San Isidro, 12 de Diciembre del 2024

RESOLUCION N° 000148-2024-PROMPERU/GG

Resolución de Gerencia General

VISTOS: El Informe N° 013-2024-PROMPERU/GG-OTI-BMF y el Memorando N° 344-2024-PROMPERU/GG-OTI de la Oficina de Tecnologías de la Información, el Informe N° 098-2024-PROMPERU/GG-OPP de la Oficina de Planeamiento y Presupuesto, y el Informe N° 561-2024-PROMPERU/GG-OAJ de la Oficina de Asesoría Jurídica;

CONSIDERANDO:

Que, según el artículo 2 de la Ley N° 30075, Ley de Fortalecimiento de la Comisión de Promoción del Perú para la Exportación y el Turismo – PROMPERÚ, la entidad es competente para formular, aprobar y ejecutar estrategias y planes de promoción de bienes y servicios exportables, así como de turismo interno y receptivo, promoviendo y difundiendo la imagen del Perú en materia turística y de exportaciones, de conformidad con las políticas, estrategias y objetivos sectoriales;

Que, el Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, tiene como objetivo establecer el marco de gobernanza del gobierno digital para la adecuada gestión de la identidad digital, servicios digitales, arquitectura digital, interoperabilidad, seguridad digital y datos, así como el régimen jurídico aplicable al uso transversal de tecnologías digitales en la digitalización de procesos y prestación de servicios digitales por parte de las entidades de la Administración Pública en los tres niveles de gobierno;

Que, en el literal b) del artículo 95 del 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, se indica que la gestión de riesgos de seguridad en el entorno digital está integrada en la toma de decisiones, diseño de controles de seguridad en los servicios digitales y procesos de la entidad;

Que, en el numeral 07 del punto 3.10 de la Resolución de Contraloría N° 320-2006-CG, Aprueban Normas de Control Interno, se establece que, para el adecuado ambiente de control en los sistemas informáticos, se requiere que éstos sean preparados y programados con anticipación para mantener la continuidad del servicio. Para ello se debe elaborar, mantener y actualizar periódicamente un plan de contingencia debidamente autorizado y aprobado por el titular o funcionario designado donde se estipule procedimientos previstos para la recuperación de datos con el fin de afrontar situaciones de emergencia;

Que, el numeral 1.1 del artículo 1 de la Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD, Establecen la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información en las entidades públicas, señala que las entidades públicas usan obligatoriamente la Norma Técnica Peruana NTP ISO/IEC 27001 vigente para el análisis, diseño, implementación, operación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información - SGSI. Asimismo, aseguran que el SGSI establezca como alcance mínimo a los procesos misionales y aquellos relevantes para la operación y funcionamiento de la entidad pública;

Que, de conformidad con la Resolución Directoral N° 022-2022-INACAL/DN, la NTP-ISO/IEC 27001 actual es la NTP-ISO/IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistema de gestión de la seguridad de la información. Requisitos. 3° Edición, en cuyo acápite 5.30. de la Tabla A.1. del Anexo A denominado "Preparación de las TIC para la continuidad del negocio", regula que, la preparación de las TIC debe planificarse, implementarse, mantenerse y probarse en función de los objetivos de continuidad del negocio y los requisitos de continuidad de las TIC;

Que, con Memorando N° 344-2024-PROMPERU/GG-OTI la Oficina de Tecnologías de la Información solicita la aprobación del Plan de contingencia de tecnologías de la información, remitiendo el Informe N° 013-2024-PROMPERU/GG-OTI-BMF elaborado por el señor Brandon José Luis Morales Fernández, Oficial de Seguridad Y Confianza Digital;

Que, mediante Informe N° 098-2024-PROMPERU/GG-OPP, la Oficina de Planeamiento y Presupuesto emite opinión, en el marco de sus competencias, recomendando la aprobación del Plan de Contingencia de Tecnologías de la Información;

Que, a través del Informe N° 561-2024-PROMPERU/GG-OAJ, de la Oficina de Asesoría Jurídica indica que resulta jurídicamente viable lo solicitado en relación con la emisión de la resolución de aprobación del Plan de Contingencia de Tecnologías de la Información;

De conformidad con lo dispuesto en el Decreto Legislativo N° 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital; el 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; la Resolución de Secretaría de Gobierno y Transformación Digital N° 003-2023-PCM/SGTD, Establecen la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información en las entidades públicas; la Resolución Directoral N° 022-2022-INACAL/DN; el literal g) del artículo 15 del Texto Integrado del Reglamento de Organización y Funciones de la Comisión de Promoción del Perú para la Exportación y el Turismo – PROMPERÚ, aprobado por Resolución de Presidencia Ejecutiva N° 060-2019-PROMPERU/PE; y, la Resolución de Presidencia Ejecutiva N° 174-2024-PROMPERU/PE;

Con el visto bueno de la Oficina de Tecnologías de la Información, la Oficina de Planeamiento y Presupuesto, y la Oficina de Asesoría Jurídica;

SE RESUELVE:

Artículo 1° – Aprobar el Plan de contingencia de tecnologías de la información de la Comisión de Promoción del Perú para la Exportación y el Turismo – PROMPERÚ, que en Anexo forma parte integrante de la presente Resolución.

Artículo 2° – Notificar la presente Resolución a la Secretaría de Gobierno y Transformación Digital de la Presidencia del Consejo de Ministros, para los fines pertinentes.

Artículo 3°.- El responsable de actualización de la información del Portal de Transparencia de PROMPERÚ, en un plazo no mayor de cinco (5) días calendario contados desde el día siguiente de ser notificado con la presente Resolución, deberá hacer la publicación correspondiente en el Portal de Transparencia de la Entidad.

Regístrese y comuníquese.

Firmado digitalmente
ANGEL WILDER NAVARRO DIAZ
Gerente General (e)

PLAN DE CONTINGENCIA DE TECNOLOGÍAS DE INFORMACIÓN DE PROMPERÚ

2024

Firmado digitalmente por
MORALES FERNANDEZ Brandon
Jose Luis FAU 20307167442 hard
Motivo: Doy V° B°
Fecha: 18.11.2024 16:14:06 -05:00

FIRMA DIGITAL
Firmado digitalmente por:
NAVARRO DIAZ Angel Wilder
FAU 20307167442 hard
Motivo: Doy V° B°
Fecha: 21/11/2024 13:03:06-0500

FIRMA DIGITAL
Firmado digitalmente por:
RENGIFO TAM William David
FAU 20307167442 hard
Motivo: Doy V° B°
Fecha: 18/11/2024 16:27:16-0500

Contenido

1. INTRODUCCIÓN

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

En tal sentido, y como buena práctica de TI se ha elaborado el Plan de Contingencia de tecnologías de la información de la Comisión de Promoción del Perú para la Exportación y el Turismo PROMPERÚ, dado que la Institución es vulnerable a diferentes hechos que pueden interrumpir los servicios informáticos y afectar el normal funcionamiento de las actividades en la Institución, lo que no sólo afecta a usuarios internos sino también a usuarios externos asimismo el Plan se encuentra alineado al Objetivo estratégico Institucional OEI.08 “Reducir la vulnerabilidad ante riesgos de desastres Fortalecer la capacidad operativa del PROMPERÚ”, del Plan Estratégico Institucional (PEI) 2022 – 2025.

Así, el presente plan establece los objetivos, el alcance y metodología del plan, a fin de lograr minimizar el impacto negativo de la interrupción de los servicios informáticos, contribuyendo a que la Institución esté preparada ante cualquier eventualidad de contingencia a nivel de tecnología de información, toda vez que se está considerando acciones del antes, durante y después de los incidentes.

2. MARCO TEORICO

2.1 PLAN DE CONTINGENCIA

Es un documento que reúne un conjunto de procedimientos alternativos para facilitar el normal funcionamiento de las Tecnologías de Información y de Comunicaciones (TIC), cuando alguno de sus servicios se ha afectado negativamente por causa de algún incidente interno o externo a la organización.

Este plan permite minimizar las consecuencias en caso de incidente con el fin de reanudar las operaciones en el menor tiempo posible en forma eficiente y oportuna. Asimismo, en cada plan de contingencia, se establece las acciones a realizarse en las siguientes etapas:

- Antes de la eventualidad, se contemplará la evaluación de la situación actual de las tecnologías de información en la Institución, a fin de mitigar el nivel de riesgo de las eventualidades. Su importancia radica en que las acciones permitirán disminuir la probabilidad de ocurrencia de una eventualidad que afecte los servicios informáticos.

- Durante la eventualidad, se contemplan estrategias frente a las emergencias. Las acciones descritas en estas estrategias permitirán recuperar la actividad normal frente a la emergencia.

- Después de la eventualidad, se contempla estrategias para la restauración o recuperación. Incluye las acciones a realizarse para regresar al estado normal de los servicios informáticos.

2.2 IMPORTANCIA DEL PLAN DE CONTINGENCIA DE TI

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

Beneficios de contar con un Plan de Contingencia de TI:

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

2.3 OBJETIVO DE TIEMPO DE RECUPERACIÓN (RTO)

Es un valor clave en la planificación de la continuidad del negocio y en la gestión de desastres de TI. El RTO indica el tiempo máximo tolerable que un sistema, aplicación o función crítica puede estar fuera de servicio antes de que su indisponibilidad afecte gravemente a la organización.

2.4 CÁLCULO DEL RTO

El cálculo del RTO no se basa en una fórmula matemática estricta, sino más bien en un análisis de negocio y riesgo. Se puede determinar a partir del juicio de experto de los especialistas o personal de la OTI, así como también, a partir de varios factores que dependen de la criticidad del sistema y del impacto en las operaciones si ese sistema está inactivo. Bajo estos criterios se van a establecer los RTO de los servicios o sistemas críticos de PROMPERU.

3. ANÁLISIS DE CONTEXTO INTERNO Y EXTERNO

Fortalezas	Debilidad
✓ Alto compromiso de la Alta Dirección ✓ Alta Dirección firma los documentos de seguridad ✓ Presupuesto para iniciativas de seguridad a los procesos de negocio ✓ Existe un comité de Gobierno y Transformación Digital ✓ Existe coordinación directa entre el oficial de seguridad y confianza digital y la Alta Dirección ✓ Dentro del PEI se ha incluido aspectos de protección de seguridad de la información ✓ Existe asistencia aceptable a las charlas de sensibilización en seguridad de la información ✓ Se tiene plataforma tecnológica actualizada (no existe tecnología legacy) ✓ Buen clima laboral ✓ Se realizan simulacros de sismo con la participación del personal.	✓ Falta de comunicación entre los líderes de los procesos y el Oficial de seguridad y confianza digital ✓ Falta de configuraciones y actualizaciones a las políticas de seguridad de los equipos de infraestructura ✓ No se Apoya en la capacitación permanente del personal responsable ✓ Posibilidad de conflicto de interés dado que el Oficial depende del jefe de TI ✓ Alta rotación de personal ejecutivos

Oportunidad	Amenazas
✓ Presupuesto para adquirir componentes de energía de contingencia en las sedes principales. ✓ Realización de Ethical Hacking para subsanar las vulnerabilidades ✓ Posibilidad de ampliar el alcance del SGSI	Aspecto político: ✓ Cambios en la alta Dirección Aspecto económico ✓ Falta de presupuesto para proyectos de protección de datos personales Aspecto tecnológico: ✓ Hackers que puedan aprovechar en Páginas webs tecnológicas (ocurrió en 2023 un incidente grave) ✓ Activación de malware en ellos equipos de usuarios finales que ingresan con sus equipos personales (algunos sin validación de antivirus dado que las licencias se encuentran limitadas) Aspectos legales: ✓ Sanciones y multas por incumplimiento de la ley de protección de datos personales (no se tiene implementado o registrado ningún banco de datos)

4. POLÍTICA DEL PLAN DE CONTINGENCIA DE TI

4.1. Desarrollo del Plan de Contingencia:

- Se debe desarrollar un plan de contingencia de TI que identifique los sistemas críticos, riesgos potenciales y procedimientos de recuperación.
- El plan debe incluir un análisis de impacto en el negocio para determinar la importancia de cada sistema y la prioridad en su recuperación.

4.2. Gestión de Riesgos:

- Se deben identificar y evaluar regularmente los riesgos que podrían afectar los servicios de TI, como fallas de hardware, ataques cibernéticos, desastres naturales o errores humanos.
- Se implementarán controles preventivos y mitigantes para reducir la probabilidad de ocurrencia de estos riesgos.

4.3. Procedimientos de Respaldo y Recuperación:

- Los datos críticos deben ser respaldados regularmente y almacenados en ubicaciones seguras.
- Los procedimientos de recuperación deben estar documentados y ser accesibles al personal autorizado.

4.4. Pruebas y Simulacros:

- El plan de contingencia debe ser probado periódicamente para asegurar su efectividad. Esto incluye simulacros de recuperación de sistemas críticos y validación de respaldos de datos.
- Los resultados de las pruebas deben ser documentados y utilizados para realizar ajustes en el plan.

4.5. Capacitación del Personal:

- Todo el personal de TI debe recibir capacitación sobre sus roles y responsabilidades en el plan de contingencia.
- Se deben realizar sesiones de capacitación anuales para actualizar el conocimiento y asegurar que todos estén preparados para una contingencia.

4.6. Revisión y Actualización:

- El plan de contingencia debe revisarse y actualizarse anualmente o después de cualquier cambio significativo en la infraestructura de TI o en los requisitos del negocio.
- Cualquier actualización debe ser aprobada por la alta dirección y comunicada al personal correspondiente.

4.7. Cumplimiento

- Todos los empleados y contratistas deben cumplir con esta política y seguir las pautas establecidas en el plan de contingencia de TI. El incumplimiento de esta política podría resultar en sanciones disciplinarias.

5. OBJETIVOS

5.1 Objetivo General

Establecer disposiciones para garantizar la continuidad de los servicios informáticos de PROMPERÚ, en caso de la ocurrencia de alguna eventualidad que interrumpa su funcionamiento, a fin que su restablecimiento sea en el menor tiempo posible.

5.2 Objetivo Específicos

- Identificar, analizar y proteger los servicios informáticos de PROMPERÚ ante riesgos posibles que pueden afectarlos y, por ende, afectar las operacionesde la Institución.
- Establecer actividades de preparación y acciones que permitan una restauración adecuada de los servicios informáticos en caso de interrupciones,de forma que no se tenga pérdida o afectación a la información.
- Contar con personal debidamente capacitado y organizado para afrontar adecuadamente las contingencias que puedan presentarse con respecto a los servicios informáticos de PROMPERÚ.
- Establecer actividades que permitan evaluar los resultados obtenidos de la ejecución del plan de contingencia, permitiendo a su vez una mejora continua a dicho plan.

6. CUMPLIMIENTO NORMATIVO

- Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado.
- Ley N° 28551, Ley que establece la obligación de elaborar y presentar planes de contingencia
- Ley N° 29664, Ley que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD).
- Ley N° 29733 - Ley de Protección de Datos Personales
- Decreto Supremo N° 018-2017 –PCM, Decreto Supremo que aprueba medidas para fortalecer la planificación y operatividad del Sistema Nacional de Gestión de Riesgos de Desastres mediante la adscripción y transferencia de funciones al Ministerio de Defensa a través del Instituto Nacional de Defensa Civil–INDECI y otras disposiciones.
- Decreto Supremo N° 034-2014-PCM, Decreto Supremo que aprueba el Plan Nacional de Gestión del Riesgos de Desastres - PLANAGERD 2014-2021.
- Decreto Supremo Nº 048-2011-PCM, Decreto Supremo que aprueba el Reglamento de la Ley Nº 29664, que crea el Sistema Nacional de Gestión del Riesgo de Desastres (SINAGERD).
- Decreto Supremo N° 083-2022-PCM - Reglamento de Seguridad Digital, Reglamento de Seguridad Digital, aprobado en 2022, establece que las entidades del sector público deben implementar políticas de seguridad digital, que incluyen la gestión de incidentes y contingencias.
- Directiva N° 003-2021-JUS/DGTAIPD - Directiva de Gestión de Riesgos de Seguridad de la Información.
- Directiva N° 001-2022-PCM/SEGDI - Gobierno Digital, que establece directivas para el Gobierno Digital, donde se enfatiza la necesidad de que las entidades públicas tengan un Plan de Contingencia para sus sistemas de TI, en línea con las normativas de gestión de la seguridad de la información.
- Resolución Ministerial N° 028-2015-PCM, aprobación de los Lineamientos para la Gestión de la Continuidad Operativa de las entidades públicas en los tres niveles de Gobierno.
- Resolución Ministerial N° 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana “NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición”, en todas las entidades integrantes del Sistema Nacional de Informática.
- Resolución Contraloría General Nº 320-2006-GC que aprueba las Normas de Control Interno para el Sector Público.

7. ALCANCE

Las disposiciones contenidas en el presente Plan de Contingencia son de cumplimiento obligatorio para PROMPERÚ y sus respectivas unidades de organización.

8. DEFINICIONES

8.1 Amenaza

Causa potencial de un incidente de seguridad de la información no deseado, que puederesultar en un daño para la organización o el sistema**.**

8.2 Malware

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, etc.

8.3 Plan de Contingencia

Plan que contiene las acciones a ejecutar en caso de la materialización del riesgo, con el fin de garantizar la continuidad de los servicios y parque informático de PROMPERÚ, en caso de la ocurrencia de alguna eventualidad que interrumpa su funcionamiento.

8.4 Probabilidad

Posibilidad de que un evento determinado ocurra en un periodo de tiempo dado.

8.5 Riesgo

Posibilidad de que suceda algún evento adverso que tendrá un impacto sobre el cumplimiento de los objetivos institucionales o de los procesos para la presentación de servicios al ciudadano. Se expresa en términos de probabilidad y consecuencias.

8.6 Sistema de Información

Es un conjunto de elementos organizados a fin de administrar datos e información necesarios para lograr un objetivo. Dichos sistemas están formados por personas, equipos y procedimientos.

8.7 Vulnerabilidad

Debilidad de un activo o grupo de activos o controles, que pueden ser explotadas por una o varias amenazas. Una vulnerabilidad en sí misma no causa daños.

9. METODOLOGÍA DE TRABAJO

Si bien los Planes de contingencia de tecnologías de la información se realizan a fin de prevenir fallas o accidentes en las operaciones de una entidad, para la elaboración de los mismos es importante tener en cuenta el estado de la infraestructura informática y de los servicios informáticos de la Institución, por lo que los planes de cada Institución son muy propios, y cuentan con 3 características principales comunes en todo su desarrollo, los cuales involucran acciones antes, durante y después de un incidente.

En ese sentido, para el desarrollo del presente Plan debemos guiarnos en una serie de fases que van desde la planificación hasta la mejora continua, a fin de establecer un ciclo de vida que permita optimizar los esfuerzos en función de preservar la operatividad de TI en PROMPERÚ. Por ello se tiene lo siguiente:

- ✓ Fase 1: Planificación
- ✓ Fase 2: Determinación de Vulnerabilidades
- ✓ Fase 3: Estrategias del Plan de Contingencia
- ✓ Fase 4: Elaboración del Plan de Contingencia
- ✓ Fase 5: Implementación del Plan de Contingencia
- ✓ Fase 6: Monitoreo

Metodología de implementación de un Plan de Contingencia de TI

Elaboración propia

A continuación, se detallan cada uno de las fases:

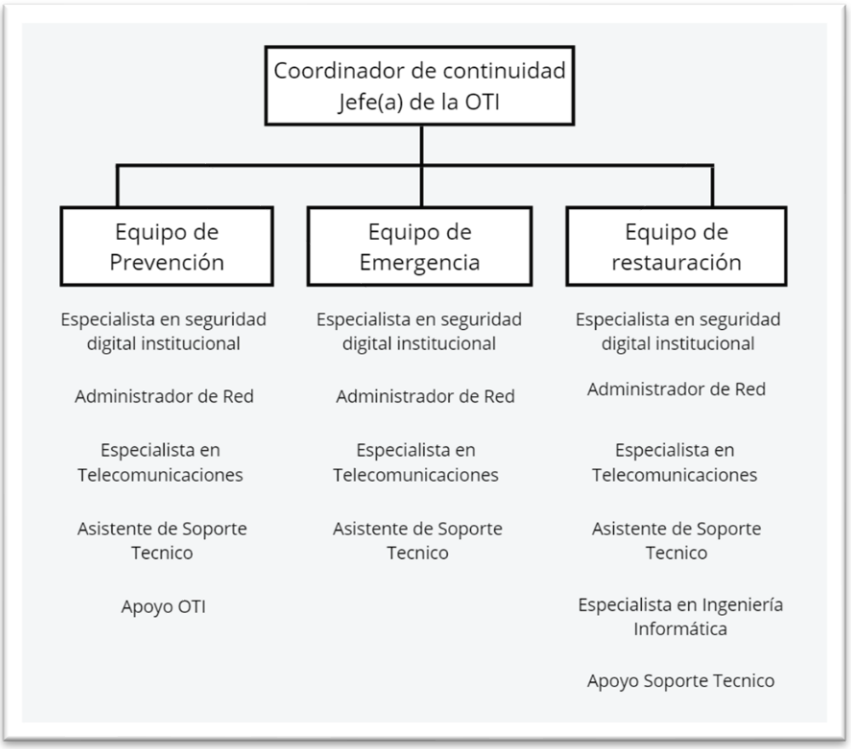
9.1 Fase 1: Planificación

Organización

La Oficina de Tecnologías de la Información (OTI), depende directamente de la Gerencia General (GG), y es responsable de administrar y brindar soluciones informáticas y soporte técnico en materia de tecnologías de la Información (TIC) a los órganos de PROMPERÚ, para la mejor ejecución de susfunciones, así como, desarrollar el soporte tecnológico y soluciones informáticas para la operatividad de la red nacional de información científica e interconexión telemática.

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

Organigrama de la organización del plan de contingencias de Tecnologíasde la Información



Fuente: Elaboración propia

Roles, funciones y responsabilidades dentro del Plan

A continuación, se describe los roles, responsabilidades y funciones que deben desarrollar los distintos equipos del Plan de Contingencia de Tecnologías de la Información:

9.1.1. Coordinador de Continuidad.

Sera representado por el/la jefe(a) de la OTI y tiene las siguientes funciones:

- Coordinar, dirigir y decidir respecto a acciones o estrategias a seguiren caso de una continencia dado.
- Monitorear, supervisar y vigilar la recuperación de infraestructura deTI 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 delPlan de Contingencia de Tecnologías de la Información, cuando las operaciones del centro de datos hayan sido restablecidas.

9.1.2. 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 todas las herramientas omedios necesario para realizar la recuperación de los servicios de tecnologías de la información, en el menor tiempo posible.

El responsable del Equipo de Prevención es el Oficial de Seguridad y Confianza Digital. A continuación, se detalla las funciones por cada miembrodel equipo de prevención:

Oficial de Seguridad y Confianza Digital:

- Establecer y supervisar los procedimientos de seguridad de losservicios de TI.
- Coordinar la realización de pruebas de restauración de hardware y Software.
- Participar en las pruebas de simulacro.

Especialista en Telecomunicaciones:

- 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 delCentro de Datos de PROMPERÚ.
- Ejecutar, verificar y probar 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 deDatos.
- Mantener actualizado el diagrama de red, servidores y ladocumentación de configuración de los equipos de comunicaciones.
- Monitorear la red y definir medidas preventivas para minimizar las contingencias.
- Realizar pruebas de funcionamiento 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 críticos.

Especialista en Ingeniería Informática:

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

Especialista en Administración de Base de Datos:

- Realizar copias de respaldo de las Bases de Datos de los aplicativosde la entidad.
- Realizar las pruebas de restauración de base de datos.

9.1.3 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 impactoque pueda tener en los equipos de TI de PROMPERÚ, y procurando salvaguardar su pérdida o deterioro.

El responsable del Equipo de emergencia es el responsable de infraestructura y telecomunicaciones.

A continuación, se detalla las funciones por cada miembro del equipo de emergencia:

Especialista en Telecomunicaciones:

- 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 de PROMPERÚ.
- Realizar la evaluación de condiciones de los equipos informáticos y comunicaciones del Centro de Datos durante la emergencia.
- Informar al coordinador de Continuidad de OTI las acciones deemergencias ejecutadas.

Especialista en Ingeniería Informática:

- Coordinar acciones para la verificación del estado de los sistemas informáticos, alojados en los servidores de aplicaciones.
- Coordinar acciones para verificar el estado de la base de datos de los sistemas informáticos de PROMPERÚ.
- Coordinar acciones para verificar los logs de los sistemasinformáticos afectados durante la emergencia.

Administrador de Base de Datos:

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

Asistente de Soporte Técnico:

- Realizar la evaluación de la afectación de los equipos informáticos utilizado por los usuarios finales (Computadoras, estabilizadores, impresoras, celulares, 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.

Oficial de Seguridad y Confianza Digital:

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

9.1.4. Equipo de Restauración.

Es el equipo encargado de ejecutar todas las acciones después de habersido controlado el desastre o siniestro, con el fin de restituir en el menortiempo posible la operatividad de los equipos tecnológico y recuperar el servicio informático de PROMPERÚ, de manera conjunta con elcoordinador de Continuidad y los especialistas.

El responsable del Equipo de restauración es el Especialista de infraestructura y telecomunicaciones. A continuación, se detalla las funciones por cada miembro del equipo de restauración:

Especialista en Telecomunicaciones:

- Iniciar el proceso de recuperación de los servicios de TI, realizando pruebas de funcionamiento en los equipos afectados deinfraestructura del centro de datos de PROMPERÚ.
- Restaurar la información de los equipos afectados de la infraestructura informática que afecten los servicios del centro de datos de PROMPERÚ.
- 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.
- Iniciar el proceso de recuperación de los servicios relacionado a la Central telefónica de PROMPERÚ.
- Realizar la evaluación de las condiciones de los equipos de telecomunicaciones, durante la emergencia.

Especialista en Ingeniería Informática:

- 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 condicionesde los sistemas de información de PROMPERÚ.

Administrador de Base de Datos:

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

Asistente de Soporte Técnico:

- Verificar el funcionamiento de los equipos de cómputo de PROMPERÚ afectada, distribuyendo el trabajo entre los técnicos de soporte.
- 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 PROMPERÚ, luego de afectado el proceso de recuperación.

Oficial de Seguridad y Confianza Digital:

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

9.2 Fase 2: Determinación de Vulnerabilidades

En esta fase se realiza la identificación de las aplicaciones críticas, los recursos y el periodo máximo de recuperación de los servicios de TI de PROMPERÚ, considerando todos los elementos susceptibles de provocar eventos que conlleven activar la contingencia.

9.2.1. Procesos y recursos críticos

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

Tabla N° 1 – Procesos y recursos críticos de TI

Proceso	Aplicaciones y/o recursos	Tiempo de Recuperación (RTO)
infraestructura Tecnológica y Comunicaciones	Equipos de comunicaciones	24 h
	Equipos de protección eléctrica del centro de datos (UPS)	48 h
	Cableado de red de datos	24 h
	Enlaces de cobre y fibra óptica para interconexión entre la sede central y el centro de datos	12 h
	Sistema de almacenamiento - storage	48 h
	Medios de respaldo (backup)	24 h
	Servidores de red críticos: Directorio Activo, File Server,Base de Datos, otros.	24 h
	Central Telefónica	24 h
Desarrollo y Mantenimiento de soluciones tecnológica	Sistemas de información administrativos	48 h
	Base de datos y repositorios utilizados por los sistemas Y aplicativos.	48 h
Soporte Técnico de las Soluciones y Recursos Tecnológicos	Estaciones de trabajo del personal crítico (computadoraspersonales y portátiles)	24 h
Jefatura de OTI	Personal crítico responsable de los procesos de TIC	12 h

RTO: Tempe de recuperación objetivo, es determinado mediante Juicio de expertos.

9.2.2. Identificación de amenazas

Permite identificar aquellas amenazas que pudieran vulnerar los servicios de TI de PROMPERÚ, considerando la ubicación geográfica, el contexto actual de la sede central y centro de datos, así como del juicio de experto.

Tabla N° 2 – Tipos de Amenazas a los servicios de TI

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
05	Ataque cibernético.	
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

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:

Tabla N° 3 – Determinación de la Probabilidad

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

A continuación, se detalla el resultado obtenido, en base a la metodología de gestión de riesgos, mediante la cual se ha determinado el valor de probabilidad por cada amenaza**:**

Tabla N°4 – Probabilidad estimada de las amenazas a los servicios de TI

N°	Amenaza (Evento)	Nivel de Probabilidad de ocurrencia (valor)	Nivel de Probabilidad Estimada
1	Terremoto	2	Bajo
2	Inundación y aniego en el Centro de Datos	1	Muy Bajo
3	Incendio en el Centro de Datos	1	Muy Bajo
4	Falla en telecomunicaciones	3	Medio
5	Ataque cibernético	3	Medio
6	Falla del suministro eléctrico en el Centro de Datos y gabinetes de comunicación	3	Medio
7	Falla del hardware y software	3	Medio
8	Ausencia o no disponibilidad del personal crítico de TI	2	Bajo
9	Pandemia y/o Epidemia	2	Bajo

9.2.3. Identificación de controles existentes

La identificación de controles existentes, permiten conocer que tan protegidos están los recursos de TI de PROMPERÚ frente a cada amenaza. Los controles existentes son los siguientes:

9.2.3.1. Cámaras de vigilancia para la seguridad física de los bienes informáticos.
9.2.3.2. Mantenimiento de UPS. El mantenimiento de UPS está a cargo de la OTI.
9.2.3.3. Mantenimiento para equipos de aire acondicionado del Centro de Datos.
9.2.3.4. Redundancia en los enlaces de comunicaciones (fibra óptica).
9.2.3.5. Sistema contra incendios en el Centro de Datos. (extintores).
9.2.3.6. Respaldo de información y custodia de medios de respaldo.

9.2.3.7. Solución antivirus instalada en los servidores de red y computadoras.

9.2.4. Evaluación del Nivel de Riesgo

Para determinar el Nivel de Riesgo de un recurso de TI crítico de PROMPERÚ, se consideraron los controles existentes que mitigan la afectación de la amenaza descritos en el numeral 7.2.2, así como el valor del Nivel de Probabilidad de ocurrencia Identificado en la tabla N° 3 – Probabilidad estimadade las amenazas a los servicios de TI, y los valores definidos de acuerdo a la aplicación de la metodología de gestión de riesgos descrita tabla de impacto (Tabla N°5) y cálculo del nivel de riesgo (Tabla N° 7).

Para calcular el resultado del impacto, se considera el valor del nivel del impacto, definido en la aplicación de la metodología de Gestión de riesgos, de acuerdo a la siguiente tabla:

Tabla N°5 Determinación del Impacto:

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 críticosmás 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 deinformación 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.

El valor obtenido ha sido en base a la metodología de Gestión de Riesgos (Tabla N°5) que ha determinado el impacto por cada amenaza, siendo el resultado siguiente:

Tabla N°6 Resultado del impacto de los servicios de TI

Item	Recursos Críticos / Amenazas (Eventos)	Terremoto	Inundación y aniego en el Centro de Datos	Incendio en el Centro de Datos	Falla en telecomunicaciones	Ataque cibernético	Falla del suministro eléctrico en el Centro de Datos y gabinetes de comunicación	Falla del hardware y software	Ausencia o no disponibilidad del personal crítico de TI	Pandemia y/o Epidemia
1	Equipos de comunicaciones.	4	4	5	5	5	2	3	2	1
2	Equipos de protección eléctrica del centro de datos (UPS)	4	4	5	2	1	2	4	3	1
3	Aire acondicionado del Centro de Datos.	4	4	5	1	1	2	4	3	1
4	Infraestructura del Centro de Datos.	4	4	5	1	1	3	5	4	3
5	Cableado de red de datos.	4	4	5	3	1	1	3	2	1
7	Sistema de almacenamiento (storage).	4	4	5	3	5	2	4	3	1
8	Servidores de red	4	4	5	3	5	2	5	4	1
9	Medios de respaldo	4	4	5	3	5	2	3	3	1
10	Sistemas de información y portales web	4	4	5	3	5	2	5	4	1
11	Base de datos utilizados por los sistemas y aplicativos.	4	4	5	3	5	2	5	4	1
12	Estaciones de trabajo del personal crítico (computadoras personales y portátiles)	4	4	5	3	5	2	3	3	2

Cálculo del Nivel de Riesgo: Se desarrolla considerando el mayor Nivel de Riesgo del recurso afectado por la amenaza que se está analizando. Para la identificación del Nivel de Riesgo se considera la siguiente matriz:

Tabla N° 7 Matriz del Nivel de Riesgo

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				

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

Tabla N° 8 – Resultado de la evaluación de riesgos de los servicios de TI

Item	Recursos Críticos / Amenazas (Eventos)	Terremoto	Inundación y aniego en el Centro de Datos	Incendio en el Centro de Datos	Falla en telecomunicaciones	Ataque cibernético	Falla del suministro eléctrico en el Centro de Datos y gabinetes de comunicación	Falla del hardware y software	Ausencia o no disponibilidad del personal crítico de TI	Pandemia y/o Epidemia
1	Equipos de comunicaciones.	8	8	5	15	15	6	9	4	1
2	Equipos de protección eléctrica del centro de datos (UPS)	8	8	5	6	3	6	12	9	1
3	Aire acondicionado del Centro de Datos.	8	8	5	3	3	6	12	6	1
4	Infraestructura del Centro de Datos.	8	8	5	3	3	9	15	8	3
5	Cableado de red de datos.	8	8	5	9	3	3	9	4	1
7	Sistema de almacenamiento (storage).	8	8	5	9	15	6	12	6	1
8	Servidores de red	8	8	5	9	15	6	15	8	1
9	Medios de respaldo	8	8	5	6	15	6	9	6	1
10	Sistemas de información y portales web	8	8	5	9	15	6	15	8	1
11	Base de datos utilizados por los sistemas y aplicativos.	8	8	5	9	15	6	15	8	1
12	Estaciones de trabajo del personal crítico (computadoras personales y portátiles)	8	8	5	9	15	6	9	6	2

9.2.5. Escenarios de riesgo

Se han establecido los siguientes escenarios que corresponden a amenazas con probabilidad de nivel medio o superior:

a) Destrucción e indisponibilidad del centro de datos por terremoto.
b) Falla en el funcionamiento de los sistemas de información y portales web por delito informático (ataque cibernético, virus, etc.).
c) Indisponibilidad de los servidores de red por falla de hardware y software.
d) Interrupción de comunicaciones por fallas en el suministro eléctrico del Centro de Datos y/o en los gabinetes de comunicación de la sede central.
e) Falla en los equipos de telecomunicaciones de PROMPERÚ.

A continuación, se detallan los escenarios de riesgo y su impacto, para activar el Plan de Contingencia de Tecnologías de la Información conforme a la aplicación de la clasificación de gestión de riesgos que se describe en el Anexo N° 1

Tabla N° 9 – Escenario de Riesgos

Escenario de Riesgo	Descripción	Impacto
a) Destrucción e indisponibilidad del centro de datos	Este escenario consiste en que el Centro de Datos deje de funcionar o se destruya, como resultado de un terremoto o incendio, lo cual podría ocasionar caídas de servicios y destrucción de los equipos informáticos alojados en el centro datos, como también los componentes del mismo.	Extremo
b) Falla en el funcionamiento de los sistemas de información y portales web	Se refiere a la falla lógica o caída de los sistemas de información, aplicativos y portales web, lo cual produce que la información o servicios brindados por ellos no estén disponibles.	Extremo
c) Indisponibilidad de los servidores de red por falla de hardware y software.	Se refiere al fallo físico o lógico de los servidores físicos y virtuales, lo cual produce que la información o servicios brindados por ellos no estén disponibles.	Extremo
d) Interrupción de comunicaciones por fallas en el suministro eléctrico del Centro de Datos y/o en el gabinete de comunicación de PROMPERÚ	Este escenario consiste en el corte o interrupción de las comunicaciones entre la sede central y el centro de datos, así como los servicios publicados en internet, como resultado de fallas del sistema eléctrico o equipos de suministro eléctrico, así como el corte de energía eléctrica, lo cual ocasionar caídas de servicios informáticos y pérdidas de comunicación en los equipos de infraestructura tecnológica.	Alto
e) Falla en los equipos de telecomunicaciones de PROMPERÚ	Se refiere al fallo físico o lógico de los equipos de comunicaciones (Switches, Firewall, Controlador etc.) lo cual produce que la información o servicios brindados por ellos no estén disponibles.	Extremo

9.3 Fase 3: Estrategias del Plan de Contingencias

A continuación, se presentan estrategias para la contingencia operativa en caso de un desastre:

9.3.1. Estrategias de prevención de tecnologías de la información

a) Almacenamiento y respaldo

1. Realización de copias de respaldo de la información almacenada y procesada en el Centro de Datos.

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

3. 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 Oficial de Seguridad y Confianza 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 y UTI, 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: Oficial de Seguridad y Confianza 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

9.3.2. 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 de PROMPERÚ 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:

Acciones durante la emergencia

1. Notificar y reunir a los demás integrantes del equipo de Emergencia y Restauración.
2. Informar al coordinador de continuidad sobre la situación presentada, para decidir la realización de la Declaración de Contingencia.
3. Determinar si el área afectada es segura para el personal (en caso de catástrofe).
4. Estudiar y evaluar la dimensión de los daños a los equipos, y elaborar un informe de los daños producidos.
5. 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.

9.3.3. Estrategia para la restauración de tecnologías de la información

El alcance de las estrategias para la restauración o recuperación involucra las acciones que deben realizarse luego de suscitada una emergencia o desastre, a fin de recuperar la información y los servicios informáticos de PROMPERÚ para estabilizar la infraestructura tecnológica luego del evento suscitado.

El ciclo considerado para la estrategia de recuperación de tecnologías de la información es el siguiente:

Tabla N° 6 – Prioridad de atención durante la restauración de TI

Prioridad de Atención	Descripción
1	Atención prioritaria: Sistemas de información y equipos que requieran alta disponibilidad de atención a los usuarios y manejen alto volumen de información. Ejemplo: Trámite documentario, Sistema Administrativo Financiero (SIAF), Sistema de gestión administrativa (SIGA), Portal Web institucional, servidores de bases de datos, entre otros.
2	Atención normal: Sistemas de información y equipos no relacionados con la atención a los usuarios y manejen bajo volumen de información. Ejemplo: Sistemas que no requirieran conectividad y/o que cuenten con mayor plazo para la consulta y disponibilidad de información, etc
3	Atención baja: Sistemas de información de uso interno, uso poco frecuente y/o que manejan bajo volumen de información. Asimismo equipos de apoyo. Ejemplo: Intranet entre otros

Los sistemas de información y equipos informáticos, con la respectiva prioridad de atención, en caso de activarse la contingencia informática, se describen en el Anexo N° 2 y Anexo N° 3.

9.4 Fase 4: Elaboración del Plan de Contingencia

Una vez identificados los eventos de contingencia y los escenarios de riesgo, se procede con el desarrollo de los procedimientos del Plan de Contingencia, agrupados por las categorías indicadas previamente, lo cual comprenderá los eventos de mayor impacto, identificado en la matriz de riesgos de contingencia y serán abordados tal como se indica en la siguiente tabla, asimismo en el anexo N°4 se detalla cada formato del procedimiento del plan de contingencia.

Tabla N° 7 – Eventos de mayor impacto para el Plan de Contingencia de información

N°	Evento	Exposición al Riesgo	Procedimiento Plan de Contingencia
1	Incendio en el centro de datos	Extremo	01
2	Terremoto /Sismo	Extremo	02
3	Ataque Cibernético	Extremo	03
4	Falla del suministro eléctrico en el Centro de Datos y gabinetes de comunicación.	Alto	04

9.5 Fase 5: Implementación del Plan de Contingencia

La implementación del presente plan iniciará en un plazo no mayor de treinta (30) días calendarios después de su aprobación.

Para tal efecto, el/la Oficial de Seguridad y Confianza Digital, 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.

De los simulacros y pruebas a realizarse se establece un cronograma para ejecutar las acciones pertinentes y evaluar la efectividad de los planes de contingencia en escenarios recreados en ambientes seguros planificados por la OTI. Ver cronograma en el Anexo 5.

9.6 Fase 6: Monitoreo

Dado que las condiciones del inmueble de PROMPERÚ pueden variar con el tiempo, lo mismo que los bienes informáticos, incluidos los equipos informáticos del Centro de Datos, es importante que se realice una verificación
del Plan de Contingencia.

Las acciones de verificación se deben realizar de manera semestral 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 plande atención que abarque todos los bienes informáticos de la Institución
- 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.

10. ACTUALIZACIÓN

El presente Plan puede ser revisado y actualizado en un periodo recomendable de un (01) año o, cuando por razones extraordinaria el coordinador de continuidad estime conveniente.

ANEXO N° 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 realicenacciones 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 presentar se 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.
2-1	**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 N° 2

LISTADO DE EQUIPOS DE CENTRO DE DATOS Y GABINETE CLASIFICADOS POR PRIORIDAD DE ATENCIÓN PARA LA RECUPERACIÓN

N°	Tipo de equipo	Rol	Descripción	Prioridad
1	Switchs	Comunicación	Switches Core, Switches de acceso y Datos	1
2	UPS	Energía	Equipo de suministro eléctrico para servidores y equipos de comunicación	1
3	Storage	Almacenamiento	Almacenamiento de Servidor Virtuales y servicios	1
4	Aire condicionado de Enfriamiento	Enfriamiento	Aire acondicionamiento de para centro de datos.	1
5	Disco de almacenamiento	Almacenamiento	ESD y SAS	1
6	Máquina Virtual	Servicios	DNS, DHCP, Web, Base de datos y Aplicaciones internas	1
7	Access Point	Red inalámbrica	Equipo de red	3

ANEXO N°3

LISTADO DE PORTALES WEB, LANDINGS O MINISITIOS CLASIFICADOS POR PRIORIDAD DE ATENCIÓN PARA LA RECUPERACIÓN

Servidores críticos alojados en la Nube				
Nº	**Nombre**	**Descripción**	**Tipo**	**Prioridad**
1	MARCA PERU - Licenciatarios	Portal de solicitud de solicitud de uso de la Marca País y la gestión de Licenciatarios.	Plataforma Web	1
2	AULA VIRTUAL EXPORTACIONES	Página web que administra el contenido de cursos para las empresas y personas interesadas en el sector exportaciones	Plataforma Web	1
3	YTUQUEPLANES	Web que fomenta el turismo interno y brinda información de paquetes turísticos	Portal	2
4	Portal PERU MODA	Portal que soporta los principales procesos del evento Perú Moda	Portal	2
5	ANDEN DE CONTENIDOS - REGISTRO USUARIOS EXTERNOS	Permite el registro de usuarios externos en la plataforma de terceros Elvis DAM	Landing	2
6	COEXPOSITORES	Portal de soporte a la gestión de inscripción de los coexpositores de las ferias de turismo internacionales	Plataforma Web	2
7	TURISMO IN	Portal desarrollado con el fin de capacitar y brindar información relevante y especializada sobre la demanda del turismo local y mundial a los empresarios, profesionales y universitarios del sector	Portal	2
8	ALPACA DEL PERU	Portal de campaña para promocionar la alpaca y la variedad de usos en la industria textil del Perú	Landing	2
9	APOYO A TERCEROS (MAT)	Brinda un aporte parcial para actividades de terceros cuyo retorno promocional contribuirá al logro de los objetivos estratégicos de PROMPERÚ.	Plataforma Web	2
10	MINISITIO PISCO SPIRIT OF PERU	Minisitio con información del pisco peruano	Minisitio	2
11	FILM IN PERU	Página web que busca favorecer el desarrollo de diversas industrias creativas, fortalecer y formalizar a profesionales del sector audiovisual nacional	Minisitio	2
12	CAFES DEL PERU	Página web que muestra información sobre cafés del Perú	Landing	2

13	TOOLKIT	Página web que permite acceder a estudios, publicaciones, manuales y otros recursos de la Marca Perú	Minisitio	2
14	CULTURA SOSTENIBLE	Desde PROMPERÚ acompañamos a las empresas exportadoras peruanas en su camino hacia la implementación de modelos de negocio sostenible.	Minisitio	2
15	CoffeesfromPERU	Portal de la Marca sectorial de Cafés	Minisitio	2
16	Superfoods Perú	Portal de la Marca sectorial de super alimentos	Minisitio	2
17	MINISITE TE AYUDAMOS	Exportemos tiene un minisite de cara al usuario parala atención de Preguntas frecuentes y material complementario	Minisitio	2
18	INVESTPERU	Landing para personas y empresas interesadas en invertir en el Perú, parte de Perú Info	Landing	2
19	LANDING ROADSHOP MADRID	Son eventos coordinados entre la OCEX de esas ciudades y la Dirección de Promoción de Inversiones Empresariales con el fin de atraer potenciales inversionistas en los sectores priorizados como Alta tecnología, Energías Renovables, Manufactura, Industrias Alimentarias, Textil y Turismo	Landing	2
20	LANDING ROADSHOP LONDRES	Son eventos coordinados entre la OCEX de esas ciudades y la Dirección de Promoción de Inversiones Empresariales con el fin de atraer potenciales inversionistas en los sectores priorizados como Alta tecnología, Energías Renovables, Manufactura, Industrias Alimentarias, Textil y Turismo	Landing	2
21	LANDING ROADSHOP MIAMI	Son eventos coordinados entre la OCEX de esas ciudades y la Dirección de Promoción de Inversiones Empresariales con el fin de atraer potenciales inversionistas en los sectores priorizados como Alta tecnología, Energías Renovables, Manufactura, Industrias Alimentarias, Textil y Turismo	Landing	2
22	YTUQUEPLANES - PERU MUCHO GUSTO LIMA	Sección en ytuqueplanes que promueve el evento turístico y gastronómico Perú mucho gusto	Landing	2
23	YTUQUEPLANES - IQUITOS LA ISLA BONITA	One page en ytuqueplanes que promociona la película: Iquitos la isla bonita	One Page	2

24	TURISMO IN SUMMIT	One page en turismoin que reemplaza a la página turismoinday	One Page	2
25	LANDING ROADSHOP LOS ANGELES	Son eventos coordinados entre la OCEX de esas ciudades y la Dirección de Promoción de Inversiones Empresariales con el fin de atraer potenciales inversionistas en los sectores priorizados como Alta tecnología, Energías Renovables, Manufactura, Industrias Alimentarias, Textil y Turismo	Landing	2
26	LANDING ROADSHOP FILM IN PERU	Son eventos coordinados entre la OCEX de esas ciudades y la Dirección de Promoción de Inversiones Empresariales con el fin de atraer potenciales inversionistas en los sectores priorizados como Alta tecnología, Energías Renovables, Manufactura, Industrias Alimentarias, Textil y Turismo	Landing	2

Sistemas Administrativos o internos alojados en el Centro de Datos

Nº	Sistema	Descripción	Área Usuario	Prioridad
1	ERP – PROMPERU Oracle eBusiness Suite R12	Sistema integrado de soporte a la gestión administrativa financiera, los principales funcionales son: Presupuesto : Control presupuestal; Compras : generación de solicitudes de bienes y servicios, órdenes de compra/servicio, acta de conformidad; Almacén : control del inventario y su valorización, generación de requisición de almacén, control de almacén, Activos Fijos : administración de los activos fijos y patrimonio, Contabilidad : conciliación bancaria, registros contables, cuentas por pagar y cobrar; Recursos Humano : datos personales, académicos y laborales, planillas de pago.	TODOS	1
2	Sistema de Planeamiento y Presupuesto - Éxito	Sistema de formulación, programación, seguimiento y control presupuestal, integrado al ERP-PROMPERU. La ejecución es controlada por cada centro de costo, meta, objetivo y fuente de financiamiento. Las unidades orgánicas proceden al registro de los datos propios de las actividades establecidas en el POI - Plan Operativo Institucional de cada ejercicio presupuestal.	TODOS	1
3	BI - Sistema de Inteligencia de Negocios Oracle Business Intelligence / Power BI	Sistema de Inteligencia de negocios, reposición de información, datawarehouse institucional basado en Oracle Business Intelligence 11g. Brinda soporte al análisis información relevante sobre las exportaciones e importaciones, presupuesto y ejecución.	DPE / SG	1
4	Sistema de Contratos y Convenios y Carta Fianza	Sistema de registros y control de los contratos, convenios institucionales y cartas fianza. Administrado funcionalmente por la Oficina de Asesoría Jurídica de PROMPERU	TODOS	1
5	Sistema de Gestión Documental (SGD)	Sistema que permite registrar, realizar seguimiento los documentos internos y externos a través de Mesa de Partes. El sistema permite firmar	TODOS	1

		electrónicamente dichos documentos		
6	Ventanilla virtual Front y admin	Mesa de partes virtual (para usuario interno y ciudadano)	UIGD	1
7	Intranet	Sistema colaborativo interno de PROMPERU, plataforma de reunión y participación de los colaboradores, destacan la información de onomásticos, eventos y actividades, además de encontrar las principales herramientas o sistemas institucionales.	TODOS	2
8	MailLing List	Actualiza base de datos de empresas y personas con los que la institución coordina en sus diferentes procesos o gestiones. Relacionado con la gran mayoría de sistemas	DPT	2
9	Proyecto Modulo de sistema de Recursos Humanos (e-STATAL)	Legajo / Asistencia / Planilla	ORH	2
10	Atención al Turista	Registra las visitas de los turistas a las oficinas de IPERU por solicitud de información	IPERU	2
11	Asistencia al Turista	Registra las asesorías y quejas a los turistas por los servicios que han adquirido	IPERU	2
12	Información Turística	Banco de información de consulta IPERU	IPERU	2
13	Actividades IPERU	Registros de las participaciones de IPERU en determinados eventos	IPERU	2
14	Estadísticas IPERU	Consultas de los registros de asistencia y atención	IPERU	2
15	Reserva de Sala	Separación de salas de los diversos ambientes que tiene PROMPERU	TODOS	2

* La presente tabla se actualizará conforme se implemente sistemas sin necesidad de modificar el presente plan.

ANEXO N°4

FORMATOS DEL PROCEDIMIENTOS DE CONTINGENCIA INFORMÁTICO Y RESTAURACIÓN DE SERVICIOS DE TI

Pliego PROMPERÚ	Evento: Incendio en el Centro de Datos	FPC – 01

1. PROCEDIMIENTO DE PREVENCIÓN

a) Situación actual

- Cada oficina cuenta con un extintor, los mismos que cuentan con verificaciones técnicas cada periodo de tiempo y cumplen los estándares de calidad para asegurar su funcionamiento optimo en caso de uso. Adicionalmente el personal administrativo del edificio, se encuentra capacitado en el funcionamiento de extintores.
- Sobre el caso de incendios, se precisa que el inmueble y cada una de las oficinas cuenta con puertas cortafuego, lo que ayudaría a contener el fuego, por un periodo de tiempo, en la ubicación en que se haya generado.
- El Centro de Datos cuenta con aire acondicionado en funcionamiento constante que pueden prevenir que se produzca y empeore el evento.
- Sobre el Centro de Datos, no se tiene un centro de datos alterno; y en caso un incendio logre destruir un 50% de las oficinas antes de ser controlado, el impacto en el Centro de datos sería alto, toda vez que los equipos se verían realmente afectado y la información almacenada ahí también se afectaría.
- La información generada por las aplicaciones alojadas en la nube es respaldada constantemente en línea; la información generada por aplicaciones alojadas en equipos del Centro de Datos se respalda localmente de forma periódica y progresiva. Por tanto, de darse el incendio en el lapso previo al envío de los respaldos locales a la nube, se tiene riesgo de pérdida de la información.
- Cabe precisar que no se tiene habilitado un lugar para que la totalidad de empleados trabajen en tanto el inmueble sea restaurado.
- laptops

Infraestructura:

- Centro de Datos

Recursos Humanos

- Personal de la entidad.

b) Objetivo

Establecer las acciones que se ejecutarán ante un incendio a fin de minimizar el tiempo de interrupción de las operaciones de PROMPERÚ, sin exponer la seguridad de las personas.

c) Personal Encargado

El/La coordinador/a de Continuidad, es quien debe dar los lineamientos y dar cumplimiento a las Condiciones de Prevención de Riesgo del presente Plan. Por su parte, el Grupo de Prevención debe realizar las acciones descritas en el punto e).

d) Condiciones de Prevención de Riesgo
- Inspecciones de seguridad realizadas periódicamente al centro de datos.
- Mantenimiento de las salidas libres de obstáculos.
- Funcionamiento de los extintores contra incendio
- Funcionamiento de las luces de emergencia.
- Mantenimiento de detectores de humo contra incendio.

e) Acciones del Equipo de Prevención
- Evaluar en coordinación con el coordinador de Continuidad un ambiente para el Centro de Datos.
- Establecer, organizar, ejecutar y supervisar procedimientos de respaldo y restauración de información como base de datos, código fuentes y ejecutables.
- Programar, supervisar el mantenimiento preventivo a los equipos del Centro de Datos.
- Realizar periódicamente el mantenimiento preventivo y correctivo del UPS.
- Realizar periódicamente el mantenimiento preventivo y correctivo de los servidores alojado en el Centro de Datos.
- Mantener vigente los extintores contra incendio.

2. PROCEDIMIENTO EJECUCIÓN

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

b) Personal que autoriza la contingencia informática
El/La Coordinador/a de Continuidad.

c) Personal Encargado
Equipo de Emergencia.

d) Acciones para ejecutar a corto plazo
- Desconectar el fluido eléctrico y cerrar las llaves de gas u otros líquidos inflamables si corresponde.
- Establecer medidas que permitan garantizar que los respaldos realizados estén totalmente funcionales y que permita recuperar la información exacta a partir de los mismos.
- Realizar de forma más frecuente el backup de la información en la nube.
- Evaluar el alcance del desastre en cada área de responsabilidad y notificar y reunir a los demás integrantes del equipo de Emergencia y Restauración.

e) Duración
La duración total del evento dependerá del grado del incendio y los daños a la infraestructura.

3. PROCEDIMIENTO DE RECUPERACIÓN

a) Personal Encargado
El personal encargado es el/la Coordinador/a de Continuidad y el Equipo de Restauración, cuyo rol principal es asegurar el normal desarrollo de los servicios de TI de PROMPERÚ.

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.
- Movilizar al equipo de restauración al sitio alterno de recuperación.
- Establecer contacto con los proveedores clave y terceros para proporcionar instrucciones

inmediatas y/o notificarles cualquier requisito de ayuda sobre la recuperación de negocio.

c) Mecanismos de Comprobación

El equipo de emergencia, presentará un informe al/el coordinador de Continuidad, explicando qué parte de las actividades u operaciones de tecnologías de la información han sido afectadas, el impacto general y cuáles son las acciones tomadas.

d) Desactivación del Plan de Contingencia

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

Pliego PROMPERÚ	Evento: Terremoto /Sismo	FPC – 02

1. PROCEDIMIENTO DE PREVENCIÓN

a) Situación actual:

- Actualmente la institución cuenta con luces de emergencia en determinados puntos, así como cuenta con señalización de zonas seguras de la Entidad.
- Cada oficina cuenta con un brigadista de emergencia quien coordina la correcta evacuación del personal y el auxilio respectivo en cuanto se tengan las condiciones apropiadas.
- Se realiza simulacros de prevención ante cualquier posible sismo y/o terremoto que pudiera ocurrir.
- Actualmente no se cuenta con un centro de datos alterno ante un posible terremoto y/o sismo que pudiera ocurrir y consigo perjudicar el equipamiento que se encuentra dentro del centro de datos de PROMPERÚ.
- Se cuenta con servicios y servidores alojado en la nube, el mismo que no severía afectado ante cualquier sismo o terremoto que pudiera ocurrir.

b) Objetivo

Establecer las acciones que se ejecutarán ante un terremoto/sismo a fin de minimizar el tiempo de interrupción de las operaciones de PROMPERÚ, sin exponer la **seguridad** de las personas.

c) Personal Encargado

El/la coordinado/ra de Continuidad de PROMPERÚ, es quien debe dar los lineamientos y dar cumplimiento a las Condiciones de Prevención de Riesgo del presente Plan. El Equipo de Prevención debe realizar las acciones descritas en el punto e).

d) Condiciones de Prevención de Riesgo

- Realización de simulacros de evacuación con la participación de todo el personal de PROMPERÚ.
- Conformación de las brigadas de emergencia, y capacitarlas anualmente.
- 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 del Equipo de Prevención

- Establecer, organizar, ejecutar y supervisar procedimientos de respaldo y restauración de información de base de datos, código fuentes y ejecutables.
- Programar, supervisar el mantenimiento preventivo a los equipos componentes del Centro de Datos.
- Mantener actualizado el inventario hardware y software utilizado en el Centro de Datos de PROMPERÚ.
- Llevar un control de versiones de las fuentes de los sistemas de información y portales de PROMPERÚ.

2. PROCEDIMIENTO DE EJECUCIÓN

a) Eventos que activan la contingencia

La contingencia se activará al ocurrir un sismo. El proceso de contingencia se activará inmediatamente después de ocurrir el evento

b) Personal que autoriza la contingencia informática

El/La Coordinador/a de Continuidad.

c) Personal Encargado

Equipo de Emergencia.

d) Acciones para ejecutar a corto plazo

- Desconectar el fluido eléctrico y cerrar las llaves de gas u otros líquidos inflamables.
- Se hará sonar la sirena o alarma para casos de sismo, dando aviso al personal, que posteriormente será evacuado de las instalaciones.
- El personal integrante de la brigada para casos de sismos actuará de inmediato, manteniendo la calma en el lugar y dirigiendo a las demás personas por las rutas de escape establecidas.
- Todo el personal se reunirá en zonas preestablecidas como seguras hasta que el sismo culmine. Se esperará un tiempo prudencial, ante posibles réplicas. En caso de tratarse de un sismo de magnitud leve, los trabajadores retornarán a sus labores; sin embargo, de producirse un sismo de gran magnitud, el personal permanecerá en áreas seguras y se realizarán las evaluaciones respectivas de daños y estructuras antes de reiniciar las labores.
- Se rescatará a los afectados por el sismo, brindándoles inmediatamente los primeros auxilios y, de ser necesario, se les evacuará al hospital o centro de salud más próximo.
- Evaluación de los daños ocasionados por el sismo sobre las instalaciones físicas, ambientes de trabajo, 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.

e) Duración

- La duración del evento dependerá del grado del sismo, la probabilidad de réplicas y los daños ala infraestructura.

3. PROCEDIMIENTO DE RECUPERACIÓN

a) Personal Encargado

El personal encargado es el/la Coordinador/a de Continuidad y el Equipo de Restauración, cuyo rolprincipal es asegurar el normal desarrollo de los servicios y operaciones de TI de PROMPERÚ.

b) Descripción de actividades

- Brindar atención inmediata de las personas accidentadas.
  Mantener al personal en las zonas de seguridad previamente establecidas por un tiempo prudencial hasta el cese de las réplicas.
- Retirar todos los escombros que pudieran generarse por el sismo, los mismos que serán colocados en el depósito de residuos sólidos o cualquier espacio que designe la Entidad.
- 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.
- Supervisar el progreso de las operaciones de recuperación y de servicios de TI.
- El Equipo de restauración de TI restaurarán el espacio de trabajo para permitir que el personal crítico de la oficina pueda operar, para lo cual deberán:
  - Ejecutar los procedimientos de recuperación de la plataforma tecnológica.
  - Verificar que las aplicaciones críticas se hayan recuperado y estén funcionando

correctamente.
- Confirmar los puntos de recuperación de datos de las aplicaciones.
- Verificar que las funcionalidades de comunicación están funcionando correctamente.
- Verificar que equipos básicos como escáner, impresora estén disponibles y operacionalespara dar soporte a los requisitos de la entidad.
- Asegurar que el ambiente del área de trabajo, las aplicaciones están funcionando según loestimado una vez concluida la emergencia o siniestro.

c) Mecanismos de Comprobación
El/La equipo de restauración, presentará un informe al coordinador de Continuidad, explicando quéparte de las actividades u operaciones de tecnologías de la información han sido afectadas, el impacto en general y cuáles son las acciones tomadas.

d) Desactivación del Plan de Contingencia
El/La Coordinador/a de Continuidad desactivará el Plan de Contingencia.

Pliego PROMPERÚ	Evento: Ataque cibernético	FPC – 03

1. PROCEDIMEINTO DE PREVENCIÓN

a) Situación actual:
- Si bien la instalación de software, sea propietario o de desarrollo interno, es realizado y/o supervisado por la OTI, pueden existir algunos riesgos de manipulación de software en equipos sin autorización ni supervisión de la OTI, pudiendo ser afectado por un tipo de malware como por ejemplo ransomware.
- Se cuenta con una solución antimalware corporativo, el cual se actualiza de forma continua.
- El personal no es consciente a plenitud sobre el riesgo e impacto de hacer uso de software sin supervisión de la OTI, así como de abrir correos electrónicos de dudosa procedencia o hacer uso de dispositivos de almacenamiento externos sin los cuidados adecuados. Todo esto podría dañar no sólo al bien informático sino también a la información almacenada.
- Se cuenta con mecanismos de seguridad perimetral, para evitar el acceso no autorizado a la red institucional.
- Existen políticas de seguridad de la información y controles aplicados para reducir o mitigar las posibles amenazas de seguridad de la información.

b) Objetivo
Restaurar la operatividad de los equipos y servicios después de eliminar los malware o reinstalar las aplicaciones dañadas.

c) Personal Encargado
El 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.
- Aplicación de filtros para restricción de correo entrante, y revisión de archivos adjuntos en los correos y así prevenir la infección de los terminales de trabajo por virus.
- Contar con antivirus instalados en cada estación de trabajo y debe estar actualizado permanentemente.
- Contar con equipos de respaldo ante posibles fallas de las estaciones y servidores, para su reemplazo provisional hasta su desinfección y habilitación.
- Restricción del acceso a Internet a las estaciones de trabajo que por su uso no lo requieran.

- 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.
- Capacitar y concientizar al personal de PROMPERÚ, sobre la importancia de laseguridad de la información.

e) Acciones del Equipo de Prevención
- Establecer, organizar, ejecutar y supervisar procedimientos de respaldo de información procesada y almacenada en el Centro de Datos.
- Monitorear la seguridad de la información de la Entidad a través de las soluciones adquiridas para la ciberseguridad.
- Llevar un control de versiones de las fuentes de los sistemas de información y portales de la entidad.
- 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. PROCEDIMIENTO DE EJECUCIÓN

a) Eventos que activan la contingencia
- Mensajes de error durante la ejecución de programas.
- Lentitud en el acceso a las aplicaciones.
- Falla en el sistema operativo y aplicaciones de los equipos.
- Indisponibilidad de los sistemas de información o portales web.

b) Personal que autoriza la contingencia informática
El/La Coordinador/a de Continuidad y el/la Oficial de Seguridad y Confianza Digital pueden activar la contingencia.

c) Personal Encargado
Equipo de prevención

d) Acciones para ejecutar a corto plazo
- Desconectar de la red de datos de PROMPERÚ, el servidor o la estación infectada vulnerada.
- Informar al personal sobre el ataque inminente y realizar las recomendaciones generales para evitar mayores infecciones.
- 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.
- Informar a la Secretaria de Gobierno y Transformación Digital sobre el ciberataque y coordinar con ellos las medidas a ejecutar.
- Guardar la muestra del virus detectado y remitirlo al proveedor del antivirus. En el caso de hacking a aplicaciones, se debe guardar el archivo modificado, a nivel de software y base de datos.
- En caso no solucionarse el problema, formatear el equipo y restaurar copia de respaldo

e) Duración
En caso se confirme un ataque cibernético en estaciones de trabajo la duración del evento no deberá ser mayor de 24 horas y en servidores de centro de datos de 04 horas.

3. PROCEDIMIENTO DE RECUPERACIÓN

a) Personal Encargado

El 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 e informará a su jefe inmediato para reanudar las labores de trabajo.

b) Descripción de actividades

- Instalación y configuración de software, drivers y servicios necesarios para el funcionamiento de la información a recuperar en el Pliego PROMPERÚ.
- Instalación del motor de base de datos, con sus respectivas librerías y niveles de seguridad.
- Realización de la restauración de la base de datos con la última copia de seguridad disponible.
- Conectar el servidor o la estación de trabajo a la red de PROMPERÚ.
- Efectuar las pruebas necesarias con el usuario final de los equipos y/o sistemas de información afectados.
- Ejecutar análisis de vulnerabilidad
- Comunicar el restablecimiento del servicio.

c) Mecanismos de Comprobación

Se registrará el incidente Sistema de Gestión de Tickets utilizado por soporte técnico de la OTI y se informará al Comité de Gestión de Gobierno Digital.

El/La Especialista de infraestructura de Redes y/o el personal de soporte técnico, según sea el caso, presentará un informe a el/la jefe/a de OTI, informando que parte del servicio u operaciones se han visto afectadas, y cuáles son las acciones tomadas.

e) Desactivación del Plan de Contingencia

El/La Coordinador/a de Continuidad desactivará el Plan de Contingencia

Pliego PROMPERÚ	Evento: Falla del suministro eléctrico en el Centro de Datos	FPC – 04

1. PROCEDIMIENTO DE PREVENCIÓN

a) Situación actual:

- El Centro de Datos cuenta con luces de emergencia en determinados puntos, pero se debe validar si estos son suficientes, así como también aspectos técnicos de la luminaria.
- La continuidad del fluido eléctrico del Centro de Datos está soportada por un UPS que dan un promedio de 2 horas para el apagado progresivo de los equipos, dichos UPS emiten correos de advertencia al ponerse en funcionamiento, lo que alerta a los especialistas de la OTI, para que ejecuten las acciones correspondientes para un apagado adecuado.
- Es importante que el personal se concientice sobre la importancia de usar adecuadamente el tiempo que brindan los UPS para el apagado de los servicios alojados en los servidores del centro de datos, a fin de realizar adecuadamente el apagado de los equipos y evitar que queden defectuosos y/o dañar información.
- No se realizan simulacros de interrupciones de fluido eléctrico en el Centro de Datos, y no existen procedimientos formales de apago y encendido del mismo

b) Objetivo

Restaurar las funciones consideradas como críticas para el servicio.

c) Personal Encargado

- El/la Coordinador/a de Continuidad, es el responsable de atender y supervisar las respuestas ante el incidente.
- El/La Jefe/a de la Unidad de Logística es el responsable de realizar las coordinaciones para restablecer el suministro de energía eléctrica con los proveedores de energía.
- El Equipo de Prevención debe realizar las acciones descritas en el punto e).

d) Condiciones de Prevención de Riesgo

- Para los servicios diarios que realiza PROMPERÚ se cuenta con equipo UPS necesario para asegurar el suministro eléctrico en los equipos consideradas como críticos (revisar el cuadro de servicios críticos).
- El Equipo UPS cuentan con mantenimiento preventivo y con suficiente energía para soportar una operación continua de 02 horas como mínimo. El tiempo variará de acuerdo a la función que cumplan.
- Realización de pruebas periódicas del equipo UPS para asegurar su correcto funcionamiento.
- Capacidad del 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 2 horas.

e) Acciones del Equipo de Prevención.
- Revisar periódicamente y de forma conjunta con Servicios Generales las instalaciones eléctricas del Centro de Datos y programar y supervisar el mantenimiento preventivo y correctivo a los equipos componentes del Centrode Datos.
- Coordinar y supervisar el mantenimiento preventivo de pozos a tierra, aire acondicionado del Centro de Datos, UPS al menos trimestralmente.
- Verificar que la red eléctrica utilizada en el Centro de Datos 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 la sala de energía del centro de datos de PROMPERÚ.

2. PROCEDIMIENTO 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. Personal que autoriza la contingencia informática
El/La Coordinador/a de Continuidad.

c. Personal Encargado
Equipo de Emergencia.

d. Acciones para ejecutar a corto plazo
- Contar con la disponibilidad del personal para la reparación rápida de los equipos.
- Establecer con la empresa que brinda servicios de nube, mecanismos para una comunicación anticipada de las actualizaciones (u otras acciones) que vayan a realizar y que pudiese impactar en los servicios del PROMPERÚ, de forma tal que se puedan ejecutar simulacros y evaluar su impacto, previniendo una interrupción de los servicios.
- Acceder a las cintas de respaldo para la restauración de la información en el servidor averiado
- Verificar que el equipo se encuentre en garantía, de lo contrario de implementará un nuevo servidor virtual.

e. Duración
El tiempo máximo de la contingencia no debe sobrepasar las seis (6) horas

3. PROCEDIMIENTO DE RECUPERACIÓN

a) Personal Encargado
El Equipo de Restauración, quienes se encargarán de realizar las acciones de recuperación necesarias.

b) Descripción de 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/La Especialista de infraestructura y Redes, presentará un informe a el/la jefe/a de OTI, informando que parte del servicio y equipos han fallado, y cuáles son las acciones correctivas a realizar.

d) Desactivación del Plan de Contingencia

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

CONTROL DE CAMBIOS

Versión	Fecha	Autor	Descripción del cambio	Aprobado por
1.0	04/11/2024	Oficial de Seguridad y Confianza Digital Brandon Jose Luis Morales Fernandez	Creación inicial del documento.	