PLAN DE CONTINGENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN

Mincetur
Ministerio de Comercio Exterior y Turismo

Firmado digitalmente por DAVILA STEIN Alfredo Raphael FAU 20504774288 soft
Oficina: Oficina de Informática
Motivo: Doy visto bueno
Fecha: 2025/04/23 15:49:28-0500

VERSIÓN DEL DOCUMENTO: 2.0

I. INTRODUCCIÓN

Las tecnologías de la información y comunicaciones (TIC) y la automatización de los procesos son elementales en el éxito de toda institución gubernamental o privada, considerando que los servicios que estos proveen son críticos y necesarios para el logro de sus objetivos; motivo por el cual se debe garantizar su completa operatividad minimizando la presencia de interrupciones.

El Plan de Contingencia de TI permite lograr que las interrupciones que se puedan presentar no impacten profundamente en la continuidad de los servicios que la Oficina de Informática administra. Siguiendo los planes, procedimientos y medidas correctivas se conseguirá recuperar los servicios en corto tiempo y con la mejor prestación posible luego de producido los sucesos generadores de fallos o interrupciones.

Este plan debe ser entendido en toda su magnitud y compartido especialmente por los funcionarios de la Alta Dirección del MINCETUR, quienes deben considerar que los gastos en medidas de seguridad informática son una inversión que es retribuida en la continuidad de los servicios brindados a los usuarios internos del MINCETUR y a la ciudadanía en general.

Es por ello que el presente documento ayudará a comprender la importancia de implementar, mantener y respetar las directivas y normas de seguridad referidas a las tecnologías de la información. Actualmente, es de obligación implícita que toda Institución tenga de manera documentada un Plan de Contingencia de TI ante la presencia de sucesos generadores de fallas o interrupciones.

En resumen, debemos realizar un análisis de la situación, generar hipótesis de los posibles escenarios, plantearse objetivos y metas, generar roles y responsabilidades y dar instrucciones de coordinación.

Cuando nos preparamos, mejoramos la capacidad de respuesta. No hay respuesta, sin asistencia del personal. La rehabilitación es la recuperación provisional/temporal y la reconstrucción hace referencia a la recuperación definitiva.

El Plan de Contingencia de TI es un conjunto de acciones orientadas a planificar, organizar y mejorar la capacidad de respuesta frente a los probables efectos de los eventos adversos.

II. OBJETIVO

Garantizar la continuidad operativa de los servicios que brinda el MINCETUR, ante la presencia de eventos que puedan alterar su normal funcionamiento, restableciéndolo en el menor tiempo posible, a través de la puesta en marcha de procedimientos, actividades y elementos requeridos para afrontar la contingencia.

III. FINALIDAD

La finalidad de este documento es proporcionar una guía de referencia que pueda ser utilizada en caso de contingencia tecnológica, en concordancia con la implementación del Sistema de Gestión de Seguridad de la Información y el plan de continuidad operativa en MINCETUR.

IV. ALCANCE

Contempla la plataforma tecnológica que soporta los servicios de los sistemas de información críticos del MINCETUR. Adicionalmente, se consideran los riesgos y soluciones del ambiente físico, relacionados con la operación de los procesos principales del centro de datos del MINCETUR.

V. ORGANIZACIÓN

Con el fin de ejecutar adecuadamente el Plan de Contingencia de TI del MINCETUR se cuenta con un Comité de Contingencia, conformado por:

a) Director General de la Oficina de Informática
b) Director de Informática (Coordinador del Plan de Contingencia de TI)
c) Coordinador de Infraestructura Tecnológica
d) Coordinador de Desarrollo de Sistemas
e) Oficial de Seguridad y Confianza Digital

Siendo sus principales funciones en relación con el plan de contingencia de TI:

a) Director General de la Oficina de Informática
- Coordinar la implementación del Plan de Contingencia de TI del MINCETUR.

b) Coordinador del Plan de Contingencia de TI
- Es el canal de comunicación entre los equipos operativos a través del cual se transmitirán las decisiones tomadas en torno a las acciones del Plan de Contingencias TI y el plan de pruebas, los niveles de ejecución y el estado de los recursos informáticos que cubre el plan. Es el que autoriza la activación y puesta en marcha del Plan de Contingencias TI cuando lo considere necesario.

c) Coordinador de Infraestructura Tecnológica
- Supervisar el funcionamiento de los servicios del centro de datos.
- Coordinar con los proveedores de servicios de TI contratados (equipos de comunicaciones, servidores, grupo electrógeno, UPS, entre otros).
- Coordinar con el grupo operativo de Infraestructura Tecnológica, quienes ejecutarán los procedimientos de respaldo y restauración, la carga de archivos de datos de las aplicaciones, y las actividades necesarias para la recuperación de los servicios.

d) Coordinador de Desarrollo de Sistemas

- Verificar el correcto funcionamiento de las aplicaciones durante y después de la contingencia.
- De ser necesario, interactuar con los responsables que brinden soporte a las aplicaciones.
- Colaborar con el grupo operativo de Infraestructura Tecnológica en la recuperación de las aplicaciones.

e) Oficial de Seguridad y Confianza Digital

- Evaluar los riesgos que puedan presentarse durante las pruebas y/o ejecución del Plan de Contingencia de TI
- Participar de las pruebas del plan de contingencia de TI
- Analizar los procesos del plan de contingencia y establecer oportunidades de mejora.
- Coordinar la permanente actualización y consolidación de los anexos del plan.

Se deberá contar con una lista actualizada de los integrantes del Comité de Contingencia, de acuerdo al formato del **Anexo N° 01: "Integrantes del Comité de Contingencia".**

VI. DEFINICIONES

Para la mejor comprensión del contenido se detallan los siguientes conceptos.

a) Amenaza:
Cualquier situación o evento que pueda afectar la disponibilidad de los sistemas informáticos, redes o datos de la institución.

b) Centro de Datos: Espacio donde se concentran los recursos necesarios para el procesamiento de la información de una organización. Dentro de este concepto también se consideran los ambientes de comunicaciones de los diferentes pisos de MINCETUR.

c) Confidencialidad: Asegurar que el acceso a la información, sólo lo tengan las personas autorizadas.

d) Desastre: Es un hecho natural o provocado por el ser humano y que tiene efectos negativos, sea incendio, inundación, robo, ataque, sismo entre otros; son los desastres que pueden detener un negocio de forma temporal o permanente.

e) Disponibilidad: Se refiere a que la información se encuentre accesible en el momento que se requiera.

f) Incidente: Es cualquier evento que interrumpa el funcionamiento normal de un servicio afectando ya sea a uno, a un grupo o a todos los usuarios de un servicio, un incidente puede ser un inadecuado funcionamiento de los servicios de TI; estos pueden producir una reducción en la calidad de los servicios de TI.

g) Integridad: Se refiere a que los valores de los datos se mantengan tal como fueron puestos intencionalmente en un sistema. Las técnicas de integridad sirven para prevenir que existan valores errados en los datos provocados por el

software de la base de datos, por fallas de programas, del sistema, hardware o errores humanos.

h) **Plan de Contingencia:** Son las acciones a ejecutar en caso se materialicen los riesgos, con el fin de dar continuidad a los servicios de tecnología de información y comunicaciones de la entidad.

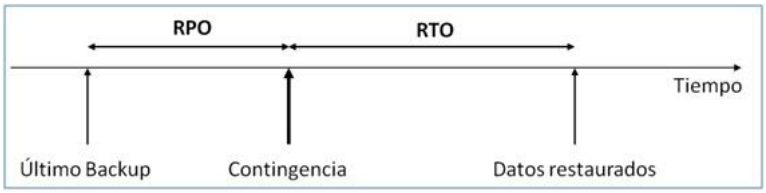
i) **Plan de Continuidad del Negocio:** Establece un esquema que ayuda a una organización a recuperarse después de un desastre. Es decir, es un mapa que detalla cómo una organización puede continuar operando mientras dura la recuperación del desastre

j) **Privacidad:** Se define como el derecho que tienen los individuos y organizaciones para determinar, ellos mismos, a quién, cuándo y qué información referente a ellos será difundida o transmitida a otros.

k) **Proceso Crítico:** Todo aquel proceso considerado indispensable para la continuidad de las operaciones y servicios, cuya falta o ejecución deficiente, puede producir un impacto negativo en la operatividad e incumplimiento de metas u objetivos de la Institución.

l) **RPO (Punto de Recuperación Objetivo):** Está muy relacionado a la copia de respaldo de información, puesto que está definido por el periodo de la posible pérdida de información desde la última copia de respaldo, hasta la caída de los servicios informáticos y comunicaciones. La definición es crucial para mejorar el programa de copias de respaldo de información. Si tenemos una actualización muy frecuente en las bases de datos, entonces la actualización de la copia de respaldo debe realizarse a una mayor frecuencia, con esto se mejora las probabilidades de recuperación una vez producida la contingencia.

m) **RTO (Tiempo de Recuperación Objetivo):** Es un tiempo objetivo para la reanudación de los servicios después de una contingencia, es decir es el tiempo durante el cual la institución puede tolerar la falta de funcionamiento de los sistemas informáticos o la caída del nivel de servicio asociado, sin afectar la continuidad de la Organización



n) **Seguridad de la Información:** Se refiere a un conjunto de medidas preventivas y reactivas tomadas por las organizaciones con la finalidad de resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad.

o) **SLA (Acuerdos de Nivel de Servicio):** Se crean para documentar los compromisos que se deben cumplir con los clientes. Los SLA especifican compromisos, es decir los niveles de servicio acordados entre el proveedor de servicios sea interno o externo y la Oficina de Informática.

p) **Vulnerabilidad:** Es el grado de pérdida de un elemento o grupo de elementos. Nivel de ser susceptible a sufrir un daño o interrupción por la ocurrencia de un peligro o amenaza.

VII. PLAN DE CONTINGENCIA DE TI

7.1. IDENTIFICACION DE PROCESOS Y/O ACTIVIDADES PRIORITARIAS

El Plan de Contingencia de TI del MINCETUR, ha sido elaborado, tomando como base el Plan de Continuidad Operativa de la Entidad; y el marco normativo vigente dispuesto, priorizando los procesos críticos requeridos para la continuidad operativa del MINCETUR y/o las actividades transversales que administra la Oficina de Informática.

7.2. IDENTIFICACIÓN Y PRIORIZACIÓN DE RIESGO

Para implementar el Plan de Contingencia de TI necesitamos identificar las amenazas y vulnerabilidades de tal modo que se puedan priorizar los riesgos para tomar las medidas correctivas necesarias y controlar sus efectos en caso de manifestarse alguno de los escenarios.

Descripción de los riesgos

7.2.1. EXTERNOS

a) **Modificación a la normatividad tecnológica - (R1).** Riesgo externo que consisten en los posibles cambios a la normatividad de las tecnologías de información y comunicaciones cuyas implementaciones afecten el funcionamiento de los sistemas de información, que pueden afectar el proceso y generar cambios en los sistemas que no se implementan de inmediato lo que puede generar retardos o inoperancia del sistema afectado. Tipo de riesgo: Cumplimiento.

b) **Incumplimiento al objeto contractual por parte de los proveedores - (R2).** Riesgo externo que consiste en el atraso que puede presentar la ejecución de los contratos de actualización, modificación, mantenimiento y soporte del hardware, software por deficiencias en el desarrollo precontractual y/o por deficiencias en la supervisión del contrato que involucren a los sistemas de información catalogados como críticos que al presentarse genera inoperancia de los sistemas de información o mala imagen de la entidad por aplicativos desactualizados. Tipo de riesgo: Cumplimiento.

c) **Ataques Informáticos o actividades anómalas - (R3).** Riesgo externo que tiene alta probabilidad de ocurrencia y consiste en el ataque y alteración o extracción de la información que es considerada confidencial o clasificada como reservada por deficiencia en las políticas de seguridad o configuración ineficiente de los cortafuegos de la entidad. Al materializarse, el impacto es

negativo ya que puede ocasionar demandas y sanciones a la entidad, mala imagen institucional. Tipo de riesgo: Tecnológico.

d) **Pérdida de suministro eléctrico - (R4).** Riesgo externo. Corresponde al corte del servicio de energía eléctrica por parte de falla externa en el proveedor del servicio, corte eléctrico que genera interrupción del funcionamiento de los equipos donde se alojan los aplicativos críticos de la entidad, que puede dejar los servicios y aplicativos inoperantes. Tipo de riesgo: Tecnológico.

e) **Caída en el servicio de internet - (R5).** Riesgo externo. Consiste en las fallas técnicas por parte del proveedor del servicio de internet, lo que ocasionaría suspensión de los servicios de correo y de los aplicativos críticos de la entidad. Tipo de riesgo: Tecnológico.

f) **Caída del servicio telefónico - (R6).** Riesgo externo correspondiente a la suspensión del servicio por daños o fallas en el software o hardware de telefonía IP, que de presentarse genera la ausencia de comunicación telefónica en la entidad. Tipo de riesgo: Tecnológico.

g) **Caída de servicios por virus informático - (R7).** Riesgo externo. Es el riesgo de infección de los equipos servidores que puede presentarse en la entidad por mala configuración del sistema antivirus o por ausencia de política de seguridad lo que genera la suspensión total o parcial del funcionamiento o de la prestación de un servicio de red, inoperancia o inestabilidad de los sistemas. Tipo de riesgo: Tecnológico.

h) **Suspensión del servicio por sismo, inundación o incendio - (R8).** Riesgo externo. Hace referencia al riesgo que corre la entidad en caso se presente un evento de sismo, inundación o incendio que afecte la infraestructura tecnológica de los sistemas de información críticos generando suspensión total o parcial del funcionamiento o de la prestación de un servicio de red, inoperancia de los sistemas o inestabilidad de los mismos. Tipo de riesgo: Operativo.

7.2.2. INTERNOS

a) **Retrasos en el proceso precontractual de la entidad en contratos relacionados con la infraestructura tecnológica de la entidad. - (R9).** Riesgo interno que corresponde a retrasos en el proceso precontractual de la entidad en contratos relacionados con la infraestructura tecnológica por deficiente planeación del proceso de contratación, falta de personal capacitado para realizar los estudios previos de contratación. Lo que puede ocasionar Inoperancia y/o desactualización de los sistemas de información. Tipo de riesgo: Operativo.

b) **Contratación sin asistencia técnica, soluciones inadecuadas o incompatibilidad frente a los requerimientos y recursos disponibles - (R10).** Riesgo interno que se relaciona con deficientes procesos de análisis, evaluación, planeación y toma de decisiones sobre la elección de las alternativas tecnológicas a ser implementadas y con el probable desconocimiento de las características / especificaciones técnicas de los recursos disponibles y las necesarias en cada una de las soluciones

elegidas. Al materializarse el riesgo la infraestructura tecnológica puede generar inoperancia de los sistemas de información. Tipo de riesgo: Operativo.

c) **Falla técnica en equipos servidores o de comunicaciones - (R11).** Riesgo interno que corresponde al daño físico o lógico de un equipo servidor o de comunicaciones que afecta el funcionamiento de un sistema de información crítico o de servicio por falta de mantenimiento preventivo a los equipos o por mal uso de los equipos que hace que el servicio quede inoperante o inestable. Tipo de riesgo: Tecnológico.

d) **Falla técnica en sistemas de información - (R12).** Riesgo interno, corresponde al riesgo de presentarse errores de lógica en programación o incompatibilidad entre software que afectan a los sistemas de información que genera inoperancia o inestabilidad de dichos sistemas. Tipo de riesgo: Tecnológico.

e) **Ausencia de personal de la Oficina de Informática que brindan soporte y mantenimiento a los sistemas de información - (R13).** Riesgo interno. Corresponde a la falta o inasistencia en un momento dado, de un ingeniero o técnico de la Oficina de Informática que realiza actividades de soporte a usuarios o de administración técnica sobre un sistema de información crítico, lo que genera inoperancia o inestabilidad de los sistemas de información. Tipo de Riesgo: Operativo.

f) **Mal uso de hardware y/o software por parte de los funcionarios de la entidad - (R14).** Riesgo interno. Consiste en el riesgo que corre la entidad por un uso inadecuado de los equipos de cómputo, software y/o sistemas de información por parte de los funcionarios por deficiencias en el conocimiento y uso de las herramientas tecnológicas o por uso mal intencionado de los mismos lo que puede generar interrupción del funcionamiento de los equipos donde se alojan los sistemas de información críticos de la entidad, que puede dejar los servicios y aplicativos inoperantes. Tipo de riesgo: Tecnológico.

g) **Calentamiento del centro de datos - (R15).** Riesgo interno que consiste en el aumento de temperatura dentro del centro de datos y falta de ventilación, por deficiencia del sistema de ventilación o mal funcionamiento del sistema de aire acondicionado de precisión acorde a las necesidades de la entidad lo que puede generar recalentamiento de los equipos servidores, de comunicaciones y telefónicos dejándolos inoperantes junto con los servicios que se encuentran alojados en ellos. Tipo de riesgo: Tecnológico.

7.3. ANÁLISIS Y CLASIFICACIÓN DE LOS RIESGOS

El Oficial de Seguridad y Confianza Digital en coordinación con el Coordinador de Infraestructura Tecnológica y el Coordinador de Desarrollo deben mantener actualizada la matriz de riesgos, dado que los riesgos son dinámicos en el tiempo y nuevas amenazas se pueden presentar, es por ello que el análisis de riesgo debe ser una actividad periódica y documentada.

La Calificación del Riesgo: Se logra a través de la estimación de la probabilidad de ocurrencia y el impacto que puede causar la materialización del riesgo. La

primera representa el número de veces que el riesgo se ha presentado en un determinado tiempo o puede presentarse y la segunda se refiere a la magnitud de sus efectos.

Probabilidad: Posibilidad de ocurrencia del riesgo. Se puede medir con criterios de:

- Frecuencia, si se ha materializado.
- Factibilidad teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo.

Probabilidad	Descripción	Frecuencia	Valor
Casi seguro	El evento probablemente ocurriría en la mayoría de los casos	Más de una vez al año	5
Probable	El evento probablemente ocurriría en la mayoría de los casos	Al menos una vez en el último año	4
Posible	El evento podría ocurrir en algún momento	Al menos una vez en los últimos dos años	3
Improbable	El evento podría ocurrir en algún momento	Al menos una vez en los últimos cinco años	2
Raro	El evento podría ocurrir solo en circunstancias excepcionales	No se ha presentado en los últimos cinco años	1

Impacto: Consecuencias que puede ocasionar a la organización la materialización del riesgo.

Impacto	Descripción	Valor
Catastrófico	Si el hecho llegara a presentarse, tendría desastrosas consecuencias o efectos sobre la entidad: - Pérdida de recursos esenciales. - Disminución del rendimiento de los procesos de negocio. - Suspensión de los sistemas críticos. - Pérdida de información crítica. - Deterioro de la imagen institucional.	5
Mayor	Si el hecho llegara a presentarse, tendría altas consecuencias o efectos sobre la entidad. - Investigaciones - Sanciones - Demandas	4
Moderado	Si el hecho llegara a presentarse, tendría medianas consecuencias o efectos sobre la entidad.	3
Menor	Si el hecho llegara a presentarse, tendría bajo impacto o efecto sobre la entidad.	2

Insignificante	Si el hecho llegará a presentarse tendría consecuencias o efectos mínimos sobre la entidad: - Pérdida de recursos críticos pero que cuentan con elementos de respaldo. - Pérdida de información considerada no crítica. - Suspensión temporal del servicio.	1

Evaluación del Riesgo: Permite comparar los resultados de su calificación, con los criterios definidos para establecer el grado de exposición de la entidad al riesgo; de esta forma es posible distinguir entre los riesgos **EXTREMOS, ALTOS, MODERADOS, BAJOS** y fijar las prioridades de las acciones requeridas para su tratamiento.

(R): Corresponde al número del riesgo dentro de las matrices de análisis y evaluación de los riesgos.

MATRIZ DE CALIFICACIÓN, EVALUACIÓN Y RESPUESTA A LOS RIESGOS

PROBABILIDAD	IMPACTO				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Casi Seguro (5)	A	A	E	E	E
Probable (4)	M	A	A	E	E
Posible (3)	B	M	A	E	E
Improbable (2)	B	B	M	A	E
Raro (1)	B	B	M	A	A

B: Zona de riesgo baja: Asumir el riesgo
M: Zona de riesgo moderada: Asumir el riesgo, reducir el riesgo
A: Zona de riesgo Alta: Reducir el riesgo, evitar, compartir o transferir
E: Zona de riesgos extrema: Reducir el riesgo, evitar, compartir o transferir

Zona de riesgo	PROBABILIDAD – IMPACTO (combinaciones)	Tratamiento
Extrema	25-34-35-44-45-53- 54-55	Reducir el riesgo, evitar, compartir o transferir
Alta	14-15-24-33-42- 43-51-52	Reducir el riesgo, evitar, compartir o transferir
Moderada	13-23-32-41	Asumir el riesgo, reducir el riesgo
Baja	11-12-21-22-31	Asumir el riesgo

Los riesgos que se tendrán en cuenta en este Plan de Contingencias de TI son los catalogados como EXTREMOS Y ALTOS, es decir aquellos que afectan en forma drástica la imagen institucional, la pérdida de información crítica, la suspensión parcial o total del funcionamiento de la plataforma tecnológica, los sistemas de información y servicios de tecnologías de información y

comunicaciones considerados como críticos; esta valoración se da en términos de las consecuencias que acarrearía dicho incidente o evento.

Los riesgos potenciales que pueden afectar la continuidad y operatividad normal de la plataforma tecnológica, los sistemas de información y servicios de tecnologías de información y comunicaciones; pueden ser externos o internos; se muestran en los cuadros siguientes:

Cuadro de Riesgos Externos

N°	DESCRIPCION DEL EVENTO	PROBABILIDAD DE OCURRENCIA	IMPACTO	NIVEL DE RIESGO
1	Modificación a la normatividad tecnológica	3	3	ALTO
2	Incumplimiento al objeto contractual por parte de los proveedores	3	3	ALTO
3	Ataques informáticos o actividades anómalas	4	5	EXTREMO
4	Pérdida de suministro eléctrico	4	3	EXTREMO
5	Caída en el servicio de internet	3	3	ALTO
6	Caída del servicio telefónico	3	2	MODERADO
7	Caída de servicios por virus informático	4	3	ALTO
8	Suspensión del servicio por sismo, inundación o incendio	3	5	EXTREMO

Cuadro de Riesgos Internos

N°	DESCRIPCION DEL EVENTO	PROBABILIDAD DE OCURRENCIA	IMPACTO	NIVEL DE RIESGO
1	Retrasos en el proceso precontractual de la entidad en contratos relacionados con la infraestructura tecnológica de la entidad.	1	5	ALTO
2	Contratación sin asistencia técnica, Soluciones Inadecuadas o Incompatibilidad frente a los Requerimientos y Recursos Disponibles.	2	4	ALTO

3	Falla técnica en equipos servidores o de comunicaciones.	3	3	ALTO
4	Falla técnica en sistemas de información	3	3	ALTO
5	Ausencia de personal de la Oficina de Informática que brindan soporte y mantenimiento a los sistemas de información.	3	3	ALTO
6	Mal uso de hardware y/o software por parte de los funcionarios de la entidad	3	2	MODERADO
7	Calentamiento del centro de datos	1	5	ALTO

7.4. PLAN DE RECUPERACIÓN

Luego del análisis de los escenarios de riesgos, se contempla tres escenarios con mayor probabilidad de ocurrencia y con impacto mayor:

- **Escenario 1** Indisponibilidad de operación del Centro de Datos causado por **pérdida de suministro eléctrico**;
- **Escenario 2**: Indisponibilidad de los servicios del Centro de Datos debido a **ataques informáticos o actividades anómalas**; y
- **Escenario 3** Indisponibilidad de los servicios del centro de datos debido a **desastres por sismo de gran magnitud**.

Las actividades que se desarrollarán en esta etapa se pueden clasificar en:

- Actividades Previas al Incidente.
- Actividades Durante el Incidente.
- Actividades Posteriores al Incidente.

7.4.1. ACTIVIDADES PREVIAS AL INCIDENTE

Son todas las actividades de planeamiento, preparación, entrenamiento y ejecución de las tareas de resguardo de la información, que nos aseguren un proceso de recuperación con el menor tiempo posible en la entidad.

En esta fase de planeamiento se debe identificar los recursos relacionados a:

a) Sistemas de Información.
La OI deberá tener un inventario actualizado de los sistemas de información de acuerdo al formato indicado en el **Anexo N° 02: "Inventario de Sistemas de Información del MINCETUR"**, tanto los sistemas administrados por la OI y los sistemas administrados por las áreas usuarias.

b) Servicios de Infraestructura TI.
La OI deberá tener un inventario actualizado de los servicios de infraestructura TI de acuerdo al formato indicado en el **Anexo N° 03: "Inventario de Servicios de Infraestructura TI del MINCETUR"**, tanto los administrados por OI en el Centro de Datos como los administrados por proveedores.

c) Equipos Servidores de Datos.
La OI deberá tener un inventario actualizado de los servidores físicos y virtuales, de acuerdo al formato indicado en el **Anexo N° 04: "Inventario de Servidores de Datos del MINCETUR"**.

d) Respaldo de Información.
La OI implementará las copias de respaldo de la información, de acuerdo a la directiva que regula el respaldo y restauración de la información de la entidad.

Adicionalmente se deberá contar con el directorio actualizado de los proveedores, de acuerdo al formato indicado en el **Anexo N° 05: "Directorio Telefónico de Proveedores"** que brinden servicios de tecnologías de información y comunicaciones.

e) Procedimientos Operativos.
La OI deberá contar con procedimientos operativos que servirán como guía en el momento de contingencia, detallando las actividades a realizar. (**Anexo N° 6:** Procedimiento de Apagado y Encendido de los equipos del Data Center)

f) Directorio de la OI.
La OI deberá contar un directorio del personal de la OI, que participa en la ejecución del Plan de Contingencia de TI. (**Anexo N° 7:** Directorio de la OI)

7.4.2. ACTIVIDADES DURANTE EL INCIDENTE

Activación del Plan de Contingencia de TI

El Plan de Contingencia lo activa el Coordinador del plan de contingencia luego de evaluar si es posible superar el evento antes de cumplido el RTO, para lo cual se sigue los siguientes pasos:

a) Respuesta Inicial
Ante cualquier notificación de un evento que afecte a los servicios del Centro de Datos, el responsable de infraestructura tecnológica informará el estado situacional de los servicios afectados al Coordinador del Plan de Contingencia de TI.

b) Decisión de Interrupción de los servicios del Centro de Datos.
El Coordinador del Plan de Contingencia de TI tiene como principal función tomar una decisión con respecto a la activación del Plan de Contingencia en base al diagnóstico de la situación de la Infraestructura Tecnológica, en términos de equipos, funciones críticas y aplicaciones impactadas.

c) Declaración de la Contingencia
Si el Coordinador del Plan de Contingencia de TI verifica que no es posible superar el evento antes de cumplido el tiempo especificado en el

RTO (Objetivo del Tiempo de Recuperación), entonces el Coordinador del Plan de Contingencia de TI activa el Plan de Contingencia de TI.

Protocolo de Recuperación (Nivel mínimo de servicios)

El objetivo es restablecer la funcionalidad de los sistemas y aplicaciones del Ministerio de Comercio Exterior y Turismo, ante la ocurrencia de una incidencia.

a) ESCENARIO 1: Indisponibilidad de operación del Centro de Datos causado por pérdida del suministro eléctrico.

Indisponibilidad de operación del Centro de Datos causado por pérdida del suministro eléctrico		
1. Plan de Prevención		
1.1 Proceso Normal		
Los servicios críticos deben estar operativos de forma continua. **Funciones:** ✓ Permiten el acceso de usuarios a la red con login, así como el acceso a recursos compartidos. ✓ Gestionar el control de acceso a recursos informáticos, por los usuarios que lo requieran. ✓ Ingreso a los sistemas informáticos. ✓ Base de Datos para aplicativos de uso del MINCETUR. ✓ Intranet, Extranet, Entre Otros.		
1.2 Entorno de Ejecución		
Plataforma de Servidores Virtuales		
1.3 Personal Encargado		
Responsable	**Roles**	**Teléfono/Anexo**
Responsable de Servidores	Administrador de los servidores críticos del Centro de Datos.	Central: 513-6100 Anexo: 2127, 2128
Apoyo de Servidores	Soporte en la Administración de los servidores críticos del Centro de Datos.	Central: 513-6100 Anexo: 2136
1.4 Condiciones de Prevención		
✓ Actualización de los parches de seguridad del sistema operativo semanalmente. ✓ Actualización de parches de seguridad de las Bases de Datos. ✓ Actualización diaria de Antivirus. ✓ Operatividad permanente de Firewall.		

Indisponibilidad de operación del Centro de Datos causado por pérdida del suministro eléctrico
✓ Restricción del acceso a cada servidor, sólo para personal autorizado. ✓ Copias de respaldo diarias de la configuración de los servidores, la información almacenada y las aplicaciones. ✓ Disponer de servidores virtuales de contingencia con características similares a los originales, de modo que puedan entrar en operación ante cualquier evento de interrupción en el servidor original. ✓ Realizar periódicamente análisis de vulnerabilidades internas y externas a los servidores. ✓ Realizar el parchado y configuraciones de seguridad a los servidores del Centro de Datos. ✓ Monitorear actividades y/o tráfico inusual en la red de la entidad.
2. Plan de Ejecución
2.1 Evento que Activa el Plan de Contingencia
Pérdida de sistema eléctrico o suministro de energía al Centro de Datos causando posible indisponibilidad de los servicios que brinda el Centro de Datos (Servidor Controlador de Dominio, Servicio de correo electrónico, Servidor de Base de Datos, Servidor DNS y DHCP, Servidor Intranet, Servidor Extranet, Servidor Portal, Servidor de Aplicaciones Windows, entre otros).
2.1.1 Procesos Antecedente

Responsable	**Actividad**
Software de monitoreo	Alerta la pérdida de suministro eléctrico, a través del Tablero de Transferencia Automática (TTA) y del UPS.
Responsable operativo de Infraestructura Tecnológica	Verifica encendido automático del grupo electrógeno (GE) y el estado de funcionamiento de los UPS. De encontrar alguna falla, el responsable operativo de Infraestructura Tecnológica indaga las causas del problema y de no superarse en el breve plazo se reporta el problema al Coordinador de Infraestructura Tecnológica.
Responsable de Infraestructura Tecnológica.	En caso de que el incidente no tenga una solución inmediata el Coordinador de Infraestructura Tecnológica comunicará la situación al Coordinador del Plan de Contingencia de TI.
Coordinador del Plan de Contingencia de TI.	Evalúa impacto y tiempo de recuperación. Si el tiempo de recuperación es mayor al límite de tiempo de suministro de energía de los UPS y del Grupo Electrógeno, entonces se “activa” el Procedimiento de contingencia de Apagado y/o Encendido del Centro de Datos.

Indisponibilidad de operación del Centro de Datos causado por pérdida del suministro eléctrico		
2.1.2 Procesos Consecuentes		
Responsable	**Actividad**	
Coordinador del Plan de Contingencia de TI.	Coordina el Apagado y/o Encendido del Centro de Datos con el Coordinador de Infraestructura Tecnológica, de acuerdo al Anexo N°06.	
Responsable de Infraestructura Tecnológica.	Ejecuta el procedimiento de apagado y encendido del Centro	
Responsable de Infraestructura Tecnológica.	Notifica al Coordinador del Plan de Contingencia de TI sobre la situación actual.	
Coordinador del Plan de Contingencia de TI.	Verifica la operatividad y buen funcionamiento del Centro de Datos como resultado de la ejecución de pruebas de funcionamiento realizadas por el responsable de Infraestructura.	
Responsable de Desarrollo de Sistemas.	Verifica el correcto funcionamiento de las aplicaciones durante la contingencia. De ser necesario interactúa con proveedores que brinden soporte a las aplicaciones. Informa al Coordinador del Plan de Contingencia de TI que las pruebas de funcionamiento han sido realizadas satisfactoriamente.	
Coordinador del Plan de Contingencia de TI.	Elaborar informe sobre el evento ocurrido y las acciones realizadas. De ser necesario se actualizará el Plan de Contingencia de TI.	
2.2 Personal que Activa / Autoriza la Contingencia		
Coordinador del Plan de Contingencia de TI.		
Responsable	**Roles**	**Teléfono / Anexo**
Director de Informática.	Coordinador del Plan de Contingencia de TI.	Central: 513-6100 Anexo: 2103

b) ESCENARIO 2 – Posible indisponibilidad de los servicios del Centro de Datos debido a los ataques informáticos o actividades anómalas.

Indisponibilidad de los servicios del Centro de Datos

debido a los ataques informáticos o actividades anómalas

1. Plan de Prevención

1.1 Proceso Normal

Los servicios críticos deben estar operativos de forma continua.

Funciones:

- ✓ Permiten el acceso de usuarios a la red con login, así como el acceso a recursos compartidos.
- ✓ Gestionar el control de acceso a recursos informáticos, por los usuarios que lo requieran.
- ✓ Ingreso a los sistemas informáticos.
- ✓ Base de Datos para aplicativos de uso del MINCETUR.
- ✓ Intranet, Extranet, Entre Otros.

1.2 Entorno de Ejecución

Plataforma de Servidores Virtuales

1.3 Personal Encargado

Responsable	Roles	Teléfono / Anexo
Responsable de Servidores	Administrador de los servidores críticos del Centro de Datos.	Central: 513-6100 Anexo: 2127,2128
Apoyo de Servidores	Soporte en la Administración de los servidores críticos del Centro de Datos.	Central: 513-6100 Anexo: 2136

1.4 Condiciones de Prevención

- ✓ Actualización de los parches de seguridad del sistema operativo semanalmente.
- ✓ Actualización de parches de seguridad de las Bases de Datos
- ✓ Actualización diaria de Antivirus.
- ✓ Operatividad permanente de Firewall.
- ✓ Restricción del acceso a cada servidor, sólo para personal autorizado.
- ✓ Copias de respaldo diarias de la configuración de los servidores, la información almacenada y las aplicaciones.
- ✓ Disponer de Servidores virtuales de Contingencia con características similares a los originales, de modo que puedan entrar en operación ante cualquier evento de interrupción en el servidor original.
- ✓ Realizar periódicamente análisis de vulnerabilidades internas y externas a los servidores.
- ✓ Realizar el parchado y configuraciones de seguridad a los servidores del Centro de Datos.
- ✓ Disponer de una herramienta de monitoreo que informe de actividad o tráfico inusual en la red.

Indisponibilidad de los servicios del Centro de Datos

debido a los ataques informáticos o actividades anómalas

2. Plan de Ejecución

2.1 Eventos que Activan el Plan de Contingencia

Ataques informáticos o actividades anómalas que puedan causar posible indisponibilidad de los servicios que brinda el Centro de Datos, entre ellos: Servidor Controlador de Dominio, Servicio de correo electrónico, Servidor de Base de Datos, Servidor DNS y DHCP, Servidor Intranet, Servidor Extranet, Servidor Portal, Servidor de Aplicaciones Windows, entre otros.

2.1.1 Procesos Antecedentes

Responsable	Actividad
Software de monitoreo / Usuarios del MINCETUR	Comunicar al responsable de Infraestructura Tecnológica sobre el problema de indisponibilidad de los servicios del Centro de Datos debido a un ataque informático o actividades anómalas.
Responsable de Infraestructura Tecnológica	Ejecuta las acciones necesarias para superar el incidente y aplica el procedimiento de **Recopilación de evidencias de ataque informático, e**nfocadas en cubrir las siguientes actividades: 1. Limitar el alcance del ataque. 2. No alterar las evidencias del ataque. 3. Notificar al personal del equipo de contingencia. 4. Registrar todas las actividades e involucrados en la detección y contención del ataque. 5. Identificar la vulnerabilidad y/o amenaza asociada al ataque. 6. Corregir la vulnerabilidad o aplicar contramedidas para mitigar el riesgo. En caso que la falla no tenga una solución inmediata el responsable de Infraestructura Tecnológica comunicará la situación al Coordinador del Plan de Contingencia de TI.
Coordinador del Plan de Contingencia de TI.	Evalúa impacto, si el servicio se encuentra comprometido autoriza la activación del plan de contingencia y se gestiona el registro del incidente.

2.1.2 Procesos Consecuentes

Responsable	Actividad
Coordinador del Plan de Contingencia de TI.	Coordina la activación del nuevo Servidor de Producción con el responsable de Infraestructura Tecnológica.

Indisponibilidad de los servicios del Centro de Datos debido a los ataques informáticos o actividades anómalas	
Responsable de Infraestructura Tecnológica	Ejecuta las acciones necesarias para la activación del nuevo Servidor de Producción. Notifica al Coordinador del Plan de Contingencia de TI sobre la situación actual.
Coordinador del Plan de Contingencia de TI.	Verifica la operatividad y buen funcionamiento del nuevo Servidor de Producción, como resultado de la ejecución de pruebas de funcionamiento realizadas por el responsable de Infraestructura Tecnológica
Responsable de Desarrollo de Sistemas.	Verifica y garantiza el correcto funcionamiento de las aplicaciones. De ser necesario interactúa con proveedores que brinden soporte a las aplicaciones. Informa al Coordinador del Plan de Contingencia de TI que las pruebas de funcionamiento han sido realizadas satisfactoriamente.
Coordinador del Plan de Contingencia de TI.	Elaborar informe sobre el evento ocurrido y las acciones realizadas. De ser necesario se actualizará el Plan de Contingencia de TI.

2.2 Personal que Activa / Autoriza la Contingencia

Coordinador del Plan de Contingencia de TI.

Responsable	Roles	Teléfono / Anexo
Director de Informática.	Coordinador del Plan de Contingencia de TI.	Central: 513-6100 Anexo: 2103

3. Plan de Ejecución

3.1 Personal Encargado

Para la ejecución del Plan de Contingencia de TI interviene el personal designado como equipo de contingencia.

c) ESCENARIO 3– Indisponibilidad de los servicios del Centro de Datos debido a desastres por Sismo de Gran Magnitud

Indisponibilidad de los servicios del Centro de Datos

Debido a desastre por sismo de gran magnitud

1. Plan de Prevención

1.1 Proceso Normal

Los servicios críticos deben estar operativos de forma continua.

Funciones:

- ✓ Permiten el acceso de usuarios a la red con login, así como el acceso a recursos compartidos.
- ✓ Gestionar el control de acceso a recursos informáticos, por los usuarios que lo requieran.
- ✓ Ingreso a los sistemas informáticos.
- ✓ Base de Datos para aplicativos de uso del MINCETUR.
- ✓ Intranet, Extranet, Entre Otros.

1.2 Entorno de Ejecución

Plataforma de Servidores Virtuales

1.3 Personal Encargado

Responsable	Roles	Teléfono / Anexo
Responsable de Servidores	Administrador de los servidores críticos del Centro de Datos.	Central: 513-6100 Anexo: 2127,2128
Apoyo de Servidores	Soporte en la Administración de los servidores críticos del Centro de Datos.	Central: 513-6100 Anexo: 2136

1.4 Condiciones de Prevención

- ✓ Gestionar la contratación del servicio de Datacenter de contingencia en la nube, a fin de contar con un Data Center alterno que sirva de contingencia al Data Center principal ubicado en la sede central del MINCETUR, lo que permitirá brindar continuidad operativa de los servicios informáticos críticos, en caso de un eventual desastre natural.
- ✓ Asegurar que los servidores en el Datacenter alterno estén disponibles con la actualización de los parches de seguridad del sistema operativo.
- ✓ Restricción del acceso a cada servidor del entorno alterno, sólo para personal autorizado.
- ✓ Gestionar la contratación del servicio de Internet de contingencia en la sede alterna.
- ✓ Contar con un lote de equipos de cómputo personal en la sede alterna, a fin de brindar continuidad operativa a los servicios críticos de la entidad.

Indisponibilidad de los servicios del Centro de Datos **Debido a desastre por sismo de gran magnitud**	
✓ Contar con un área física en la sede alterna que permita desarrollar las actividades de administración de los servidores críticos en la nube.	
2. Plan de Ejecución	
2.1 Eventos que Activan el Plan de Contingencia	
Sismo de gran magnitud que puedan causar indisponibilidad de los servicios que brinda el Centro de Datos, entre ellos: Servidor Controlador de Dominio, Servidor de archivos, Servidor de Base de Datos, Servidor DNS y DHCP, Servidor Intranet, Servidor Extranet, Servidor de Aplicaciones Windows, entre otros.	
2.1.1 Procesos Antecedentes	
Responsable	**Actividad**
Software de monitoreo / Usuarios del MINCETUR	Comunicar al responsable de Infraestructura Tecnológica sobre el problema de indisponibilidad de los servicios del Centro de Datos debido a un sismo de gran magnitud.
Responsable de Infraestructura Tecnológica	Ejecuta las acciones necesarias para superar el evento, en caso que la falla no tenga una solución inmediata el responsable de Infraestructura Tecnológica comunicará la situación al Coordinador del Plan de Contingencia de TI.
Coordinador del Plan de Contingencia de TI.	Evalúa impacto y tiempo de recuperación. Si el tiempo de recuperación es mayor al límite de tiempo establecido en dicho escenario, y autoriza restaurar los servicios desde el Datacenter de contingencia en la nube.
2.1.2 Procesos Consecuentes	
Responsable	**Actividad**
Coordinador del Plan de Contingencia de TI.	Coordina la activación del servicio de Datacenter de contingencia en la nube con el responsable de Infraestructura Tecnológica.
Responsable de Infraestructura Tecnológica	Ejecuta las acciones necesarias para la activación del servicio de Datacenter de contingencia en la nube. Notifica al Coordinador del Plan de Contingencia de TI sobre la situación actual.
Coordinador del Plan de Contingencia de TI.	Verifica la operatividad y buen funcionamiento del servicio de Datacenter de contingencia en la nube, como resultado de las pruebas de funcionamiento realizadas por el responsable de Infraestructura Tecnológica

Indisponibilidad de los servicios del Centro de Datos **Debido a desastre por sismo de gran magnitud**	
Responsable de Desarrollo de Sistemas.	Verifica y garantiza el correcto funcionamiento de las aplicaciones. De ser necesario interactúa con proveedores que brinden soporte a las aplicaciones. Informa al Coordinador del Plan de Contingencia de TI que las pruebas de funcionamiento han sido realizadas satisfactoriamente.
Coordinador del Plan de Contingencia de TI.	Elaborar informe sobre el evento ocurrido y las acciones realizadas. De ser necesario se actualizará el Plan de Contingencia de TI.

2.2 Personal que Activa / Autoriza la Contingencia

Coordinador del Plan de Contingencia de TI.

Responsable	Roles	Teléfono / Anexo
Director de Informática.	Coordinador del Plan de Contingencia de TI.	Central: 513-6100 Anexo: 2103

Protocolo de Restauración (Volver a Estado de Operación)

El objetivo es retornar al estado normal de operaciones de los servicios críticos del Centro de Datos Principal.

a) ESCENARIO 1: Posible indisponibilidad de operación del Centro de Datos causado por pérdida del suministro eléctrico

Posible indisponibilidad de operación del Centro de Datos **causado por pérdida del suministro eléctrico**	
Descripción de Actividades de Restauración de Servicios Críticos	
Responsable	**Actividad**
Coordinador del Plan de Contingencia de TI.	Coordina con el responsable de Infraestructura Tecnológica, la recuperación de los Servicios del Centro de Datos.

Posible indisponibilidad de operación del Centro de Datos causado por pérdida del suministro eléctrico	
Responsable de Infraestructura Tecnológica	Determina el grado de pérdida, el impacto de la misma y las acciones a tomar. De ser necesario, se coordinará con el proveedor del servicio de suministro eléctrico para determinar el periodo de resolución de la falta de suministro eléctrico y de esta manera tomar las acciones necesarias en cuanto al funcionamiento del grupo electrógeno.
Coordinador del Plan de Contingencia de TI.	En el caso de que se requiera la compra de un nuevo equipo o contratación de un servicio, se coordinará con la Oficina General de Administración. Se solicitará al responsable de Infraestructura Tecnológica, realizar los pasos correspondientes para la activación del nuevo equipo o servicio.
Responsable de Infraestructura Tecnológica	En caso se haya visto afectado alguno de los servidores críticos se hará uso de las copias de respaldo. Aplicando el procedimiento **"Restauración de la Información"** Se aplicará el procedimiento al servidor afectado.
Responsable de Infraestructura Tecnológica	Notifica al Coordinador del Plan de Contingencia de TI sobre la situación actual.
Mecanismos de Comprobación	
Responsable	**Actividad**
Responsable de Infraestructura Tecnológica	Verifica la operatividad y buen funcionamiento de los Servicios del Centro de Datos mediante la ejecución de pruebas de funcionamiento**,** para cada uno de los servidores críticos.
Responsable de Desarrollo de Sistemas.	Verifica la operatividad y buen funcionamiento de los Sistemas / Aplicaciones en los servidores críticos.
Desactivación del Plan de Contingencia	
Responsable	**Actividad**
Coordinador del Plan de Contingencia de TI.	Una vez confirmado que las pruebas de funcionamiento han sido realizadas satisfactoriamente, comunica al Director General de la OI el retorno a la normalidad.

b) ESCENARIO 2: Indisponibilidad de los servicios del Centro de Datos debido a los ataques informáticos o actividades anómalas

No aplica, debido a que la restauración de un servidor es la solución definitiva.

c) ESCENARIO 3: Indisponibilidad de los servicios del Centro de Datos debido a desastre por sismo de gran magnitud.

Indisponibilidad de los servicios del Centro de Datos debido a desastre por sismo de gran magnitud	
Descripción de Actividades de Restauración de Servicios Críticos	
Responsable	**Actividad**
Coordinador del Plan de Contingencia de TI.	Coordina con el responsable de Infraestructura Tecnológica, la recuperación de máquinas virtuales desde el Datacenter de contingencia en la nube pública.
Responsable de Infraestructura Tecnológica	Determina el grado de pérdida, el impacto y las acciones a tomar. Ejecuta las acciones correctivas necesarias. Si la falla no puede ser resuelta por el responsable de Infraestructura Tecnológica, se procederá a restaurar desde las máquinas virtuales implementadas en el Datacenter de contingencia en la nube pública.
Coordinador del Plan de Contingencia de TI.	Se solicitará al Responsable de Infraestructura Tecnológica, realizar los pasos correspondientes para la activación del servicio de Datacenter de contingencia en la nube.
Responsable de Infraestructura Tecnológica	Restaura la(s) copia(s) de respaldo. Aplicar procedimiento: **"Recuperación de máquinas virtuales en la nube".**
Responsable de Infraestructura Tecnológica	Notifica al Coordinador del Plan de Contingencia de TI sobre la situación actual.
Mecanismos de Comprobación	
Responsable	**Actividad**
Coordinador del Plan de Contingencia de TI.	Verifica la operatividad y buen funcionamiento del servicio de Datacenter de contingencia en la nube, como resultado de las pruebas de funcionamiento realizadas por el Responsable de Infraestructura Tecnológica y por el Responsable de Desarrollo de Sistemas.

Desactivación del Plan de Contingencia	
Responsable	**Actividad**
Coordinador del Plan de Contingencia de TI.	Una vez confirmado que las pruebas de funcionamiento han sido realizadas satisfactoriamente, comunica al Director General de la OI el retorno a la normalidad.

ACTIVIDADES DESPUÉS DEL INCIDENTE

- **Evaluación de daños.**

  Inmediatamente después que el evento haya concluido, se deberá evaluar la magnitud del daño que se ha producido, qué sistemas se han afectado, qué equipos han quedado no operativos, cuáles se pueden recuperar, y en cuánto tiempo, entre otros.

- **Evaluación de resultados.**

  Una vez concluidas las labores de Recuperación del (los) Sistema(s) que fueron afectados por el incidente, debemos de evaluar objetivamente, todas las actividades realizadas, qué tan bien se hicieron, qué tiempo tomaron, qué circunstancias modificaron (aceleraron o entorpecieron) las actividades, cómo se comportaron los equipos de trabajo, etc. De la evaluación de resultados y del siniestro en sí, deberían de salir dos tipos de recomendaciones, una la retroalimentación del Plan de Contingencia y otra una lista de recomendaciones para minimizar los riesgos y pérdida que ocasionaron el siniestro.

- **Retroalimentación de lo planificado.**

  Con la evaluación de resultados, debemos de optimizar la planificación original, mejorando las actividades que tuvieron algún tipo de dificultad y reforzando los elementos que funcionaron adecuadamente. El otro elemento es evaluar cuál hubiera sido el costo para MINCETUR de no haber tenido el Plan de Contingencia llevado a cabo.

7.5. PLAN DE PRUEBAS DEL PLAN DE CONTINGENCIA DE TI

7.5.1. OBJETIVO

Las pruebas del Plan de Contingencia de TI se establecen como un proceso continuo cuyos objetivos son:

- Determinar si las estrategias y procedimientos de contingencia definidos son viables.
- Identificar nuevos escenarios de riesgo.
- Analizar estrategias y procedimientos de contingencia adicionales para la mejora continua del Plan de Contingencia de TI.
- Mantener el Plan de Contingencia de TI actualizado.

7.5.2. ALCANCE

El alcance del presente Plan de Pruebas está limitado a los siguientes eventos de riesgo / escenarios de prueba:

Código de Contingencia	Nombre del Evento
CNTG-01	Indisponibilidad de operación del Centro de Datos causado por pérdida del suministro eléctrico.
CNTG-02	Indisponibilidad de los servicios del Centro de Datos debido a ataques informáticos o actividades anómalas.
CNTG-03	Indisponibilidad de los servicios del centro de datos por Desastres de Sismo de gran Intensidad.

7.5.3. DEFINICIÓN

El Plan de Contingencia de TI se debe probar por lo menos una (01) vez al año o cuando ocurra un evento determinado, como cambios en la organización, en los procesos o la tecnología.

Descripción de la Prueba

a) Prueba de campo - simulación parcial o segmentada

Se simula un tipo de impacto a través de los eventos de riesgo definidos. La prueba se limita a los activos tecnológicos mencionados en el alcance. La prueba permite al Coordinador del Plan de Contingencia de TI y su equipo ejecutar los procedimientos de contingencia y poder validar una o más partes del plan, haciendo uso del checklist de prueba.

b) Premisa

La prueba inicia desde que el Coordinador del Plan de Contingencia de TI coordina la activación de la contingencia.

c) Checklist – Prueba del Plan de Contingencia

Es una herramienta que se utiliza para la ejecución de las pruebas del Plan de Contingencia de TI. Dicha herramienta permite al Coordinador del Plan de Contingencia de TI, controlar los tiempos de cada actividad a ejecutar durante las pruebas.

d) Responsabilidades de los participantes / involucrados

Participante / Involucrado	Responsabilidad
• Coordinador del Plan de Contingencia de TI.	-Elaborar el Plan de Pruebas -Liderar la ejecución de la prueba del Plan de Contingencia de TI

Participante / Involucrado	Responsabilidad
	-Elaborar y presentar el Informe de Resultado de las Pruebas
• Responsable de Infraestructura / Redes / Servidores • Responsable de Desarrollo de Sistemas	-Ejecutar la prueba del Plan de Contingencia de TI -Validar el desarrollo de la prueba. -Da conformidad a los resultados de las pruebas.
• Oficial de Seguridad de la Información	-Supervisar el desarrollo de la prueba y custodiar las evidencias generadas

e) Lugar de la prueba

La prueba del Plan de Contingencia de TI se realizará en la Oficina de Informática del Ministerio de Comercio Exterior y Turismo (Calle Uno Oeste N° 050 – Sótano 1 - Urb. Corpac - San Isidro)

f) Cronograma de pruebas

El Cronograma de pruebas se deberá definir con la debida anticipación, con la finalidad de conseguir la presencia de todos los involucrados en dichas pruebas.

g) Resultado de la prueba

Los resultados de las pruebas deberán ser presentados en un informe, el cual deberá contener al menos la siguiente información:

- ✓ Escenario de Pruebas
- ✓ Detalle de Ejecución de Pruebas
- ✓ Resultado de las Pruebas

7.5.4. CHECKLIST DE ESCENARIOS

a) CHECKLIST DE PRUEBAS PARA EL ESCENARIO 1:

CNTG-01 – Indisponibilidad de operación del Centro de Datos causado por pérdida del suministro eléctrico.			Tiempo de Recuperación Objetivo (RTO)		
Recuperación de la Contingencia					
N°	**Actividad**	**Responsable**	**Inicio**	**Fin**	**Total Horas/Min**
1	Coordina el apagado del interruptor termo magnético (ITM) que se ubica en la sub estación eléctrica de MINCETUR y que alimenta exclusivamente el Centro de Datos.	Coordinador del Plan de Contingencia de TI			30 min

CNTG-01 – Indisponibilidad de operación del Centro de Datos causado por pérdida del suministro eléctrico.					Tiempo de Recuperación Objetivo (RTO)
Recuperación de la Contingencia					
2	Verificar recepción de correo desde el Tablero de Transferencia Automática (TTA) y del UPS	Responsable de Infraestructura Tecnológica /Oficial de Seguridad de la Información			10 min
3	Verificar el tiempo de encendido del grupo electrógeno (30 segundos)	Responsable de Infraestructura Tecnológica			10 min
4	Verificar el tiempo de operación en batería del UPS	Responsable de Infraestructura Tecnológica			10 min
5	Verificar el estado de operación del aire acondicionado	Responsable de Infraestructura Tecnológica			10 min
6	Verificar el estado de operación de los cuartos de comunicaciones.	Responsable de Infraestructura Tecnológica			20 min
7	En caso se necesite apagar (cuando no funcione el grupo electrógeno) el centro de datos, se deberá notificar al Coordinador del Plan de Contingencia de TI	Responsable de Infraestructura Tecnológica			20 min
8	Se procede con el **apagado** de los equipos del centro de datos, de acuerdo al Anexo N°06.	Responsable de Infraestructura Tecnológica			4 hs
9	Verificar si la energía eléctrica comercial se haya restablecido para proceder con el **encendido** de los equipos del Data Center, de acuerdo al Anexo N°06	Responsable de Infraestructura Tecnológica			4hs
10	Verifica la operatividad y buen funcionamiento del Centro de Datos mediante la ejecución de pruebas de funcionamiento realizadas por el Responsable de Infraestructura.	Responsable de Infraestructura Tecnológica			1hs
11	Verifica y garantiza el correcto funcionamiento de las aplicaciones durante la contingencia. De ser necesario interactúa con proveedores que brinden soporte a las aplicaciones.	Responsable de Desarrollo de Sistemas.			1 hs

CNTG-01 – Indisponibilidad de operación del Centro de Datos causado por pérdida del suministro eléctrico.					Tiempo de Recuperación Objetivo (RTO)
Recuperación de la Contingencia					
12	Informa al Coordinador del Plan de Contingencia de TI que las pruebas de funcionamiento han sido realizadas satisfactoriamente.	Responsable de Infraestructura Tecnológica			10 min
13	Comunica a los usuarios mediante correo electrónico, que pueden hacer uso de los Servicios del Centro de Datos.	Coordinador del Plan de Contingencia de TI.			30 min
14	Elaborar informe de las pruebas	Coordinador del Plan de Contingencia de TI.			2 hs

b) CHECKLIST DE PRUEBAS PARA EL ESCENARIO 2:

CNTG-02 – Indisponibilidad de los servicios del Centro de Datos debido a ataques informáticos o actividades anómalas					Tiempo de Recuperación Objetivo (RTO)
Recuperación de la Contingencia					
N°	**Actividad**	**Responsable**	**Inicio**	**Fin**	**Total Horas**
1	Coordina la activación de las pruebas, indicando el escenario.	Coordinador del Plan de Contingencia de TI			30 min
2	Simula la caída del servicio o modificación anómala de datos a través del apagado de la tarjeta de red o modificación de la página web institucional.	Responsable de Infraestructura Tecnológica			10 min
3	Verifica la notificación de correos mediante el Software de monitoreo de uso institucional	Responsable de Infraestructura Tecnológica			30 min

CNTG-02 – Indisponibilidad de los servicios del Centro de Datos debido a ataques informáticos o actividades anómalas					Tiempo de Recuperación Objetivo (RTO)
Recuperación de la Contingencia					
4	Comunicar al Coordinador del Plan de Contingencia de TI sobre el problema de indisponibilidad de los servicios del Centro de Datos debido a un ataque externo o actividades anómalas.	Responsable de Infraestructura Tecnológica			10 min
5	Analiza la situación presentada y toma decisiones de acuerdo a los 2 casos presentados: **Caso 1.** Denegación de servicio – Se coordina con el proveedor del servicio de internet y seguridad perimetral, la aplicación de políticas que controlen la denegación del servicio. Para desarrollar esta actividad se debe tener en cuenta lo siguiente: 1. Limitar el alcance del ataque. 2. No alterar las evidencias del ataque. 3. Registrar todas las actividades e involucrados en la detección y contención del ataque. 4. Identificar la vulnerabilidad y/o amenaza asociada al ataque. 5. Corregir la vulnerabilidad o aplicar contramedidas para mitigar el riesgo. De ser necesario se “activa” el Procedimiento de respaldo y recuperación de la información. **Caso 2.** Modificación de la Página – Se implementa el mensaje de página en mantenimiento.	Responsable de Infraestructura Tecnológica			2hs 1hs
6	Notifica al Coordinador del Plan de Contingencia de TI sobre la situación actual.	Responsable de Infraestructura Tecnológica			10 min
7	Verifica la operatividad y buen funcionamiento del Centro de Datos mediante la ejecución de pruebas de funcionamiento realizadas por el responsable de Infraestructura.	Responsable de Infraestructura Tecnológica			2hs

CNTG-02 – Indisponibilidad de los servicios del Centro de Datos debido a ataques informáticos o actividades anómalas					Tiempo de Recuperación Objetivo (RTO)
Recuperación de la Contingencia					
8	Verifica y garantiza el correcto funcionamiento de las aplicaciones durante la contingencia. De ser necesario interactúa con proveedores que brinden soporte a las aplicaciones.	Responsable de Desarrollo de Sistemas.			2hs
9	Informa al Coordinador del Plan de Contingencia de TI que las pruebas de funcionamiento han sido realizadas satisfactoriamente.	Responsable de Desarrollo de Sistemas.			10 min
10	Comunica al Director General de la Oficina de Informática el resultado de las pruebas.	Coordinador del Plan de Contingencia de TI.			30 min
11	Elabora el informe de prueba	Coordinador del Plan de Contingencia de TI.			2hs

c) CHECKLIST DE PRUEBAS PARA EL ESCENARIO 3

CNTG-03.-Indisponibilidad de operación del Centro de Datos causado por Desastre de Sismo de Gran Magnitud					Tiempo de Recuperación Objetivo (RTO)
Recuperación de la Contingencia					
N°	**Actividad**	**Responsable**	**Inicio**	**Fin**	**Total Horas**
1	Dispone la disposición del equipo de Emergencia de OI en la Sede Alterna	Coordinador del Plan de Contingencia de TI			10 min
2	Verifica la conectividad de los enlaces de suministro eléctrico	Responsable de Infraestructura Tecnológica /Oficial de Seguridad de la Información			1 hs
3	Verificar la conectividad del enlace de transmisión de datos	Responsable de Infraestructura Tecnológica			30 min
4	Verificar los enlaces de comunicaciones para el sistema de emergencia	Responsable de Infraestructura Tecnológica			30 min
5	Verificar el estado de operación de los cuartos de comunicaciones	Responsable de Infraestructura Tecnológica			30 min
6	Verifica y garantiza el correcto funcionamiento de las aplicaciones durante la contingencia. De ser necesario interactúa con proveedores que brinden soporte a las aplicaciones	Responsable de Desarrollo de Sistemas			1 hs
7	Informa al Coordinador del Plan de Contingencia de TI que las pruebas de Operatividad y funcionamiento del Centro de datos han sido realizadas satisfactoriamente.	Responsable de Infraestructura Tecnológica			10 min
8	Informa al Coordinador del Plan de Contingencia de TI que las pruebas de funcionamiento de aplicaciones han sido realizadas satisfactoriamente.	Responsable de Desarrollo de Sistemas			10 min

CNTG-03.-Indisponibilidad de operación del Centro de Datos causado por Desastre de Sismo de Gran Magnitud					Tiempo de Recuperación Objetivo (RTO)
Recuperación de la Contingencia					
9	Comunica al Director General de la Oficina de Informática el resultado de las pruebas.	Coordinador del Plan de Contingencia			30 min
10	Elabora el informe de Prueba	Coordinador del Plan de Contingencia TI			2hs.

ANEXOS:

Anexo N°01: Integrantes del comité de contingencia

N°	Integrantes	Principal			Alterno		
		Nombres y apellidos	Celular	Correo	Nombres y apellidos	Celular	Correo
1	Director General de la Oficina de Informática						
2	Director de la Oficina de Informática (Coordinador)						
3	Responsable de Infraestructura Tecnológica						
4	Responsable de Desarrollo de Sistemas						
5	Oficial de Seguridad y Confianza Digital						

Anexo N° 02: "Inventario de Sistemas de Información del MINCETUR"

N°	Nombre del Sistema Informático	Descripción	U.O. Funcional	Interno/Externo	Administrador del Sistema

Anexo N° 03: "Inventario de Servicios de Infraestructura TI del MINCETUR"

N°	Descripción del servicio	Responsable principal	Responsable alterno
1.			

Anexo N° 04: "Inventario de Servidores de Datos del MINCETUR"

N°	Descripción del equipo	Marca	Modelo	Serie

Anexo N° 05: "Directorio Telefónico de Proveedores"

Servicio	**Nombre o Razón Social**	**Personal contratista**	**Teléfonos / Celulares**	**Correos**

Anexo N° 06: "Procedimiento de Apagado y Encendido de los equipos del Data Center" Documento confidencial para uso de la Oficina de Informática

Anexo N° 07: "Lista de Contactos Oficina de Informática"

N°	**CARGO**	**INTEGRANTE PRINCIPAL**		
		NOMBRES Y APELLIDOS	**CELULAR**	**CORREO**