, puede causar daño a los equipos, sobre todo a los servidores que manejan información continuamente.

Incendio

Aunque la probabilidad de un incendio grave es baja, las consecuencias potenciales serían significativas. Por ello, es esencial estar preparados para gestionar situaciones de gran magnitud que puedan ocasionar graves pérdidas.

Incidente

Es el resultado de la materialización de una amenaza o de un ataque, como fallas de suministro eléctrico o intentos de borrar un archivo protegido.

Av. Alameda de los Incas
Cajamarca - Perú
076 602660 - 076 602661
contactenos@municaj.gob.pe

Integridad

Se refiere a la conservación de los datos tal como fueron ingresados en un sistema. Las técnicas de integridad previenen la introducción de valores incorrectos debido a errores de software, fallas del sistema, hardware o errores humanos. El concepto abarca tanto la precisión y fiabilidad de los datos como la confidencialidad en su manejo.

Seguridad:

Conjunto de medidas destinadas a proteger los datos o información de modificaciones, destrucciones o divulgaciones no autorizadas, ya sean accidentales o intencionales.

6. MARCO TEÓRICO

6.1. Plan de Contingencia Informático

Este documento compila una serie de procedimientos alternativos diseñados para asegurar la continuidad de los servicios de Tecnologías de Información cuando estos se vean afectados por incidentes internos o externos a la organización. El Plan de Contingencia busca minimizar el impacto de dichos incidentes, permitiendo reanudar las operaciones de manera eficiente y oportuna. El plan se estructura en tres etapas clave:

- **Prevención**: Acciones proactivas para mitigar el riesgo de incidentes.
- **Emergencia**: Respuesta inmediata durante la ocurrencia del incidente.
- **Recuperación**: Estrategias para restaurar el estado normal posterior a la contingencia.

6.2. Plan de prevención

Este plan consiste en un conjunto de acciones, decisiones y verificaciones orientadas a prevenir la ocurrencia de eventos adversos, reduciendo y mitigando su probabilidad en los factores identificados. Es la parte principal del Plan de Contingencia, ya que al disminuir las probabilidades de contingencias, se minimiza el impacto en las operaciones.

6.3. Plan de emergencia

Es un conjunto detallado de acciones a implementar inmediatamente ante la aparición de un incidente, activando mecanismos alternos que suplen las actividades normales cuando estas no

Av. Alameda de los Incas
Cajamarca - Perú
076 602660 - 076 602661
contactenos@municaj.gob.pe

están disponibles. Las acciones deben estar claramente definidas y ser fácilmente comprensibles para el personal encargado de la contingencia, garantizando una respuesta efectiva y coordinada.

6.4. Plan de recuperación

Este plan abarca las acciones necesarias para restablecer de manera oportuna la capacidad operativa, los procesos y los recursos del servicio que fueron impactados por un evento de contingencia.

6.5. Plan de pruebas

Este plan incluye una serie de pruebas diseñadas para evaluar aspectos específicos del sistema. Cada prueba debe definir claramente los objetivos, los criterios de medición, el procedimiento a seguir, y los resultados esperados, asegurando así la efectividad y fiabilidad del Plan de Contingencia.

7. METODOLOGÍA

Para el desarrollo del presente Plan de Contingencia Informático se ha tomado las siguientes 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

7.1. Fase 1: Planificación

7.1.1. Diagnóstico

La Municipalidad Provincial de Cajamarca cuenta con las siguientes normas, procedimientos y controles referente a seguridad de la información:

a) Procedimiento de gestión de copias de respaldo.
b) Directiva para el uso de las computadoras, internet y correo electrónico.

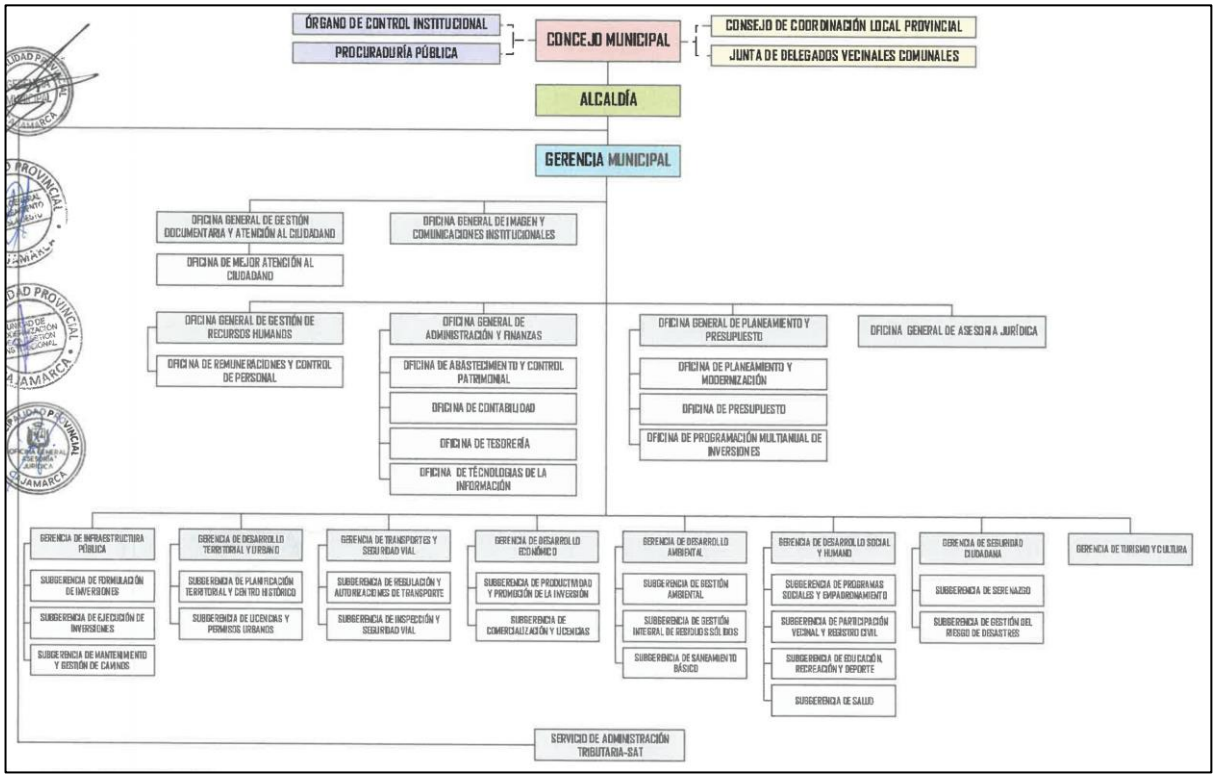
Sin embargo, ninguno de estos documentos está probado formalmente.

Av. Alameda de los Incas
Cajamarca - Perú
076 602660 - 076 602661
contactenos@municaj.gob.pe

7.1.2. Marco Institucional

La Municipalidad Provincial de Cajamarca es el gobierno local de la provincia de Cajamarca, encargada de promover el desarrollo integral de la Provincia de Cajamarca; impulsando un gobierno abierto e inclusivo, a través de la entrega de servicios municipales de calidad y oportunos. En la Figura 1 describe su estructura orgánica:

Figura 1. Estructura Orgánica de la MPC



Fuente: Ordenanza Municipal 842-CMPC, que aprueba el Reglamento de Organización y Funciones (ROF) y Estructura Orgánica de la MPC.

7.1.3. Oficina de Tecnologías de la Información - OTI

La Oficina de Tecnologías de Información es la unidad orgánica responsable de coordinar, organizar, ejecutar y controlar la implementación, desarrollo y mantenimiento de los sistemas de la municipalidad, así mismo promover el máximo acceso y uso de la tecnología de la información por parte de los ciudadanos e integrantes de la gestión municipal.

Son funciones de la Oficina de Tecnologías de Información:

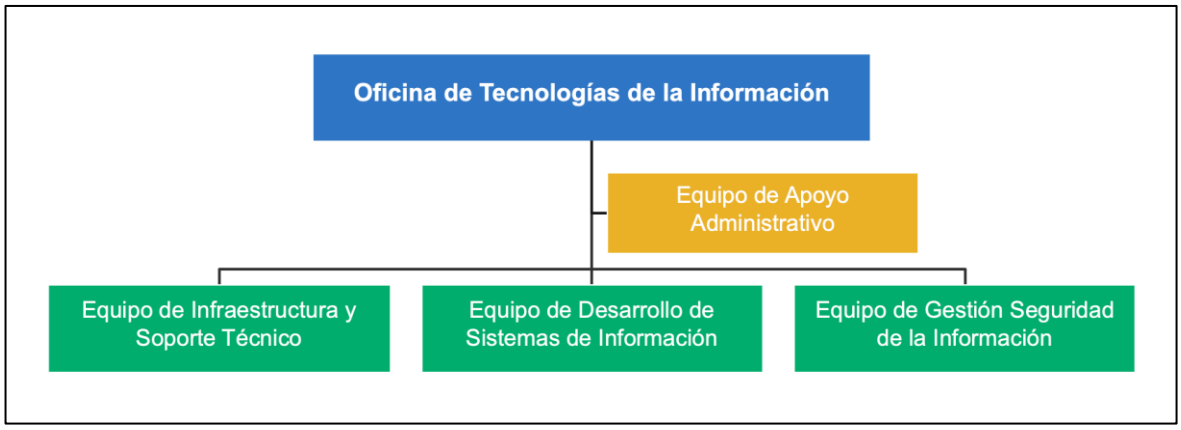
c) Formular, proponer y ejecutar el plan de gobierno digital en concordancia con los objetivos estratégicos institucionales y las necesidades de los órganos de la entidad.

Av. Alameda de los Incas
Cajamarca - Perú
076 602660 - 076 602661
contactenos@municaj.gob.pe

d) Formular, proponer, ejecutar y evaluar los planes informáticos en concordancia con los objetivos institucionales y necesidades de los órganos de la entidad.
e) Identificar y evaluar necesidades y oportunidades de implementación de las Tecnologías de la Información y Comunicaciones a nivel institucional.
f) Cumplir con las normas, estándares y directivas emitidas por el ente rector del Sistema Nacional de Transformación Digital.
g) Elaborar y actualizar directivas, metodologías y estándares para la gestión de los recursos informáticos.
h) Administrar los recursos informáticos, así como proveer el soporte técnico requerido para los usuarios y recursos.
i) Promover y coordinar acciones con los demás órganos para la adecuada gestión de la seguridad de la información.
j) Asesorar con herramientas informáticas y necesidades de capacitación en acciones de transparencia, gobierno digital, entre otras, que permitan mejorar las intervenciones de la municipalidad.
k) Emitir opinión técnica en el ámbito de su competencia.
l) Otras funciones que le asigne el Jefe de la Oficina General de Administración y Finanzas dentro del ámbito de sus competencias y aquellas que le sean dadas por normativa expresa.

La Oficina de Tecnologías de Información, no tiene una estructura interna formal, que haya sido definida en algún documento aprobado, si no que, como muestra la Figura 2, se organiza de manera informal en 4 equipos:

Figura 2. Estructura Interna de la Oficina de Tecnologías de la Información de la MPC

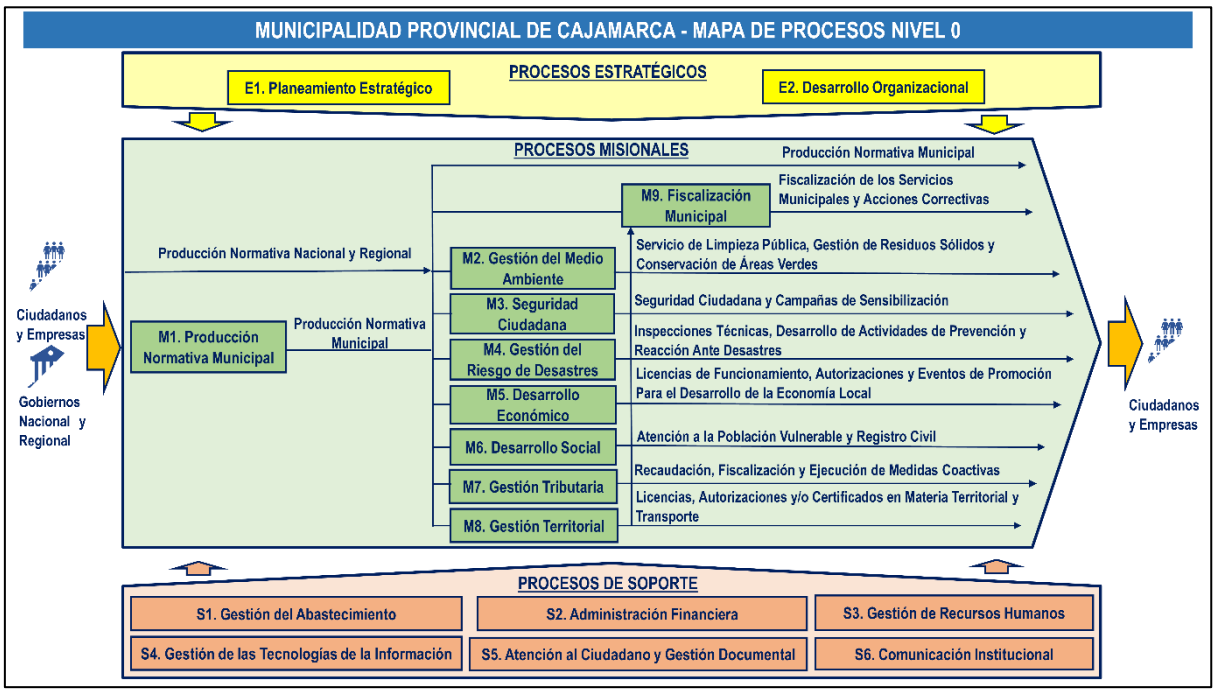


Av. Alameda de los Incas
Cajamarca - Perú
076 602660 - 076 602661
contactenos@municaj.gob.pe

7.1.4. Procesos de la entidad

La Figura 3 visualiza el Mapa de Procesos de la entidad, que cuenta con 2 proceso estratégicos, 9 misionales y 6 de soporte:

Figura 3. Mapa de Procesos de la MPC



Fuente: Oficina de Modernización de la MPC.

La Tabla 1 lista los procesos y su relación con los sistemas de información en funcionamiento en la entidad.

Tabla 1. Procesos relacionados con sistemas de información

Tipo de Proceso	Proceso	Sistema de Información
ESTRATÉGICO	E1. Planeamiento Estratégico	
	E2. Desarrollo Organizacional	
MISIONAL	M1. Producción Normativa Municipal	
	M2. Gestión de Medio Ambiente	• Sistema de JASS • Sistema de Registro de Canes
	M3. Seguridad Ciudadana	
	M4. Gestión del Riesgo de Desastres	
	M5. Desarrollo Económico	• Sistema de Licencias de Funcionamiento

Av. Alameda de los Incas
Cajamarca - Perú
076 602660 - 076 602661
contactenos@municaj.gob.pe

	M6. Desarrollo Social	• Sistema de Carnet Sanitario • Sistema de Fichas de empadronamiento para personas con discapacidad - OMAPED
	M7. Gestión Tributaria	• Sistema de Facturación Web
	M8. Gestión Territorial	• Sistema de TUC's • Sistema de Infracciones de Tránsito
	M9. Fiscalización Municipal	• Sistema de Gestión de expedientes de Procuraduría
SOPORTE	S1. Gestión de Abastecimiento	• Módulo de Gestión de Combustible
	S2. Administración Financiera	• SIGA • SIAF • Sistema de Cheques
	S3. Gestión de Recursos Humanos	• Sistema Integrado de Recursos Humanos • Sistema de Licencias y Vacaciones • Sistema de Convocatorias • Sistema de Consultas PIDE • Sistema de Asistencia del Trabajador • Sistema de Gestión de Relojes Biométricos faciales • Sistema de Carga de Marcaciones de Asistencia Relojes Dactilares
	S4. Gestión de Tecnologías de la Información	• Sistema de Mesa de Ayuda • Panel de Aplicaciones • Archivos Públicos • Portal de Transparencia (NO MEF)
	S5. Atención al Ciudadano y Gestión Documental.	• Sistema de Casilla Electrónica • Sistema de Gestión Documentaria Cero Papel
	S6. Comunicación Institucional	• Correo Institucional Zimbra

7.1.5. Organización operativa del Plan de Contingencia Informática

La organización del plan de continencia estará integrada por un Coordinador, quien será el jefe de la Oficina de Tecnologías de la Información, y tres equipos, de prevención, emergencia y restauración como se detalla en la figura:

Av. Alameda de los Incas
Cajamarca - Perú
076 602660 - 076 602661
contactenos@municaj.gob.pe

Figura 4. Organización operativa del Plan de Contingencia Informática

7.1.6. Roles, funciones y responsabilidades

a) Coordinador: Jefe de la Oficina de Tecnologías de la Información

Está representado por el Jefe de la Oficina de Tecnologías de la Información y tiene las siguientes funciones:

- Coordinar, dirigir y decidir sobre las acciones o estrategias a seguir en escenarios específicos de contingencia.
- Determinar cuándo activar el Plan de Contingencia Informático.
- Monitorear, supervisar y vigilar la recuperación de la infraestructura tecnológica en el Centro de Datos.
- Contactar a los proveedores para el reemplazo de hardware, software y/o activación de servicios afectados.
- Evaluar la extensión de la contingencia y sus posibles consecuencias sobre la infraestructura tecnológica.
- Notificar y mantener informada a la Alta Dirección sobre el evento de desastre, el progreso de la recuperación y cualquier problema que surja durante la ejecución del plan.
- Declarar el fin de la ejecución del Plan de Contingencia Informático cuando las operaciones del Centro de Datos hayan sido restablecidas.

Av. Alameda de los Incas
Cajamarca - Perú
076 602660 - 076 602661
contactenos@municaj.gob.pe

b) Equipo de Prevención

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

A continuación, se detallan las funciones por cada integrante del equipo de prevención:

El **Coordinador de Gestión Seguridad de la Información** tiene las siguientes funciones:

- Monitorear la red y el funcionamiento de los servidores del Centro de Datos y la operatividad de los servicios digitales.
- Realizar las copias de respaldo por base de datos, código fuente, ejecutables y archivos de los sistemas de información.
- Monitorear incidencias de seguridad de la información.
- Realizar análisis de vulnerabilidades de sistemas de información, sistemas operativos y otros.
- Desarrollar capacitaciones de sensibilización sobre seguridad de la información y buenas prácticas en el uso de los sistemas informáticos.

El **Coordinador de Infraestructura y Soporte Técnico** tiene las siguientes funciones:

- Monitorear los equipos de redes y comunicaciones de toda la entidad.
- Mantener actualizado el inventario de infraestructura tecnológica de la entidad.
- Solicitar y supervisar el mantenimiento del sistema de refrigeración del Centro de Datos.
- Verificar el estado de las garantías y/o vigencias tecnológicas de los equipos informáticos de usuario final.

El **Coordinador de Desarrollo de Sistemas de Información** tiene las siguientes funciones:

- Mantener actualizado el inventario de sistemas de información de la entidad.
- Mantener actualizado el código fuente y ejecutables en el sistema de control de versiones.
- Realizar la documentación, consolidación y validación de los manuales de los sistemas en producción.
- Realizar periódicamente las pruebas de restauración de los sistemas de información en producción de la entidad.

Av. Alameda de los Incas
Cajamarca - Perú
076 602660 - 076 602661
contactenos@municaj.gob.pe

- Realizar las pruebas de restauración de bases de datos y elaborar el informe de las actividades realizadas.

c) Equipo de Emergencia

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

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

El **Coordinador de Gestión Seguridad de la Información** tiene las siguientes funciones:

- Notificar el desastre o incidencia al coordinador de contingencia informática.
- Ejecutar las actividades de emergencia detalladas en el Plan de Contingencia Informático de acuerdo con el escenario de riesgo presentado.
- Comunicar al Coordinador de contingencia informática las acciones de emergencia ejecutadas.
- Realizar la evaluación de las condiciones de la información almacenada en los diferentes sistemas y bases de datos.

El **Coordinador de Infraestructura y Soporte Técnico** tiene las siguientes funciones:

- Realizar la evaluación y evaluación preliminar de la infraestructura tecnológica del Centro de Datos y los equipos de redes de la entidad.
- Ejecutar las acciones de emergencia detalladas en el Plan de contingencia Informático de acuerdo con el escenario de riesgo presentado.
- Apoyar en las acciones que se requieran.

El **Coordinador de Desarrollo de Sistemas de Información** tiene las siguientes funciones:

- Realizar las labores de verificación y validación de operación relacionadas con los sistemas de información y a las bases de datos instalados en el Centro de Datos.
- Realizar la evaluación de las condiciones de los aplicativos informáticos y sistemas de información.
- Apoyar en las acciones que se requieran.

Av. Alameda de los Incas
Cajamarca - Perú
076 602660 - 076 602661
contactenos@municaj.gob.pe

d) Equipo de Restauración

Este equipo es el encargado de ejecutar las acciones necesarias luego de que el siniestro o desastre esté controlado. Su finalidad es restituir en el menor tiempo posible el funcionamiento de los equipos tecnológicos y recuperar el estado de los servicios informáticos de la MPC.

El **Coordinador de Gestión Seguridad de la Información** tiene las siguientes funciones:

- Verificar la operatividad de los servicios digitales de la entidad.
- Restaurar las copias de respaldo de las bases de datos correspondientes establecidas en el Plan de Contingencia Informático, en caso sea necesario.
- Restaurar o desplegar los sistemas de información establecidas en el Plan de Contingencia Informático, en caso sea necesario.
- Validar y actualizar, en caso corresponda, la información documentada del Plan de Contingencia Informático de acuerdo con el escenario de riesgo presentado.
- Notificar las actividades de recuperación ejecutadas al Coordinador de contingencia informática.

El **Coordinador de Infraestructura y Soporte Técnico** tiene las siguientes funciones:

- Iniciar el proceso de recuperación de la infraestructura tecnología del Centro de Datos y los equipos de redes de la entidad.
- Elaborar un informe técnico que incluya las acciones de recuperación de la infraestructura tecnología del Centro de Datos y los equipos de redes de la entidad.

El **Coordinador de Desarrollo de Sistemas de Información** tiene las siguientes funciones:

- Verificar el funcionamiento de las bases de datos institucionales.
- Verificar el correcto funcionamiento de los sistemas de información.

7.2. Fase 2: Determinación de vulnerabilidades y escenarios de contingencia

En esta fase se han identificaron las amenazas a los sistemas de información y los equipos de tecnologías de la información, los controles existentes, y se identificaron los riesgos asociados, que derivaron en escenarios de riesgo para la entidad.

Av. Alameda de los Incas
Cajamarca - Perú
076 602660 - 076 602661
contactenos@municaj.gob.pe

7.2.1. Identificación de amenazas

Se ha identificado las amenazas que pueden afectar a los sistemas de información, la infraestructura del Centro de Datos y los equipos de redes que soportan la red interna de la entidad. Las que se detalla en la Tabla 2.

Tabla 2. Lista de Amenazas

Ítem	Amenaza	Tipo
1	Terremoto	Natural
2	Inundación	Natural
3	Incendio	Natural
4	Corte de internet	Tecnológico
5	Fallo del suministro eléctrico	Tecnológico
6	Falla de Infraestructura del Centro de Datos	Tecnológico
7	Falla de equipos de redes	Tecnológico
8	Falla de sistemas de Información	Tecnológico
9	Ciberataque	Tecnológico
10	Ataque físico al Centro de Datos o equipos de redes	Físico

7.2.2. Identificación de controles existentes

En la Tabla 3, se detalla controles existentes en la entidad:

Tabla 3. Controles existentes

Ítem	Descripción
1	Acuerdos de niveles de servicio con proveedor de servicio de Internet
2	Cámaras de vigilancia en el exterior del Centro de Datos.
3	Equipo informático de seguridad perimetral.
4	Equipo informático de Antispam.
5	Sistema contra incendios en el Centro de Datos.
6	Respaldo de información en Storage en el Centro de Datos.
7	Respaldo de información en NAS fuera del Centro de Datos.

Av. Alameda de los Incas
Cajamarca - Perú
076 602660 - 076 602661
contactenos@municaj.gob.pe

8	Solución antivirus instalada en los servidores y computadoras.
9	Actualización mensual de parches de seguridad de sistemas operativos en servidores.
10	Uso de conexiones remotas seguras con VPN.
11	Sistema de monitorización de redes.
12	Sistema de administración de eventos e información de seguridad.

7.2.3. Evaluación del nivel de riesgo

La probabilidad de ocurrencia se refiere a la posibilidad de que una amenaza se materialice y afecte a sistemas o equipos. Para el presente Plan, se ha clasificado la probabilidad de ocurrencia de acuerdo con los antecedentes, como se puede observar en la Tabla 4:

Tabla 4. Clasificación de Probabilidad de Ocurrencia

Probabilidad	Valor	Descripción
Baja	4	Se puede presentar al menos una vez en 5 años o más.
Media	6	Se puede presentar al menos una vez en 3 años.
Alta	8	Se puede presentar al menos una vez al año.
Muy Alta	10	Se puede presentar al más de una vez al año.

Para el impacto, se ha clasificado de acuerdo con la gravedad, como se detalla en la Tabla 5:

Tabla 5. Clasificación del Impacto

Impacto	Valor	Descripción
Bajo	4	No representa un impacto importante. Se cuenta con controles suficientes que reducen el impacto o se puede prescindir del servicio por un tiempo limitado.
Medio	6	El impacto sobre la confidencialidad, integridad y disponibilidad de la información es limitado en tiempo y alcance. Su efecto afecta a un proceso de soporte o actividad específica que puede resolverse en un corto plazo.
Alto	8	Impacta en forma grave a un área o servicio específico, se puede llegar a comprometer información confidencial, paralizar o retrasar procesos claves por un tiempo considerable.
Muy Alto	10	Impacta en forma severa a toda la MPC. Compromete la confidencialidad o integridad de información crítica o la continuidad de las operaciones por paralización de los servicios más allá de los tiempos tolerables por la entidad.

Av. Alameda de los Incas
Cajamarca - Perú
076 602660 - 076 602661
contactenos@municaj.gob.pe

La identificación del nivel de riesgo se ha considerado la matriz de la Tabla 6:

Tabla 6. Matriz del nivel de riesgo

NIVEL DE RIESGO (Probabilidad de ocurrencia por impacto)			***Impacto***			
			Bajo	Medio	Alto	Muy Alto
			4	6	8	10
Probabilidad de ocurrencia	Bajo	4	16 (bajo)	24 (bajo)	32 (medio)	40 (medio)
	Medio	6	24 (bajo)	36 (medio)	48 (alto)	60 (alto)
	Alto	8	32 (medio)	48 (alto)	64 (alto)	80 (muy alto)
	Muy Alto	10	40 (medio)	60 (alto)	80 (muy alto)	100 (muy alto)

La interpretación de cada cuadrante de calor o nivel de riesgo de la amenaza en evaluación se detalla en la Tabla 7:

Tabla 7. Interpretación del nivel de riesgo

Valor	**Descripción**
Bajo	Riesgo aceptable, sin revisión y no se requieren acciones.
Medio	Riesgo aceptable con revisión de la dirección, y se evalúa tomar acciones.
Alto	Riesgo no aceptable, se requiere de una acción correctiva, pero se permite planificar plazos y compromisos.
Muy Alto	Riesgo no aceptable, se requiere acción correctiva inmediata.

En la Tabla 8 se evalúa los riesgos asociados con cada amenaza, se asigna su probabilidad y su impacto, y se obtiene el nivel de cada riesgo:

Tabla 8. Resultado de la evaluación de riesgos

Ítem	**Amenaza**	**Riesgos asociados**	**Probabilidad**	**Impacto**	**Nivel de riesgo**
1	Terremoto	Indisponibilidad del Centro de Datos	4	10	40
2	Inundación	Indisponibilidad del Centro de Datos	4	10	40
3	Incendio	Indisponibilidad del Centro de Datos	4	10	40

Av. Alameda de los Incas
Cajamarca - Perú
076 602660 - 076 602661
contactenos@municaj.gob.pe

4	Corte de servicio de internet	Falla de Sistemas de Información *por falla de conexión a internet*	6	6	36
5	Corte de servicio de internet	Indisponibilidad del servicio de firma digital *por falla de conexión a internet*	6	6	36
6	Corte de servicio de internet	Desconexión de red de sectores de la entidad *por falla en los enlaces de comunicación dependientes de servicio de internet*	4	8	32
7	Corte de servicio de internet	Indisponibilidad de Sistemas de Información desde el internet *por falla de conexión a internet*	6	10	60
8	Fallo del suministro eléctrico	Indisponibilidad del Centro de Datos *por corte de suministro eléctrico.*	10	10	100
9	Fallo del suministro eléctrico	Daño de Infraestructura del Centro de Datos *por corte intempestivo de suministro eléctrico*	8	10	80
10	Fallo del suministro eléctrico	Daño de equipos de redes *por corte intempestivo de suministro eléctrico*	10	8	80
11	Falla de Infraestructura del Centro de Datos	Indisponibilidad del Centro de Datos *por falla del sistema de refrigeración*	10	10	100
12	Falla de Infraestructura del Centro de Datos	Indisponibilidad del Centro de Datos *por falla del switch core*	10	10	100
13	Falla de Infraestructura del Centro de Datos	Indisponibilidad de Sistemas de Información desde el internet *por falla del Firewall*	6	10	60
14	Falla de Infraestructura del Centro de Datos	Corte de acceso a internet *por falla del Firewall*	4	10	40
15	Falla de Infraestructura del Centro de Datos	Indisponibilidad de Sistemas de Información *por falla de servidores*	10	10	100
16	Falla de equipos de redes	Indisponibilidad de Sistemas de Información en sectores de la entidad *por falla del equipo de redes*	10	6	60
17	Falla de sistemas de Información	Indisponibilidad de Sistemas de Información *por bugs de sistemas*	6	6	36
18	Falla de sistemas de Información	Indisponibilidad de Sistemas de Información *por error de configuración en producción*	4	8	32
19	Falla de sistemas de Información	Indisponibilidad de Sistemas de Información *por falla de servicios complementarios*	6	6	36
20	Ciberataque	Perdida, robo o modificación de datos *por explotación de vulnerabilidades de sistemas de información*	4	10	40
21	Ciberataque	Perdida, robo o modificación de datos *por explotación de errores de configuración*	4	10	40
22	Ciberataque	Pérdida, robo o modificación de datos *por ataque de malware*	4	10	40
23	Ciberataque	Secuestro de información *por ataque de Ransomware*	4	10	40

Av. Alameda de los Incas
Cajamarca - Perú
076 602660 - 076 602661
contactenos@municaj.gob.pe

24	Ciberataque	Acceso no autorizado a Correo Electrónico, Suplantación de Identidad y propagación de correos *por ataque de phishing*	10	6	60
25	Ciberataque	Indisponibilidad de Sistemas de Información *por ataque de Denegación de Servicio*	4	10	32
26	Ciberataque	Obtención de credenciales de acceso *por ataque de ingeniería social*	4	10	40
27	Ciberataque	Perdida, robo o modificación de datos *por ataque de Zero-Day*	4	10	40
28	Ataque físico al Centro de Datos o equipos de redes	Daño o robo de infraestructura del Centro de Datos o equipos de redes *por sabotaje de trabajadores o extrabajadores*	4	10	40
29	Ataque físico al Centro de Datos o equipos de redes	Daño a infraestructura del Centro de Datos o equipos de redes *por vandalismo*	4	10	40

7.2.4. Escenarios de riesgo

Teniendo en considerando los resultados de evaluación de nivel de riesgo, se ha determinado los escenarios de alto y muy alto riesgo contenidos en la Tabla 9:

Tabla 9. Escenarios de alto y muy alto riesgo

Ítem	Escenario	Descripción
1	Indisponibilidad de Sistemas de Información desde el internet *por falla de conexión a internet*	Una interrupción en la conexión a internet impide el acceso externo a los sistemas de información de la entidad, afectando los servicios utilizados por los ciudadanos.
2	Indisponibilidad del Centro de Datos *por corte de suministro eléctrico.*	La interrupción del suministro eléctrico deja fuera de servicio el Centro de Datos, provocando la caída de todos los sistemas de información y servicios alojados en él.
3	Daño de Infraestructura del Centro de Datos *por corte intempestivo de suministro eléctrico*	Un corte abrupto de energía puede dañar el sistema de refrigeración, switch core, firewall, servidores u otros equipos, resultando en pérdida de datos e indisponibilidad de sistemas.
4	Daño de equipos de redes *por corte intempestivo de suministro eléctrico*	Daños en equipos de red por cortes eléctricos repentinos pueden ocasionar perdida de conectividad y acceso a sistemas de información en sectores de la entidad.
5	Indisponibilidad del Centro de Datos *por falla del sistema de refrigeración*	El fallo del sistema de enfriamiento del Centro de Datos provoca un aumento de temperatura, forzando el apagado de equipos para prevenir daños por sobrecalentamiento.
6	Indisponibilidad del Centro de Datos *por falla del switch core*	La falla del switch principal interrumpe el tráfico de red interna y la conexión a internet, causando la caída de todos los sistemas de información de la entidad.

Av. Alameda de los Incas
Cajamarca - Perú
076 602660 - 076 602661
contactenos@municaj.gob.pe

7	Indisponibilidad de Sistemas de Información desde el internet *por falla del Firewall*	Un fallo en el firewall bloquea conexiones legítimas, impidiendo el acceso externo a los sistemas de información.
8	Indisponibilidad de Sistemas de Información *por falla de servidores*	La falla de servidores que alojan sistemas de información interrumpe el acceso para usuarios internos y externos.
9	Indisponibilidad de Sistemas de Información en sectores de la entidad *por falla del equipo de redes*	Fallos en equipos de red provocan la pérdida de acceso a los sistemas de información en sectores de la entidad.
10	Acceso no autorizado a Correo Electrónico, Suplantación de Identidad y propagación de correos *por ataque de phishing*	Un ataque de phishing exitoso puede comprometer cuentas de correo electrónico, permitiendo la suplantación de identidades y el envío de correos maliciosos, lo que podría resultar en la inclusión del dominio de la entidad en listas negras de servicios de correo.

7.3. Fase 3: Estrategias del Plan de Contingencias

A continuación, se presentan estrategias de recuperación en caso ocurra un escenario de riesgo.

7.3.1. Estrategias de prevención

- Evaluar la migración de la infraestructura tecnológica a la cloud computing, que garantice disponibilidad, integridad y confidencialidad de la información.
- Evaluar la implementación de un generador eléctrico para asegurar la continuidad del suministro energético en caso de fallas, para el Centro de Datos.
- Asegurar el buen funcionamiento de los sistemas críticos mediante mantenimientos preventivos programados, incluyendo el sistema de detección y extinción de incendios, sistema de refrigeración, UPS y servidores.
- Realizar revisiones semestrales de obsolescencia tecnológica y programación de renovación a los equipos del Centro de Datos.
- Implementar y mantener sistemas de seguridad física en el Centro de Datos, como control de acceso, vigilancia,
- Implementar equipos redundantes para la seguridad perimetral (Firewalls) y el Switch Core.
- Realizar copias de respaldo periódicas de sistemas de información, configuraciones, equipos de redes, código fuente, ejecutables, software base y sistemas operativos.
- Evaluar la implementación de un sistema de un sistema de Backups completo.
- Contratar un software antivirus corporativo para proteger servidores y estaciones de trabajo contra software malicioso.
- Implementar un equipo de seguridad de aplicaciones web (WAF).

Av. Alameda de los Incas
Cajamarca - Perú
076 602660 - 076 602661
contactenos@municaj.gob.pe

- Implementar un equipo de administración de ancho de banda.
- Implementar políticas de contraseñas robustas, gestión de privilegios.
- Realizar pruebas periódicas de análisis de vulnerabilidades y hacking ético para garantizar la seguridad de la información.
- Configurar un sistema de alerta para fallas en el suministro eléctrico y cortes del servicio de internet.
- Monitorizar la red, el funcionamiento de los servidores y toda infraestructura tecnológica posible.
- Capacitar regularmente al personal de seguridad de la información y a los trabajadores en buenas prácticas y seguridad informática, asegurando un conocimiento actualizado de las medidas de protección.

7.3.2. Estrategias de emergencia

- Establecer un procedimiento de notificación inmediata de la emergencia a los responsables y partes interesadas, asegurando una comunicación clara y continua con todos los niveles de la organización durante todo el proceso.
- Mantener registros detallados de los incidentes y eventos, así como de las acciones realizadas para su resolución, incluyendo el tiempo necesario para la restauración total o parcial de los servicios.
- Priorizar la restauración de equipos y sistemas de información, recuperando datos desde copias de respaldo para minimizar la pérdida de información, y verificando la integridad de los datos restaurados.
- Realizar pruebas en los sistemas restaurados para asegurar que funcionan correctamente antes de reintegrarlos a la red, garantizando una rápida y efectiva recuperación operativa.

7.3.3. Estrategias de restauración

- Realizar una evaluación detallada de los daños y un análisis de impacto para determinar la gravedad del incidente y sus efectos en la operación.
- Priorizar la restauración de sistemas críticos, asegurando la recuperación de la información más reciente desde copias de respaldo, y reparando o reemplazando hardware dañado para restaurar la funcionalidad completa.
- Restituir el funcionamiento de sistemas de información, servidores, equipos de red y otra infraestructura tecnológica, aplicando parches y actualizaciones necesarios para protegerlos

Av. Alameda de los Incas
Cajamarca - Perú
076 602660 - 076 602661
contactenos@municaj.gob.pe

de vulnerabilidades, y verificando la integridad de los datos y sistemas restaurados para asegurar la ausencia de corrupción o pérdida de información.

- Realizar pruebas de funcionamiento y rendimiento en los sistemas restaurados, garantizando su operatividad óptima antes de su reintegración a la red.
- Implementar un retorno gradual a las operaciones normales, asegurando la completa funcionalidad y seguridad de todos los sistemas.
- Mantener una comunicación clara y continua con todos los niveles de la organización durante todo el proceso de recuperación, y documentar cada paso tomado para referencia futura, auditorías, y revisión.
- Evaluar la eficacia de la respuesta y recuperación, identificando áreas de mejora, y actualizar las políticas, procedimientos de seguridad, y el plan de contingencias basados en las lecciones aprendidas.
- Proporcionar capacitación adicional al personal, enfocándose en la prevención y respuesta efectiva según las lecciones aprendidas.

7.4. Fase 4: Elaboración del Plan de Contingencia

El Plan de Contingencia Informático está alineado con los escenarios de mayor nivel de riesgo, los cuales se abordarán en planes independientes, según se detalla en la Tabla 10 :

Tabla 10. Eventos o amenazas de mayor impacto para el Plan de Contingencia Informatico

Ítem	Escenario	Nivel de riesgo
1	Indisponibilidad de Sistemas de Información desde el internet *por falla de conexión a internet*	Alto
2	Indisponibilidad del Centro de Datos *por corte de suministro eléctrico.*	Muy Alto
3	Daño de Infraestructura del Centro de Datos *por corte intempestivo de suministro eléctrico*	Muy Alto
4	Daño de equipos de redes *por corte intempestivo de suministro eléctrico*	Muy Alto
5	Indisponibilidad del Centro de Datos *por falla del sistema de refrigeración*	Muy Alto
6	Indisponibilidad del Centro de Datos *por falla del switch core*	Muy Alto
7	Indisponibilidad de Sistemas de Información desde el internet *por falla del Firewall*	Alto
8	Indisponibilidad de Sistemas de Información *por falla de servidores*	Muy Alto
9	Indisponibilidad de Sistemas de Información en sectores de la entidad *por falla del equipo de redes*	Alto
10	Acceso no autorizado a Correo Electrónico, Suplantación de Identidad y propagación de correos *por ataque de phishing*	Alto

Av. Alameda de los Incas
Cajamarca - Perú
076 602660 - 076 602661
contactenos@municaj.gob.pe

Aun cuando existen escenarios de alto y muy alto riesgo, para la elaboración de los Planes de Contingencia se han tomado todas las amenazas o eventos que pudieran ocurrir, en la Tabla 11 se detalla la lista planes de contingencia

Tabla 11. Lista de Planes de Contingencia Informático

Ítem	Amenaza	Plan de Contingencia Informático
1	Terremoto	PCI-01
2	Inundación	PCI-02
3	Incendio	PCI-03
4	Corte de internet	PCI-04
5	Fallo del suministro eléctrico	PCI-05
6	Falla de Infraestructura del Centro de Datos	PCI-06
7	Falla de equipos de redes	PCI-07
8	Falla de sistemas de Información	PCI-08
9	Ciberataque	PCI-09
10	Ataque físico al Centro de Datos o equipos de redes	PCI-10

En el Anexo N° 3 se presenta los Formatos de Plan de Contingencia Informático por amenaza o evento, que es el desarrollo de cada Plan de Contingencia Informático

7.5. Fase 5: Definición y ejecución de Plan de pruebas

El plan de pruebas se centra en simular situaciones de contingencia ante incidencias que afecten equipos, información y procesos, replicando escenarios reales en los que los respaldos puedan ser utilizados. Para garantizar la efectividad de la prueba, se diseñará un conjunto de casos de prueba funcionales que serán ejecutados por los equipos operativos de la OTI. Estos equipos se encargarán de probar, verificar y documentar cualquier incidencia que surja durante la prueba, proporcionando retroalimentación para corregir y mejorar el plan.

El Plan de Pruebas incluirá la siguiente información:

- Metodología: Descripción de la prueba a realizar.
- Alcance: Áreas afectadas y personal involucrado.
- Resultados: Observaciones y conclusiones.

Av. Alameda de los Incas
Cajamarca - Perú
076 602660 - 076 602661
contactenos@municaj.gob.pe

En el Anexo 4 se establece Formatos de control y certificación de pruebas de Plan de Contingencia Informático. Las pruebas relacionadas con este plan se deberán ejecutar de forma anual, con el objetivo de evaluar la preparación de la entidad ante posibles siniestros y realizar los ajustes necesarios.

7.6. Fase 6: Implementación del Plan de Contingencia Informático

La implementación del presente plan se realizará a partir del tercer mes de su aprobación. Para tal efecto, el coordinador de la contingencia informática, así como los equipos de prevención, de emergencia y de restauración deben cumplir con lo indicado en el Anexo N° 3, Formatos de Plan de Contingencia Informático por amenaza o evento.

7.7. 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:

- Monitorización de la infraestructura tecnológica del Centro de Datos y equipos de red de la entidad.
- Monitorización de sistemas de información y servicios online.
- Revisión continua del sistema de copias de respaldo (backups).
- Revisión continua de la infraestructura tecnológica del Centro de Datos y equipos de red de la entidad.

Av. Alameda de los Incas
Cajamarca - Perú
076 602660 - 076 602661
contactenos@municaj.gob.pe

ANEXOS

Anexo 1: Sistemas de información clasificadas por prioridad de atención ante recuperación

Ítem	Sistema de Información	Descripción	Unidad Orgánica Usuaria	Motor de DB	Tipo	Prioridad
1	SIAF	Sistema Integrado de Administración Financiera, para hacer certificaciones y devengados para el pago de los bienes y servicios, registro de gastos e ingresos de la institución	Oficina General de Administración y Finanzas	BID/BM	Desktop	1
2	SIGA	Sistema Integrado de Gestión Administrativa, maneja el proceso logístico de las adquisiciones de bienes y servicios	Todas	Microsoft SQL Server	Desktop	1
3	Sistema de Carnet Sanitario	Gestión de carnets sanitarios de atención al público	Subgerencia de Salud	MySQL	Web	1
4	Sistema de Casilla Electrónica	Gestión trámites online por parte de la ciudadanía en general	Oficina de Mejor Atención al Ciudadano	PostgreSQL	Web	1
5	Sistema de Facturación en Escritorio	Emisión de comprobantes de pago	Oficina de Tesorería	MySQL	Desktop	1
6	Sistema de Facturación Web	Emisión de comprobantes de pago	Oficina de Tesorería	MySQL	Web	1
7	Sistema de Gestión Documental MPC	Gestión documental de la entidad de manera digital	Todas	PostgreSQL	Web	1
8	Sistema de Infracciones de Tránsito	Gestión las actas infracciones de tránsito, actas de internamiento, ordenes de pago de multas de infracciones y ordenes de liberación.	Subgerencia de Inspección y Seguridad Vial	MySQL	Web	1
9	Sistema de Licencias de Funcionamiento	Gestión de Licencias de Funcionamiento de Locales Comerciales en la Distrito de Cajamarca.	Subgerencia de Comercialización y Licencias	MySQL	Web	1
10	Sistema de TUC's	Gestión de Tarjetas Únicas de Circulación	Subgerencia de Regulación y Autorizaciones de Transporte	MySQL	Web	1
11	Panel de Aplicaciones	Acceso a los sistemas de información de la entidad	Todas	PostgreSQL	Web	2
12	Sistema de Cheques	Gestión de cheques para los proveedores	Oficina de Tesorería	MySQL	Web	2
13	Sistema de Convocatorias	Publicación de Convocatorias de Personal	Oficina General de Gestión de Recursos Humanos	PostgreSQL	Web	2
14	Sistema de JASS	Gestión de Juntas Administradoras de Agua y Saneamiento	Subgerencia de Saneamiento Básico	MySQL	Web	2
15	Sistema de Mesa de Ayuda - Help Desk	Gestión de tickets de soporte técnico informático	Oficina de Tecnologias de la Información	MySQL	Web	2
16	Sistema de Registro de Canes	Gestión de datos de mascotas caninas	Subgerencia de Gestión Ambiental	MySQL	Web	2
17	Sistema del CAC - Gestión Colas y Tickets	Gestión de tickets de atención al ciudadano	Oficina de Mejor Atención al Ciudadano	MySQL	Web	2
18	Sistema Integrado de Recursos Humanos	Gestión de Planillas, Boletas, Contratos y Control de Personal del Personal	Oficina de Remuneraciones y Control de Personal	PostgreSQL	Web	2
19	Archivos Públicos	Archivos para descarga pública	Todas	PostgreSQL	Web	3

Av. Alameda de los Incas
Cajamarca - Perú
076 602660 - 076 602661
contactenos@municaj.gob.pe

20	Módulo de Carga de Marcaciones de Relojes Biométricos	Procesamiento de marcaciones de relojes sin conectividad a servidor Biotime.	Oficina de Remuneraciones y Control de Personal	PostgreSQL	Desktop	3
21	Módulo de Gestión de expedientes de Procuraduría	Gestión de expedientes en procuraduría	Procuraduría Pública	MySQL	Web	3
22	Portal de Transparencia (NO MEF)	Portal de publicación de resoluciones, directivas y otros, enlazado al Portal de Transparencia Estándar del Estado	Todas	PostgreSQL	Web	3
23	Sistema de Asistencia del Trabajador	Sistema para la consulta marcaciones del trabajador	Todas	PostgreSQL	Web	3
24	Sistema de Boletas Trabajador	Sistema de descargas de Boletas de Pago del trabajador	Oficina de Remuneraciones y Control de Personal	PostgreSQL	Web	3
25	Sistema de Combustible	Gestión de vales de combustible.	Oficina de Abastecimiento y Control Patrimonial	MySQL	Web	3
26	Sistema de Consultas PIDE	Consulta de datos de personas a la RENIEC, propiedades a SUNARP, SUNAT.	Oficina General de Gestión de Recursos Humanos, Oficina General de Asesoría Jurídica	PostgreSQL	Web	3
27	Sistema de Escalafón	Gestión de escalafón de la entidad	Oficina General de Gestión de Recursos Humanos	MySQL	Web	3
28	Sistema de Fichas de empadronamiento para personas con discapacidad - OMAPED	Gestión de fichas de personas con discapacidad	Subgerencia de Programas Sociales y Empadronamiento	PostgreSQL	Web	3
29	Sistema de Gestión de Relojes biométricos - BIOTIME	Sistema de administración de marcaciones de trabajadores de la entidad	Oficina de Remuneraciones y Control de Personal	PostgreSQL	Web	3
30	Sistema de Licencias y Vacaciones	Gestión de licencias y vacaciones de los trabajadores de entidad	Oficina de Remuneraciones y Control de Personal		Web	3
31	Sistema de Patrimonio - SISPAT	Gestión de bienes y asignación de la entidad	Oficina de Abastecimiento y Control Patrimonial	MySQL	Web	3
32	Sistema de Trámite Documentario - Solo Consultas	Sistema de tramites antiguos solo para consulta	Todas	MySQL	Web	3

Av. Alameda de los Incas
Cajamarca - Perú
076 602660 - 076 602661
contactenos@municaj.gob.pe

Anexo 2: Equipos del Centro de Datos clasificados por prioridad de atención ante recuperación

Ítem	Tipo de Equipo	Rol	Descripción	Prioridad
1	Refrigeración	Refrigeración	Equipo de refrigeración y control de temperatura del Centro Datos	1
2	UPS	Energía	Equipo de suministro eléctrico ante falla de suministro externo	1
3	Switch	Switch Core	Equipo de administración y distribución de la red de toda la entidad	2
4	Firewall	Seguridad Perimetral	Equipo de NATEO y filtrado de trafico de red entrante y saliente	2
5	Servidor	Virtualización 01	Máquinas virtuales	3
6	Servidor	Virtualización 02	Máquinas virtuales	3
7	Servidor	Virtualización 03	Máquinas virtuales	3
8	Servidor	Virtualización 05	Máquinas virtuales	3
9	Servidor	Virtualización 06	Máquinas virtuales	3
10	Servidor	Virtualización 07	Máquinas virtuales	3
11	Servidor	Virtualización 08	Máquinas virtuales	3
12	Servidor	Virtualización 09	Máquinas virtuales	3
13	Servidor	Directorio Activo	Directorio Activo	3
14	Servidor	Videovigilancia	Grabación de cámaras de videovigilancia	3
15	Servidor	Backup	Copias de respaldo de base de datos	3
16	Servidor	Telefonía	Telefonía IP	3

Av. Alameda de los Incas
Cajamarca - Perú
076 602660 - 076 602661
contactenos@municaj.gob.pe

Anexo 3: Formatos de Plan de Contingencia Informático por amenaza o evento

PCI-01	Amenaza o evento: Terremoto

1. Procedimiento de Prevención

1.1. Descripción de la Amenaza

Un terremoto es un fenómeno natural impredecible que puede causar daños severos a la infraestructura física del centro de datos, afectando la continuidad operativa de los sistemas de información. Este plan se aplica al Centro de Datos, donde un terremoto puede provocar la pérdida de servicios críticos, fallas en el hardware, interrupciones en la red eléctrica y la destrucción de datos.

1.2. Objetivo

El objetivo de este plan es minimizar el impacto de un terremoto en la operatividad de los sistemas de información, garantizar la integridad y disponibilidad de los datos, y asegurar la rápida recuperación de los servicios críticos tras un evento sísmico.

1.3. Personal Encargado

Equipo de Prevención del Plan de Contingencias Informático.

1.4. Acciones preventivas

- Revisar regularmente la infraestructura y equipos.
- Realizar mantenimiento de los sistemas de refrigeración y UPS.
- Realizar copias de respaldo de datos.
- Monitorear el rendimiento y la seguridad de los servidores.
- Realizar pruebas de recuperación de desastres en los sistemas de información.

2. Procedimiento de Ejecución

2.1. Eventos que activan la contingencia

- Detección de un terremoto.
- Daños visibles en las instalaciones o interrupción de servicios críticos.

2.2. Personal que autoriza la contingencia informática

Coordinador del Plan de Contingencia Informático

2.3. Personal Encargado

Equipo de Prevención del Plan de Contingencias Informático.

2.4. Acciones para ejecutar a corto plazo

- Verificar el estado del centro de datos y equipos de red.
- Coordinar la reparación o reemplazo de los equipos dañados.
- Asegurar la integridad de los datos y sistemas.
- Restaurar respaldos si es necesario.
- Monitorear el rendimiento de los servidores y sistemas.
- Verificar la operatividad de los sistemas de información.
- Implementar soluciones temporales si es necesario.

2.5. Duración

La duración de la ejecución del plan de contingencia dependerá de la naturaleza y gravedad del terremoto. Se estima un tiempo máximo de 24 horas para la restauración completa del servicio.

3. Procedimiento de Restauración

3.1. Personal Encargado

Equipo de Restauración del Plan de Contingencias Informático.

3.2. Descripción de actividades

- Reparar o reemplazar los equipos de red y del centro de datos dañados.
- Restaurar la infraestructura de red y del centro de datos a su estado operativo normal.
- Restaurar los datos y sistemas desde los respaldos si es necesario.
- Verificar la integridad y seguridad de los datos y sistemas.
- Asegurar que los servidores estén operando correctamente.

Av. Alameda de los Incas
Cajamarca - Perú
076 602660 - 076 602661
contactenos@municaj.gob.pe

• Verificar la operatividad de los sistemas de información. • Implementar soluciones permanentes si es necesario. • Realizar pruebas de funcionalidad y rendimiento.
3.3. Mecanismos de Comprobación
• Validar la integridad de los datos restaurados. • Confirmar la plena operatividad de todos los sistemas de información. • Inspeccionar la infraestructura para verificar que esté libre de daños adicionales.
3.4. Desactivación del Plan de Contingencia
El plan se desactivará una vez que todos los sistemas estén completamente operativos y se confirme que no hay riesgos adicionales para la continuidad de las operaciones de la entidad.

PCI-02	Amenaza o evento: Inundación
1. Procedimiento de Prevención	
1.1. Descripción de la Amenaza	
Una inundación puede ser causada por lluvias intensas o fallos en sistemas de drenaje. Este tipo de evento puede dañar la infraestructura física, causar cortes de energía y poner en riesgo la continuidad operativa del centro de datos.	
1.2. Objetivo	
Proteger la infraestructura tecnológica y la integridad de los datos, minimizando el impacto de una inundación en las operaciones críticas del centro de datos y asegurando una rápida recuperación de los servicios esenciales.	
1.3. Personal Encargado	
Equipo de Prevención del Plan de Contingencias Informático.	
1.4. Acciones preventivas	
• Inspeccionar la infraestructura para asegurar el correcto funcionamiento del sistema de drenaje. • Realizar simulacros de inundación para asegurar la efectividad de los procedimientos de emergencia.	
2. Procedimiento de Ejecución	
2.1. Eventos que activan la contingencia	
• Aviso de inundación inminente con posible afectación del centro de datos. • Inundación parcial o total con posible afectación a la infraestructura tecnológica. • Fallo en los sistemas de drenaje.	
2.2. Personal que autoriza la contingencia informática	
Coordinador del Plan de Contingencia Informático	
2.3. Personal Encargado	
Equipo de Emergencia del Plan de Contingencias Informático.	
2.4. Acciones para ejecutar a corto plazo	
• Desconectar inmediatamente los equipos en riesgo de ser alcanzados por el agua. • Evaluar el nivel de daño a la infraestructura y equipos. • Iniciar la restauración de servicios críticos utilizando respaldos.	
2.5. Duración	
La contingencia estará activa hasta que las áreas afectadas estén secas y seguras, y los sistemas de información se hayan restaurado completamente.	
3. Procedimiento de Restauración	
3.1. Personal Encargado	
Equipo de Restauración del Plan de Contingencias Informático.	
3.2. Descripción de actividades	

Av. Alameda de los Incas
Cajamarca - Perú
076 602660 - 076 602661
contactenos@municaj.gob.pe

• Inspeccionar y reparar las instalaciones dañadas por la inundación. • Restaurar los sistemas y servicios desde los respaldos de datos. • Secar y limpiar las áreas afectadas para evitar daños futuros. • Realizar pruebas para asegurar que todos los sistemas estén funcionando correctamente.
3.3. Mecanismos de Comprobación
• Validar la integridad y operatividad de los sistemas restaurados. • Inspeccionar la infraestructura para confirmar que está libre de humedad y daños. • Realizar pruebas de rendimiento y seguridad en los sistemas críticos.
3.4. Desactivación del Plan de Contingencia
El plan se desactivará una vez que todos los sistemas estén operativos y se confirme que no hay riesgos adicionales de inundación o daños relacionados.

PCI-03	Amenaza o evento: Incendio
1. Procedimiento de Prevención	
1.1. Descripción de la Amenaza	
Un incendio es un evento catastrófico que puede causar la destrucción total o parcial de la infraestructura tecnológica, incluyendo servidores, redes de comunicación y otros equipos esenciales. Además, puede interrumpir el suministro eléctrico y poner en peligro la seguridad del personal.	
1.2. Objetivo	
El objetivo es minimizar el riesgo de incendio, proteger la infraestructura tecnológica y garantizar la rápida restauración de los servicios críticos en caso de un incidente.	
1.3. Personal Encargado	
Equipo de Prevención del Plan de Contingencias Informático.	
1.4. Acciones preventivas	
• Revisar y mantener regularmente los sistemas de detección y extinción de incendios. • Realizar revisiones de seguridad eléctrica para prevenir cortocircuitos y sobrecargas. • Capacitar al personal en la utilización de extintores y procedimientos de evacuación. • Reducir la cantidad de materiales inflamables en áreas críticas.	
2. Procedimiento de Ejecución	
2.1. Eventos que activan la contingencia	
• Activación del sistema de detección de incendios. • Presencia de humo o fuego en el centro de datos o en áreas adyacentes. • Fallos en la infraestructura debido a daños causados por el fuego.	
2.2. Personal que autoriza la contingencia informática	
Coordinador del Plan de Contingencia Informático	
2.3. Personal Encargado	
Equipo de Emergencia del Plan de Contingencias Informático.	
2.4. Acciones para ejecutar a corto plazo	
• Activar el sistema de extinción de incendios. • Desconectar de inmediato los equipos eléctricos para prevenir cortocircuitos. • Evacuar al personal del área afectada de acuerdo con el plan de evacuación. • Evaluar los daños a la infraestructura y equipos una vez extinguido el incendio. • Iniciar la restauración de los sistemas críticos desde los respaldos si es necesario.	
2.5. Duración	
La contingencia estará activa hasta que el incendio esté completamente controlado y los sistemas hayan sido restaurados.	

Av. Alameda de los Incas
Cajamarca - Perú
076 602660 - 076 602661
contactenos@municaj.gob.pe

3. Procedimiento de Restauración
3.1. Personal Encargado
Equipo de Restauración del Plan de Contingencias Informático.
3.2. Descripción de actividades
• Evaluar el daño total causado por el incendio a la infraestructura y equipos. • Restaurar los sistemas y servicios desde los respaldos. • Reemplazar o reparar cualquier equipo dañado. • Realizar pruebas exhaustivas para asegurar que todos los sistemas estén funcionando correctamente y de forma segura.
3.3. Mecanismos de Comprobación
• Verificar la integridad y operatividad de los sistemas restaurados. • Inspeccionar la infraestructura para confirmar que está libre de daños residuales y que los sistemas de detección y extinción de incendios están nuevamente operativos. • Realizar auditorías de seguridad para prevenir futuros incidentes.
3.4. Desactivación del Plan de Contingencia
El plan se desactivará una vez que todos los sistemas estén completamente restaurados, los riesgos de incendio hayan sido mitigados, y la infraestructura esté en condiciones seguras de operatividad.

PCI-04	**Amenaza o evento: Corte de internet**
1. Procedimiento de Prevención	
1.1. Descripción de la Amenaza	
Un corte de internet puede ser causado por fallos en el proveedor de servicios, interrupciones físicas en la infraestructura de red, ataques cibernéticos, o desastres naturales. Esta situación puede afectar la comunicación externa e interna, el acceso a servicios en la nube, y la operatividad de sistemas críticos que dependen de la conectividad.	
1.2. Objetivo	
Garantizar la continuidad operativa de los sistemas críticos y minimizar el impacto de la pérdida de conectividad a internet, asegurando alternativas de comunicación y acceso a datos.	
1.3. Personal Encargado	
Equipo de Prevención del Plan de Contingencias Informático.	
1.4. Acciones preventivas	
• Monitorear continuamente la estabilidad de las conexiones de internet. • Implementar en sistemas de información procedimientos manuales, para el caso de funcionalidades que requieren acceso a internet. • Capacitar al personal en el uso de sistemas de comunicación alternativos.	
2. Procedimiento de Ejecución	
2.1. Eventos que activan la contingencia	
• Pérdida de conectividad a internet en la entidad. • Fallo prolongado en los servicios de internet de un proveedor.	
2.2. Personal que autoriza la contingencia informática	
Coordinador del Plan de Contingencia Informático	
2.3. Personal Encargado	
Equipo de Emergencia del Plan de Contingencias Informático.	
2.4. Acciones para ejecutar a corto plazo	
• Activar procesos manuales para el casos de sistemas de información que presentan fallas de funcionamiento. • Utilizar las conexiones de respaldo como redes móviles o VPNs para mantener la comunicación. • Informar al personal sobre la contingencia y proporcionar instrucciones sobre los canales de comunicación alternativos.	

Av. Alameda de los Incas
Cajamarca - Perú
076 602660 - 076 602661
contactenos@municaj.gob.pe

• Monitorear continuamente la conectividad para evaluar la estabilidad del servicio.
2.5. Duración
La contingencia permanecerá activa hasta que se restablezca la conectividad principal y se verifique su estabilidad.
3. Procedimiento de Restauración
3.1. Personal Encargado
Equipo de Restauración del Plan de Contingencias Informático.
3.2. Descripción de actividades
• Restablecer la conexión de internet principal y verificar su funcionalidad. • Revisar la infraestructura de red para identificar y mitigar las causas del corte de internet.
3.3. Mecanismos de Comprobación
• Verificar la conectividad a internet mediante pruebas de carga y estabilidad. • Monitorear la red para asegurarse de que no haya vulnerabilidades residuales.
3.4. Desactivación del Plan de Contingencia
El plan se desactivará una vez que la conectividad a internet haya sido restaurada completamente y se confirme que los sistemas están operativos sin interrupciones.

PCI-05	Amenaza o evento: Fallo del suministro eléctrico
1. Procedimiento de Prevención	
1.1. Descripción de la Amenaza	
El fallo del suministro eléctrico es una interrupción en la fuente de energía que puede ser causada por desastres naturales, fallos en la infraestructura de la red eléctrica, o sobrecargas. Esto puede resultar en la pérdida de operatividad de los sistemas, daño a los equipos, y pérdida de datos no guardados.	
1.2. Objetivo	
El objetivo es garantizar la continuidad de la operatividad de los sistemas críticos, proteger la infraestructura tecnológica y asegurar la recuperación rápida de los servicios en caso de un corte de suministro eléctrico.	
1.3. Personal Encargado	
Equipo de Prevención del Plan de Contingencias Informático.	
1.4. Acciones preventivas	
• Verificar y dar mantenimiento regularmente los UPS. • Capacitar al personal en la operación de los equipos de respaldo de energía.	
2. Procedimiento de Ejecución	
2.1. Eventos que activan la contingencia	
• Pérdida del suministro eléctrico en la instalación. • Fallo prolongado de la red eléctrica sin solución inmediata por parte del proveedor. • Fallo en los equipos UPS.	
2.2. Personal que autoriza la contingencia informática	
Coordinador del Plan de Contingencia Informático	
2.3. Personal Encargado	
Equipo de Emergencia del Plan de Contingencias Informático.	
2.4. Acciones para ejecutar a corto plazo	
• Activar los sistemas UPS para mantener la energía en los equipos críticos. • Apagar los servidores pasados los 15 minutos de corte de suministro eléctrico, posteriormente apagador todos los equipos del Centro de Datos. • Informar al personal sobre la contingencia y los procedimientos a seguir.	

Av. Alameda de los Incas
Cajamarca - Perú
076 602660 - 076 602661
contactenos@municaj.gob.pe

2.5. Duración
La contingencia permanecerá activa hasta que el suministro eléctrico sea restaurado de manera estable y segura, y se verifique que todos los sistemas están operativos.
3. Procedimiento de Restauración
3.1. Personal Encargado
Equipo de Restauración del Plan de Contingencias Informático.
3.2. Descripción de actividades
• Restaurar el suministro eléctrico principal. • Verificar la operatividad de todos los sistemas y equipos conectados a la energía restaurada. • Documentar y analizar el incidente para identificar mejoras en el plan de contingencia.
3.3. Mecanismos de Comprobación
• Monitorear operatividad de servidores y sistemas de información. • Monitorear la infraestructura para asegurar que no haya daños residuales tras el fallo de energía. • Revisar los logs y auditorías de los sistemas para identificar cualquier irregularidad durante el evento.
3.4. Desactivación del Plan de Contingencia
El plan se desactivará una vez que el suministro eléctrico haya sido restaurado y todos los sistemas estén operativos y estables sin depender de las soluciones de respaldo.

PCI-06	**Amenaza o evento: Falla de Infraestructura del Centro de Datos**
1. Procedimiento de Prevención	
1.1. Descripción de la Amenaza	
La falla de infraestructura del centro de datos puede incluir problemas en la climatización, el suministro eléctrico, la seguridad física, o la conectividad de red, lo que puede causar interrupciones en los servicios, pérdida de datos, o daños a los equipos.	
1.2. Objetivo	
El objetivo es asegurar la continuidad operativa de los sistemas críticos, minimizar los impactos de la falla, y restaurar la infraestructura del centro de datos en el menor tiempo posible.	
1.3. Personal Encargado	
Equipo de Prevención del Plan de Contingencias Informático.	
1.5. Acciones preventivas	
• Monitorización de la infraestructura del centro de datos. • Realizar inspecciones periódicas de toda la infraestructura tecnológica del Centro de Datos. • Realizar mantenimiento preventivo del sistema de refrigeración del Centro de Datos. • Realizar mantenimiento preventivo del sistema UPS del Centro de Datos. • Realizar mantenimiento preventivo de equipos de redes del Centro de Datos. • Realizar mantenimiento preventivo de servidores del Centro de Datos. • Realizar copias de respaldo de datos y sistemas de información de manera regular. • Mantener el inventario los equipos del Centro de Datos actualizado.	
2. Procedimiento de Ejecución	
2.1. Eventos que activan la contingencia	
• Fallo en los sistemas de refrigeración que afecte la temperatura y humedad del centro de datos. • Interrupción del suministro eléctrico que no pueda ser soportada por los sistemas UPS o generadores. • Falla en la conectividad de red que afecte la operatividad de los sistemas alojados en el centro de datos.	
2.2. Personal que autoriza la contingencia informática	
Coordinador del Plan de Contingencia Informático	
2.3. Personal Encargado	

Av. Alameda de los Incas
Cajamarca - Perú
076 602660 - 076 602661
contactenos@municaj.gob.pe

Equipo de Emergencia del Plan de Contingencias Informático.
2.4. Acciones para ejecutar a corto plazo
• Activar los sistemas de respaldo de energía y climatización si es necesario. • Desconectar o reubicar equipos críticos para evitar daños por condiciones inadecuadas. • Implementar planes de recuperación de red si la conectividad está comprometida. • Informar al personal sobre la situación y proporcionar instrucciones sobre la continuidad de las operaciones. • Monitorear continuamente el estado del centro de datos para evaluar la situación.
2.5. Duración
La duración de la ejecución del plan de contingencia dependerá de la naturaleza y gravedad del fallo. Se estima un tiempo máximo de 24 horas para la restauración completa del servicio.
3. Procedimiento de Restauración
3.1. Personal Encargado
Equipo de Restauración del Plan de Contingencias Informático.
3.2. Descripción de actividades
• Restablecer los sistemas de energía, climatización y conectividad de red en el centro de datos. • Verificar la operatividad de todos los equipos y sistemas una vez que la infraestructura haya sido restaurada. • Inspeccionar la infraestructura para identificar y corregir la causa del fallo. • Documentar el incidente y actualizar los procedimientos de contingencia con las lecciones aprendidas.
3.3. Mecanismos de Comprobación
• Realizar pruebas de estabilidad y rendimiento en todos los sistemas críticos del centro de datos. • Monitorear los sistemas para asegurar que no haya daños residuales o riesgos de futuros fallos. • Revisar los logs y auditorías de los sistemas para identificar cualquier irregularidad durante el evento.
3.4. Desactivación del Plan de Contingencia
El plan se desactivará una vez que la infraestructura del centro de datos haya sido restaurada completamente, y todos los sistemas estén operativos y estables sin depender de soluciones temporales o de respaldo.

PCI-07	Amenaza o evento: Falla de equipos de redes
1. Procedimiento de Prevención	
1.1. Descripción de la Amenaza	
La falla de equipos de redes que conectan el centro de datos con las estaciones de trabajo de los usuarios finales puede resultar en la pérdida de conectividad, afectando la capacidad de los usuarios para acceder a sistemas y aplicaciones críticas, lo que interrumpe la operatividad normal.	
1.2. Objetivo	
El objetivo es asegurar la continuidad de la conectividad entre el centro de datos y las estaciones de trabajo, minimizar el impacto de las fallas en los equipos de red, y restaurar la conectividad en el menor tiempo posible.	
1.3. Personal Encargado	
Equipo de Prevención del Plan de Contingencias Informático.	
1.4. Acciones preventivas	
• Realizar mantenimiento preventivo y actualizaciones de firmware en los equipos de red para asegurar su operatividad. • Monitorear la red para detectar problemas potenciales y actuar antes de que escalen. • Mantener una documentación detallada de la infraestructura de red y procedimientos para la respuesta rápida ante fallas.	
2. Procedimiento de Ejecución	
2.1. Eventos que activan la contingencia	
• Falla de switches, routers, o cualquier otro equipo de red que interrumpa la conectividad entre el centro de datos y las estaciones de trabajo.	

Av. Alameda de los Incas
Cajamarca - Perú
076 602660 - 076 602661
contactenos@municaj.gob.pe

• Problemas en la infraestructura de red que afecten la capacidad de los usuarios finales para acceder a sistemas y aplicaciones. • Pérdida de conectividad de red que no pueda ser resuelta con procedimientos estándar.
2.2. Personal que autoriza la contingencia informática
Coordinador del Plan de Contingencia Informático
2.3. Personal Encargado
Equipo de Emergencia del Plan de Contingencias Informático.
2.4. Acciones para ejecutar a corto plazo
• Activar equipos de red redundantes o de respaldo si están disponibles. • Redireccionar el tráfico de red para minimizar el impacto en los usuarios finales. • Informar al personal sobre la situación y los pasos a seguir para mantener la operatividad. • Monitorear el estado de la red y los equipos en tiempo real para evaluar la situación y la efectividad de las medidas tomadas.
2.5. Duración
La duración de la ejecución del plan de contingencia dependerá de la naturaleza y gravedad del fallo. Se estima un tiempo máximo de 24 horas para la restauración completa del servicio.
3. Procedimiento de Restauración
3.1. Personal Encargado
Equipo de Encargado del Plan de Contingencias Informático.
3.2. Descripción de actividades
• Restaurar o reemplazar los equipos de red afectados. • Verificar que la conectividad ha sido completamente restaurada y que no hay problemas residuales. • Realizar pruebas de conectividad y rendimiento en la red para asegurar que todos los sistemas están operativos. • Documentar el incidente y actualizar los procedimientos de contingencia según las lecciones aprendidas.
3.3. Mecanismos de Comprobación
• Realizar pruebas en los sistemas conectados a la red para asegurar su operatividad. • Monitorear el rendimiento de la red para identificar cualquier problema que pueda haber surgido durante el incidente.
3.4. Desactivación del Plan de Contingencia
El plan se desactivará una vez que todos los equipos de red estén operativos y la conectividad entre el centro de datos y las estaciones de trabajo haya sido restaurada completamente, sin depender de soluciones temporales.

PCI-08	Amenaza o evento: Falla de sistemas de Información
1. Procedimiento de Prevención	
1.1. Descripción de la Amenaza	
Las fallas en los sistemas de información pueden incluir errores de software (bugs), configuraciones incorrectas, fallos en las actualizaciones, o vulnerabilidades no gestionadas, que pueden afectar la disponibilidad, integridad, y confidencialidad de los datos, así como la operatividad de las aplicaciones críticas.	
1.2. Objetivo	
El objetivo es minimizar los impactos de las fallas en los sistemas de información, restaurar la operatividad normal de los sistemas en el menor tiempo posible, y evitar la recurrencia de dichos problemas.	
1.3. Personal Encargado	
Equipo de Restauración del Plan de Contingencias Informático.	
1.4. Acciones preventivas	
• Realizar revisiones periódicas de los sistemas de información y configuraciones. • Desplegar actualizaciones de manera controlada y bajo supervisión. • Mantener un entorno de pruebas que refleje el entorno de producción para detectar problemas antes de desplegar cambios.	

Av. Alameda de los Incas
Cajamarca - Perú
076 602660 - 076 602661
contactenos@municaj.gob.pe

• Monitorear disponibilidad de los sistemas de información.
2. Procedimiento de Ejecución
2.1. Eventos que activan la contingencia
• Detectar un bug que afecte la operatividad de un sistema crítico. • Identificar una configuración incorrecta que ponga en riesgo la seguridad o funcionalidad de un sistema. • Fallos en la implementación de actualizaciones que resulten en problemas operativos. • Cualquier otro fallo en los sistemas de información que comprometa la continuidad operativa.
2.2. Personal que autoriza la contingencia informática
Coordinador del Plan de Contingencia Informático
2.3. Personal Encargado
Equipo de Restauración del Plan de Contingencias Informático.
2.4. Acciones para ejecutar a corto plazo
• Verificar el estado de los sistemas de información afectados. • Coordinar la reparación o reemplazo de los componentes fallidos. • Asegurar la integridad de los datos y sistemas. • Restaurar respaldos si es necesario. • Monitorear el rendimiento de los servidores y sistemas. • Verificar la operatividad de los sistemas de información. • Implementar soluciones temporales si es necesario. • Identificar y corregir bugs o configuraciones incorrectas.
2.5. Duración
La contingencia permanecerá activa hasta que el sistema de información afectado esté completamente restaurado y funcionando correctamente, sin depender de soluciones temporales. Se estima un tiempo máximo de 24 horas para la restauración completa del servicio.
3. Procedimiento de Restauración
3.1. Personal Encargado
Equipo de Restauración del Plan de Contingencias Informático.
3.2. Descripción de actividades
• Implementar la solución definitiva al problema detectado, ya sea mediante corrección de bugs, ajuste de configuraciones o instalación de parches. • Restaurar cualquier dato que haya sido afectado por la falla y validar la integridad de los mismos. • Realizar pruebas exhaustivas para asegurar que el problema ha sido completamente resuelto y que no hay efectos colaterales. • Documentar el incidente, las soluciones implementadas y las lecciones aprendidas para mejorar la prevención futura.
3.3. Mecanismos de Comprobación
• Realizar pruebas funcionales y de rendimiento en el sistema de información restaurado. • Monitorear el sistema en las horas y días siguientes a la restauración para asegurar su estabilidad. • Revisar logs y auditorías para confirmar que no se han producido otros problemas asociados a la falla.
3.4. Desactivación del Plan de Contingencia
El plan se desactivará una vez que el sistema de información esté plenamente operativo y estable, sin necesidad de depender de soluciones temporales o parches de emergencia.

PCI-09	**Amenaza o evento: Ciberataque**
1. Procedimiento de Prevención	
1.1. Descripción de la Amenaza	

Av. Alameda de los Incas
Cajamarca - Perú
076 602660 - 076 602661
contactenos@municaj.gob.pe

Los ciberataques pueden tomar diversas formas, como malware, ransomware, ataques de denegación de servicio (DDoS), phishing, explotación de vulnerabilidades, errores de configuración, ingeniería social, y ataques de zero-day. Estas amenazas pueden comprometer la seguridad, integridad, y disponibilidad de los sistemas de información, así como exponer datos sensibles.
1.2. Objetivo
El objetivo es prevenir, detectar, y mitigar los efectos de ciberataques, asegurando la continuidad operativa, la protección de la información, y la rápida recuperación de los sistemas afectados.
1.3. Personal Encargado
Equipo de Prevención del Plan de Contingencias Informático.
1.4. Acciones del Equipo de Prevención
• Mantener los sistemas operativos, aplicaciones y software de seguridad actualizados con los últimos parches y correcciones. • Monitoreo continuo para la detección temprana de actividades sospechosas y posibles ciberataques. • Capacitar al personal sobre prácticas seguras, detección de phishing, y respuestas adecuadas ante intentos de ingeniería social. • Realizar copias de respaldo de datos, asegurando que estas estén protegidas contra ciberataques. • Segmentar la red para limitar la propagación de malware o accesos no autorizados en caso de una brecha de seguridad. • Realizar revisiones periódicas de seguridad para identificar y corregir vulnerabilidades. • Desplegar y mantener actualizado el software de seguridad, como antivirus, firewalls, y sistemas de detección de intrusiones. • Implementar políticas de control de acceso estricto y autenticación multifactor en sistemas críticos. • Realizar simulaciones de ciberataques para evaluar la eficacia de las medidas de seguridad y la preparación del personal. • Monitorear continuamente la red y los sistemas para detectar y responder a amenazas en tiempo real.
2. Procedimiento de Ejecución
2.1. Eventos que activan la contingencia
• Detectar malware o ransomware activo en los sistemas. • Identificación de intentos de phishing exitosos o acceso no autorizado a cuentas de usuario. • Detectar un ataque DDoS que afecte la disponibilidad de servicios. • Descubrimiento de explotación de una vulnerabilidad o error de configuración en sistemas críticos. • Identificación de un ataque de zero-day o cualquier otro tipo de amenaza avanzada persistente (APT).
2.2. Personal que autoriza la contingencia informática
Coordinador del Plan de Contingencia Informático
2.3. Personal Encargado
Equipo de Emergencia del Plan de Contingencias Informático.
2.4. Acciones para ejecutar a corto plazo
• Aislar los sistemas comprometidos para evitar la propagación del ciberataque. • Identificar la naturaleza y el alcance del ataque a través de análisis de incidentes. • Informar a los usuarios y al personal relevante sobre el incidente y las medidas a seguir. • Implementar medidas de contención como desactivar cuentas comprometidas, bloquear IPs sospechosas, y cerrar vulnerabilidades identificadas. • Iniciar procedimientos de recuperación para restaurar sistemas y datos desde copias de seguridad si es necesario.
2.5. Duración
La contingencia permanecerá activa hasta que la amenaza haya sido contenida y mitigada, y los sistemas afectados hayan sido completamente restaurados a su estado normal de operación
3. Procedimiento de Restauración
3.1. Personal Encargado
Equipo de Restauración del Plan de Contingencias Informático.
3.2. Descripción de actividades
• Realizar una limpieza completa del sistema para eliminar cualquier rastro de malware o actividad maliciosa.

Av. Alameda de los Incas
Cajamarca - Perú
076 602660 - 076 602661
contactenos@municaj.gob.pe

- Restaurar datos desde copias de respaldo de datos en caso de pérdida o cifrado de archivos.
- Aplicar parches de seguridad y realizar cambios en la configuración para prevenir futuras explotaciones.
- Realizar pruebas exhaustivas de seguridad para confirmar que el sistema es seguro y está libre de amenazas.
- Documentar el incidente, las respuestas implementadas y las lecciones aprendidas para mejorar la preparación futura.

3.3. Mecanismos de Comprobación

- Realizar revisiones de seguridad para asegurar que todas las vulnerabilidades han sido corregidas y no hay presencia de amenazas residuales.
- Monitorear el sistema durante un periodo posterior al incidente para detectar cualquier signo de actividad sospechosa.
- Verificar la integridad y disponibilidad de los sistemas y datos restaurados.

3.4. Desactivación del Plan de Contingencia

El plan se desactivará una vez que todos los sistemas y datos hayan sido restaurados, y la infraestructura esté protegida contra futuros ciberataques. Se debe realizar un análisis post-incidente para mejorar las estrategias de prevención y respuesta ante futuras amenazas.

PCI-10	Amenaza o evento: Ataque físico al Centro de Datos o equipos de redes

1. Procedimiento de Prevención

1.1. Descripción de la Amenaza

Un ataque físico al centro de datos o a los equipos de redes que conectan el centro de datos con las estaciones de trabajo puede causar daños directos a la infraestructura tecnológica, resultando en interrupciones en la operatividad de los sistemas, pérdida de datos, y potenciales brechas de seguridad.

1.2. Objetivo

El objetivo es proteger la infraestructura física del centro de datos y los equipos de redes, minimizar los daños en caso de un ataque, y restaurar la operatividad de los sistemas afectados en el menor tiempo posible.

1.3. Personal Encargado

Equipo de Emergencia del Plan de Contingencias Informático.

1.4. Acciones preventivas

- Realizar revisiones de seguridad física en el centro de datos y los puntos de red críticos.
- Implementar medidas adicionales de seguridad según los resultados de las auditorías.
- Capacitar al personal en protocolos de respuesta ante un ataque físico.
- Mantener un inventario actualizado de los equipos y su ubicación exacta dentro de las instalaciones.

2. Procedimiento de Ejecución

2.1. Eventos que activan la contingencia

- Intento o ataque físico confirmado contra el centro de datos o los equipos de redes.
- Acceso no autorizado o daños físicos a las instalaciones que comprometen la seguridad y operatividad de los sistemas.
- Detección de intrusos o señales de sabotaje en las instalaciones.

2.2. Personal que autoriza la contingencia informática

Coordinador del Plan de Contingencia Informático

2.3. Personal Encargado

Equipo de Emergencia del Plan de Contingencias Informático.

2.4. Acciones para ejecutar a corto plazo

- Informar a todo el personal y a las autoridades pertinentes sobre el ataque y las medidas a seguir.
- Monitorear el estado de la infraestructura y los sistemas para evaluar la magnitud del daño y las acciones necesarias.

2.5. Duración

La contingencia permanecerá activa hasta que las instalaciones afectadas estén seguras, los equipos dañados hayan sido reparados o reemplazados, y la operatividad de los sistemas haya sido restaurada completamente.

3. Procedimiento de Restauración

Av. Alameda de los Incas
Cajamarca - Perú
076 602660 - 076 602661
contactenos@municaj.gob.pe

3.1. Personal Encargado
Equipo de Restauración del Plan de Contingencias Informático.
3.2. Descripción de actividades
• Reparar o reemplazar los equipos de redes y cualquier otra infraestructura tecnológica que haya sido dañada. • Verificar que todas las medidas de seguridad física se han restablecido y reforzado si es necesario. • Restaurar los sistemas de información desde los respaldos si hubo pérdida o daño de datos. • Realizar pruebas exhaustivas para asegurar que la infraestructura y los sistemas de información funcionan correctamente después de la restauración.
3.3. Mecanismos de Comprobación
• Realizar revisiones de seguridad física post-incidente para asegurar que todas las vulnerabilidades han sido mitigadas. • Monitorear los sistemas de información y la infraestructura para detectar cualquier signo de falla residual o compromiso. • Revisar y analizar los logs de seguridad para verificar que no hubo accesos no autorizados durante el incidente.
3.4. Desactivación del Plan de Contingencia
El plan se desactivará una vez que todas las instalaciones y equipos hayan sido reparados o reemplazados, y la seguridad y operatividad de la infraestructura y los sistemas de información hayan sido completamente restauradas.

Av. Alameda de los Incas
Cajamarca - Perú
076 602660 - 076 602661
contactenos@municaj.gob.pe

Anexo 4: Formato de control y certificación de pruebas de Plan de Contingencia Informático

CONTROL Y CERTIFICACIÓN DE PRUEBAS DE CONTINGENCIA

Prueba N°	
Escenario de Prueba:	
Unidad Orgánica Responsable	

INFORMACIÓN DEL PROCESO

Metodología		
Alcance		
Condiciones de Ejecución	Equipo	
	Sistema de Información	
	Ubicación	
	Fecha del Backup	

RESULTADOS DEL LA PRUEBA

Resultado	Satisfactorio		Satisfactorio con observaciones		Deficiente	
Observaciones						

ACTUALIZACIONES DEL PLAN DE CONTINGENCIAS

Cambios o actualizaciones en el Plan de Contingencia:	

ACTUALIZACIÓN DE PARTICIPANTES

Participante	Cargo	Firma

Av. Alameda de los Incas
Cajamarca - Perú
076 602660 - 076 602661
contactenos@municaj.gob.pe