RESOLUCIÓN GERENCIAL GENERAL REGIONAL

Nº 237 -2024-GGR-GR PUNO

Puno, ...24 SEP. 2024.....

EL GERENTE GENERAL REGIONAL DEL GOBIERNO REGIONAL PUNO

Vistos, el expediente 2024-0012568, sobre aprobación del PLAN DE CONTINGENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN 2024-2025;

CONSIDERANDO:

Que, el Jefe de la Oficina de Tecnologías de la Información, ha emitido el Informe N° 000132-2024-GRP/OTI de fecha 14 de agosto del 2024, dirigido al Gerente General Regional, para elevar la propuesta del PLAN DE CONTINGENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN 2024-2025;

Que, el objetivo del Plan mencionado en considerando precedente es *"Establecer disposiciones y definir normas y procedimientos necesario para garantizar la continuidad de los servicios de tecnologías de la información (TI) del Gobierno Regional Puno en caso de que ocurra alguna eventualidad que interrumpa su funcionamiento, asegurando su restablecimiento en el menor tiempo posible, así como la seguridad y confiabilidad de los sistemas de información y comunicación.",* en la introducción se menciona que *"... se ha elaborado el Plan de Contingencia de Tecnologías de la Información del Gobierno Regional Puno, dado que la institución es vulnerable a diversos eventos que pueden interrumpir los servicios informáticos y afectar el funcionamiento normal de sus actividades..."*; y

Estando al Informe N° 000132-2024-GRP/OTI e Informe N° 000153-2024-GRP/OTI del Jefe de la Oficina de Tecnologías de la Información, Informe N° 000272-2024-GRP/SGP de la Sub Gerencia de Planeamiento, Informe N° 00982-2024-GRP/GRPPM de la Gerencia Regional de Planeamiento, Presupuesto y Modernización, y Proveído 026036-2024-GRP/GGR de Gerencia General Regional;

En el marco de lo establecido por la Resolución Ejecutiva Regional Nº 076-2023-GR PUNO/GR;

SE RESUELVE:

ARTÍCULO ÚNICO.- APROBAR el PLAN DE CONTINGENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN 2024-2025, que en siete (07) rubros, y en cuarenta (40) folios, forma parte de la presente resolución.

REGÍSTRESE, COMUNÍQUESE Y CÚMPLASE.

JUAN OSCAR MACEDO CARDENAS
GERENTE GENERAL REGIONAL

GOBIERNO REGIONAL PUNO

PLAN DE CONTINGENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN

2024-2025

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN

Elaborado por: Oficina de Tecnologías de la Información

Código	PCTI-GORE-PUNO.01.00
Versión	1.0
Fecha de versión	14-08-2024
Nombre del archivo	pcti_gore_puno

ÍNDICE

ÍNDICE DE TABLAS

I. INTRODUCCIÓN

Una organización puede enfrentar situaciones de emergencia que provoquen efectos adversos, ocasionando pérdidas humanas, ambientales y materiales, entre otros. El tiempo y la capacidad de respuesta con los que cuenta la entidad son fundamentales para enfrentar y controlar cualquier emergencia, ya sea interna o externa. En este sentido, y como una buena práctica de Tecnologías de Información (TI), se ha elaborado el Plan de Contingencia de Tecnologías de la Información del Gobierno Regional Puno, dado que la Institución es vulnerable a diversos eventos que pueden interrumpir los servicios informáticos y afectar el funcionamiento normal de sus actividades. Esto no solo impacta a los usuarios internos, sino también a los externos. Además, el Plan se alinea con el compromiso de fortalecer la capacidad operativa del Gobierno Regional Puno. Así, el presente plan establece los objetivos, el alcance y la metodología del mismo, con el fin de minimizar el impacto negativo de la interrupción de los servicios informáticos, contribuyendo a que la Institución esté preparada para cualquier contingencia en el ámbito de la tecnología de la información, considerando acciones antes, durante y después de los incidentes.

II. OBJETIVOS

2.1. General

Establecer disposiciones y definir normas y procedimientos necesarios para garantizar la continuidad de los servicios de tecnologías de la información (TI) del Gobierno Regional Puno en caso de que ocurra alguna eventualidad que interrumpa su funcionamiento, asegurando su restablecimiento en el menor tiempo posible, así como la seguridad y confiabilidad de los sistemas de información y comunicación.

2.2. Específicos

- Identificar y diagnosticar los procesos críticos detalladamente del Gobierno Regional Puno.
- Establecer un organigrama claro y funcional para el equipo de contingencia del Gobierno Regional Puno.
- Implementar políticas y directivas de procesos que permitan la restauración de los servicios informáticos del Gobierno Regional Puno en el menor tiempo posible.
- Determinar acciones que permitan evaluar el avance, logros y resultados obtenidos con la ejecución del plan de contingencia, facilitando la realización de cambios necesarios para mejorar el plan.
- Establecer actividades que contribuyan al cumplimiento de los objetivos institucionales y garanticen la continuidad de los servicios informáticos brindados a los ciudadanos por el Gobierno Regional Puno.
- Contar con personal debidamente capacitado y organizado para afrontar adecuadamente las contingencias que puedan presentarse y que puedan perjudicar la continuidad de los servicios y procesos informáticos.

III. ALCANCE

El Plan de Contingencia de Tecnología de la Información, incluye los elementos referidos a los sistemas de información, aplicativos informáticos, bases de datos, equipos tecnológicos e instalación, así mismo contar profesional especializado y demás servicios administrados por la Oficina de Tecnologías de la Información (OTI), direccionado a minimizar eventuales riesgos ante situaciones adversas que atentan contra el normal funcionamiento de los servicios informáticos de la entidad.

IV. BASE LEGAL

- Ley N° 27658: Ley Marco de Modernización de la Gestión del Estado.
- Ley N° 27867: Ley orgánica de Gobiernos Regionales
- Resolución Ministerial N° 004-2016-pcm: Aprueban 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.
- Ley N° 29664, Ley que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD)
- Ley N° 29733 de Protección de Datos Personales del Perú que regula aquellos casos en que no se requiere solicitar autorización al titular de los datos personales para su tratamiento.
- Decreto Supremo N° 004-2013-PCM, que aprueba la Política Nacional de Modernización de la Gestión Pública.
- Decreto Supremo N° 029-2021-PCM, que aprueba el Reglamento de la Ley de Gobierno Digital busca impulsar la incorporación de las tecnologías digitales en los servicios ofrecidos por las entidades públicas en favor de la reactivación económica del país.
- Decreto Supremo N° 048-2011-PCM, que crea el Sistema Nacional de Gestión de Riesgo de Desastres - SINAGERD
- Decreto Supremo N° 085-2023-PCM, que aprueba la Política Nacional de Transformación Digital al 2030
- Decreto Supremo N° 157-2021-PCM, que aprueba el Reglamento del Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital.
- Decreto de Urgencia N° 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital.
- Decreto de Urgencia N° 007-2020, Decreto de Urgencia que aprueba el Marco de Confianza Digital y dispone medidas para su fortalecimiento.
- Decreto Legislativo N° 1412, que aprueba la Ley de Gobierno Digital.
- Decreto Legislativo N° 604, que crea Ley de Organización y funciones del Instituto Nacional de Estadística e Informática (INEI), esta norma pertenece al compendio Normativa sobre Transformación Digital.
- Decreto Legislativo N° 1246, que aprueba diversas medidas de simplificación administrativa y Decreto Supremo N° 016-2020-PCM que amplía los servicios de información en el marco del Decreto Legislativo N°1246, del Decreto Legislativo N° 1427 y del Plan Nacional de Competitividad y Productividad.
- Decreto Supremo N° 033-2018-PCM, que crea la Plataforma Digital Única del Estado Peruano y establecen Disposiciones adicionales para el desarrollo del Gobierno Digital.

- Decreto Supremo N° 118-2018-PCM, mediante el cual se declara de interés nacional el desarrollo del Gobierno Digital, la innovación y la economía digital con enfoque territorial.
- Decreto Supremo N° 003-2013-JUS, que consta de VI Títulos, ciento treinta y un (131) Artículos, tres (03) Disposiciones Complementarios Finales y tres (03) Disposiciones Complementarias Transitorias, que forma parte integrante del presente Decreto Supremo.
- Resolución Ministerial N° 119-2018-PCM, que dispone la creacipon de un Comité del Gobierno Digital en cada entidad de la Administración Pública.
- Resolución Ministerial N° 087-2019-PCM, mediante el cual se Aprueban disposiciones sobre la conformación y funciones del Comité de Gobierno Digital.

MARCO TEÓRICO

5.1 Plan de contingencia informático

Este documento compila un conjunto de procedimientos alternativos destinados a asegurar el funcionamiento normal de las TI, cuando alguno de sus servicios se vea negativamente afectado por un incidente o inconveniente, ya sea interno o externo de la institución. Este plan tiene como objetivo minimizar las consecuencias de dichos incidentes, permitiendo reanudar las operaciones de manera eficiente y oportuna. Además, define las acciones a llevar a cabo en las siguientes etapas.

- Antes, como plan de prevención para mitigar incidencias.
- Durante, como plan de emergencia y/o solución en el momento de presentarse el incidente.
- Después, como plan de recuperación una vez superado el incidente para regresar al estado de operatividad.

5.2. Definiciones

Incidente: circunstancia o suceso que sucede de manera inesperada y que puede afectar al desarrollo de una actividad, aunque no forme parte de él. En nuestro contexto, es una interrupción de las condiciones normales de operación en cualquier proceso informático.
Riesgo: es un evento (o condición incierta) que podría ocurrir y generar un impacto positivo (una oportunidad) o negativo (una amenaza) en un proyecto, afectando al menos uno de los objetivos del proyecto.
Vulnerabilidad: es una debilidad que permite a un atacante comprometer la confidencialidad, integridad y disponibilidad de un sistema y/o infraestructura. Las vulnerabilidades pueden ser debido a tantos fallos de diseños, errores en la configuración o a procedimientos no robustos.
Amenaza: cualquier evento que puede explotar una vulnerabilidad.
Método de análisis de riesgos: los métodos de análisis de riesgos son técnicas que se emplean para evaluar los riesgos de un proyecto o un proceso. Estos métodos ayudan a tomar decisiones que permiten implementar medidas de prevención para evitar peligros potenciales o reducir su impacto.
Plan de prevención: es el conjunto de acciones, decisiones y comprobaciones orientadas a prevenir la presencia de un evento no deseado, con el propósito de disminuir y mitigar la probabilidad de ocurrencia de este en las categorías identificadas en el presente plan. El

plan de prevención es la parte principal del Plan de Contingencia porque permite aminorar y atenuar la probabilidad de ocurrencia de un estado de contingencia.

Plan de ejecución: es el conjunto detallado de acciones a realizar en el momento que se presenta el incidente y activa la contingencia como un mecanismo alterno que permitirá reemplazar a la actividad normal cuando este no se encuentra disponible. Las acciones descritas dentro del plan de ejecución deben ser completamente claras y definidas de forma tal que sean de conocimiento y entendimiento inequívoco del personal involucrado en atender la contingencia.

VI. METODOLOGIA

El desarrollo del presente Plan seguirá la siguiente metodología basada en las siguientes cinco (5) fases:

a) Fase 1: Planificación.
b) Fase 2: Identificación de riesgos.
c) Fase 3: Identificación de soluciones.
d) Fase 4: Implementación.
e) Fase 5: Monitoreo.

6.1. Fase 1: Planificación

La fase de planificación es la etapa donde se definen los procesos y prepara el esfuerzo de planificación de contingencia/continuidad de los servicios informáticos.

6.1.1. Definición y mapeo de procesos

a) Identificación de Procesos Crítico

El objetivo es identificar y catalogar los procesos críticos del Gobierno Regional Puno, que son esenciales para la continuidad de las operaciones y servicios a la comunidad. Para logar se sugiere realizar las siguientes acciones:

Revisión de Documentación Existente:

- Recopilar y revisar la documentación existente sobre los procesos operativos del Gobierno Regional.
- Consultar manuales de procedimientos, informes de auditoría y registros históricos para obtener una visión general de los procesos.

Entrevistas con Personal Clave:

- Realizar entrevistas con líderes y personal clave de cada área del Gobierno Regional para identificar los procesos que consideran más críticos.
- Documentar la importancia y el impacto de cada proceso en la operación general de la entidad.

Análisis de Impacto:

- Evaluar el impacto potencial de la interrupción de cada proceso en las operaciones del Gobierno Regional y en la comunidad.

- Establecer criterios para definir la criticidad de los procesos (por ejemplo, impacto en la salud, seguridad, economía, etc.).

Catalogación de Procesos:

- Crear un catálogo de procesos críticos, clasificándolos según su nivel de criticidad y prioridad de recuperación.
- Asegurar que cada proceso identificado esté bien documentado y descrito.

Validación con Partes Interesadas:

- Presentar la lista de procesos críticos a las partes interesadas clave (directores, jefes de departamento, etc.) para su validación y ajustes necesarios.

b) Diagnóstico

El objetivo es realizar un diagnóstico detallado de los procesos críticos identificados para evaluar su estado actual, vulnerabilidades y áreas de mejora. Se sugieren realizar las siguientes acciones:

Análisis de Procesos:

- Desglosar cada proceso crítico en sus componentes y actividades específicas.
- Documentar los flujos de trabajo y las interdependencias entre los diferentes procesos.

Evaluación de Recursos:

- Identificar los recursos humanos, tecnológicos y materiales necesarios para la ejecución de cada proceso.
- Evaluar la disponibilidad y capacidad de estos recursos para soportar el proceso en condiciones normales y de contingencia.

Identificación de Vulnerabilidades:

- Analizar posibles vulnerabilidades y puntos de falla en cada proceso crítico.
- Evaluar riesgos asociados, tales como fallos tecnológicos, dependencia de proveedores externos, o falta de personal clave.

Evaluación de Desempeño Actual:

- Revisar indicadores de desempeño y eficiencia actuales de cada proceso.
- Identificar problemas recurrentes, cuellos de botella y áreas de baja eficiencia.

Recomendaciones para la Mejora:

- Proponer acciones correctivas y mejoras para fortalecer la resiliencia de cada proceso crítico.
- Recomendar actualizaciones tecnológicas, capacitaciones, o cambios en los procedimientos para mitigar las vulnerabilidades identificadas.

Informe de Diagnóstico:

- Elaborar un informe detallado con los hallazgos del diagnóstico de cada proceso crítico.

- Incluir un plan de acción con prioridades y plazos para implementar las mejoras recomendadas.

6.1.2. Evaluación de recursos

a) Inventario de Activos Tecnológicos

Es importante crear un inventario exhaustivo de todos los activos tecnológicos del Gobierno Regional Puno para evaluar su disponibilidad, condición y criticidad en relación con los procesos operativos. Para ello se sugiere realizar las siguientes acciones:

Recolección de Datos:
- Recopilar información sobre todos los activos tecnológicos actuales, incluyendo hardware, software, redes, bases de datos y otros recursos digitales.
- Utilizar registros existentes, como listas de equipos, licencias de software y contratos de mantenimiento.

Clasificación de Activos:
- Clasificar los activos tecnológicos según su tipo (por ejemplo, servidores, computadoras, dispositivos de red, etc.).
- Asignar un identificador único a cada activo para facilitar su seguimiento y gestión.

Evaluación de Condición y Utilización:
- Evaluar el estado actual de cada activo, incluyendo su antigüedad, condición física y rendimiento.
- Determinar la frecuencia de uso y la criticidad de cada activo en relación con los procesos operativos.

Documentación de Detalles:
- Documentar detalles importantes de cada activo, como el fabricante, modelo, número de serie, ubicación física, propietario y soporte técnico.
- Incluir información sobre contratos de mantenimiento, garantías y ciclos de actualización.

Verificación y Actualización del Inventario:
- Realizar una verificación física de los activos para asegurar la precisión del inventario.
- Establecer un proceso regular para la actualización y revisión del inventario.

b) Evaluación de Interdependencias

El objetivo es analizar las interdependencias entre los activos tecnológicos y los procesos operativos para identificar posibles puntos de falla y asegurar la resiliencia del sistema. Las acciones a realizar son:

Mapeo de Interdependencias:

- Crear un mapa de interdependencias que muestre cómo los activos tecnológicos están conectados entre sí y con los procesos críticos.
- Identificar sistemas y dispositivos que dependen unos de otros para funcionar correctamente.

Análisis de Puntos Críticos:

- Identificar los puntos críticos donde la falla de un activo puede tener un impacto significativo en múltiples procesos.
- Evaluar el riesgo asociado a cada punto crítico y su potencial impacto en la continuidad operativa.

Evaluación de Redundancias y Resiliencia:

- Revisar la existencia de sistemas redundantes y mecanismos de respaldo para los activos tecnológicos críticos.
- Evaluar la capacidad de recuperación y la resiliencia de los sistemas ante fallos y contingencias.

Documentación de Dependencias:

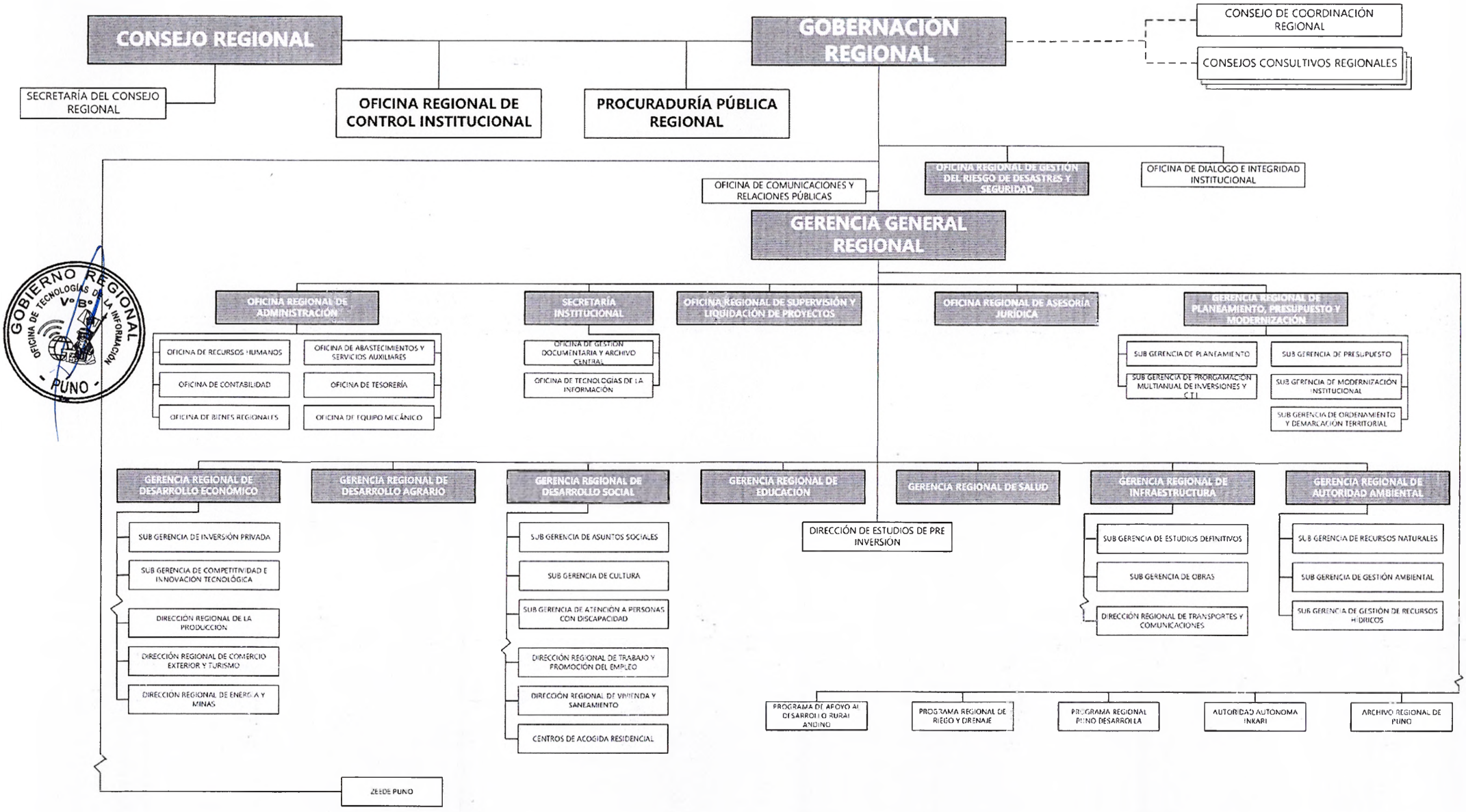
- Documentar todas las interdependencias y los puntos críticos identificados, detallando cómo se pueden mitigar los riesgos asociados.
- Incluir recomendaciones para mejorar la resiliencia y reducir las dependencias críticas.

Validación con Partes Interesadas:

- Presentar los hallazgos de la evaluación de interdependencias a las partes interesadas clave para su validación.
- Incorporar comentarios y ajustar el análisis según sea necesario.

6.1.3. Organización

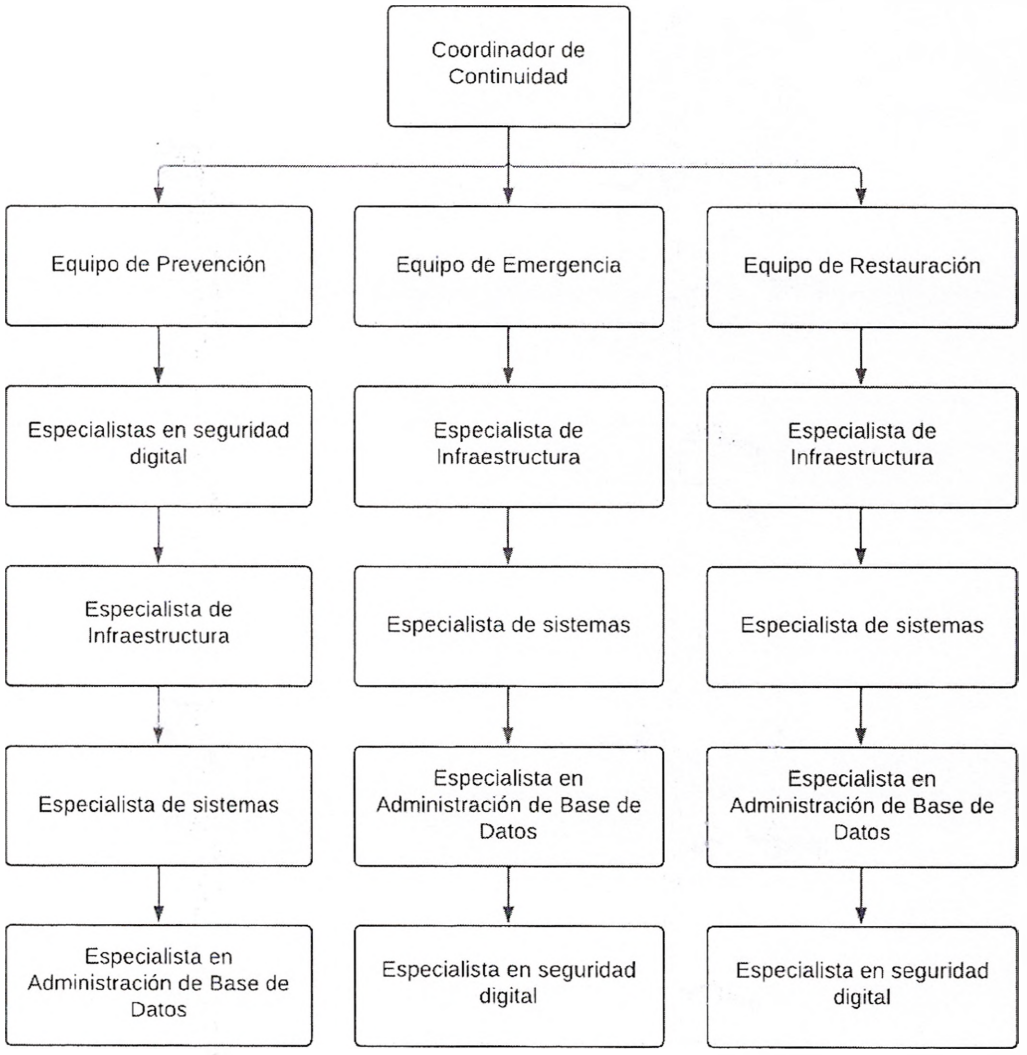
a) Organigrama estructural del Gobierno Regional Puno



Organigrama estructural del Gobierno Regional Puno

a) Definición del Organigrama del Equipo de Contingencia

Es necesario establecer un organigrama claro y funcional para el equipo de contingencia del Gobierno Regional Puno, asegurando que cada miembro tenga roles y responsabilidades bien definidos.



Descripción de Roles y Responsabilidades

Director de Continuidad

Será representado por el jefe de la OTI y tiene las siguientes funciones:

- Coordinar, dirigir y decidir respecto a acciones o a estrategias a seguir en caso de una situación de contingencia dada.
- Monitorear, supervisar y vigilar la recuperación de infraestructura de TI en el Centro de Datos.
- Tomar decisión de activar el Plan de Contingencia de Tecnologías de la Información.
- Declarar el evento de término de la ejecución de las operaciones del Plan de Contingencia tecnológica.

Equipo de Prevención

Es el equipo encargado de ejecutar las acciones preventivas, antes que ocurra un siniestro o desastre, con el fin de evitar se concrete el siniestro o desastre y en caso ocurriese, tener toras las herramientas o medios necesarios para realizar la recuperación de los servicios de tecnologías de la información, en el menor tiempo posible.

Especialista en seguridad digital

- Establecer y supervisar los procedimientos de seguridad e los servicios de TI.
- Coordinar la realización de pruebas de restauración de hardware y software.
- Participar en las pruebas de simulacro.
- Verificar las pruebas de copias de respaldo (backup).

Especialista en infraestructura:

- Contactar a los proveedores para el reemplazo de hardware, software y/o activación de servicios para los sistemas afectados.
- Verificar la realización del mantenimiento preventivo de los equipos del Centro de Datos.
- Mantener actualizado el inventario de hardware, software del Centro de Datos del Pliego.
- Ejecutar y verificar las copias de respaldo (backup).
- Programar el mantenimiento preventivo de los equipos de comunicaciones y de los equipos de Centro de Datos, considerando el tiempo de vida útil y garantía de los mismos.
- Elaborar informes técnicos de conformidad, luego de los mantenimientos efectuados.
- Elaborar informes periódicos del funcionamiento del centro de Datos.
- Mantener actualizado el diagrama de red, servidores y la documentación de configuración de los equipos de comunicaciones.
- Monitorear la red y definir medidas preventivas para minimizar las contingencias.
- Realizar pruebas previas de recuperación.
- Monitorear el funcionamiento de la central telefónica.
- Mantener actualizado el software que utiliza la central telefónica.
- Mantener actualizado la lista de teléfonos y anexos.

Especialista de sistemas

- Coordinar el manteamiento de los sistemas de información existentes.
- Mantener un control actualizado de las versiones de las fuentes de los sistemas de información y de los portales de la entidad.
- Mantener un control de la documentación y validación de los manuales de los sistemas en producción.
- Coordinar periódicamente las pruebas de restauración de las fuentes de los sistemas informáticos de la entidad.

Especialista en administración de base de datos

- Realizar copias de respaldo de las Bases de Datos de los aplicativos de la entidad.

- Realizar las pruebas de restauración de base de datos en coordinación con la especialista de seguridad de la Información.

Equipo de Emergencia

Es el equipo encargado de ejecutar las acciones requeridas durante la materialización del siniestro o desastre. Con el fin de mitigar el impacto que pueda tener en los equipos de TI, y procurando salvaguardar su pérdida o deterioro.

Especialista de infraestructura

- Informar sobre el desastre o incidencia al coordinador de Continuidad.
- Ejecutar las acciones de emergencia en los equipos informáticos y los componentes instalados en el centro de datos.
- Realizar la evaluación de condiciones de los equipos informáticos y comunicaciones del centro de datos durante la emergencia.
- Ejecutar las acciones de emergencia en los equipos.
- Informar al coordinador de continuidad de OTI las acciones de emergencias ejecutadas.

Especialista de sistemas

- Coordinar acciones para la verificación del estado de los sistemas informáticos, alojados en los servidores.
- Coordinas acciones para verificar el estado de base de datos de los sistemas informáticos del Gobierno Regional Puno.
- Coordinar acciones para verificar los logs de los sistemas informáticos afectados durante la emergencia.

Especialista en administración de base de datos

- Realizar la evaluación de la información almacenada en las diferentes bases de datos, durante la emergencia.

Especialista en seguridad digital

- Apoyar en labores de verificación y validación de operación de los servicios de TI.

Responsabilidades de todo el equipo

- Realizar la evaluación de la afectación de los equipos informáticos utilizado por los usuarios finales (Computadoras, estabilizadores, impresoras, teléfonos fijos, entre otros).
- Realizar la evaluación de la afectación de los equipos informáticos utilizado por los usuarios finales (Computadoras, estabilizadores, impresoras, teléfonos fijos, entre otros).
- Informa al coordinador de continuidad, sobre casos críticos encontrados en los equipos de los usuarios finales que afecta la continuidad de operaciones o pérdida de información.

Equipo de restauración

Es el equipo encargado de ejecutar todas las acciones después de haber sido controlado el desastre o siniestro, con el fin de restituir en el menor tiempo posible la operatividad de los equipos tecnológicos y recuperar el servicio informático, de manera conjunta con el coordinador de continuidad y los especialistas.

Especialista de infraestructura:

- Iniciar el proceso de recuperación de los servicios de TI, realizando pruebas de funcionamiento de los equipos afectados de infraestructura dentro de datos.
- Restaurar la información que afecten los servicios del centro de datos.
- Informar al coordinador de continuidad de TI las acciones de recuperación ejecutadas.
- Elaborar un informe técnico, que incluya las acciones de recuperación de los equipos de comunicación, central telefónica y de los equipos del centro de datos.
- Realizar la evaluación de las condiciones de los equipos de telecomunicaciones, durante la emergencia.

Especialista de sistemas

- Coordinar y verificar el estado de los sistemas alojados en los servidores de aplicaciones
- Coordinar el estado de la base de datos de los sistemas de información.
- Coordinar y monitorear la restauración de los sistemas de información y ejecución de pruebas para la verificación de su funcionalidad.
- Verificar que los sistemas de información estén funcionando correctamente.
- Elaborar un informe técnico que incluya la evaluación de condiciones de los sistemas de información.

Especialista en administración en base de datos

- Verificar el funcionamiento de las bases de datos.
- En caso sea requerido, realizar la creación de base de datos en servidores alternos.
- Restaurar las copias de respaldo correspondientes.
- Realizar las pruebas de funcionamiento.
- Elaborar un informe técnico que incluya la evaluación de condiciones de los datos, luego de afectado el proceso de recuperación.

Especialista en seguridad digital

- Supervisar la restauración de los servicios de TI.
- Validar la información documentada de los procedimientos de restauración utilizada.

Responsabilidad de todo el equipo

- Verificar el funcionamiento de los equipos de cómputo afectados, distribuyendo el trabajo.
- Solucionar problemas de conexión de los equipos informáticos, impresoras, escáner, entre otros.

- Elaborar un informe técnico que incluya la evaluación de condiciones de equipos informáticos de la entidad, luego de afectado el proceso de recuperación.

6.2. Fase 2 Identificación de riesgos

El desarrollo del plan de contingencia informático efectivo, es fundamental evaluar el impacto que tendría la interrupción de los servicios informáticos en el Gobierno Regional Puno. Tal interrupción podría provocar descontento entre los usuarios, pérdidas de equipos de hardware y software, pérdidas económicas, y un deterioro de la imagen institucional, entre otros efectos adversos.

En función de estos factores, es esencial encontrar un equilibrio entre las actividades de prevención y recuperación, teniendo en cuenta sus costos financieros respectivos. Como Oficina de Tecnologías de la Información, es crucial identificar los riesgos a los que se enfrenta la infraestructura de TI del Gobierno Regional Puno. Sin este conocimiento, es inviable formular un plan de contingencia que asegure la prevención y recuperación de la continuidad de los servicios informáticos frente a posibles desastres.
Para lograr esto, se deben enumerar y evaluar los riesgos potenciales, según su probabilidad e impacto. Este análisis permitirá identificar las posibles amenazas y determinar la probabilidad de que ocurran, así como detectar los puntos más vulnerables de la infraestructura de TI. Los resultados de este análisis detallado proporcionarán la información necesaria para proponer medidas de prevención y recuperación que se ajusten a las necesidades reales de los servicios proporcionados por el Gobierno Regional Puno.

Los desastres, ya sean causados por eventos naturales o humanos, pueden ocurrir en cualquier momento y lugar. Las causas más representativas que podrían desencadenar cada uno de los escenarios contemplados en el Plan de Contingencias se detallan en el siguiente cuadro.

Causas	Escenarios
Fallas de corte de cable UTP. Fallas de tarjeta de red. Fallas de punto de switch. Fallas de punto patch panel. Fallas de punto de red.	No hay comunicación entre la PC cliente y el servidor.
Fallas de componentes de hardware del servidor. Falta de suministro. Falla de software (sistema operativo, aplicación). Sobrepasar el límite de almacenamiento del disco. Servidor colapsado en su totalidad.	Falla de un servidor.
Accidente. Enfermedad. Renuncia intempestiva.	Ausencia parcial o permanente del personal de la OTI.
Corte general del fluido eléctrico de la red pública.	Interrupción del fluido eléctrico durante la ejecución de los procesos.
Fallas de equipos de comunicación (router, switch, antenas).	Pérdida del servicio de internet.

Fallas en el software de acceso a internet (proxy, firewall). Falla del servidor Pérdida del servicio por parte del proveedor de internet	
Incendio Sabotaje Corto circuito Terremoto	Indisponibilidad del parque informático (destrucción de la sala de servidores, daños en el parque informático y daños en la infraestructura del local).
Software malicioso Ciberataques Phishing Ransomware Vulnerabilidades en el software sin parchear Acceso no autorizado (hackeo)	Amenazas cibernéticas

Tabla 1: Escenarios y causas de incidencias

6.2.1. Procesos y recursos críticos

En este proceso se deben detallar los procesos, aplicaciones y recursos críticos con su expectativa del tiempo de recuperación:

Proceso	Aplicaciones y/o recursos	Tiempo de restauración
Gestión de infraestructura tecnológica	Equipos de comunicaciones	01 hora
	Equipos de protección eléctrica del dentro de datos entre otros	01 hora
	Infraestructura del Centro de Datos	01 hora
	Cableado de red de datos	01 hora
	Enlaces de cobre y fibra óptica para interconexión entre sede central y el centro de datos	01 hora
	Sistema de almacenamiento	01 hora
	Medios de respaldo (backup)	01 hora
	Servidores de red críticos: Directorio activo, File server, Base de datos	02 hora
	Central telefónica	01 hora
Desarrollo y mantenimiento de soluciones tecnológicas	Sistemas de información administrativos	02 horas
	Base de datos y repositorios utilizados por los sistemas y aplicativos	02 horas
Soporte técnico de las soluciones y recursos tecnológicos	Estaciones de trabajo personal crítico (computadores personales y portátiles)	02 horas
Gestión de gobierno Ti	Personal crítico responsable de los procesos del TIC	02 horas

Tabla 2: Procesos y recursos críticos de TI

El tiempo de recuperación objetivo debe ser determinado mediante juicio de expertos.

6.2.2. Identificación de amanezcas

Permite identificar aquellas amenazas que pudieran vulnerar los servicios de TI del Gobierno Regional Puno. Para la identificación de estos, debe considerarse la ubicación geográfica, el contexto actual de la sede central y el centro de datos, así como los juicios de expertos. Entre las amenazas, se sugiere incluir:

N°	Amenaza (Evento)	Tipo
01	Terremoto/Sismo.	Siniestros Naturales
02	Inundación y aniego en el centro de datos.	
03	Incendio en el centro de datos.	
04	Falla en telecomunicaciones.	Tecnológicos y/o cibernéticos
05	Incidente de seguridad informática	
06	Falla de hardware y software	
07	Falla del suministro eléctrico en el centro de datos y gabinetes de comunicación.	Físico y ambiental
08	Ausencia o no disponibilidad del personal crítico de TI.	Humanos
09	Pandemia y/o epidemia	Ambiental

Tabla 3: Tipos de amenazas a los servicios de TI.

Una vez determinadas las amenazas que pueden afectar los recursos críticos de TI, se calcula el nivel de probabilidad de ocurrencia, para lo cual se utilizó los valores definidos en la metodología de Gestión de riesgos que se encuentra en la siguiente Tabla:

Valor	Clasificación	Definición
1	Muy bajo	Puede que no se haya presentado u ocurrir en situaciones excepcionales (Por Ejemplo: Nunca ha ocurrido)
2	Bajo	Puede ocurrir en pocas situaciones (Por Ejemplo: Ha sucedido en la historia de la institución)
3	Medio	Puede ocurrir a largo plazo (Por Ejemplo: Ocurre una vez al año)
4	Alto	Se produce por tendencia o constantemente (Por Ejemplo: Ocurre una vez al mes)
5	Muy alto	Se produce a corto plazo y sin interrupciones (Por Ejemplo: Ocurre una o más veces a la semana)

Tabla 4: Determinación de la Probabilidad

En base a las dos tablas anteriores, debe detallarse el nivel de riesgo de cada una de las amenazas y la probabilidad de que estas ocurran.

N°	Amenaza (Evento)	Nivel de Probabilidad de ocurrencia (valor)	Nivel de Probabilidad Estimada
1	Terremoto/Sismo.	1	Muy bajo
2	Inundación y aniego en el centro de datos.	1	Muy bajo
3	Incendio en el centro de datos.	2	Bajo
4	Falla en telecomunicaciones.	3	Medio
5	Incidente de seguridad informática	3	Medio
6	Falla de hardware y software	3	Medio
7	Falla del suministro eléctrico en el centro de datos y gabinetes de comunicación.	4	Alto
8	Ausencia o no disponibilidad del personal crítico de TI.	3	Medio
9	Pandemia y/o epidemia	2	Bajo

Tabla 5: Probabilidad estimada de las amenazas a los servicios de TI

Cada amenaza debe ser evaluada basada en la experiencia y bajo el juicio de expertos.

6.2.3. Identificación de controles existentes

Identificar los controles existentes, permite conocer que tan protegidos están los recursos de TI frente a cada amenaza. Entre los controles pueden considerarse los siguientes:

- Cámaras de vigilancia para la seguridad física de los bienes informáticos.
- Grupo electrógeno para el centro de datos operativo.
- Mantenimiento de UPS.
- Mantenimiento de equipos de aire acondicionado del Centro de Datos.
- Redundancia en los enlaces de comunicaciones (tipo de conexión) y de internet.
- Sistema contra incendios en el Centro de Datos.
- Respaldo de información y custodia externa de medios de respaldo.
- Solución antivirus instaladas en los servidores de red y computadoras.
- Medidas de ciberseguridad.

6.2.4. Evaluación del Nivel de Riesgo

Para determinar el nivel de riesgo de un recurso de TI crítico, se consideran los controles existentes que mitigan la afectación de la amenaza descritos en el numeral 6.2.2, así como el valor del Nivel de probabilidad de ocurrencia identificado en la Tabla 4: Probabilidad estimada de amenazas de los servicios de TI, y los valores

definidos en la tabla de determinación del impacto (Tabla 6) y cálculo del nivel del riesgo (Tabla 8)

Nivel	Descripción	Impacto
5	Grave	Si el evento llegara a presentarse, tendría un trágico impacto, comprometiendo la confidencialidad o integridad de información crítica de la entidad o la continuidad de las operaciones por paralización de los servicios críticos más allá de los tiempos tolerables por el negocio.
4	Mayor	Si el evento llegara a presentarse, tendría un alto impacto comprometiendo la confidencialidad o integridad de información crítica de la entidad o la continuidad de las operaciones por paralización de los servicios críticos más allá de los tiempos tolerables por el negocio (se puede llegar a comprometer documentos internos clasificados como confidenciales, paralizar o retrasar procesos claves de la entidad por un tiempo considerable).
3	Moderado	Si el evento llegara a presentarse, tendría un moderado impacto sobre la confidencialidad, integridad y disponibilidad de la información es limitado en tiempo y alcance. Su efecto es para un proceso de soporte o actividad específica que puede subsanarse en corto plazo.
2	Menor	Si el evento llegara a presentarse, tendría un menor impacto (El impacto es leve y se puede prescindir del mismo en un tiempo limitado).
1	Insignificante	Si el evento llegara a presentarse, no representa un impacto importante para la entidad.

Tabla 6: Determinación del Impacto

Con los valores de la Tabla 6: Determinación del impacto, se realiza una tabla que cruza los recursos críticos de TI con las amenazas como se muestra a continuación:

Ítem	Recursos críticos / Amenazas	Terremoto	Inundación y aniego en el Centro de datos	Incendio en el Centro de Datos	Fallas en telecomunicaciones	Incidente de Seguridad Informática	Falla del suministro eléctrico en el Centro de -datos y gabinetes de comunicación	Falla del Hardware y software	Pandemia y/ epidemia
1	Equipos de comunicaciones.	5	5	5	4	5	3	5	1

2	Equipos de protección eléctrica del centro de datos y grupo electrógeno	5	5	5	1	5	3	5	1
3	Infraestructura del Centro de Datos	5	5	5	1	5	3	5	1
4	Cableado de red de datos	5	5	5	3	5	3	5	1
5	Sistema de almacenamiento	5	4	5	3	5	3	5	1
6	Servidores de red	5	4	5	3	5	4	5	1
7	Medios de respaldo	5	4	5	3	5	3	5	1
8	Sistemas de información portables web	5	4	5	1	5	4	2	1
9	Base de datos utilizados por los sistemas y aplicativos	5	4	5	2	5	4	5	1
10	Estaciones de trabajo del personal crítico (computadoras personales y portátiles)	4	5	5	2	5	4	5	1

Tabla 7: Resultado del impacto de los servicios de TI

La tabla debe llenarse de acuerdo a la determinación del impacto (Tabla 6).
El cálculo de nivel de riesgo se desarrolla considerando el mayor nivel de riesgo del recurso afectado por la amenaza es se está analizando. Para la identificación del nivel de riesgo se considera la siguiente matriz:

PROBABILIDAD						
	Muy Alto (5)	5	10	15	20	25
	Alto (4)	4	8	12	16	20
	Medio (3)	3	6	9	12	15
	Bajo (2)	2	4	6	8	10
	Muy Bajo (1)	1	2	3	4	5
		Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Grave (5)
		IMPACTO				

Tabla 8: Matriz del Nivel de Riesgo

A continuación, se obtendrá el resultado de la evaluación del riesgo de los servicios de TI:

Ítem	Recursos críticos / Amenazas	Terremoto	Inundación y aniego en el Centro de datos	Incendio en el Centro de Datos	Fallas en telecomunicaciones	Incidente de Seguridad Informática	Falla del suministro eléctrico en el Centro de datos y gabinetes de comunicación	Falla del Hardware y software	Pandemia y/ epidemia
1	Equipos de comunicaciones.	5	5	10	12	15	12	15	2
2	Equipos de protección eléctrica del centro de datos y grupo electrógeno	5	5	10	3	15	12	15	2
3	Infraestructura del Centro de Datos	5	5	10	3	15	12	15	2
4	Cableado de red de datos	5	5	10	9	15	12	15	2
5	Sistema de almacenamiento	5	4	10	9	15	12	15	2
6	Servidores de red	5	4	10	9	15	16	15	2
7	Medios de respaldo	5	4	10	9	15	12	15	2
8	Sistemas de información portables web	5	4	10	3	15	16	6	2
9	Base de datos utilizados por los sistemas y aplicativos	5	4	10	6	15	16	15	2
10	Estaciones de trabajo del personal crítico (computadoras personales y portátiles)	4	5	10	6	15	16	15	2

Tabla 9: Resultado de la evaluación de riesgos de los servicios de TI

La tabla debe ser llenada de acuerdo a la matriz del nivel de riesgo (Tabla 8).

6.3. Fase 3 Identificación de soluciones

A continuación, se presenta la propuesta de estrategias para la contingencia operativa en caso de desastres:

6.3.1. Estrategias de prevención de tecnologías de la información

a. Almacenamiento y respaldo
   - Realización de copias de respaldo de la información almacenada y procesada en el Centro de Datos.

- Realización de copias de instaladores de las aplicaciones, de software base, sistema operativo, utilitarios, etc.
- Verificar la ejecución periódica de las tareas programadas de respaldo de información y comprobación de los medios de respaldo.

Periodicidad: Trimestral
Responsables: Especialista de infraestructura y el especialista de seguridad digital.

b. Entorno de réplica
El plan incluye una estrategia para recuperar y ejecutar operaciones de sistemas en instalaciones alternativas por un periodo extendido, propios de la entidad. Y el especialista de Infraestructura, identifica un ambiente adecuado para la recuperación de equipos y servicios de tecnologías de la información del Centro de Datos.
Periodicidad: anual.
Responsables: Especialista de Infraestructura

c. Evaluación y gestión de proveedores
Actualizar el listado de proveedores claves de servicios y recursos de TI y mantener listas detalladas de necesidades de equipos y sus especificaciones técnicas.
Periodicidad: Semestral.
Responsables: Especialista de Infraestructura

d. Entrenamiento y personal de reemplazo
El personal de la OTI debe entrenarse en el proceso de recuperación de los servicios de TI. El entrenamiento se evalúa para verificar que ha logrado sus objetivos. Al inicio de cada año se debe realizar un programa de vacaciones que garantice la presencia permanente del personal crítico de las diferentes áreas y procesos de OTI, tales como soporte técnico, redes y comunicaciones, sistemas de información y bases de datos, así como seguridad de la información.
Periodicidad: Semestral.
Responsables: Especialista de seguridad digital

e. Renovación tecnológica
Se desarrolla la programación en el plan operativo Institucional que incluye acciones de renovación tecnológica.
Periodicidad: Anual.
Responsables: Especialista de Infraestructura

6.3.2. Estrategia frente a emergencias en tecnologías de la información
El alcance de las estrategias frente a emergencias involucra las acciones que deben realizarse durante una emergencia o desastre, a fin de salvaguardar la información del Gobierno Regional Puno y garantizar la continuidad de los servicios informáticos para lo cual se definen las acciones para mitigar las pérdidas que puedan producirse en una emergencia o desastre.

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

a. Notificar y reunir a los demás integrantes del equipo de Emergencia y Restauración.

b. Informar al coordinador de continuidad sobre la situación presentada, para decidir la realización de la Declaración de Contingencia.
c. Determinar si el área afectada es segura para el personal (en caso de catástrofe).
d. Estudiar y evaluar la dimensión de los daños a los equipos, y elaborar un informe de los daños producidos.
e. Proveer facilidades al personal encargado de la recuperación, con la finalidad de asegurar que se realicen las tareas asignadas en los procedimientos que forman parte de este plan.

6.4. Fase 4 Implementación

La implementación del presente plan debe iniciar en un plazo no mayor de treinta (30) días calendarios después de su aprobación y haber designado a los especialistas correspondientes.

Para tal efecto, el/la Oficial de Seguridad de la Información, en coordinación con el Especialista de infraestructura, realizaran las siguientes funciones:

a. Supervisar las actividades de copias de respaldo y restauración.
b. Establecer procedimientos de seguridad en los sitios de recuperación.
c. Organizar las pruebas de restauración de hardware, software y servicios de Tecnologías de Información (TI).
d. Participar en las pruebas y simulacros de desastres.

6.5. Fase 5 Monitoreo

Las acciones de monitoreo se deben realizar de manera trimestral y bajo un ambiente controlado, donde se comprueben que con las acciones definidas los bienes y servicios informáticos respondan de acuerdo a lo esperado, considerando que los procesos pueden variar y afectar la disponibilidad de los sistemas. Por lo que, es importante la ejecución de simulacros de interrupción de servicios informáticos, los cuales deben estar definidos, de forma que se pueda determinar el nivel de éxito de los mismos. Para dichos simulacros se debe considerar lo siguiente:

- Definir a los responsables del simulacro por las diferentes áreas interesadas.
- Evaluar los riesgos, validar el inventario de recursos.
- Elaborar un plan de atención del Centro de Datos, y según corresponda un plan de atención que abarque todos los bienes informáticos del Gobierno Regional Puno.
- Se debe comunicar a todo el personal de la Institución sobre los simulacros.
- Se debe realizar una evaluación conjunta con todos los responsables definidos para el simulacro, y plasmar en un documento las mejoras que se requieren plantear.
- Comunicar a todos los interesados el resultado de la evaluación del simulacro.

En base a los resultados obtenidos se realiza la modificación y mantenimiento del presente plan, para lo cual se establecen controles formales para dichas modificaciones. Asimismo, todos los responsables mencionados en el presente plan deberán tener conocimiento de los cambios. Como parte del mantenimiento del plan de contingencia, se debe contemplar el entrenamiento al personal de la OTI, a través de capacitaciones virtuales o presenciales de acuerdo a lo planificado por el coordinador de continuidad, y será de manera anual, a fin de

que puedan dar una respuesta adecuada a las eventualidades que puedan afectar los servicios informáticos.

VII. ANEXOS

Anexo 1: Clasificación de Riesgos.
Anexo 2: Listado de aplicaciones y sistemas de información.
Anexo 3: Listado de equipos del centro de datos.
Anexo 4: Formatos del plan de contingencia informático y restauración de la OTI.

ANEXO 1

Clasificación de Riesgos:

Los riesgos serán clasificados de acuerdo con los niveles definidos por los propietarios de Riesgos, según su grado de exposición, lo cual se muestra en la siguiente tabla:

Nivel	Criterio	Descripción
25 – 20	**EXTREMO**	Genera un alto impacto a la Institución y es muy probable que ocurran. Aquel riesgo que al presentarse puede causar una afectación directa a la estrategia, no se debe continuar con las actividades hasta que se realicen acciones que aporten a la mitigación de este.
16 – 12	**ALTO**	Genera un impacto a la Institución, y es más probable que ocurran. Aquel riesgo que al presentarse puede originar una afectación a los procesos de negocio, se debe realizar acciones correctivas a corto o mediano plazo a fin de mitigar el nivel de riesgo e iniciar acciones preventivas con el fin que el riesgo no se manifieste.
10 – 5	**MEDIO**	Genera un impacto a la Institución, y es probable que ocurran ocasionalmente. Aquel riesgo que al presentarse puede originar una afectación a los procesos de soporte, se debe tomar acciones a mediano o largo plazo a fin de que el riesgo no se manifieste.
4 – 3	**LIGERO**	Genera bajo impacto a la Institución y es poco probable que ocurran. Aquel riesgo que al presentarse no genera afectación en prestación de servicio de la Institución. Se recomienda actividades de retención del riesgo.
3 – 1	**BAJO**	No generan impacto a la Institución y es improbable que ocurra. Aquel riesgo que al presentarse no afecta el funcionar de la Institución. Se pueden continuar con las actividades sin llevar a cabo controles adicionales.

ANEXO 2

LISTADO DE APLICACIONES Y SISTEMAS DE INFORMACIÓN

N°	Sistema / Aplicativo	Descripción	Área usuaria	Motor DB	Tipo
1	SIAF	Sistema Integrado de Administración Financiera	Oficina de tecnologías de la información	Visual Fox Pro	Escritorio
2	SIGA	Sistema Integrado de Gestión Administrativa	Oficina de tecnologías de la información	SQL	Escritorio
3	SGD	Sistema de gestión documental	Oficina de tecnologías de la información	Postgresql	Web
4	SILUCIA	Sistema de logística y almacén	Oficina de abastecimiento y servicios auxiliares	MySQL	Web
5	SIEES	Sistema integrado de elaboración, evaluación y seguimiento de expedientes técnicos	Sub gerencia de estudios definitivos	MySQL	Web
6	COXHA	Sistema de conciliaciones	Oficina de contabilidad	MySQL	Web
7	MARI	Sistema de papeletas	Oficina de tecnologías de la información	MySQL	Web
8	ROCIO	Sistema de archivo	Oficina de tecnologías de la información	MySQL	Web
9	SONIX	Sistema de administración de usuarios	Oficina de tecnologías de la información	MySQL	Web
10	SEGMON	Sistema de seguimiento y monitoreo de obras	Sub gerencia de programación multianual de inversiones y C.T.I	MySQL	Web

ANEXO 3

LISTADO DE EQUIPOS (SERVIDORES) DEL DATA CENTER

N°	Tipo de equipo	Rol	Descripción de prioridad
1	Servidor Pentium II	SISABA Y SISALM	BAJA
2	Servidor Pentium IV	SERVIDOR ARCHIVOS Y BACKUPS	BAJA
3	Servidor Core 2 Quad	SERVIDOR DE ANTIVIRUS	BAJA
4	Servidor Core 2 Quad	BACKUP Y OTROS	BAJA
5	Servidor Core 2 Quad	SIAL	MEDIA
6	Servidor AMD OPTERON	SIGA	MEDIA
7	Intel(R) Xeon(R) CPU 2650	SIAF	ALTA
8	Servidor Core 2 Quad	SIEES	ALTA
9	Intel(R) Xeon(R) Silver 4114	SGD	ALTA

ANEXO 4

FORMATOS DEL PLAN DE CONTINGENCIA INFORMÁTICO Y RESTAURACIÓN

Evento: Terremoto/Sismo	**Formato 1**

1. PLAN DE PREVENCIÓN

a) Descripción del evento

Los sismos son movimientos en el interior de la tierra, que generan una liberación repentina de energía, que se propaga en forma de ondas provocando el movimiento del terreno.

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

Infraestructura

- Dependencias Gobierno Regional Puno y/o Data Center.

Recursos Humanos

- Personal de la entidad.

b) Entorno

Este evento puede afectar las instalaciones del Gobierno Regional Puno y del Centro de Datos (Data Center).

c) Personal Encargado

Equipo de prevención, el cual debe dar cumplimiento a las Condiciones de Prevención de Riesgo del presente Plan y realizar las acciones descritas en el punto e).

d) Condiciones de Prevención de Riesgo

- Inspecciones de seguridad realizadas periódicamente.
- Contar con un plan de evacuación de las instalaciones del Gobierno Regional Puno, el mismo que debe ser de conocimiento de todo el personal que labora en todas las sedes.
- Realización de simulacros de evacuación con la participación de todo el personal.
- Conformación de las brigadas de emergencia, y capacitarlas semestralmente.
- Mantenimiento de las salidas libres de obstáculos.
- Señalización de las zonas seguras y las salidas de emergencia.
- Funcionamiento de las luces de emergencia.
- Definición de los puntos de reunión en caso de evacuación.

e) Acciones preventivas

- Evaluar el ambiente para el Data Center.
- Establecer, organizar, ejecutar y supervisar procedimientos de respaldo y restauración de información base de datos, código fuentes y ejecutables.
- Programar, supervisar el mantenimiento preventivo a los equipos componentes del Data Center.

- Mantener actualizado el inventario hardware y software utilizado en el Data Center de la entidad.
- Llevar un control de versiones de las fuentes de los sistemas de información.

2. PLAN DE EJECUCIÓN

a) Eventos que activan la contingencia
La contingencia se activará al ocurrir un sismo o terremoto. El proceso de contingencia se activará inmediatamente después de ocurrir el evento.

b) Procesos Relacionados antes del evento
- Tener la lista actualizada de los servidores por Direcciones y/o Unidades.
- Mantenimiento del orden y limpieza de los ambientes de la Oficinas Centrales y Data Center.
- Inspecciones trimestrales de seguridad externa.
- Realización de simulacros internos en horarios que no afecten las actividades.

c) Personal que autoriza la contingencia informática
Coordinador de Continuidad de los servicios de la OTI.

d) Personal Encargado
Equipo de emergencia.

e) Descripción de las actividades después de activar la contingencia
- Desconectar el fluido eléctrico y cerrar las llaves de gas u otros líquidos inflamables si corresponde.
- Evacuar las oficinas de acuerdo a las disposiciones de los Brigadistas de Evacuación, utilizando las rutas establecidas durante los simulacros. Considerar las escaleras de emergencia, señalización de rutas, zonas de agrupamiento del personal, etc. Por ningún motivo utilizar los ascensores.
- Verificar que todo el personal del GORE Puno que labora en el área se encuentre bien.
- Brindar los primeros auxilios al personal afectado si fuese necesario.
- Alejarse de las lunas (ventanas) para evitar sufrir cortes por roturas y/o desprendimiento de trozos de vidrio.
- Evaluación de los daños ocasionados por el sismo sobre las instalaciones físicas, ambientes de trabajo, estanterías, instalaciones eléctricas, documentos, etc.
- Inventario general de documentación, personal, equipos, etc. y/o recursos afectados, indicando el estado de operatividad de los mismos.
- Limpieza de las áreas afectadas por el sismo. En todo momento se coordinará con personal de mantenimiento, para las acciones que deban ser efectuadas por ellos.

f) Duración
- Los procesos de evacuación del personal deberán ser calmados y demorar 5 minutos como máximo.
- La duración total del evento dependerá del grado del sismo, la probabilidad de réplicas y los daños a la infraestructura.

3. PLAN DE RECUPERACIÓN

a) Personal Encargado

Equipo de restauración, cuyo rol principal es asegurar el normal desarrollo de los servicios y operaciones de la OTI del GORE Puno.

b) Descripción de actividades

El plan de recuperación está orientado a recuperar en el menor tiempo posible las actividades afectadas durante la interrupción del servicio.

En caso, el evento haya sido de considerable magnitud, se deberá:

- Verificar la disponibilidad de recursos para la contingencia como: manuales técnicos de instalación del sistema de información, almacenamiento de datos, sistemas comunicación, hardware, y copias de respaldo.
- Establecer contacto con los proveedores clave y terceros para proporcionar instrucciones inmediatas y/o notificarles cualquier requisito de ayuda sobre la recuperación de negocio.
- Supervisar el progreso de las operaciones de recuperación y de servicios de TI.
- Restauración de los servicios y operaciones de TI. El equipo encargado, restaurará el espacio de trabajo para permitir que el personal crítico de la oficina pueda operar, para lo cual deberán:
  - ✓ Ejecutar los procedimientos de recuperación de la plataforma tecnológica. Verificar que las aplicaciones críticas se hayan recuperado y estén funcionando correctamente.
  - ✓ Confirmar los puntos de recuperación de datos de las aplicaciones. Verificar que las funcionalidades de comunicación están funcionando correctamente.
  - ✓ Verificar que equipos básicos como escáner, impresora estén disponibles y operacionales para dar soporte a los requisitos de la entidad.
  - ✓ Asegurar que el ambiente del área de trabajo, las aplicaciones y las telecomunicaciones están funcionando, una vez concluida la emergencia o siniestro.
  - ✓ Registrar todos los gastos operacionales relacionados con la continuidad del negocio.

c) Mecanismos de Comprobación

El equipo de recuperación presentará un informe al Coordinador de Continuidad de OTI explicando qué parte de las actividades u operaciones de tecnologías de la información han sido afectadas y cuáles son las acciones tomadas.

d) Desactivación del Plan de Contingencia

El Coordinador de Continuidad de OTI desactivará el Plan de Contingencia Informático una vez que se haya tomado las acciones descritas en el presente Plan de Recuperación.

e) Proceso de Actualización

El proceso de actualización será con base en el informe presentado por el Equipo recuperación, luego del cual se determinará las acciones a tomar.

Evento: Delito Informático	Formato 2

1. PLAN DE PREVENCIÓN

a) Descripción del evento

Alteración de datos de los portales y sistemas de información a través de ataque cibernético (hacking) y/o malware.

El malware es un software malicioso o software malintencionado, que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario, eliminando datos del equipo. Incluye virus, gusanos, troyanos, keyloggers, botnets, ransomwares o secuestradores, spyware, adware, hijackers, keyloggers, rootkits, bootkits, rogues, etc.

Este evento incluye los siguientes elementos mínimos identificados, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia, los cuales se muestran a continuación.

Hardware

- Servidores
- Estaciones de trabajo

Software

- Software base
- Sistemas de información aplicativos y portales

b) Entorno

Este evento se puede darse en cualquiera de los servidores y estaciones ubicadas en el Data Center en Oficinas Centrales.

c) Personal Encargado

Equipo de prevención, es el responsable del correcto funcionamiento de los servidores, estaciones de trabajo, sistemas de información y servicios de TI de acuerdo a sus perfiles.

d) Condiciones de Prevención de Riesgo

- Instalación de parches de seguridad en los equipos.
- Establecimiento de políticas de seguridad para prevenir el uso de aplicaciones no autorizadas en las estaciones de trabajo. Realización de simulacros de evacuación con la participación de todo el personal.
- Deshabilitación de los puertos de comunicación USB en las estaciones de trabajo que no los requieran habilitados, para prevenir la conexión de unidades de almacenamiento externo.
- Capacitación al Equipo de Prevención, sobre Ethical Hacking a las Bases de Datos, Sistemas Operativos, Servidores y Sistemas Informáticos.
- Ejecución de ataques de Hacking Ético por terceros especializados.

e) Acciones del Equipo de Prevención de la OTI

- Establecer, organizar, ejecutar y supervisar procedimientos de respaldo de información de la información procesada y almacenada en el Centro de Datos.
- Llevar un control de versiones de las fuentes de los sistemas de información.
- Realizar pruebas de restauración de la información almacenada en los repositorios y bases de datos.

- Documentar y validar los manuales de restauración de los sistemas de información en producción.

2. PLAN DE EJECUCIÓN

a) Eventos que activan la contingencia
   - Mensajes de error durante la ejecución de programas.
   - Lentitud en el acceso a las aplicaciones.
   - Falla general en el equipo (sistema operativo, aplicaciones).

b) Procesos Relacionados antes del evento
   Cualquier proceso relacionado con el uso de las aplicaciones en los servidores y en las estaciones de trabajo.

c) Personal que autoriza la contingencia informática
   Coordinador de Continuidad de los servicios de la OTI.

d) Personal Encargado
   Equipo de emergencia.

e) Descripción de las actividades después de activar la contingencia
   - Desconectar o retirar de la red de datos del GORE Puno, el servidor o la estación infectada o vulnerada.
   - Verificar si el equipo se encuentra infectado, utilizando un detector de malware/virus actualizado. En el caso de aplicaciones, verificar si el código o la información de las bases de datos ha sido alterada.
   - Rastrear de ser necesario el origen de la infección u ataque (archivo infectado, correo electrónico, hacking, etc.)
   - Guardar la muestra del virus detectado y remitirlo al proveedor del antivirus utilizado. En el caso de hacking a aplicaciones, se debe guardar el archivo modificado, a nivel de software y base de datos.
   - Eliminar el agente causante de la infección, es decir, remover el malware/virus del sistema.
   - Probar el sistema.
   - En caso no solucionarse el problema, formatear el equipo y restaurar copia de respaldo.

f) Duración
   La duración del evento no deberá ser mayor DOS HORAS en caso se confirme la presencia de un virus en estaciones de trabajo y de CUATRO HORAS en servidores de red. Esperar la indicación del Equipo de seguridad, Redes y Comunicaciones para reanudar el trabajo.

3. PLAN DE RECUPERACIÓN

a) Personal Encargado
   Equipo de restauración, luego de restaurar el correcto funcionamiento del servidor, estación de trabajo (PC, laptop), sistemas de información y portales web, coordinará con el usuario responsable del mismo y/o director del área para reanudar las labores de trabajo con el equipo o sistema que fue afectado.

b) Descripción de actividades
   Se informará al Coordinador de Continuidad de la OTI el tipo de malware/virus, o tipo de ataque encontrado y el procedimiento usado para removerlo.
   Estas actividades deben contemplar como mínimo:

- Instalación y puesta a punto de un cómputo compatible y hardware necesarios para la instalación del sistema de información con las características mínimas exigidas.
- Instalación y configuración del sistema operativo, drivers y servicios necesarios para el funcionamiento del sistema de información a recuperar.
- Instalación y configuración del sistema de información y el motor de la base de datos, con sus respectivas librerías y niveles de seguridad.
- Instalación de aplicaciones adicionales necesarias para el funcionamiento del sistema de información.
- Realización de la restauración de la base de datos con la última copia de seguridad disponible (Restore).
- Reinicio del servicio, prueba y afinamiento del sistema de información.
- Conectar el servidor o la estación a la red del GORE Puno.
- Efectuar las pruebas necesarias con el usuario final de los equipos y/o sistemas de información afectados.
- Solicitar la conformidad de la restauración realizada del equipo y/o sistema de información afectado.
- Comunicar el restablecimiento del servicio.

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

c) Mecanismos de Comprobación

Se llenará el formato de incidentes de seguridad de la información y se informará al Coordinador de Continuidad de la OTI. El personal del Equipo de Recuperación, presentará un informe al Coordinador de Continuidad de la OTI, explicando que parte del servicio u operaciones se han visto afectadas, y cuáles son las acciones tomadas.

d) Desactivación del Plan de Contingencia

El Coordinador de Continuidad de OTI desactivará el Plan de Contingencia Informático una vez que se haya tomado las acciones descritas en el presente Plan de Recuperación.

e) Proceso de Actualización

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

Evento: Falla de hardware y software	Formato 3

1. PLAN DE PREVENCIÓN

a) Descripción del evento

El hardware de servidores es el recurso principal para almacenar, procesar y proteger los datos, permitiendo acceso controlado y procesamiento de transacciones rápido para cumplir con los requisitos de las aplicaciones de la entidad.

El software

En ausencia del mismo, los sistemas de información que dependen del mismo no pueden funcionar, siendo la parte afectada o causa de la contingencia, los cuales se muestran a continuación:

Hardware

- Servidores
- Storage

Software

- Aplicativos usados por el GORE Puno y de servicio al ciudadano.

Información

- Información contenida en las bases de datos
- Información contenida en repositorios de información

b) Entorno

Se puede producir durante el servicio, afectando a las aplicaciones usadas para dar soporte a las operaciones del GORE Puno.

c) Personal Encargado

Equipo de prevención, es el responsable del correcto funcionamiento de los servidores, estaciones de trabajo, sistemas de información y servicios de TI de acuerdo a sus perfiles.

d) Condiciones de Prevención de Riesgo

- Revisión periódica de los registros (logs) de los servidores, para prevenir mal funcionamiento de los mismos.
- Contar con los backups diarios de datos de las aplicaciones en desarrollo/producción de la entidad, así como de las imágenes de los servidores.
- Contar con servicios de soporte y mantenimiento que contemple actividades de prevención, revisión del sistema y mantenimiento general.
- Disponer de servidores de bases de datos de contingencia, con la instalación del motor de base de datos.
- Disponer de servidores de Aplicaciones de contingencia, con software de instalación.

e) Acciones del Equipo de Prevención de la OTI

- Establecer, organizar, ejecutar y supervisar procedimientos de respaldo y restauración de información.
- Programar, supervisar el mantenimiento preventivo a los equipos componentes del Data Center.
- Mantener actualizado el inventario hardware y software utilizado en el Centro de Datos del Gore Puno.

- Realizar monitoreo del funcionamiento de los servidores instalados en el Centro de Dato para su correcto funcionamiento.
- Realizar revisiones de obsolescencia tecnológica de los servidores y componentes internos de forma anual.

2. PLAN DE EJECUCIÓN

a) Eventos que activan la contingencia
- Fallas en la conexión. Indisponibilidad del sistema de información y/o aplicativo.
- Identificación de falla en la pantalla de las estaciones de trabajo y/o servidores de aplicaciones..

b) Procesos Relacionados antes del evento
- Disponibilidad de las copias de respaldo.
- Disponibilidad de instaladores de sistemas operativos y motor de base de datos.

c) Personal que autoriza la contingencia informática
Coordinador de Continuidad de los servicios de la OTI.

d) Personal Encargado
Equipo de emergencia.

e) Descripción de las actividades después de activar la contingencia
- Realizar la revisión del servidor averiado, buscando un recurso de reemplazo verificando que dicho equipo cuente con garantía, de lo contrario se implementará un nuevo servidor virtual configurado de acuerdo a lo requerido.
- Solicitar las cintas de respaldo para poder proceder a la restauración de la Información almacenada en el servidor averiado.

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

3. PLAN DE RECUPERACIÓN

a) Personal Encargado
Equipo de restauración, luego de validar la corrección del problema de acceso a los servidores, y el Coordinador de Continuidad de la OTI informará a los directores y/o directores de áreas para la reanudación de las operaciones de los servicios afectados en el servidor averiado.

b) Descripción de actividades
El plan de recuperación estará orientado a recuperar en el menor tiempo posible las actividades afectadas durante la interrupción del servicio afectado por falla de los servidores.
Se debe realizar como mínimo las siguientes actividades:
- Instalación y puesta a punto de un cómputo compatible y hardware necesarios para la instalación del sistema de información con las características mínimas exigidas.
- Instalación y configuración del sistema operativo, drivers y servicios necesarios para el funcionamiento del sistema de información a recuperar.
- Instalación y configuración del sistema de información y el motor de la base de datos, con sus respectivas librerías y niveles de seguridad.

- Proceder a la restauración de las copias de respaldo, de la información de los servidores afectados.
- Verificar que la data y los aplicativos se hayan restaurado correctamente.
- Ejecutar pruebas de acceso a los sistemas y aplicaciones.
- Brindar los permisos de acceso a los usuarios finales.
- Remitir un mensaje electrónico a los usuarios del GORE Puno informando la reanudación de los servicios.

En función a esto, se tomarán las medidas preventivas del caso y se revisará el plan de contingencia para actualizarlo en caso sea necesario.

c) Mecanismos de Comprobación

Se registrará el incidente, en los dispositivos definidos por la Unidad de Gestión Informática, precisando las acciones realizadas.

El Equipo de restauración, presentará un informe al Coordinador de Continuidad de la OTI, explicando que parte del servicio u operaciones se han visto afectadas, y cuáles son las acciones tomadas.

d) Desactivación del Plan de Contingencia

El Coordinador de Continuidad de OTI desactivará el Plan de Contingencia Informático una vez que se haya tomado las acciones descritas en el presente Plan de Recuperación.

e) Proceso de Actualización

En base al informe presentado por el Equipo de restauración, quienes identifican las causas de la pérdida o fallas de la base de datos institucional, se determinará las acciones preventivas necesarias que deberían incluirse en el presente plan. En caso existiese información pendiente de actualización, el personal encargado deberá iniciar las labores de actualización de los procedimientos o guías de recuperación de servidores.

Evento: Falla del suministro eléctrico en el Centro de Datos y Comunicación	Formato 4

1. PLAN DE PREVENCIÓN

a) Descripción del evento

Falla general del suministro de energía eléctrica en el Centro de Datos. Este evento incluye los siguientes elementos mínimos identificados, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia:

Servicios Públicos:

- Suministro de energía eléctrica

Hardware

- Servidores y sistema de almacenamiento de información (storage).
- Estaciones de Trabajo.
- Equipos de Comunicaciones.

Equipos diversos

- UPS
- Aire acondicionado

b) Entorno

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

c) Personal Encargado

Equipo de prevención, es el responsable de realizar las coordinaciones para restablecer el suministro de energía eléctrica.

d) Condiciones de Prevención de Riesgo

- Durante las operaciones diarias del servicio u operaciones del Gore Puno se contará con los UPS necesarios para asegurar el suministro eléctrico en los equipos consideradas como críticos.
- Equipos UPS cuentan con mantenimiento preventivo y con suficiente energía para soportar una operación continua de 30 minutos como mínimo. El tiempo variará de acuerdo a la función que cumplan los equipos UPS.
- Realización de pruebas periódicas de los equipos UPS para asegurar su correcto funcionamiento.
- Capacidad de los UPS para proteger los servidores de archivos, base de datos y aplicaciones, previniendo la pérdida de datos durante las labores. La autonomía del equipo UPS no deberá ser menor a 30 minutos.
- Disponibilidad de UPS para proteger los equipos de vigilancia (cámaras, sistemas de grabación) y de control de acceso a las instalaciones del GORE Puno (puertas, contactos magnéticos, etc.)
- Coordinar la verificación del cableado eléctrico de Oficinas Centrales, una vez por año.
- Coordinar la instalación de luces de emergencia con tolerancia de 15 minutos, accionados automáticamente al producirse el corte de fluido eléctrico, los cuales deben estar instalados en los ambientes críticos.

e) Acciones del Equipo de Prevención de la OTI

- Revisar periódicamente y de forma conjunta con la Unidad de Servicios Administrativos las instalaciones eléctricas del Centro de Datos de la entidad.
- Coordinar y supervisar el mantenimiento preventivo de cableado a tierra, aire acondicionado de precisión del Data Center y UPS, trimestralmente.
- Verificar que la red eléctrica utilizada en el Data Center y la red de cómputo de Oficinas Centrales sea estabilizada. En caso no existan se debe gestionar la implementación de lo requerido con el área respectiva.
- Revisar la presencia de exceso de humedad en el Centro de Datos.

2. PLAN DE EJECUCIÓN

a) Eventos que activan la contingencia
Corte de suministro de energía eléctrica en los ambientes del GORE Puno.

b) Procesos Relacionados antes del evento
Cualquier actividad de servicio dentro de las instalaciones.

c) Personal que autoriza la contingencia informática
Coordinador de Continuidad de los servicios de la OTI.

d) Personal Encargado
Equipo de emergencia.

e) Descripción de las actividades después de activar la contingencia

- Informar a el/la director/a de la unidad o área el problema presentado.
- Comunicar a la empresa prestadora de servicios de energía eléctrica la falta de energía.
- Dar aviso del corte de energía eléctrica en forma oportuna a todas las áreas del GORE Puno y coordinar las acciones necesarias.
- Las actividades afectadas por la falta de uso de aplicaciones, deberán iniciar sus procesos de contingencia a fin de no afectar las operaciones en curso.
- En el caso de los equipos que entren en funcionamiento automático con UPS´s, se deberá monitorear el tiempo de autonomía del equipo y no exceder el indicado anteriormente.

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

3. PLAN DE RECUPERACIÓN

a) Personal Encargado
Personal del Equipo de restauración, son quienes se encargarán de realizar las acciones de recuperación necesarias.

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

- Al retorno de la energía comercial se verificará por el lapso de media hora que no haya interrupciones o fluctuaciones de energía.
- Proceder a encender la plataforma tecnológica ordenadamente de acuerdo al siguiente detalle:

- ✓ Equipos de Comunicaciones (router, switches core, switches de acceso).
- ✓ Equipos de almacenamiento (storage).
- ✓ Servidores físicos por orden de prioridad.
- ✓ Servidores virtuales por orden de prioridad.
- ✓ La contingencia finaliza cuando retorna la energía eléctrica y todos los equipos se encuentran operativos brindando servicio.

c) Mecanismos de Comprobación

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

d) Desactivación del Plan de Contingencia

El Coordinador de Continuidad de OTI desactivará el Plan de Contingencia Informático una vez que se recupere la funcionalidad del suministro eléctrico y la operatividad de los sistemas y servicios de tecnología de la información.

e) Proceso de Actualización

En base al informe que describe los problemas presentados, se determinarán las acciones de prevención a tomar.