"Decenio de la Igualdad de Oportunidades para Mujeres y Hombres"
"Año del Fortalecimiento de la Soberanía Nacional"
"Año del Bicentenario del Congreso de la República del Perú"

Plan de Recuperación de los Servicios de Tecnología de la Información

Ministerio de Transporte y Comunicaciones

OGTI - Oficina General de Tecnología de la Información

AGOSTO 2022

INDICE

Jirón Zorritos 1203 – Lima - Perú
Central telefónica. (511) 615-7800
www.gob.pe/mtc

INTRODUCCIÓN

El presente documento define el Plan de Recuperación de servicios informáticos de tecnología de la información del Ministerio de Transportes y Comunicaciones - MTC como un proceso continuo de planeación, desarrollo, pruebas y ejecución de procedimientos para la recuperación de los servicios críticos de la entidad ante un posible evento o siniestro que pueda afectar su normal funcionamiento. Estas acciones buscan asegurar la reanudación eficiente y efectiva de los servicios y operaciones de tecnologías de la información del MTC en el menor tiempo e impacto posible.

Firmado digitalmente por:
REQUENA CASTRO Jesus
Nicanor FAU 20131379944 soft
Motivo: Doy V° B°
Fecha: 29/09/2022 11:20:12-0500

Jirón Zorritos 1203 – Lima - Perú
Central telefónica. (511) 615-7800
www.gob.pe/mtc

PLAN DE RECUPERACIÓN DE LOS SERVICIOS DE TECNOLOGÍA DE LA INFORMACIÓN

1. OBJETIVOS

1.1. Objetivo General

Restaurar los servicios de tecnología de información necesarios para ejecutar las actividades críticas identificadas de la entidad, permitiendo una posterior recuperación de las condiciones previas a su ocurrencia.
Garantizar la continuidad de los servicios de tecnología de la información del Ministerio de Transporte y Comunicaciones - MTC, ante eventos que podrían alterar su normal funcionamiento, a fin de que se restablezcan en el menor tiempo posible.

1.2. Objetivos Específicos

- Identificar los servicios críticos de tecnología de la información del MTC.
- Identificar y analizar riesgos que pueden afectar las operaciones y procesos informáticos de la Institución.
- Establecer las estrategias adecuadas para asegurar la continuidad de los servicios informáticos en caso de interrupción y que permita restablecer éstos en el menor tiempo posible.
- Definir procedimientos, tareas y responsables para la recuperación de los servicios críticos de tecnología de la información ante la ocurrencia de eventos que afecten su normal funcionamiento.

2. ALCANCE

El desarrollo e implementación del plan de recuperación de los servicios de tecnología de la información del MTC incluye a todos los elementos que forman parte o soportan a los sistemas de información como son: servidores, software, equipos informáticos, bases de datos, equipos de comunicaciones, personal técnico y otros recursos administrados por la Oficina General de Tecnología de Información – OGTI del MTC.

Los servicios informáticos críticos que brinda el MTC son usados por los ciudadanos a nivel nacional, y las áreas usuarias son las direcciones u oficinas del MTC.

3. BASE LEGAL:

- Ley N° 27685, "Ley Marco de Modernización de la Gestión del Estado".
- Ley N° 29370, "Ley de Organización y funciones del Ministerio de Transportes y Comunicaciones", determina y regula el ámbito de competencias, las funciones y la estructura orgánica básica del Ministerio de Transportes y Comunicaciones.
- 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 de Urgencia No 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital.
- Decreto Supremo No 157-2021-PCM, Decreto Supremo que aprueba el Reglamento del Decreto de Urgencia No 006-2020, Decreto de Urgencia que crea el Sistema Nacional de Transformación Digital.
- Resolución Ministerial No 246-2007-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la gestión de la seguridad de la información. 2a. Edición" en todas las entidades integrantes del Sistema Nacional de Informática.
- Resolución Ministerial No 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "ISO NTP/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información.

Requisitos 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática.

- Resolución Ministerial Nº 041-2017-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 12207:2016- Ingeniería de Software y Sistemas. Procesos del ciclo de vida del software. 3a Edición", en todas las entidades integrantes del Sistema Nacional de Informática.
- Resolución de Secretaría de Gobierno Digital No 002-2019-PCM/SEGDI, "Aprueban Estándares de Interoperabilidad de la Plataforma de Interoperabilidad del Estado (PIDE) y medidas adicionales para su despliegue.
- Resolución Ministerial No 046-2019-MTC/01, que aprueba el Plan de Continuidad Operativa del Ministerio de Transportes y Comunicaciones.
- Resolución Ministerial No 320-2021-PCM, que aprueba los "Lineamientos para la Gestión de la Continuidad Operativa y la Formulación de los Planes de Continuidad Operativa de las Entidades Públicas de los tres niveles de gobierno".
- Resolución Ministerial No 658-2021-MTC/01, que aprueba el texto Integrado actualizado del Reglamento de Organización y funciones del Ministerio de Transportes y Comunicaciones.
- Las referidas normas incluyen sus respectivas modificatorias, de ser el caso.

4. MARCO TEORICO:

A continuación, se desarrolla el marco teórico necesario para elaborar el "Plan de recuperación de servicio TI":

4.1. Gestión del Riesgo

Es claro que por un tema de costos y practicidad no se podría preparar procedimientos de respuesta a las contingencias a todos los activos (recursos, procesos, personas, tecnología) que utiliza una organización para operar sus servicios. Por ello, es necesario identificar los activos críticos, aquellos que están más expuestos a riesgos que afecten su disponibilidad; para esta identificación se utilizará la gestión de riesgos, que podemos resumir en tres procesos: identificación, análisis, respuesta, y control de los riesgos.

4.2. Análisis de riesgos

El primer paso para analizar los riesgos es la identificación de éstos, que se hará con base en la determinación de las amenazas a las que están expuestos los activos TIC, y a las vulnerabilidades que se tengan en la gestión de éstos.

El segundo paso, el análisis de riesgos propiamente dicho, maneja tres factores: la probabilidad de ocurrencia del riesgo; el impacto que dicho riesgo ocasionaría si se presentase; y el nivel de exposición o severidad del riesgo.

El análisis del riesgo implica la evaluación y la comprensión del riesgo; lo que permite tomar las decisiones sobre las estrategias y métodos más adecuados para su tratamiento o para aceptarlo.

4.3. Probabilidad del Riesgo (PO)

Es la cuantificación de la posibilidad de ocurrencia de un riesgo. La probabilidad del riesgo debe ser superior a cero, de lo contrario el riesgo no existe; y debe ser menor a uno, de lo contrario el riesgo se ha presentado y es un hecho. En una organización la combinación de amenazas y vulnerabilidades sobre los activos ayudan a determinar la probabilidad de ocurrencia de riesgos, la que se clasificará, para el plan, en 5 niveles, del 1 al 5. En la siguiente tabla se muestra esta clasificación.

Tabla No 1: Probabilidad de Ocurrencia de riesgos en OGTI- MTC

Valor	Nivel	Rango de Probabilidad	Criterio
5	Muy Alta (Casi Cierta)	0.801 -0.99	El riesgo puede ser inminente.

Valor	Nivel	Rango de Probabilidad	Criterio
			Es extremadamente probable que ocurra y no se tiene ningún control o los que existen son insuficientes.
4	Alta (Altamente Probable)	0.601 – 0.8	El riesgo puede presentarse con relativa certeza, dado que hay eventos que dan cuenta de su regularidad. Es muy probable que ocurra y no se cuenta con los controles o son insuficientes.
3	Media (Probable)	0.401 – 0.6	El riesgo, si bien se ha presentado anteriormente, no se tiene indicios de una regularidad: además se han tomado algunas medidas que reducen su probabilidad de ocurrencia, aunque siempre es posible que se presente. Se recomienda asumir este valor de probabilidad cuando no se tiene información que soporte un estimado. Es probable que ocurra. Adicionalmente no se tienen controles.
2	Baja (Muy poco probable)	0.201 – 0.4	El riesgo se ha presentado una sola vez en el último año. Es muy poco probable que ocurra y no se tienen controles.
1	Muy Baja (Casi improbable)	0.1 – 0.2	El riesgo se ha presentado alguna vez en los últimos 5 años. Y no hay indicios de que pueda ocurrir por ahora. Es casi imposible que ocurra **o se hacen acciones que lo controlan.**

Fuente: Plan de Contingencia Informático – MTC

4.4. Impacto del Riesgo (VI)

El impacto del riesgo mide la gravedad o magnitud del efecto adverso o pérdida a causa de la ocurrencia de este; en nuestro caso, afectando el nivel de servicio normal. La determinación del impacto puede ser cualitativa o cuantitativa; la recomendación general es que se haga estimando cuánto costaría recuperarse del riesgo ocurrido, en términos monetarios (pérdida de imagen, ventas, multas, reparaciones, re-trabajos, entre otros). Cuanto mayor sea el impacto, mayor será la magnitud que lo represente. Para nuestro caso, la clasificación del impacto será en una escala del 1 al 5; conforme se muestra en la Tabla 2.

Tabla No 2: Determinación del Impacto del riesgo

Nivel de Impacto	Valor del Impacto (VI)	Criterio
Muy Alto	5	Riesgo cuya materialización afecta directamente en el cumplimiento de la misión, pérdida patrimonial o daño significativo de la imagen, dejando sin funcionar totalmente, o por un período importante de tiempo, los servicios que entrega la institución a sus interesados externos.
Alto	4	Riesgo cuya materialización dañaría medianamente el patrimonio, imagen o logro de los objetivos sociales. Demoraría un tiempo más allá de lo aceptable reparar los daños. Además, se requeriría una cantidad importante de tiempo de la alta dirección en investigar las causas y establecer responsabilidades.
Medio	3	Riesgo cuya materialización causaría ya haya una pérdida importante en el patrimonio o un deterioro significativo de la imagen. Demoraría un tiempo ligeramente menor del máximo aceptable reparar los daños. Además, se requeriría de tiempo de la alta dirección en investigar las causas y establecer responsabilidades.

Nivel de Impacto	Valor del Impacto (VI)	Criterio
Bajo	2	Riesgo que causa un ligero daño en el patrimonio o imagen. Demoraría un tiempo mucho menor del máximo aceptable para reparar los daños. Además, se requeriría de muy poco tiempo de la alta dirección en investigar las causas y establecer responsabilidades.
Muy Bajo	1	Riesgo que puede tener un muy pequeño efecto en la institución, sobre todo en el orden interno.

Fuente: Plan de Contingencia Informático – MTC

4.5. Nivel de exposición al Riesgo

El valor del riesgo (VR) es el resultado de multiplicar la probabilidad de ocurrencia por el impacto del riesgo.

El nivel de exposición al riesgo es una medida cualitativa de este valor y se utiliza para estimar cuán fuerte puede afectar un riesgo, y permite focalizar nuestro esfuerzo en aquellos riesgos que consideremos más severos o con mayor exposición.

Generalmente, este nivel se clasifica con tres niveles: Alto, Medio y Bajo, como resultado del producto: VR = PO * VI. En la Tabla 3 se muestra esta definición. 5

Tabla No 3: Nivel de Exposición al riesgo

Nivel de Riesgo	Valor del riesgo (VR)	Criterio
Alto	10 - 25	Puede afectar seriamente a la operación y servicio de la OGTI, en términos de indisponibilidad del Servicio ofrecido, generando paralización de las operaciones más allá del tiempo tolerable, además de pérdidas económicas importantes y daños considerables a la imagen del MTC.
Medio	4 - 9	Puede afectar a los niveles de operación y servicio de la OGTI, ocasionando incumplimiento de objetivos estratégicos y pérdidas económicas al MTC.
Bajo	1 - 3	El problema de servicio de la OGTI afecta mínimamente el cumplimiento de un objetivo estratégico o servicio funcional del MTC.

Fuente: Plan de Contingencia Informático - MTC

Esta clasificación se ha hecho con el criterio de aversión al riesgo.

4.6. Definición de la Matriz Probabilidad - Impacto

Esta matriz mapea el producto de PO x VI, de modo que permite separar gráficamente el dominio de valor posible de VR, conforme se muestra en la Tabla 4.

Tabla No 4: Matriz de Probabilidad - Impacto

MATRIZ DE NIVEL DE RIESGO			VALOR DEL IMPACTO (VI)				
			Muy Bajo	Bajo	Medio	Alto	Muy Alto
			1	2	3	4	5
PROBABILIDAD DE OCURRENCIA (PO)	Muy Bajo	1	1	2	3	4	5
	Bajo	2	2	4	6	8	10
	Medio	3	3	6	9	12	15
	Alto	4	4	8	12	16	20
	Muy Alto	5	5	10	15	20	25

Fuente: Plan de Contingencia Informático - MTC

Jirón Zorritos 1203 – Lima - Perú
Central telefónica. (511) 615-7800
www.gob.pe/mtc

5. DESARROLLO DEL PLAN DE RECUPERACIÓN DE LOS SERVICIOS DE TECNOLOGÍA DE LA INFORMACIÓN:

El presente plan ha sido desarrollado con el aporte de la experiencia profesional del personal de la Oficina General de Tecnología de la Información del MTC, y la aplicación de las recomendaciones 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 y cumpliendo con lo establecido en la Resolución Ministerial No 320-2021-PCM, que aprueba los "Lineamientos para la Gestión de la Continuidad Operativa y la Formulación de los Planes de Continuidad Operativa de las Entidades Públicas de los tres niveles de gobierno".

Este plan se aplicará para situaciones de eventos que no lleguen a la condición de desastre, si no para cuando estos eventos afecten la disponibilidad de los servicios críticos de la OGTI, y por ende los servicios funcionales del MTC.

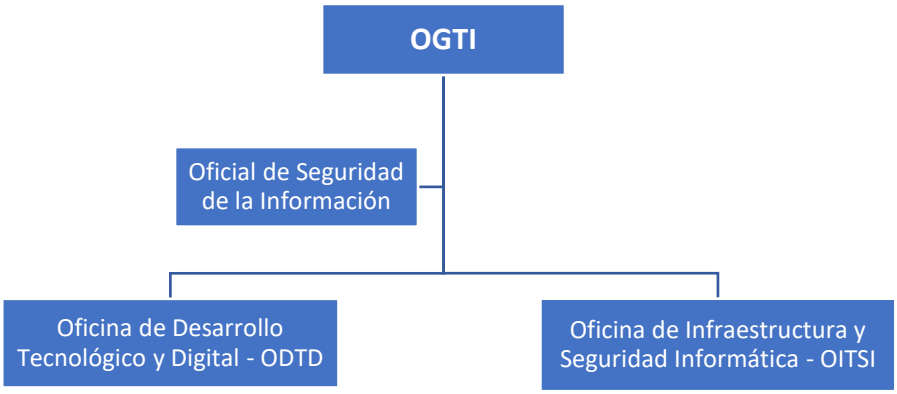
El Plan de Recuperación de los Servicios Informáticos del MTC se ha dividido en los siguientes apartados:

- Apartado 1: Organización
- Apartado 2: Identificación de los activos críticos de la OGTI
- Apartado 3: Identificación, análisis y priorización de riesgos
- Apartado 4: Procedimientos de respuesta y recuperación de servicios

5.1. ORGANIZACIÓN

De acuerdo al ROF (Reglamento de Organización y Funciones) del MTC, la Oficina General de Tecnología de la Información – OGTI está compuesta por dos oficinas o unidades orgánicas: Oficina de Desarrollo Tecnológico y Digital – ODTD y la Oficina de Infraestructura Tecnológica y Seguridad Informática - OITSI:

Organigrama OGTI



Fuente: Resolución Ministerial No 658-2021-MTC/01

Las funciones de cada oficina son:

Imagen No 01

Artículo 80.- Oficina de Desarrollo Tecnológico y Digital

La Oficina de Desarrollo Tecnológico y Digital es la unidad orgánica dependiente de la Oficina General de Tecnología de la Información encargada del diseño, implementación y control de proyectos de tecnologías digitales.

Fuente: Resolución Ministerial No 658-2021-MTC/01

Imagen No 02

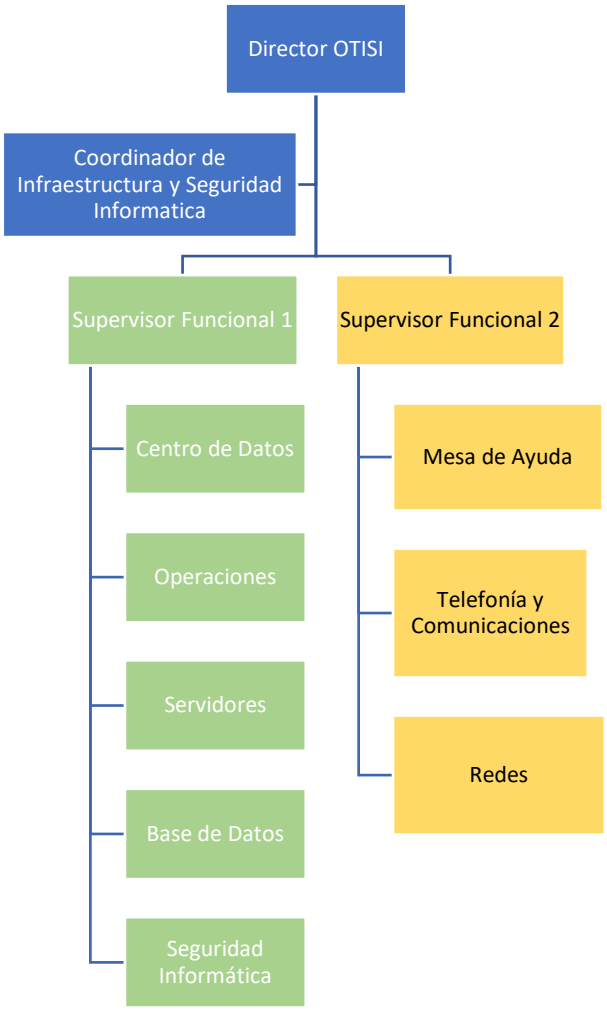
Artículo 82.- Oficina de Infraestructura Tecnológica y Seguridad Informática

La Oficina de Infraestructura Tecnológica y Seguridad Informática es la unidad orgánica dependiente de la Oficina General de Tecnología de la Información encargada del soporte técnico y la seguridad informática del ministerio.

Fuente: Resolución Ministerial No 658-2021-MTC/01

Asimismo, cada oficina está compuesta por las siguientes áreas:

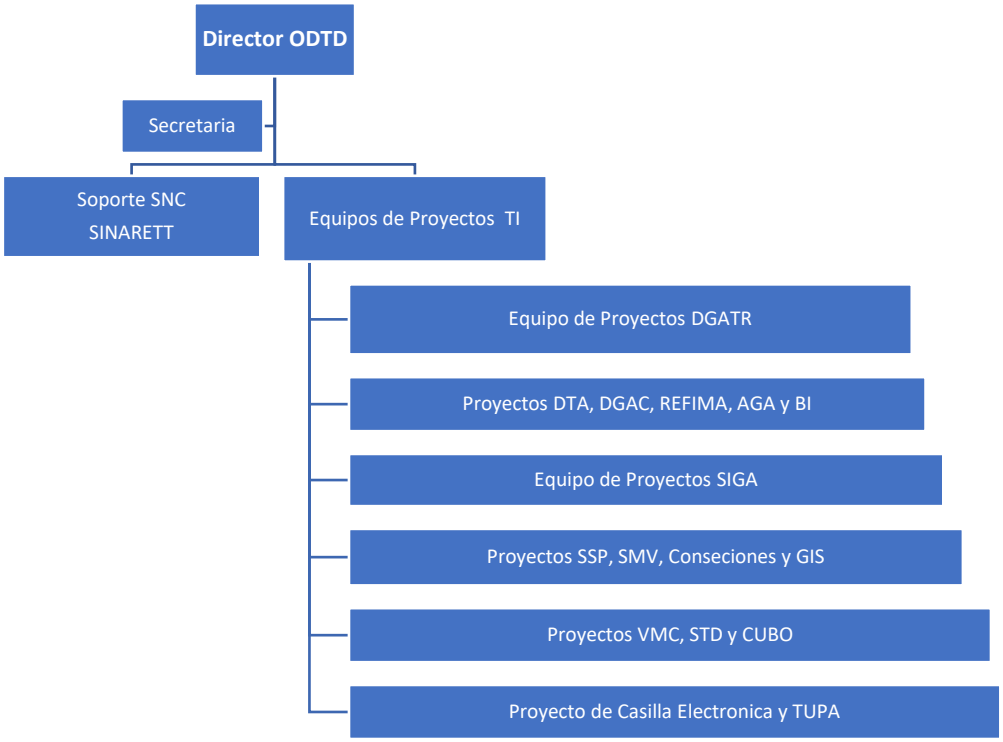
Organigrama Oficina de Infraestructura y Seguridad Informática - OITSI



Firmado digitalmente por: REQUENA CASTRO Jesus Nicanor FAU 20131379944 soft
Motivo: Doy V° B°
Fecha: 29/09/2022 11:17:15-0500

Jirón Zorritos 1203 – Lima - Perú
Central telefónica. (511) 615-7800
www.gob.pe/mtc

Organigrama Oficina de Desarrollo Tecnológico Digital - ODTD



Firmado digitalmente por: REQUENA CASTRO Jesus Nicanor FAU 20131379944 soft
Motivo: Doy V° B°
Fecha: 29/09/2022 11:17:07-0500

Para el "Plan de Recuperación de Servicios de Tecnología de la Información" las funciones son:

Director de la Oficina General de Tecnología de la Información

- ✓ Responsable de dar conformidad al Plan de Recuperación de Servicios de Tecnología de la Información y elevarlo para su aprobación.
- ✓ Gestionar los recursos necesarios para su elaboración y aplicación mediante un presupuesto ante la Entidad.
- ✓ Velar que el personal se encuentre debidamente capacitado y preparado para ejecutar el plan.

Director de la Oficina de Infraestructura Tecnológica y Seguridad Informática

- ✓ Responsable de la elaboración del Plan de Recuperación de Servicios de Tecnología de la Información y de la coordinación para su ejecución, cuando se presenten los eventos que lo activan.
- ✓ Coordinar la ejecución de las actividades del plan de pruebas.
- ✓ Coordinar con los recursos y/o proveedores externos necesarios para soportar y restaurar los servicios afectados por la contingencia.
- ✓ Evaluar el impacto de las contingencias que se presenten.
- ✓ Elaborar informes necesarios después de ocurrida la contingencia.

Director de la Oficina de Desarrollo Tecnológico y Digital

- ✓ Determinar las prioridades y plazos de recuperación de los diferentes servicios que pudieran verse afectados por incidentes que se presenten en la infraestructura tecnológica de la Entidad, en coordinación con los usuarios principales.

Oficial de Seguridad de la información

- ✓ Coordinar con el Director de la OITSI la elaboración de los informes después de ocurrida la contingencia
- ✓ Generar y proponer las políticas de seguridad de la información.

- ✓ Implantar políticas de seguridad de la información aprobadas.
- ✓ Supervisar la permanentemente actualización del plan.
- ✓ Supervisar la seguridad y privacidad de los datos.
- ✓ Supervisar el cumplimiento normativo de la seguridad de la información.
- ✓ Supervisar el cumplimiento de lo establecido en el plan.
- ✓ Supervisar la arquitectura de seguridad de la información de la organización.
- ✓ Responsable del equipo de respuesta ante incidentes de seguridad de la información de la organización.

Responsables técnicos por activo crítico

- ✓ Mantener actualizada la documentación de la configuración del activo,
- ✓ Mantener actualizados los procedimientos de operación normal del activo
- ✓ Dirigir las operaciones de respuesta ante contingencias, que involucren al activo
- ✓ Colaborar con la evaluación de daños después de la contingencia
- ✓ Mantener actualizados los procedimientos de respuesta ante las contingencias: después de ocurridas con base en los resultados; cuando haya habido cambios en el activo.

El Plan de Continuidad Operativa del MTC aprobado con Resolución Ministerial No 025-2020-MTC/01 establece en su numeral 7.2.2 la "Organización del grupo de comando, subcomando y personal técnico para la continuidad operativa" que consta de 3 niveles denominados: **Grupo de comando, Subcomando de conducción técnica y Subcomando operativo.**

En el" Grupo de comando", la OGTI es el 9no miembro de Tecnologías de la Información tal como se detalla a continuación:

Firmado digitalmente por:
REQUENA CASTRO Jesus
Nicanor FAU 20131379944 soft
Motivo: Doy V° B°
Fecha: 29/09/2022 11:16:59-0500

Imagen No 03

Tabla N° 04: Constitución del Grupo de Comando de la Continuidad Operativa del MTC

CARGO	TITULAR	1° ALTERNO	2° ALTERNO
Presidente del GCCO del MTC	Ministro de Transportes y Comunicaciones	Viceministro de Transportes	Viceministro de Comunicaciones
1er Miembro – Órgano crítico: Aeronáutica Civil	Director General de Aeronáutica Civil	Director de Seguridad Aeronáutica	Director de Certificaciones y Autorizaciones
2do Miembro – Órgano Crítico: Autorizaciones en Transportes	Director General de Autorizaciones en Transportes	Director de Servicios de Transporte Terrestre	Director de Autorizaciones de Transporte Acuático
3er Miembro – Órgano Crítico: Programas y Proyectos en Comunicaciones	Director General de Programas y Proyectos en Comunicaciones	Director de Gestión Contractual	Director de Gestión de Inversiones en Comunicaciones
4to Miembro – Órgano Crítico: Autorizaciones en Telecomunicaciones	Director General de Autorizaciones en Telecomunicaciones	Director de Servicios de Telecomunicaciones	Director de Servicios de Radiodifusión
5to Miembro – Órgano Crítico: Fiscalizaciones y Sanciones en comunicaciones	Director General de Fiscalizaciones y sanciones en Comunicaciones	Director de Fiscalizaciones de cumplimiento normativa en comunicaciones	Director de Fiscalizaciones de Cumplimiento de Títulos Habilitantes en Comunicaciones
6to Miembro –Planeamiento y Presupuesto	Director General de la Oficina de Planeamiento y Presupuesto	Director de la Oficina de Presupuesto	Director de la Oficina de Planeamiento y Cooperación Técnica
7mo Miembro – Órgano Crítico: Administración	Director General de Administración	Director de la Oficina de Finanzas	Director de la Oficina de Abastecimiento
8vo Miembro – Gestión de Recursos Humanos	Director General de la Oficina de Gestión de Recursos Humanos.	Director de la Oficina de Administración de Recursos Humanos	Director de la Oficina de Gestión del Talento Humano
9no Miembro – Tecnologías de la Información	Director de la Oficina General de Tecnología de la Información	Director de la Oficina de Desarrollo Tecnológico y Digital	Director de la Oficina de Infraestructura Tecnológica y Seguridad Informática

Fuente: R.M. N 025-2020-MTC/01 - Plan de Continuidad Operativa del MTC

Las funciones generales de este "Grupo de comando" según el Plan de Continuidad Operativa del MTC son:

Imagen No 04

Funciones generales:

1) Responsables de la implementación de las decisiones tomadas por el Grupo de Comando para la Continuidad Operativa del MTC (GCCO-MTC)
2) Implementar las actividades críticas determinadas en cada Órgano y Unidades Orgánicas (OO y UUOO) para la continuidad de las Operaciones.
3) Verificar la adecuada implementación de la sede Alterna.
4) Actuar según lo dispuesto en el Plan de Continuidad Operativa, bajo responsabilidad.

Fuente: R.M. N 025-2020-MTC/01 - Plan de Continuidad Operativa del MTC

En el "Subcomando de conducción técnica" la OGTI es el noveno 9no miembro de Tecnologías de la Información:

Imagen No 05

Tabla N° 05: Constitución del Subcomando de Conducción Técnica del MTC:

CARGO	TITULAR	1° ALTERNO	2° ALTERNO
Presidente del SCT del MTC	Secretario General	Director General de Planificación y Presupuesto	Director General de Administración
9no Miembro- Tecnologías de la Información	Director de la Oficina de Infraestructura Tecnológica y Seguridad informática	Director de la Oficina de Desarrollo Tecnológico y Digital	Responsable de Administración de Servidores

Fuente: R.M. N 025-2020-MTC/01 - Plan de Continuidad Operativa del MTC

Las funciones generales de este ""Subcomando de conducción técnica" son:

Imagen No 06

Funciones generales:

1) Responsables de la implementación de las decisiones tomadas por el Grupo de Comando para la Continuidad Operativa del MTC (GCCO-MTC)
2) Implementar las actividades críticas determinadas en cada Órgano y Unidades Orgánicas (OO y UUOO) para la continuidad de las Operaciones.
3) Verificar la adecuada implementación de la sede Alterna.
4) Actuar según lo dispuesto en el Plan de Continuidad Operativa, bajo responsabilidad.

Fuente: R.M. N 025-2020-MTC/01 - Plan de Continuidad Operativa del MTC

Finalmente, en el "Sub Comando Operativo" la OGTI es también el noveno 9no miembro:

Imagen No 07

Tabla N° 06: Constitución del Subcomando Operativo del MTC:

CARGO	TITULAR	1° ALTERNO	2° ALTERNO
Presidente del SCO del MTC	Jefe de la Oficina de Patrimonio	Jefe de Mantenimiento	Jefe de Seguridad
9no Miembro-Tecnologías de la Información	Personal designado por la Oficina General de Tecnología de la Información 1	Personal designado por la Oficina General de Tecnología de la Información 2	Personal designado por la Oficina General de Tecnología de la Información 3

Fuente: R.M. N 025-2020-MTC/01 - Plan de Continuidad Operativa del MTC

En este caso el Titular sería: el Coordinador de Infraestructura y Seguridad Informática
El 1er alterno: el Supervisor Funcional 1 de la OITSI
El 2do alterno: el Supervisor Funcional 2 de la OITSI

Las funciones generales del "Sub comando Operativo" son:

Imagen No 08

Funciones generales:

1) Implementar las decisiones del GCCO-MTC y dar continuidad a las operaciones de cada actividad critica determinada para cada OO y UUOO competente.
2) Apoyar el desarrollo de cada una de las actividades críticas determinadas para asegurar la Continuidad de Operaciones del MTC, incluyendo el traslado a la sede alterna.
3) Actúan según lo dispuesto en el Plan de Continuidad de Operaciones del MTC, bajo responsabilidad.

Fuente: R.M. N 025-2020-MTC/01 - Plan de Continuidad Operativa del MTC

5.2. SOBRE LA IMPLEMENTACIÓN DE LA SEDE ALTERNA DEL MTC

Como se observa las funciones del "Subcomando de conducción técnica" y ""Sub Comando Operativo" están relacionadas a la verificación de la adecuada implementación y traslado a una sede alterna.

Sobre el particular, el Plan de Gobierno Digital 2020 – 2022 del MTC aprobado con Resolución Ministerial N °1298-2019-MTC/01 de fecha 30 de diciembre 2019, incluye en su título V "Portafolio de proyectos de Gobierno Digital" la "Implementación de un centro de datos alterno":

Imagen No 09

N°	Proyecto	Descripción	Tipo de Proyecto	Prioridad
12	IMPLEMENTACIÓN DE UN CENTRO DE DATOS ALTERNO	Permitirá replicar toda la data del centro de datos principal a esta alterna, asegurando la disponibilidad e integridad de la información. Este centro de datos alterno se encontrará ubicado a más de 500 km de la ubicación del centro de datos principal, cumpliendo con los estándares internacionales.	Mejora de las Plataformas TIC	Media - Alta

Fuente: Plan de Gobierno Digital 2020 – 2022 del MTC

La implementación del Centro de Datos Alterno del MTC, considera la empleabilidad de un ambiente, el cual asegure la operación del equipamiento que permita brindar y asegurar la disponibilidad de los servicios y aplicaciones brindados por la entidad a los usuarios de las unidades orgánicas del MTC y a los ciudadanos a nivel nacional.

Al respecto, la Oficina de Infraestructura Tecnológica y Seguridad Informática – OITSI de la OGTI ha venido trabajando en dicho proyecto, estableciendo cuales son los requisitos mínimos que debe cumplir la implementación de un centro de datos alterno para el MTC.

Infraestructura física del Centro de Datos Alterno – MTC

El centro de datos alterno – MTC, debe cumplir con lo estipulado en la norma TIA-942, norma para el diseño de Centros de Datos y contar con certificación vigente en diseño, construcción y operación según el siguiente detalle:

Tabla No 05 -Nivel de certificación de centro de datos

Entidad Certificadora	TIA -942	Uptime Institute	ICREA
Nivel	Rated - 2	Tier II	Nivel 2

Fuente: Elaboración propia

El centro de datos alterno debe cumplir y considerar como mínimo, los siguientes aspectos:

Arquitectura - Ambientes físico

- Sala de Alta Seguridad
- Gabinetes de equipos
- Sistema de Aislamiento Sísmico

Sistema eléctrico - Sistemas de Energía Ininterrumpida

- Equipos UPS
- Transformador de aislamiento
- Dispositivo protector de sobretensiones
- Grupo electrógeno
- Tablero de Transferencia Automática
- Tableros de distribución
- Circuitos y distribución eléctrica

Refrigeración - Sistema de Climatización

- Aire acondicionado de precisión

Seguridad - Sistema de Seguridad

- Sistema de control de acceso
- Sistema de monitoreo con Cámara IP
- Sistema de detección y extinción de incendios

De la modalidad para la implementación del Centro de Datos Alterno - MTC

La implementación del Centro de Datos Alterno - MTC, considera las opciones del mercado local, así como la oportunidad de desarrollo del proyecto a cargo de los profesionales y especialistas de la institución, lo cual nos remite a los siguientes escenarios:

- **Modalidad de servicio Housing:**
  Esta solución y/o alternativa considera alquilar espacio en el site de un proveedor de servicio lo cual considera que el Ministerio de Transportes y Comunicaciones, provea el equipamiento requerido. Implica una alta inversión de compra de equipamiento.

- **Modalidad de servicio Hosting:**
  Esta solución y/o alternativa considera alquilar espacio lógico en el site de un proveedor de servicio lo cual considera que el MTC, provea las fuentes y/o códigos de los sistemas, servicios y/o aplicaciones a replicar.

- **Modalidad de construcción propia:**
  Esta solución considera el estudio técnico del cumplimiento de las consideraciones de diseño e implementación de la infraestructura física y adquisición del equipamiento necesario. Esta opción sería con los recursos y bajo la supervisión directa de la entidad.

Equipamiento mínimo del del Centro de Datos Alterno

A continuación, independiente de la modalidad escogida, se detalla las características y equipamiento minino que se debe tener en cuenta para la implementación del centro de datos alterno:

Tabla No 06
"Equipamiento de red para implementación de Centro de Datos Alterno"

Equipamiento	Cantidad
Switch de red principal, 32 puertos 40/100G	02
Switch de red de acceso, 48 Puertos 1/10/25Gbps y 8puertos 40/100Gbps	02
Transceptores Ópticos	26

Fuente: Proyecto Implementación de centro de datos alterno MTC

Los enlaces de datos requeridos son los siguientes:

Jirón Zorritos 1203 – Lima - Perú
Central telefónica. (511) 615-7800
www.gob.pe/mtc

Tabla No 07
"Enlaces de datos para implementación de Centro de Datos Alterno"

Equipamiento	Cantidad	Capacidad
Enlace para acceso a internet	01	200 Mbps
Enlace para replicación de conectividad	10	10 Gbps
Enlace para replicación de información	01	400 Mbps
Enlace para acceso a otras entidades	01	10 Mbps

Fuente: Proyecto Implementación de centro de datos alterno MTC

Tabla No 08
"Equipamiento de telefonía implementación de Centro de Datos Alterno"

Equipamiento	Cantidad
Servidores fisicos: 1TB de almacenamiento32 GB de RAM 16 vCPU	02
Cajas Thales de encriptacion SSM	02
IP Media Gateway con Thales MSM embedido	01
Tarjetas Primarias PRA-T2	03
Tarjeta GD3	01

Fuente: Proyecto Implementación de centro de datos alterno MTC

Firmado digitalmente por: REQUENA CASTRO Jesus Nicanor FAU 20131379944 soft
Motivo: Doy V° B°
Fecha: 29/09/2022 11:16:07-0500

Equipamiento para seguridad Informática

La Seguridad informática de la información que maneja el centro de Datos alterno se contempla en alta redundancia por lo cual el equipamiento a considerar es el siguiente:

- 01 Solución DDoS cloud
- 02 Firewall perimetral (HA)
- 02 Firewall WAN (HA)
- 01 Firewall de aplicaciones web
- 01 solución de E-mail Security Gateway

El servicio o solución DDS puede ser contratado con el proveedor de internet.
La protección de correo electrónico frente a spam, virus y malware avanzado, puede ser físico (01 appliance) o virtual.

Equipamiento para servidores

La disponibilidad de los recursos y el dimensionamiento necesario para los ambientes de desarrollo y producción requiere considerar el siguiente equipamiento:

- 06 Switch 10 MXL 10/40Gb – Force (Red SAN)
- 02 Switch Power Connect (Red SAN)
- 02 Switch Force S4810 (Red SAN)
- 02 Switch S4048 (Red SAN)
- 06 servidores Blade M630
- 06 servidores Blade M640
- 08 servidores Blade M830
- 02 chasis Blade M1000
- 03 servidores rackeable M730
- 01 unidad de almacenamiento 100 TB.

Equipamiento para Base de Datos

- 02 servidores rackeable Oracle X7-2
- 04 servidores rackeable Oracle S7-2
- 02 unidad de almacenamiento Oracle DE3-24C

5.3. IDENTIFICACIÓN DE LOS ACTIVOS CRITICOS DE LA OGTI

La misión de la OGTI es brindar al MTC los servicios informáticos y tecnológicos necesarios para el desarrollo de los servicios funcionales u operativos de éste; en tal sentido, resulta de vital importancia considerar los activos de la información susceptibles de sufrir eventos que provoquen un incidente que afecte la normal operación del MTC (contingencia), para ello identificamos los servicios funcionales críticos del MTC.

Se han identificado los activos críticos informáticos, que se han clasificado en dos (02) tipos:

a) **Servicios o aplicaciones críticas del MTC**:
Son los servicios web o aplicaciones considerados críticos que son usados por los ciudadanos a nivel nacional y/o por los usuarios del MTC.

b) **Activos de hardware y software críticos del MTC**:
Son los equipos de infraestructura o software que son considerados críticos y que sirven de soporte físico o lógico a los servicios o aplicaciones que brinda el MTC a nivel nacional.

Firmado digitalmente por:
REQUENA CASTRO Jesus
Nicanor FAU 20131379944 soft
Motivo: Doy V° B°
Fecha: 29/09/2022 11:16:00-0500

Jirón Zorritos 1203 – Lima - Perú
Central telefónica. (511) 615-7800
www.gob.pe/mtc

Tabla No 09

Servicios o aplicaciones críticas del MTC				
Ítem	**Descripción**	**Oficina o Dirección Usuaria**	**Responsable del activo critico**	**Usuario final**
1	Sistema Nacional de Conductores - SNC	DGPPT	Director ODTD / Jefe Proyectos OGTI	Ciudadanos a nivel nacional
2	Sistema Nacional de Sanciones - SNS	DGATR	Director ODTD / Jefe Proyectos OGTI	SUNAT, entre otras entidades publicas
3	Sistema de Mesa de Partes Virtual - MPV	OACGD	Director ODTD / Jefe Proyectos OGTI	Ciudadanos a nivel nacional
4	Casilla Electrónica MTC	OACGD	Director ODTD / Jefe Proyectos OGTI	Ciudadanos a nivel nacional
5	TUPA Digital	OACGD /OGPP-ODM	Director ODTD / Jefe Proyectos OGTI	Ciudadanos a nivel nacional
6	Sistema de Trámite Documentario - STD	OACGD	Director ODTD / Jefe Proyectos OGTI	Personal del MTC
7	Registro Nacional de Transporte Terrestre – RENAT	DGATR	Director ODTD / Jefe Proyectos OGTI	Ciudadanos a nivel nacional
8	Correo Electrónico	OGTI	Director OITSI	Personal del MTC
9	SIGA WEB	OGA	Director ODTD / Jefe Proyectos OGTI	Personal del MTC
10	SIGA- Personal	OGA	Director ODTD / Jefe Proyectos OGTI	Personal del MTC
11	SIGA- Finanzas	OGA	Director ODTD / Jefe Proyectos OGTI	Personal del MTC
12	Ellipse	DGAT	Director ODTD / Jefe Proyectos OGTI	Viceministerio de Comunicaciones - VMC
13	Sistema Integrado de Información DTA	DTA	Director ODTD / Jefe Proyectos OGTI	VMT
14	Sistema Integrado de la Dirección General de Aeronáutica Civil	DGAT	Director ODTD / Jefe Proyectos OGTI	VMT

Fuente: Elaboración propia.

Tabla No 10

Activos de hardware y software críticos del MTC					
Ítem	**Descripción**	**Cantidad**	**Función**	**Oficina o Dirección**	**Responsable del activo**
1	Equipo Firewall WAN	1	Control de tráfico a nivel LAN/WAN	OITSI	Especialista en Seguridad Informática
2	Equipo Firewall Internet	2	Seguridad perimetral	OITSI	Especialista en Seguridad Informática

Activos de hardware y software críticos del MTC					
Ítem	**Descripción**	**Cantidad**	**Función**	**Oficina o Dirección**	**Responsable del activo**
3	Software Antivirus	4000 licencias	Protección a los endpoint (PCs) contra código malicioso.	OITSI	Especialista en Seguridad Informática
4	Equipo Antispam	2	Protección frente a correo malicioso.	OITSI	Especialista en Seguridad Informática
5	Equipo Filtro de Contenido Web	1	Navegación segura a Internet.	OITSI	Especialista en Seguridad Informática
6	Switch Core	2	Administración de red en el Centro de Datos	OITSI	Administrador de Red
7	Switch de Distribución	2	Administración de red en el Centro de Datos	OITSI	Administrador de Red
8	Routers	2	Interconexión a Internet del Operador	Proveedor del Servicio de Internet / OITSI	Administrador de Red
9	Balanceador de Enlaces Internet	2	Balacear o distribuir el tráfico de red entrante de Internet en el MTC	Proveedor del Servicio de Internet / OITSI	Administrador de Red
10	Balanceador de Aplicaciones	2	Balancear o distribuir el tráfico de red entrante a servidores de aplicaciones del MTC	Proveedor del Servicio de Internet / OITSI	Administrador de Red
11	Servidores Blade	34	Procesamiento de datos de aplicaciones y servicios.	OITSI	Administración de Servidores
12	Servidores Rack	15	Procesamiento de datos de aplicaciones y servicios.	OITSI	Administración de Servidores
13	Chassis de Servidores	4	Soporte y conectividad de los servidores Blade.	OITSI	Administración de Servidores
14	Solución de Almacenamiento	3	Sistemas de almacenamiento de información.	OITSI	Administración de Servidores
15	Software de Base de Datos POSTGRESQL	1	Servicios de Base de Datos	OITSI	Asistente técnico en Base de Datos
16	Software de Base de Datos MYSQL	1	Servicios de Base de Datos	OITSI	Asistente técnico en Base de Datos
17	Software de Base de Datos MS SQL	1	Servicios de Base de Datos	OITSI	Asistente técnico en Base de Datos
18	Software de Base de Datos Oracle	2	Servicios de Base de Datos	OITSI	Asistente técnico en Base de Datos
19	Software de Virtualización	1	Herramienta de administración de la infraestructura virtual de servidores que soporta los servicios y sistemas del MTC.	OITSI	Administración de Servidores
20	Central Telefónica	1	Telefonía y comunicaciones	OITSI	Especialista en Telefonía y comunicaciones
21	Equipos UPS	2	Provisión de energía eléctrica temporal y de contingencia eléctrica al Centro de Datos - MTC	OITSI	Técnico de Centro de Datos

Activos de hardware y software críticos del MTC					
Ítem	**Descripción**	**Cantidad**	**Función**	**Oficina o Dirección**	**Responsable del activo**
22	Sistema de Extinción de Incendios	1	Mitigar eventos relacionados con el fuego al interior del Centro de Datos - MTC	OITSI	Técnico de Centro de Datos
23	Generador Eléctrico	1	Provisión de energía eléctrica de sustento ante ausencia de fluido eléctrico del proveedor - ENEL	Oficina de Abastecimiento - OGA	Sub Oficina de Servicios Generales - OABAST
24	Sistema de Aire Acondicionado	1	Control de temperatura y humedad al interior del Centro de Datos	OITSI	Técnico de Centro de Datos

Fuente: Elaboración propia.

En el Anexo No 01 del presente documento se encuentra el detalle las Tablas No 05 y 06 de los activos críticos del MTC.

5.4. IDENTIFICACIÓN, ANÁLISIS Y PRIORIZACIÓN DE RIESGOS

La identificación, análisis y priorización de riesgos se ha realizado en base al numeral 4 "Marco teórico" del presente plan. Bajo las siguientes premisas o condiciones:

- ✓ Todo servicio o activo crítico debe ser evaluado o considerado en el presente plan.
- ✓ Para todo activo critico existe uno o más riesgos identificados que debe ser evaluados, cuyo de riesgo sea medio o alto deberá generar una acción de respuesta ya sea para mitigar, evitar, transferir o aceptar el riesgo. En este último caso, en función al impacto del riesgo es recomendable prever una reserva de contingencia, a utilizar en caso se presente dicho riesgo.

En base a ello se realizó una evaluación de riesgos de cada activo crítico identificado en el numeral 5.2

A continuación, se muestra un resumen del resultado de la evaluación de riesgos calificados como "Extremo" o "Alto" por cada activo crítico identificado:

Tabla No 11 – Centro de Datos

ACTIVO	CODIGO RIESGO	NOMBRE_RIESGO	IMPACTO	PROBABILIDAD	NIVEL DEL RIESGO
Data Center	RSG-SGSI-001	Incendio en el Data Center por mantenimiento insuficiente	5	3	**Extremo**
	RSG-SGSI-004	Incendio en el Data Center por falla de funcionamiento del sistema contra incendios	5	3	**Extremo**
	RSG-SGSI-005	Incendio en el Data Center por falta de técnicas apropiadas para controlar algún evento catastrófico	5	5	**Extremo**
	RSG-SGSI-015	Fallas en el control de temperatura y humedad del Data Center por mantenimiento insuficiente	4	3	**Alto**

ACTIVO	CODIGO RIESGO	NOMBRE_RIESGO	IMPACTO	PROBABILIDAD	NIVEL DEL RIESGO
	RSG-SGSI-017	Fallas del sistema de aire acondicionado del Data Center por mantenimiento insuficiente	4	3	**Alto**
	RSG-SGSI-019	Pérdida del suministro de electricidad en el Data Center por red inestable de energía eléctrica	5	3	**Extremo**
	RSG-SGSI-020	Pérdida del suministro de electricidad en el Data Center por dependencia de proveedor de servicio público	5	3	**Extremo**
	RSG-SGSI-021	Pérdida del suministro de electricidad en el Data Center por falta de redundancia de fuentes de energía	5	3	**Extremo**
Sistema de Aire Acondicionado	RSG-SGSI-022	Fallas del sistema de aire acondicionado por mantenimiento insuficiente	4	3	**Alto**
	RSG-SGSI-027	Mal funcionamiento del equipo del sistema de aire acondicionado por mantenimiento insuficiente	4	3	**Alto**
	RSG-SGSI-028	Mal funcionamiento del equipo del sistema de aire acondicionado por uso incorrecto del software y hardware	4	3	**Alto**
	RSG-SGSI-029	Mal funcionamiento del equipo del sistema de aire acondicionado por incorrecta configuración	4	3	**Alto**
	RSG-SGSI-030	Mal funcionamiento del equipo del sistema de aire acondicionado por error humano	4	3	**Alto**
Sistema Contra Incendios	RSG-SGSI-031	Polvo, corrosión, congelación, sobrecalentamiento en el sistema contra incendios por mantenimiento insuficiente	4	3	**Alto**
Cuarto de UPS	RSG-SGSI-047	Incendio del Cuarto de UPS por	4	4	**Extremo**

Firmado digitalmente por: REQUENA CASTRO Jesus Nicanor FAU 20131379944 soft
Motivo: Doy V° B°
Fecha: 29/09/2022 11:15:23-0500

ACTIVO	CODIGO RIESGO	NOMBRE_RIESGO	IMPACTO	PROBABILIDAD	NIVEL DEL RIESGO
		Mantenimiento insuficiente			
	RSG-SGSI-048	Incendio del Cuarto de UPS por Capacitación de seguridad insuficiente	4	4	**Extremo**
	RSG-SGSI-049	Incendio del Cuarto de UPS por Error humano	4	3	**Alto**
	RSG-SGSI-050	Incendio del Cuarto de UPS por Inadecuado ambiente físico	4	4	**Extremo**
	RSG-SGSI-051	Incendio del Cuarto de UPS por Falta de técnicas apropiadas para controlar algún evento catastrófico	4	4	**Extremo**
	RSG-SGSI-052	Inundación del Cuarto de UPS por Ubicaciones en un área susceptible a las inundaciones	4	4	**Extremo**
	RSG-SGSI-053	Inundación del Cuarto de UPS por Falta de técnicas apropiadas para controlar algún evento catastrófico	4	4	**Extremo**
	RSG-SGSI-054	Daño por fenómeno sísmico en el Cuarto de UPS debido a la falta de técnicas apropiadas para controlar algún evento catastrófico	4	4	**Extremo**
Acumuladores de Energía (UPS)	RSG-SGSI-055	Polvo, corrosión, congelación, sobrecalentamiento del Acumuladores de Energía (UPS) por Mantenimiento insuficiente	4	4	**Extremo**
	RSG-SGSI-056	Polvo, corrosión, congelación, sobrecalentamiento del Acumuladores de Energía (UPS) por Susceptibilidad a la humedad, al polvo y a la suciedad	4	4	**Extremo**
	RSG-SGSI-057	Mal funcionamiento del equipo del Acumuladores de Energía (UPS) por Mantenimiento insuficiente	4	4	**Extremo**
	RSG-SGSI-058	Mal funcionamiento del equipo del Acumuladores de	4	4	**Extremo**

Firmado digitalmente por: REQUENA CASTRO Jesus Nicanor FAU 20131379944 soft
Motivo: Doy V° B°
Fecha: 29/09/2022 11:15:15-0500

ACTIVO	CODIGO RIESGO	NOMBRE_RIESGO	IMPACTO	PROBABILIDAD	NIVEL DEL RIESGO
		Energía (UPS) por Susceptibilidad a la humedad, al polvo y a la suciedad			
	RSG-SGSI-059	Mal funcionamiento del equipo Acumulador de Energía (UPS) por Falta de mecanismos de monitoreo	4	3	**Alto**
	RSG-SGSI-063	Indisponibilidad del equipo Acumulador de Energía (UPS) por Mantenimiento insuficiente	4	4	**Extremo**
	RSG-SGSI-064	Indisponibilidad del equipo Acumulador de Energía (UPS) por Error humano	4	3	**Alto**

Tabla No 12 – Área de Redes

ACTIVO	CODIGO RIESGO	NOMBRE_RIESGO	IMPACTO	PROBABILIDAD	NIVEL DEL RIESGO
Switch Core	RSG-SGSI-126	Polvo, corrosión, congelación, sobrecalentamiento del Switch Core por Mantenimiento insuficiente	5	4	**Extremo**
	RSG-SGSI-127	Polvo, corrosión, congelación, sobrecalentamiento del Switch Core por Inadecuada limpieza del ambiente físico	5	3	**Extremo**
	RSG-SGSI-128	Polvo, corrosión, congelación, sobrecalentamiento del Switch Core por Susceptibilidad a la humedad, al polvo y a la suciedad	5	3	**Extremo**
	RSG-SGSI-129	Mal funcionamiento del Switch Core por mantenimiento insuficiente	5	4	**Extremo**
	RSG-SGSI-130	Mal funcionamiento del Switch Core por Susceptibilidad a la humedad, al polvo y a la suciedad	5	2	**Alto**
	RSG-SGSI-131	Mal funcionamiento del Switch Core por Falta de mecanismos de monitoreo	5	2	**Alto**
	RSG-SGSI-134	Mal funcionamiento del Switch Core por Obsolescencia Tecnológica	5	4	**Extremo**
	RSG-SGSI-137	Uso no autorizado del Switch Core porque el	4	3	**Alto**

ACTIVO	CODIGO RIESGO	NOMBRE_RIESGO	IMPACTO	PROBABILIDAD	NIVEL DEL RIESGO
		equipo no exige el cambio periódico de contraseña			
Switch de Distribución	RSG-SGSI-148	Polvo, corrosión, congelación, sobrecalentamiento del Switch de Distribución por Mantenimiento insuficiente	4	4	**Extremo**
	RSG-SGSI-149	Polvo, corrosión, congelación, sobrecalentamiento del Switch de Distribución por Inadecuada limpieza del ambiente físico	3	4	**Alto**
	RSG-SGSI-150	Polvo, corrosión, congelación, sobrecalentamiento del Switch de Distribución por Susceptibilidad a la humedad, al polvo y a la suciedad	4	4	**Extremo**
	RSG-SGSI-151	Mal funcionamiento del Switch de Distribución por mantenimiento insuficiente	3	4	**Alto**
	RSG-SGSI-152	Mal funcionamiento del Switch de Distribución por Susceptibilidad a la humedad, al polvo y a la suciedad	4	4	**Extremo**
	RSG-SGSI-156	Mal funcionamiento del Switch de Distribución por Obsolescencia Tecnológica	4	4	**Extremo**
	RSG-SGSI-159	Uso no autorizado del Switch de Distribución porque el equipo no exige el cambio periódico de contraseña	4	3	**Alto**
	RSG-SGSI-169	Hacking del Switch de Distribución por Falta actualización del Sistema	4	3	**Alto**
Switch de Borde	RSG-SGSI-170	Polvo, corrosión, congelación, sobrecalentamiento del Switch de Borde por Mantenimiento insuficiente	3	3	**Alto**
	RSG-SGSI-172	Polvo, corrosión, congelación, sobrecalentamiento del Switch de Borde por Susceptibilidad a la humedad, al polvo y a la suciedad	3	3	**Alto**
	RSG-SGSI-173	Mal funcionamiento del Switch de Borde por mantenimiento insuficiente	3	3	**Alto**
	RSG-SGSI-174	Mal funcionamiento del Switch de Borde por Susceptibilidad a la humedad, al polvo y a la suciedad	3	3	**Alto**

Firmado digitalmente por: REQUENA CASTRO Jesus Nicanor FAU 20131379944 soft
Motivo: Doy V° B°
Fecha: 29/09/2022 11:15:00-0500

Jirón Zorritos 1203 – Lima - Perú
Central telefónica. (511) 615-7800
www.gob.pe/mtc

ACTIVO	CODIGO RIESGO	NOMBRE_RIESGO	IMPACTO	PROBABILIDAD	NIVEL DEL RIESGO
	RSG-SGSI-178	Mal funcionamiento del Switch de Borde por Obsolescencia Tecnológica	3	4	**Alto**
Internet	RSG-SGSI-560	Interrupción del servicio del Internet por Inexistencia o insuficiencia de acuerdo sobre el nivel de servicio	5	2	**Alto**
	RSG-SGSI-561	Interrupción del servicio del Internet por Problemas del proveedor respecto a los componentes del servicio	5	2	**Alto**
	RSG-SGSI-562	Interrupción del servicio del Internet por no contar con otro enlace con proveedor diferente para la navegación en internet	5	2	**Alto**
	RSG-SGSI-563	Interrupción del servicio del Internet por Tiempos de respuesta lentos en la atención del proveedor	5	2	**Alto**
Balanceador de Internet	RSG-SGSI-192	Polvo, corrosión, congelación, sobrecalentamiento por Mantenimiento insuficiente	4	4	**Extremo**
	RSG-SGSI-193	Polvo, corrosión, congelación, sobrecalentamiento por Inadecuada limpieza del ambiente físico	4	3	**Alto**
	RSG-SGSI-194	Polvo, corrosión, congelación, sobrecalentamiento del Controlador de WIFI por Susceptibilidad a la humedad, al polvo y a la suciedad	4	3	**Alto**
	RSG-SGSI-195	Mal funcionamiento por mantenimiento insuficiente	4	4	**Extremo**
	RSG-SGSI-196	Mal funcionamiento por Susceptibilidad a la humedad, al polvo y a la suciedad	4	3	**Alto**
	RSG-SGSI-200	Mal funcionamiento por Obsolescencia Tecnológica	4	4	**Extremo**
	RSG-SGSI-213	Hacking por Falta actualización del Sistema	4	3	**Alto**
	RSG-SGSI-214	Indisponibilidad por inestabilidad del fluido eléctrico	4	3	**Alto**
	RSG-SGSI-216	Indispobilidad por falta de mandenimiento	4	3	**Alto**
Controlador de WIFI	RSG-SGSI-192	Polvo, corrosión, congelación, sobrecalentamiento del Controlador de WIFI por Mantenimiento insuficiente	4	4	**Extremo**

ACTIVO	CODIGO RIESGO	NOMBRE_RIESGO	IMPACTO	PROBABILIDAD	NIVEL DEL RIESGO
	RSG-SGSI-193	Polvo, corrosión, congelación, sobrecalentamiento del Controlador de WIFI por Inadecuada limpieza del ambiente físico	4	3	**Alto**
	RSG-SGSI-194	Polvo, corrosión, congelación, sobrecalentamiento del Controlador de WIFI por Susceptibilidad a la humedad, al polvo y a la suciedad	4	3	**Alto**
	RSG-SGSI-195	Mal funcionamiento del Controlador de WIFI por mantenimiento insuficiente	4	4	**Extremo**
	RSG-SGSI-196	Mal funcionamiento del Controlador de WIFI por Susceptibilidad a la humedad, al polvo y a la suciedad	4	3	**Alto**
	RSG-SGSI-200	Mal funcionamiento del Controlador de WIFI por Obsolescencia Tecnológica	4	4	**Extremo**
	RSG-SGSI-213	Hacking del Controlador de WIFI por Falta actualización del Sistema	4	3	**Alto**
Access Point	RSG-SGSI-214	Polvo, corrosión, congelación, sobrecalentamiento del Access Point por Mantenimiento insuficiente	3	4	**Alto**
	RSG-SGSI-215	Polvo, corrosión, congelación, sobrecalentamiento del Access Point por Inadecuada limpieza del ambiente físico	3	3	**Alto**
	RSG-SGSI-216	Polvo, corrosión, congelación, sobrecalentamiento del Access Point por Susceptibilidad a la humedad, al polvo y a la suciedad	3	3	**Alto**
	RSG-SGSI-217	Mal funcionamiento del Access Point por mantenimiento insuficiente	3	4	**Alto**
	RSG-SGSI-218	Mal funcionamiento del Access Point por Susceptibilidad a la humedad, al polvo y a la suciedad	3	3	**Alto**
	RSG-SGSI-222	Mal funcionamiento del Access Point por Obsolescencia Tecnológica	3	4	**Alto**
	RSG-SGSI-235	Hacking del Access Point por Falta actualización del Sistema	3	3	**Alto**

Firmado digitalmente por: REQUENA CASTRO Jesus Nicanor FAU 20131379944 soft
Motivo: Doy V° B°
Fecha: 29/09/2022 11:14:47-0500

Jirón Zorritos 1203 – Lima - Perú
Central telefónica. (511) 615-7800
www.gob.pe/mtc

ACTIVO	CODIGO RIESGO	NOMBRE_RIESGO	IMPACTO	PROBABILIDAD	NIVEL DEL RIESGO
Fibra Óptica	RSG-SGSI-481	Falla mayor de la Fibra Óptica por Mantenimiento insuficiente	5	4	**Extremo**
	RSG-SGSI-483	Falla mayor de la Fibra Óptica por Arquitectura de red insegura	5	2	**Alto**
	RSG-SGSI-484	Hacking de la Fibra Óptica por Falta de afinamiento en los mecanismos de seguridad del equipamiento	5	2	**Alto**
	RSG-SGSI-567	Interrupción del servicio de Línea Telefónica por no contar con otro enlace con proveedor diferente para la navegación telefónica	3	4	**Alto**
	RSG-SGSI-587	Mal funcionamiento del software Omnivista por Errores conocidos en el software	4	3	**Alto**
	RSG-SGSI-593	Lentitud de los procesos del Omnivista por Software desfasado por vigencia tecnológica y sin soporte por parte del fabricante	3	3	**Alto**
	RSG-SGSI-605	Mal funcionamiento del software Call center Genesys por errores conocidos en el software	4	3	**Alto**

Firmado digitalmente por: REQUENA CASTRO Jesus Nicanor FAU 20131379944 soft
Motivo: Doy V° B°
Fecha: 29/09/2022 11:14:34-0500

Tabla No 13 – Área de Seguridad Informática

ACTIVO	CODIGO RIESGO	NOMBRE_RIESGO	IMPACTO	PROBABILIDAD	NIVEL DEL RIESGO
Firewall Principal	RSG-SGSI-263	Mal funcionamiento del Firewall principal por Falta de mecanismos de monitoreo	5	2	**Alto**
	RSG-SGSI-272	Uso no autorizado del Firewall principal por incorrecta configuración	5	2	**Alto**
	RSG-SGSI-276	Hacking del Firewall principal por Falta de mecanismos de configuración de seguridad del equipo	5	2	**Alto**
	RSG-SGSI-277	Hacking del Firewall principal por Falta de afinamiento en los mecanismos de seguridad perimetral	5	2	**Alto**
	RSG-SGSI-278	Hacking del Firewall principal por Error humano	5	2	**Alto**
Firewall WAN	RSG-SGSI-263	Mal funcionamiento del Firewall principal por Falta de mecanismos de monitoreo	5	2	**Alto**
	RSG-SGSI-272	Uso no autorizado del Firewall principal por incorrecta configuración	5	2	**Alto**
	RSG-SGSI-276	Hacking del Firewall principal por Falta de mecanismos de	5	2	**Alto**

ACTIVO	CODIGO RIESGO	NOMBRE_RIESGO	IMPACTO	PROBABILIDAD	NIVEL DEL RIESGO
		configuración de seguridad del equipo			
	RSG-SGSI-277	Hacking del Firewall principal por Falta de afinamiento en los mecanismos de seguridad perimetral	5	2	**Alto**
	RSG-SGSI-278	Hacking del Firewall principal por Error humano	5	2	**Alto**

Tabla No 14 – Área de Telefonía

ACTIVO	CODIGO RIESGO	NOMBRE_RIESGO	IMPACTO	PROBABILIDAD	NIVEL DEL RIESGO
Servidor de Telefonía	RSG-SGSI-431	Uso no autorizado del Servidor de telefonía por Error humano	3	3	**Alto**
	RSG-SGSI-432	Uso no autorizado del Servidor de telefonía por que el Servidor no exige el cambio periódico de contraseña	4	3	**Alto**
	RSG-SGSI-433	Uso no autorizado del Servidor de telefonía por falta de conciencia de seguridad	3	4	**Alto**
	RSG-SGSI-436	Uso no autorizado del Servidor de telefonía por incorrecta configuración	3	3	**Alto**
	RSG-SGSI-439	Hacking del Servidor de telefonía por Incorrecta configuración	4	3	**Alto**
	RSG-SGSI-440	Hacking del Servidor de telefonía por falta de mecanismos de configuración de seguridad del equipo	3	3	**Alto**
	RSG-SGSI-441	Hacking del Servidor de telefonía por falta de afinamiento en los mecanismos de seguridad perimetral	3	3	**Alto**
	RSG-SGSI-449	Pérdida de información del Servidor de telefonía por Error humano	3	3	**Alto**
	RSG-SGSI-451	Infección de códigos maliciosos (ej. Virus, bomba lógica, troyano) en el Servidor de telefonía por falta de antivirus	3	3	**Alto**
	RSG-SGSI-454	Fuga de información del Servidor de telefonía por Error humano	3	3	**Alto**
	RSG-SGSI-455	Fuga de información del Servidor de telefonía por Falta de conciencia de seguridad	3	3	**Alto**
	RSG-SGSI-457	Fuga de información del Servidor de telefonía por Mala administración de claves	3	3	**Alto**

Firmado digitalmente por: REQUENA CASTRO Jesus Nicanor FAU 20131379944 soft
Motivo: Doy V° B°
Fecha: 29/09/2022 11:14:24-0500

Jirón Zorritos 1203 – Lima - Perú
Central telefónica. (511) 615-7800
www.gob.pe/mtc

ACTIVO	CODIGO RIESGO	NOMBRE_RIESGO	IMPACTO	PROBABILIDAD	NIVEL DEL RIESGO
	RSG-SGSI-459	Fuga de información del Servidor de telefonía por Falta de procedimiento formal de altas, bajas y modificaciones de usuario	3	3	**Alto**
Central Telefónica	RSG-SGSI-464	Indisponibilidad del equipo del Central telefónica por Error humano	3	3	**Alto**
	RSG-SGSI-465	Indisponibilidad del equipo del Central telefónica por Obsolescencia Tecnológica	3	3	**Alto**
	RSG-SGSI-467	Hacking del Central telefónica por Incorrecta configuración	4	3	**Alto**
	RSG-SGSI-468	Hacking del Central telefónica por Falta de mecanismos de configuración de seguridad del equipo	3	3	**Alto**
	RSG-SGSI-469	Hacking del Central telefónica por falta de afinamiento en los mecanismos de seguridad perimetral	3	3	**Alto**

Tabla No 15 – Área de Servidores

ACTIVO	CODIGORIESGO	NOMBRE_RIESGO	IMPACTO	PROBABILIDAD	NIVEL DEL RIESGO
Servidor controlador de dominio	RSG-SGSI-360	Mal funcionamiento del Servidor controlador de dominio por una mala configuración inicial en el despliegue del servicio	5	1	**Alto**
	RSG-SGSI-360	Mal funcionamiento del Servidor controlador de dominio por Obsolescencia Tecnológica	5	3	**Extremo**
Correo Electrónico	RSG-SGSI-648	Pérdida de información del software de Correo Electrónico por error humano	5	2	**Alto**
	RSG-SGSI-649	Mal funcionamiento del software de Correo Electrónico por error humano	5	2	**Alto**
	RSG-SGSI-652	Mal funcionamiento del software de Correo Electrónico por software desfasado por vigencia tecnológica y sin soporte por parte del fabricante	5	2	**Alto**
	RSG-SGSI-653	Hacking del Correo Electrónico por incorrecta configuración	5	2	**Alto**
	RSG-SGSI-657	Personal no preparado para la Administración del servicio de Correo Electrónico por Error humano	5	2	**Alto**

ACTIVO	CODIGORIESGO	NOMBRE_RIESGO	IMPACTO	PROBABILIDAD	NIVEL DEL RIESGO
	RSG-SGSI-657	Personal no preparado para la administración del servicio de Correo Electrónico por falta de Capacitación	5	2	Alto
	RSG-SGSI-657	Fuga de información del Correo Electrónico por Error humano	5	2	Alto
	RSG-SGSI-658	Fuga de información del Correo Electrónico por falta de conciencia de seguridad	5	2	Alto
	RSG-SGSI-660	Fuga de información del Correo Electrónico por mala administración de claves	5	2	Alto
Servidores físicos para virtualización	RSG-SGSI-392	Mal funcionamiento de los Servidores físicos para virtualización por Mantenimiento insuficiente	5	3	Extremo
	RSG-SGSI-394	Mal funcionamiento de los Servidores físicos para virtualización por Obsolescencia Tecnológica	5	2	Alto
	RSG-SGSI-397	Uso no autorizado de los Servidores físicos para virtualización por Error humano	5	2	Alto
	RSG-SGSI-412	Indisponibilidad de los Servidores físicos para virtualización por Mantenimiento insuficiente	5	2	Alto
	RSG-SGSI-413	Pérdida de información de los Servidores físicos para virtualización por falta de copias de respaldo	5	2	Alto
	RSG-SGSI-415	Pérdida de información de los Servidores físicos para virtualización por Error humano	5	2	Alto
	RSG-SGSI-420	Fuga de información de los Servidores físicos para virtualización por Error humano	5	2	Alto
Solución de almacenamiento	RSG-SGSI-392	Mal funcionamiento por Mantenimiento insuficiente	5	3	Extremo
	RSG-SGSI-394	Mal funcionamiento por Obsolescencia Tecnológica	5	2	Alto
	RSG-SGSI-397	Uso no autorizado por Error humano	5	2	Alto
	RSG-SGSI-412	Indisponibilidad para virtualización por Mantenimiento insuficiente	5	2	Alto
	RSG-SGSI-413	Pérdida de información por falta de copias de respaldo	5	2	Alto
	RSG-SGSI-415	Pérdida de información por Error humano	5	2	Alto
	RSG-SGSI-420	Fuga de información de los por Error humano	5	2	Alto
Servidores virtuales	RSG-SGSI-681	Mal funcionamiento de los Servidores virtuales por error humano	5	2	Alto
	RSG-SGSI-683	Uso no autorizado de los Servidores virtuales por	5	2	Alto

ACTIVO	CODIGORIESGO	NOMBRE_RIESGO	IMPACTO	PROBABILIDAD	NIVEL DEL RIESGO
		mala administración de la contraseña			
	RSG-SGSI-684	Uso no autorizado de los Servidores virtuales por error humano	5	2	**Alto**
	RSG-SGSI-689	Uso no autorizado de los Servidores virtuales por incorrecta configuración	5	2	**Alto**
	RSG-SGSI-692	Hacking de los Servidores virtuales por incorrecta configuración	5	2	**Alto**
	RSG-SGSI-693	Hacking de los Servidores virtuales por falta de mecanismos de configuración de seguridad	5	2	**Alto**
	RSG-SGSI-695	Hacking de los Servidores virtuales por falta actualización del Sistema	5	2	**Alto**
	RSG-SGSI-698	Pérdida de información de los Servidores virtuales por error humano	5	2	**Alto**
	RSG-SGSI-703	Fuga de información de los Servidores virtuales por error humano	5	2	**Alto**
	RSG-SGSI-704	Fuga de información de los Servidores virtuales por falta de conciencia de seguridad	5	2	**Alto**
	RSG-SGSI-706	Fuga de información de los Servidores virtuales por mala administración de claves	5	2	**Alto**

5.5. ASEGURAMIENTO DE LAS BASES DE DATOS

El numeral 6.2 de los "Lineamientos para la Gestión de la Continuidad Operativa y la formulación de los planes de continuidad operativa de las entidades públicas de los tres niveles de gobierno" aprobado con Resolución Ministerial No 320-2021-PCM, establece la estructura de los planes de continuidad operativa en el cual se incluye el "Aseguramiento de la base de datos mediante la ejecución del Plan de Recuperación de los servicios informáticos".

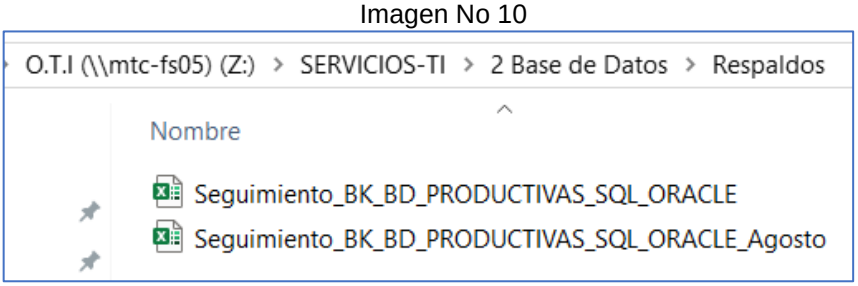
Al respecto, el área de Base de datos de la Oficina de Infraestructura Tecnológica y Seguridad Informática – OTISI de la OGTI, está encargada de configurar los respaldos de las bases de datos tipo Oracle y SQL, dichos respaldos son almacenados temporalmente en el servidor de origen o en una unidad compartida.

Luego de ello, el área de Operaciones de la OITSI es la encargada de almacenar los respaldos generados de base de datos a cintas magnéticas con ayuda de un software de respaldo configurados con librerías robóticas para el grabado en cinta magnética de tipo LTO.

Se ha configurado en las dos (02) soluciones de respaldo (EMC NetWorker 8.2 y 9.2) las copias a cinta magnética de los respaldos de las bases de datos que se generan diariamente.

Asimismo, se tienen una matriz en un archivo Excel para dar seguimiento a los respaldos de Oracle y SQL, dicho archivo se encuentra almacenado en el repositorio de Base de Datos en la siguiente ruta: Z:\SERVICIOS-TI\2 Base de Datos\Respaldos\

Imagen No 10



Del documento elaborado, se observa que diariamente se respalda un aproximado de 3.2 Tb.

Tabla No 16 - Respaldo de Bases de Datos

Tipo de BD	Cantidad de BD	Cantidad de Servidores	Peso diario (Gb.) aproximado
Oracle	15	12	890.00
SQL	145	16	2,350.00

Fuente. Elaboración propia

5.6 PROCEDIMIENTOS DE RESPUESTA Y RECUPERACIÓN

A continuación, se desarrollan los procedimientos de respuesta y recuperación de los servicios críticos identificados con riesgo alto o extremo:

Formatos de Recuperación de Servicios TI

Código:	**FRS-01**
Activo crítico:	**Switch de Core**
Evento:	**Falla o avería de uno de los dos Switches de Core**
1. Plan de prevención (antes)	
- Resguardar copia de la última configuración aplicada. - Monitorear continuamente el estado de salud (temperatura, estado de ventiladores, uso de memoria y CPU, etc.), los eventos y/o alertas y interfaces de red. - Tener actualizada la lista de contactos del proveedor de soporte técnico y fabricante.	
2. Plan o procedimiento de Recuperación (durante)	

Código:	**FRS-01**
Activo crítico:	**Switch de Core**
Evento:	**Falla o avería de uno de los dos Switches de Core**
- Acceder remotamente/presencialmente al equipo afectado - Analizar los eventos y el comportamiento del equipo afectado. - De no haber conmutado automáticamente todo el tráfico al switch core y de no restablecer la operatividad durante el tiempo prudente (de acuerdo al LSA establecido por el Área), forzar manualmente toda la carga al segundo switch de core. - Evaluar la avería del equipo afectado y resolver el incidente. - De ser necesario, escalar la avería al soporte técnico. - De ser necesario, reiniciar el equipo afectado.	
3. Plan de evaluación (después)	
- Verificar la operatividad del equipo afectado y el restablecimiento de conectividad. - Monitorear el desempeño y eventos del equipo afectado durante 24 horas. - Realizar pruebas de esfuerzo y forzar la contingencia para validar si los tiempos de recuperación se mantienen. - Documentar la avería y registrarla.	

Firmado digitalmente por: REQUENA CASTRO Jesus Nicanor FAU 20131379944 soft
Motivo: Doy V° B°
Fecha: 29/09/2022 11:13:40-0500

Código:	**FRS-02**
Activo crítico:	**Switch de Distribución**
Evento:	**Falla o avería de uno de los dos Switches de distribución**
1. Plan de prevención (antes)	
- Resguardar copia de la última configuración aplicada. - Monitorear continuamente el estado de salud (temperatura, estado de ventiladores, uso de memoria y CPU, etc.), los eventos y/o alertas y interfaces de red. - Tener actualizada la lista de contactos del proveedor de soporte técnico y fabricante.	
2. Plan o procedimiento de Recuperación (durante)	
- Acceder remotamente/presencialmente al equipo afectado - Analizar los eventos y el comportamiento del equipo afectado. - De no haber conmutado automáticamente todo el tráfico al segundo switch de distribución y de no restablecer la operatividad durante el tiempo prudente (de acuerdo al LSA establecido por el Área), forzar manualmente toda la carga al segundo switch. - Evaluar la avería del equipo afectado y resolver el incidente. - De ser necesario, escalar la avería al soporte técnico. - De ser necesario, reiniciar el equipo afectado.	
3. Plan de evaluación (después)	
- Verificar la operatividad del equipo afectado y el restablecimiento de conectividad. - Monitorear el desempeño y eventos del equipo afectado durante 24 horas. - Realizar pruebas de esfuerzo y forzar la contingencia para validar si los tiempos de recuperación se mantienen. - Documentar la avería y registrarla.	

Jirón Zorritos 1203 – Lima - Perú
Central telefónica. (511) 615-7800
www.gob.pe/mtc

Código:	**FRS-03**
Activo crítico:	**Servicio de acceso a Internet**
Evento:	**Falla o avería del servicio de acceso a Internet**

1. Plan de prevención (antes)

- Monitorear continuamente del consumo de enlace.
- Monitorear continuamente los eventos y/o alertas que generan los equipos de comunicación que brindan el servicio.
- Generar reportes de consumo de enlace y disponibilidad de equipos.
- Tener actualizada la lista de contactos del proveedor de soporte técnico y fabricante.

2. Plan o procedimiento de Recuperación (durante)

- Realizar pruebas de traza a internet y descartar el salto (Gateway) que presenta desconexión.
- Acceder remotamente/presencialmente al/los equipo(s) afectado(s).
- Analizar los eventos y el comportamiento del/los equipo(s) afectado(s).
- De no haber conmutado automáticamente todo el tráfico mediante el según enlace y de no restablecer la operatividad durante el tiempo prudente (de acuerdo al LSA establecido por el Área), forzar manualmente toda la carga al según enlace.
- Reportar la avería al proveedor de servicio.
- De ser necesario, reiniciar el/los equipo(s) afectado(s).

3. Plan de evaluación (después)

- Verificar la disponibilidad de los dos enlaces de acceso a internet.
- Monitorear la operatividad y eventos de los equipos de comunicación que brindan el servicio.
- Realizar pruebas de esfuerzo y forzar la contingencia para validar si los tiempos de recuperación se mantienen.
- Documentar la avería y registrarla.

Firmado digitalmente por: REQUENA CASTRO Jesus Nicanor FAU 20131379944 soft
Motivo: Doy V° B°
Fecha: 29/09/2022 11:13:31-0500

Código:	**FRS-04**
Activo crítico:	**Balanceador de Internet**
Evento:	**Falla o avería del balanceador de Internet**

1. Plan de prevención (antes)

- Resguardar copia de la última configuración aplicada.
- Monitorear continuamente el estado de salud (temperatura, uso de memoria y CPU, etc.), los eventos y/o alertas, las interfaces de red y el tráfico de datos.
- Tener actualizada la lista de contactos del proveedor de soporte técnico y fabricante.

2. Plan o procedimiento de Recuperación (durante)

- Acceder remotamente/presencialmente al equipo afectado
- Analizar los eventos y el comportamiento del equipo afectado.
- De no haber conmutado automáticamente todo el tráfico al balanceador de contingencia y de no restablecer la operatividad durante el tiempo prudente (de acuerdo al LSA establecido por el Área), forzar manualmente toda la carga a tal equipo.
- Evaluar la avería del equipo afectado y resolver el incidente.
- De ser necesario, escalar la avería al soporte técnico.
- De ser necesario, reiniciar el equipo afectado.

Código:	**FRS-04**
Activo crítico:	**Balanceador de Internet**
Evento:	**Falla o avería del balanceador de Internet**

3. Plan de evaluación (después)

- Verificar la operatividad del equipo afectado y el restablecimiento de conectividad.
- Monitorear el desempeño y eventos del equipo afectado durante 24 horas.
- Realizar pruebas de esfuerzo y forzar la contingencia para validar si los tiempos de recuperación se mantienen.
  Documentar la avería y registrarla

Código:	**FRS-05**
Activo crítico:	**Controlador de acceso Wifi**
Evento:	**Falla o avería del controlador de acceso Wifi**

1. Plan de prevención (antes)

- Resguardar copia de la última configuración aplicada.
- Monitorear continuamente el estado de salud (temperatura, estado de ventiladores, uso de memoria y CPU, etc.), los eventos y/o alertas y interfaces de red.
  Tener actualizada la lista de contactos del proveedor de soporte técnico y fabricante.

2. Plan o procedimiento de Recuperación (durante)

- Verificar en la consola del controlador Wi-Fi alguna avería o problema de desconexión.
- Acceder remotamente/presencialmente al/los equipo(s) afectado(s).
- Analizar los eventos y el comportamiento del/los equipo(s) afectado(s).
- De no poder restablecer los servicios del controlador, verificar las conexiones de red y/o forzar la recuperación de los servicios.
- Reportar la avería al proveedor de servicio.
- De ser necesario, reiniciar el/los equipo(s) afectado(s).

3. Plan de evaluación (después)

- Verificar la conectividad con todos los puntos de acceso conectados al Controlador Wi-Fi
- Monitorear la operatividad y eventos del controlador.
- Documentar la avería y registrarla

Código:	**FRS-06**
Activo crítico:	**Firewall Perimetral**
Evento:	**Falla o avería del Firewall perimetral**

1. Plan de prevención (antes)

a) Descripción del evento
El hardware y software de los equipos de seguridad es el recurso principal para almacenar, procesar y gestionar el acceso a los servicios de manera controlada.

b) Objetivo
Asegurar la continuidad en el acceso a los servicios de manera segura.

c) Personal Encargado
Equipo de Seguridad Informática.

Código:	**FRS-06**
Activo crítico:	**Firewall Perimetral**
Evento:	**Falla o avería del Firewall perimetral**

d) Condiciones de Prevención de Riesgo
- Revisión periódica de los registros (logs) de los equipos para prevenir mal funcionamiento de los mismos.
- Contar con los respaldos de seguridad de los equipos.
- Contar con servicios de soporte y mantenimiento que contemple actividades de prevención, revisión del equipo y mantenimiento general.
- Contar con equipos de respaldo que tengan la misma capacidad de hardware y software.

e) Acciones del Equipo de Prevención de TI
- Establecer, organizar, ejecutar y supervisar procedimientos de respaldo y restauración de información.
- 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 la entidad.

Realizar revisiones de obsolescencia tecnológica de los servidores y componentes internos de forma anual.

2. Plan o procedimiento de Recuperación (durante)

a) Eventos que activan la Contingencia
- Fallas en la conexión.
- Degradación del rendimiento del equipo.
- Falla de procesamiento de la información (políticas y reglas de acceso).

b) Personal que autoriza la contingencia
El/La Coordinador/a de Continuidad de TI debe activar la contingencia.

c) Descripción de las actividades después de activar la contingencia
- Realizar la revisión del equipo averiado, buscando un recurso de reemplazo
- Verificar la garantía del equipo y reportarlo al proveedor.
- Verificar la disponibilidad del HA para que el equipo secundario tome el control

d) Duración
El tiempo máximo de la contingencia no debe sobrepasar las cuatro (04) horas.

3. Plan de evaluación (después)

a) Personal Encargado
El Equipo Especializado, luego de validar la corrección del problema del equipo informará a los jefes y/o Directores de áreas para la reanudación de las operaciones de los servicios afectados en el equipo averiado.

b) Descripción de actividades
El plan de recuperación estará orientado a recuperar en el menor tiempo

Firmado digitalmente por: REQUENA CASTRO Jesus Nicanor FAU 20131379944 soft
Motivo: Doy V° B°
Fecha: 29/09/2022 11:13:13-0500

Código:	FRS-06
Activo crítico:	Firewall Perimetral
Evento:	Falla o avería del Firewall perimetral

posible las actividades afectadas durante la interrupción del servicio afectado por falla del equipo.

Se debe realizar como mínimo las siguientes actividades:

- Activación del equipo de secundario para que tome el control en modo "activo"
- Verificar el funcionamiento de las interfaces de comunicación.
- Ejecutar pruebas de acceso a los sistemas y aplicaciones.
- Remitir un mensaje electrónico a los usuarios del MTC informando la reanudación de losservicios.

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

c) Mecanismos de Comprobación
El/La Especialista en Seguridad Informática, presentará un informe a el/la Director/a de OGTI, explicando que parte del servicio u operaciones se han visto afectadas, y cuáles son las acciones tomadas.

d) Desactivación del Plan de Contingencia
Con el aviso de el/la Coordinador/a de Continuidad de TI, se desactivará el presente Plan.

Firmado digitalmente por: REQUENA CASTRO Jesus Nicanor FAU 20131379944 soft
Motivo: Doy V° B°
Fecha: 29/09/2022 11:13:05-0500

Código:	FRS-07
Activo crítico:	Firewall WAN
Evento:	Falla o avería del firewall WAN

1. Plan de prevención (antes)

a) Descripción del evento
El hardware y software de los equipos de seguridad es el recurso principal para almacenar, procesar y gestionar el acceso a los servicios de manera controlada.

b) Objetivo
Asegurar la continuidad en el acceso a los servicios de manera segura.

c) Personal Encargado
Equipo de Seguridad Informática.

d) Condiciones de Prevención de Riesgo
a. Revisión periódica de los registros (logs) de los equipos para prevenir mal funcionamiento de los mismos.
b. Contar con los respaldos de seguridad de los equipos.
c. Contar con servicios de soporte y mantenimiento que contemple actividades de prevención,revisión del equipo y mantenimiento general.

e) Acciones del Equipo de Prevención de TI
- Establecer, organizar, ejecutar y supervisar procedimientos de respaldo y restauración de información o backup.
- Programar, supervisar el mantenimiento preventivo a los equipos componentes del Centrode Datos.

Jirón Zorritos 1203 – Lima - Perú
Central telefónica. (511) 615-7800
www.gob.pe/mtc

Código:	**FRS-07**
Activo crítico:	**Firewall WAN**
Evento:	**Falla o avería del firewall WAN**

- Mantener actualizado el inventario hardware y software utilizado en el Centro de Datos de laentidad.

Realizar revisiones de obsolescencia tecnológica de los equipos y componentes internosde forma anual.

2. Plan o procedimiento de Recuperación (durante)

a) Eventos que activan la Contingencia
- Fallas en la conexión.
- Degradación del rendimiento del equipo.
- Falla de procesamiento de la información (políticas y reglas de acceso).

b) Personal que autoriza la contingencia
El/La Coordinador/a de Continuidad de TI debe activar la contingencia.

c) Descripción de las actividades después de activar la contingencia
a. Realizar la revisión del equipo averiado, buscando un recurso de reemplazo
b. Verificar la garantía del equipo y reportarlo al proveedor.

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

Firmado digitalmente por: REQUENA CASTRO Jesus Nicanor FAU 20131379944 soft
Motivo: Doy V° B°
Fecha: 29/09/2022 11:12:54-0500

3. Plan de evaluación (después)

a) Personal Encargado
El Equipo Especializado, luego de validar la corrección del problema del equipo informará a los Jefes y/o Directores de áreas para la reanudación de las operaciones de los servicios afectados en el equipo averiado.

b) Descripción de actividades
El plan de recuperación estará orientado a recuperar en el menor tiempo posible las actividades afectadas durante la interrupción del servicio afectado por falla del equipo.

Se debe realizar como mínimo las siguientes actividades:
- Instalación y puesta a punto de un cómputo compatible y hardware necesarios para lainstalación del sistema de información con las características mínimas exigidas.
- Verificar el funcionamiento de las interfaces.
- Ejecutar pruebas de acceso a los sistemas y aplicaciones.
- Si no es posible acceder remotamente equipo, conectarse vía consola o directamente con una laptop y verificar su configuración.
- Remitir un mensaje electrónico a los usuarios del MTC informando la reanudación de losservicios.

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

c) Mecanismos de Comprobación
El/La Especialista en Redes y Comunicaciones, presentará un informe a

Código:	**FRS-07**
Activo crítico:	**Firewall WAN**
Evento:	**Falla o avería del firewall WAN**

el/la Director/a de OGTI, explicando que parte del servicio u operaciones se han visto afectadas, y cuáles son las acciones tomadas.

d) Desactivación del Plan de Contingencia
Con el aviso de el/la Coordinador/a de Continuidad de TI, se desactivará el presente Plan.

Código:	**FRS-08**
Activo crítico:	**Servidor Blade (físico)**
Evento:	**Falla de un Servidor Blade**

1. PLAN DE PREVENCIÓN

a) Descripción del evento
Un servidor Blade es un equipo autónomo y compacto que ayuda a ahorrar energía y espacio, dentro de un centro de datos, asimismo está expuesto a sufrir fallas inesperadas de hardware, por las grandes cargas de trabajo, los siguientes elementos mínimos identificados por OGTI, deben ser considerados como parte afectada o causa de la contingencia:

Infraestructura:
- Centro de Datos - Sede Principal.

Recursos Humanos
- Personal que recibe el servicio.

b) Objetivo
Establecer las acciones que se ejecutarán ante una falla del servidor Blade a fin de minimizar el tiempo de interrupción de las operaciones del MTC, sin exponer la seguridad de las personas.

c) Entorno
Este evento puede afectar los sistemas y servicios que consumen los ciudadanos a nivel nacional y que se encuentren implementados en servidor del centro de datos.

d) Personal Encargado
El Grupo Especializado de la Oficina de Infraestructura Tecnológica y Seguridad Informática (OITSI) de la Oficina General de Tecnología de la Información del MTC, es quien debe dar los lineamientos y dar cumplimiento a las Condiciones de Prevención de Riesgo del presente Plan. Por su parte, el Equipo de Prevención de TI debe realizar las acciones descritas en el punto f).

e) Condiciones de Prevención de Riesgo
- Contar con el servicio de soporte técnico y garantía de la infraestructura de servidores del centro de datos.
- Monitoreo del estado de salud y recursos de procesamiento de los servidores del centro de datos.
- Ejecución de los mantenimientos preventivos de los servidores del centro

Firmado digitalmente por: REQUENA CASTRO Jesus Nicanor FAU 20131379944 soft
Motivo: Doy V° B°
Fecha: 29/09/2022 11:12:45-0500

Código:	**FRS-08**
Activo crítico:	**Servidor Blade (físico)**
Evento:	**Falla de un Servidor Blade**

de datos.

f) Procesos Relacionados antes del evento
- Tener el inventario y diagrama actualizado del equipamiento de los servidores del centro de datos.
- Contar con el registro de contactos de los proveedores de los servicios de soporte técnico y garantía de la marca del fabricante.

g) Acciones del Equipo de Prevención de TI
- Programar y supervisar los mantenimientos preventivos de los servidores del centro de datos.
- Realizar el monitoreo continuo del estado de salud (temperatura, estado de ventiladores, CPU, interfaces y otros.).
- Contar con los contactos actualizados del soporte técnico del fabricante y/o personal del proveedor del servicio.

2. PLAN DE EJECUCIÓN

a) Eventos que activan la contingencia
La contingencia se activará inmediatamente después de ocurrir el evento falla del servidor.

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

c) Personal Encargado
Equipo de Emergencia de TI.

d) Descripción de las actividades después de activar la contingencia
- Acceso a la consola de administración para la verificación y evaluación de la falla de hardware o componente del servidor blade.
- Validar la correcta migración de las máquinas virtuales asociada al servidor con fallas de hardware de ser el caso, para asegurar la continuidad y operatividad de los servicios.
- Comunicación con el soporte y garantía de la marca para el reemplazo del equipo o dispositivo afectado por falla de hardware irreparable de ser el caso.
- Recopilación de log del servidor con falla de hardware para ser enviado al soporte de la marca y determine la parte a entregar para su reemplazo.
- Acceder físicamente al centro de datos para el reemplazo de la parte afectada o el remplazo del servidor con falla de hardware.
- Configuración, instalación y puesta en producción del servidor y/o dispositivo afectado por falla de hardware.
- Pruebas de operatividad del servidor blade.

e) Duración
La duración total del evento dependerá del grado de la falla del hardware y la disponibilidad de la parte afectada para el reemplazo por parte del fabricante de la marca, de acuerdo al tipo de soporte mínimo 04 horas y máximo 72 horas.

Código:	**FRS-08**
Activo crítico:	**Servidor Blade (físico)**
Evento:	**Falla de un Servidor Blade**

3. PLAN DE EVALUACIÓN

a) Acciones post evento
- Realizar el informe de los daños ocasionados y remediación del evento.
- Revisar el plan de mantenimientos de la infraestructura de servidores y sus componentes.

Código:	**FRS-09**
Activo crítico:	**Chasis de servidores**
Evento:	**Falla de Chasis de Servidores**

1. PLAN DE PREVENCIÓN

a) Descripción del evento

Un chasis tiene como funcionalidad albergar múltiples servidores físicos o cuchillas dentro de él, es un sistema compacto que ayuda a ahorrar energía, cableado, espacio físico y simplifica la gestión y administración de los servidores en entornos de TI complejos automatizando las tareas de administración del ciclo de vida del servidor, asimismo está expuesto a sufrir fallas inesperadas de hardware, por las grandes cargas de trabajo, los siguientes elementos mínimos identificados por OGTI, deben ser considerados como parte afectada o causa de la contingencia:

Infraestructura:
- Centro de Datos - Sede Principal.

Recursos Humanos
- Personal que administra el servicio.

b) Objetivo

Establecer las acciones que se ejecutarán ante una falla del chasis de servidores a fin de minimizar el tiempo de interrupción de las operaciones del MTC, sin exponer la seguridad de las personas.

c) Entorno

Este evento puede afectar a todos los servidores que se encuentran configurados e implementados sobre el chasis dejando indisponibles a los sistemas y servicios que consumen los ciudadanos a nivel nacional y que se encuentren implementados en el centro de datos.

d) Personal Encargado

El Grupo Especializado de la Oficina de Infraestructura Tecnológica y Seguridad Informática (OITSI) de la Oficina General de Tecnología de la Información del MTC, es quien debe dar los lineamientos y dar cumplimiento a las Condiciones de Prevención de Riesgo del presente Plan. Por su parte, el Equipo de Prevención de TI debe realizar las acciones descritas en el punto f).

e) Condiciones de Prevención de Riesgo

Firmado digitalmente por: REQUENA CASTRO Jesus Nicanor FAU 20131379944 soft
Motivo: Doy V° B°
Fecha: 29/09/2022 11:12:26-0500

Código:	**FRS-09**
Activo crítico:	**Chasis de servidores**
Evento:	**Falla de Chasis de Servidores**

- Contar con el servicio de soporte técnico y garantía de la infraestructura de servidores del centro de datos.
- Monitoreo del estado de salud y recursos de procesamiento de los servidores del centro de datos.
- Ejecución de los mantenimientos preventivos de los servidores del centro de datos.

f) Procesos Relacionados antes del evento
- Tener el inventario y diagrama actualizado del equipamiento de los chasis de servidores del centro de datos.
- Contar con el registro de contactos de los proveedores de los servicios de soporte técnico y garantía de la marca del fabricante.

g) Acciones del Equipo de Prevención de TI
- Programar y supervisar los mantenimientos preventivos de los chasis de servidores del centro de datos.
- Realizar el monitoreo continuo del estado de salud (temperatura, estado de ventiladores, CPU, interfaces entre otros componentes).
- Contar con los contactos actualizados del soporte técnico del fabricante y/o personal del proveedor del servicio.

Firmado digitalmente por: REQUENA CASTRO Jesus Nicanor FAU 20131379944 soft
Motivo: Doy V° B°
Fecha: 29/09/2022 11:12:14-0500

2. PLAN DE EJECUCIÓN

a) Eventos que activan la contingencia
La contingencia se activará inmediatamente después de ocurrir el evento falla del chasis de servidores.

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

c) Personal Encargado
Equipo de Emergencia de TI.

d) Descripción de las actividades después de activar la contingencia
- Acceso a la consola de administración para la verificación y evaluación de la falla de hardware o componente del chasis para servidores Blade.
- Comunicación con el soporte y garantía de la marca para el reemplazo del equipo o dispositivo afectado por falla de hardware irreparable de ser el caso.
- Recopilación de log del chasis para servidores con falla de hardware para ser enviado al soporte de la marca y determine la parte a entregar para su reemplazo.
- Acceder físicamente al centro de datos para el reemplazo de la parte afectada o el remplazo total del chasis para servidores con falla de hardware.
- Configuración, instalación y puesta en producción del chasis para servidores y/o dispositivo afectado por falla de hardware.
- Pruebas de operatividad.

Código:	**FRS-09**
Activo crítico:	**Chasis de servidores**
Evento:	**Falla de Chasis de Servidores**

e) Duración
La duración total del evento dependerá del grado de la falla del hardware y la disponibilidad de la parte afectada para el reemplazo por parte del fabricante de la marca, de acuerdo al tipo de soporte mínimo 04 horas máximo 72 horas.

3. PLAN DE EVALUACIÓN

a) Acciones post evento
- Realizar el informe de los daños ocasionados y remediación del evento.
- Revisar el plan de mantenimientos de la infraestructura de servidores y sus componentes.

Código:	**FRS-10**
Activo crítico:	**Servidor principal de dominio**
Evento:	**Falla de servidor principal de dominio**

1. PLAN DE PREVENCIÓN

a) Descripción del evento
Un servidor de controlador de dominio cuenta con funciones de autenticación y autorización, proporciona un framework para otros servicios similares. Básicamente, el directorio consiste en una base de datos LDAP que contiene objetos en red, deben ser considerados como parte afectada o causa de la contingencia:

Infraestructura:
Centro de Datos - Sede Principal.

Recursos Humanos
Personal que recibe el servicio.

b) Objetivo
Establecer las acciones que se ejecutarán ante una falla del servidor de controlador de dominio a fin de minimizar el tiempo de interrupción de los servicios de red y autenticación de los usuarios del MTC.

c) Entorno
Este evento puede afectar los sistemas, servicios de red y autenticación de los usuarios del MTC y ciudadanos a nivel nacional.

d) Personal Encargado
El Grupo Especializado de la Oficina de Infraestructura Tecnológica y Seguridad Informática (OITSI) de la Oficina General de Tecnología de la Información del MTC, es quien debe dar los lineamientos y dar cumplimiento a las Condiciones de Prevención de Riesgo del presente Plan. Por su parte, el Equipo de Prevención de TI debe realizar las acciones descritas en el punto f).

e) Condiciones de Prevención de Riesgo
- Contar con el servicio de soporte técnico del servicio de controlador de

Código:	**FRS-10**
Activo crítico:	**Servidor principal de dominio**
Evento:	**Falla de servidor principal de dominio**

dominio el cual se encuentra implementados en la infraestructura virtual VMware del centro de datos.
- Monitoreo del estado de salud y recursos de procesamiento de los servidores controladores de dominio del centro de datos.
- Ejecución de backups del sysvol de los servidores controladores de dominio del centro de datos
- Ejecución de SnapShot de los servidores controladores de dominio del centro de datos.

f) Procesos Relacionados antes del evento
- Tener el inventario actualizado del equipamiento de los controladores de dominio del centro de datos.
- Contar con el registro de contactos de los proveedores de los servicios de soporte técnico de la marca del fabricante.

g) Acciones del Equipo de Prevención de TI
- Realizar el monitoreo el estado de salud de los servidores controladores de dominio del centro de datos (revisión de eventos, consumo de disco, consumo de memoria, entre otros)
- Ejecutar y supervisar las tareas de backup y snapchot de los servidores controladores de dominio.
- Contar con los contactos actualizados del soporte técnico del fabricante y/o personal del proveedor del servicio.

Firmado digitalmente por: REQUENA CASTRO Jesus Nicanor FAU 20131379944 soft
Motivo: Doy V° B°
Fecha: 29/09/2022 11:11:10-0500

2. PLAN DE EJECUCIÓN

a) Eventos que activan la contingencia
La contingencia se activará inmediatamente después de ocurrir el evento falla del servidor de dominio principal.

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

c) Personal Encargado
Equipo de Emergencia de TI.

d) Descripción de las actividades después de activar la contingencia
- Sincronización de los servidores de dominio.
- Validación del correcto funcionamiento de los servicios DNS, árbol de objetos, GPO, para asegurar la continuidad y operatividad de los servicios.
- Comunicación con el soporte de la marca para el análisis del caso presentado y solución correspondiente.
- Pruebas de operatividad del servidor controlador de dominio.

e) Duración
La duración total del evento dependerá del tamaño del backup del sysvol o de snapshot generado en la infraestructura virtual como también del soporte por parte de la marca, de acuerdo al tipo de soporte mínimo 04 horas máximo 24 horas.

3. PLAN DE EVALUACIÓN

b) Acciones post evento

Código:	**FRS-10**
Activo crítico:	**Servidor principal de dominio**
Evento:	**Falla de servidor principal de dominio**

- Realizar el informe de los daños ocasionados y remediación del evento.
- Revisar el plan de backups y ejecución de snapshot de los servidores controladores de dominios.

Código:	**FRS-11**
Activo crítico:	**Plataforma de correo electrónico Outlook**
Evento:	**Falla de la Plataforma de Correo Electrónico Outlook.**

1. PLAN DE PREVENCIÓN

a) Descripción del evento

Un servidor de correo electrónico posee un software de colaboración entre usuarios cuenta con roles de bases de datos, acceso y transporte. Entre sus funciones es la autenticación mediante protocoles de cliente (Outlook), servicio OWA (acceso web) y ActiveSync (celulares) conectándose mediante un servicio API al servidor controlador de dominio.

Infraestructura:
Centro de Datos - Sede Principal.

Recursos Humanos
Personal que recibe el servicio.

b) Objetivo

Establecer las acciones que se ejecutarán ante una falla del servidor de correo electrónico a fin de minimizar el tiempo de interrupción de servicio.

c) Entorno

Este evento puede afectar los sistemas, servicios que consumen los ciudadanos a nivel nacional y los usuarios internos del MTC.

d) Personal Encargado

El Grupo Especializado de la Oficina de Infraestructura Tecnológica y Seguridad Informática (OITSI) de la Oficina General de Tecnología de la Información del MTC, es quien debe dar los lineamientos y dar cumplimiento a las Condiciones de Prevención de Riesgo del presente Plan. Por su parte, el Equipo de Prevención de TI debe realizar las acciones descritas en el punto f).

e) Condiciones de Prevención de Riesgo

- Contar con el servicio de soporte técnico del servicio de correo electrónico el cual se encuentra implementados en la infraestructura virtual VMware del centro de datos.
- Monitoreo del estado de salud y recursos de procesamiento de los servidores de correo electrónico del centro de datos.
- Ejecución de backups de las bases de datos (full e incremental) de los servidores de correo electrónico del centro de datos
- Ejecución de Snapshot de los servidores de correo electrónico del centro de datos.

f) Procesos Relacionados antes del evento

Firmado digitalmente por: REQUENA CASTRO Jesus Nicanor FAU 20131379944 soft
Motivo: Doy V° B°
Fecha: 29/09/2022 11:11:01-0500

Código:	**FRS-11**
Activo crítico:	**Plataforma de correo electrónico Outlook**
Evento:	**Falla de la Plataforma de Correo Electrónico Outlook.**

- Tener el inventario actualizado del equipamiento del correo electrónico del centro de datos.
- Contar con el registro de contactos de los proveedores de los servicios de soporte técnico de la marca.

g) Acciones del Equipo de Prevención de TI
- Realizar el monitoreo el estado de salud de los servidores de correo electrónico del centro de datos (revisión de eventos, consumo de disco, consumo de memoria, consistencia de los servicios de correo electrónico entre otros)
- Ejecutar y supervisar las tareas de backup y snapshot de los servidores de correo electrónico.
- Contar con los contactos actualizados del soporte técnico del fabricante y/o personal del proveedor del servicio.

2. PLAN DE EJECUCIÓN

a) Eventos que activan la contingencia
La contingencia se activará después de ocurrir el evento falla del servidor de dominio principal.

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

c) Personal Encargado
Equipo de Emergencia de TI.

d) Descripción de las actividades después de activar la contingencia
- Sincronización de las bases de datos y servicios del correo electrónico.
- Validación del correcto funcionamiento de los servicios de bases de datos, acceso y transporte, para asegurar la continuidad y operatividad de los servicios.
- Comunicación con el soporte de la marca para el análisis del caso presentado y solución correspondiente.
- Pruebas de operatividad del servidor de correo electrónico.

e) Duración
La duración total del evento dependerá del tamaño del backup de las bases de datos o de snapshot generado en la infraestructura virtual como también del soporte por parte de la marca, de acuerdo al tipo de soporte mínimo 04 horas máximo 24 horas.

3. PLAN DE EVALUACIÓN

a) Acciones post evento
- Realizar el informe de los daños ocasionados y remediación del evento.
- Revisar el plan de mantenimientos de la infraestructura de servidores y sus componentes.

Firmado digitalmente por: REQUENA CASTRO Jesus Nicanor FAU 20131379944 soft
Motivo: Doy V° B°
Fecha: 29/09/2022 11:10:43-0500

Código:	**FRS-12**
Activo crítico:	**UPS**
Evento:	**Falla de equipo UPS N+1**

1. Plan de prevención (antes)

- Realizar monitoreo continuo del estado de operación de los equipos UPS del Centro de Datos (nivel de carga de baterías, carga eléctrica, voltaje, frecuencia, estado del equipo, etc.).
- Verificar la operación de los equipos en paralelo – redundante.
- Tener a la mano los teléfonos de contacto del personal o soporte técnico del proveedor.

2. Plan o procedimiento de Recuperación (durante)

- Verificar que el equipo redundante ha asumido la totalidad de carga.
- Validar el estado y niveles de operación del equipo (nivel de carga de baterías, carga eléctrica, voltaje, frecuencia, estado del equipo, etc.).

3. Plan de evaluación (después)

- Validar la operatividad del equipo afectado y el restablecimiento de modo de operación en paralelo – redundante.
- Monitorear la operación de los equipos (nivel de desempeño y eventos de los equipos por un mínimo de cinco (05) horas).
- Coordinar bajo responsabilidad la ejecución de pruebas de esfuerzo y forzar la contingencia para validar si los tiempos de recuperación se mantienen.
- Documentar y registrar.

Código:	**FRS-13**
Activo crítico:	**Sistema de extinción de incendios**
Evento:	**Falla del sistema de extinción de incendios**

1. Plan de prevención (antes)

- Realizar monitoreo continuo del estado de operación del sistema (nivel de carga de cilindro de agente extintor, lectura de alertas en panel, voltaje, frecuencia, estado del equipo, etc.).
- Verificación visual de componentes del sistema (panel central, sensores, ductos de aspiración, filtros, etc.).
- Tener a la mano los teléfonos de contacto del personal o soporte técnico del proveedor.

2. Plan o procedimiento de Recuperación (durante)

- Verificar el tipo de incidente.
- Validar la existencia real de un incidente,
- Validar la extinción del fuego en el ambiente involucrado.

3. Plan de evaluación (después)

- Validar la operatividad del sistema y estado de operación del sistema (nivel de carga de cilindro de agente extintor, verificación de alertas en panel, voltaje, frecuencia, estado del equipo, etc.).
- Coordinar bajo responsabilidad, el servicio de mantenimiento y recarga del sistema de extinción de incendios.
- Documentar y registrar.

Código:	**FRS-14**
Activo crítico:	**Sistema de aire acondicionado**
Evento:	**Falla del sistema de aire acondicionado**

1. Plan de prevención (antes)

- Realizar monitoreo continuo del estado de operación de los equipos del sistema de refrigeración (lectura de alertas en panel, voltaje, frecuencia, estado del equipo, etc.).
- Verificación visual de funcionamiento de los equipos (compresor y evaporador).
- Tener a la mano los teléfonos de contacto del personal o soporte técnico del proveedor.

2. Plan o procedimiento de Recuperación (durante)

- Verificar la conmutación de estado de los equipos de estado Stanby – Running.
- Validar el estado y niveles de operación de los equipos (lectura de alertas en panel, voltaje, frecuencia, estado del equipo, etc.).

3. Plan de evaluación (después)

- Validar la operatividad del sistema y estado de operación de los equipos del mismo (lectura de alertas en panel, voltaje, frecuencia, estado del equipo, etc.).
- Coordinar bajo responsabilidad, el servicio de mantenimiento correctivo de los equipos del sistema de refrigeración.
- Documentar y registrar.

Código:	**FRS-15**
Activo crítico:	**Central Telefónica**
Evento:	**Falla de Central Telefónica**

1. Plan de prevención (antes)

- Resguardo de copia de configuración aplicada.
- Realizar monitoreo continuo a su estado de salud (temperatura, estado de ventiladores, etc.).
- Realizar de mantenimiento lógico y físico por empresa proveedora cada 6 meses
- Tener actualizada la lista de contactos del proveedor de soporte técnico y fabricante.

2. Plan o procedimiento de Recuperación (durante)

- Acceder remotamente/presencialmente al equipo afectado
- Analizar los eventos y el comportamiento del equipo afectado.
- De no haber conmutado automáticamente forzar manualmente el funcionamiento del servidor de contingencia
- Evaluar la avería del equipo afectado y resolver el incidente.
- De ser necesario, escalar la avería al soporte técnico.
  De ser necesario, reiniciar el equipo afectado.

3. Plan de evaluación (después)

- Verificar la operatividad del equipo afectado y el restablecimiento de conectividad.
- Monitorear el desempeño y eventos del equipo afectado durante 24 horas.
- Realizar pruebas de esfuerzo y forzar la contingencia para validar si los tiempos de recuperación se mantienen.
  Documentar la avería y registrarla.

Código:	**FRS-16**
Activo crítico:	**Servidor de Telefonía (Call Center)**
Evento:	**Falla del servidor de Telefonía**

1. Plan de prevención (antes)

- Resguardo de copia de configuración aplicada.
- Realizar monitoreo continuo a su estado de salud (temperatura, estado de ventiladores, etc.).
- Realizar de mantenimiento lógico y físico por empresa proveedora cada 6 meses
  Tener actualizada la lista de contactos del proveedor de soporte técnico y fabricante.

2. Plan o procedimiento de Recuperación (durante)

- Acceder remotamente
- Analizar los eventos y el comportamiento del equipo virtual afectado.
- Validar con el área de servidores el estado del equipo virtual
- Evaluar y resolver el incidente.
- De ser necesario, escalar la avería al soporte técnico.

3. Plan de evaluación (después)

- Verificar la operatividad del equipo virtual afectado y el restablecimiento de conectividad.
- Monitorear el desempeño y eventos del equipo virtual afectado durante 24 horas.
- Documentar la avería y registrarla.

Por otro lado, en el numeral 7.1.1 "Riesgos que podrían interrumpir la continuidad de operaciones en le MTC" del Plan de Continuidad Operativa del MTC aprobado con Resolución Ministerial No 025-2020-MTC/01, se identificaron cinco peligros o riesgos que podrían ocasionar la interrupción de operaciones y de funcionamiento del MTC. El resultado del análisis y estimación de estos riesgos es el siguiente:

Imagen No 09

Tabla N° 01: Estimación de riesgo del MTC

N/O	Variables de Impacto	Sismo de Gran Magnitud y Tsunami en Lima y Callao	Incendio en sede principal	Ataque informático	Atentado terrorista	Grave alteración del orden público
1	Colapso total y/o parcial de Infraestructura	3.0	2.1	1.1	1.8	1.5
2	Colapso del suministro de energía eléctrica	2.6	2.3	1.1	1.6	1.0
3	Colapso del suministro de los servicios de agua	2.0	2.6	0.3	1.2	0.9
4	Operatividad de equipos, sistemas y medios informáticos	2.3	2.3	2.6	1.3	1.1
5	Operatividad de equipos y tecnología de comunicaciones	2.4	2.1	2.6	1.8	1.4
6	Disponibilidad de Recursos Humanos especializados en la operación de las actividades críticas	2.5	1.8	2.6	1.6	2.0
7	Disponibilidad de Recursos financieros	2.3	1.9	1.7	1.6	1.6

COEF DE IMPACTO	
Muy alto	2,6 a 3,0
Alto	2,1 a 2,5

Fuente: R.M. N 025-2020-MTC/01 - Plan de Continuidad Operativa del MTC

Como se observa aquellos riesgos con mayor impacto (alto o muy alto) son los más probables:

a) Sismo de gran magnitud y Tsunami en Lima y Callao.
b) Incendio en la sede principal del MTC.
c) Ataque informático.

Tabla No 12 - Estimación de Activos Críticos afectados según evento

No	Activo Crítico afectado	Sismo de gran magnitud y Tsunami en Lima y Callao	Incendio en la sede principal del MTC	Ataque informático.
01	Equipo Firewall WAN		X	X
02	Equipo Firewall Internet		X	X
03	Software Antivirus		X	X
04	Equipo Antispam		X	X
05	Equipo Filtro de Contenido Web		X	X
06	Switch Core (Fibra óptica)	X	X	
07	Switch de Distribución		X	
08	Routers (acceso a Internet)	X	X	X
09	Balanceador de Enlaces Internet		X	X
10	Balanceador de Aplicaciones		X	X
11	Servidores Blade	X	X	
12	Servidores Rack	X	X	
13	Chassis de Servidores	X	X	
14	Solución de Almacenamiento	X	X	
15	Software de Base de Datos POSTGRESQL			X
16	Software de Base de Datos MYSQL			X
17	Software de Base de Datos MS SQL			X
18	Software de Base de Datos Oracle			X
19	Software de Virtualización			X
20	Central Telefónica	X	X	
21	Equipos UPS	X	X	
22	Sistema de Extinción de Incendios		X	
23	Generador Eléctrico	X	X	
24	Sistema de Aire Acondicionado		X	

Fuente. Elaboración propia.

A continuación, se desarrollan los procedimientos de recuperación para los tres eventos desde el punto de vista informático y que afecten al equipamiento alojado en el Centro de Datos del MTC:

Jirón Zorritos 1203 – Lima - Perú
Central telefónica. (511) 615-7800
www.gob.pe/mtc

Formatos de Recuperación de Servicios TI

Código:	**FR - 17**
Activo crítico:	**Equipos UPS**
Evento:	**Terremoto / Sismo**

1. Plan de prevención

a) Descripción del evento

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

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

Infraestructura:
- Oficinas y/o Centro de Datos Principal

Recursos Humanos
- Personal de la entidad.

b) Objetivo

Establecer las acciones que se ejecutarán ante un sismo a fin de minimizar el tiempo de interrupción de las operaciones del Centro de Datos – MTC, sin exponer la seguridad de las personas.

c) Entorno

Este evento puede afectar las instalaciones de la Sede Central del Ministerio de Transportes y Comunicaciones y al Centro de Datos de la entidad, el cual se ubica al interior de la misma.

d) Personal Encargado

El Grupo Especializado de la Oficina de Infraestructura Tecnológica y Seguridad Informática (OITSI) de la Oficina General de Tecnología de la Información del MTC, es quien debe dar los lineamientos y dar cumplimiento a las Condiciones de Prevención de Riesgo del presente Plan.
Por su parte, el Equipo de Prevención de TI debe realizar las acciones descritas en el punto f).

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

f) Procesos Relacionados antes del evento
- Tener el inventario actualizado de los equipos UPS del Centro de Datos - MTC.

Código:	**FR - 17**
Activo crítico:	**Equipos UPS**
Evento:	**Terremoto / Sismo**

- Mantenimiento del orden y limpieza de la Sala de UPS y los ambientes del Centro de Datos – MTC.
- Inspecciones de seguridad internas y externas de los ambientes del Centro de Datos – MTC.
- Realización de simulacros internos en horarios que no afecten las actividades.

g) Acciones del Equipo de Prevención de TI
- Establecer, organizar, ejecutar y supervisar procedimientos de prueba y esfuerzo de los equipos UPS, así como la restauración de servicio de los mismos.
- Programar y supervisar el mantenimiento preventivo a los equipos UPS del Centro de Datos – MTC, en coordinación con el soporte técnico contratado.
- Realizar monitoreo continuo del estado de operación de los equipos UPS del Centro de Datos (nivel de carga de baterías, carga eléctrica, voltaje, frecuencia, estado del equipo, etc.).
- Verificar la operación de los equipos en paralelo – redundante.
- Tener a la mano los teléfonos de contacto del personal o soporte técnico del proveedor.

2. Plan de ejecución

a) Eventos que activan la contingencia
La contingencia se activará ante la ocurrencia de 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 de TI.

c) Personal Encargado
Equipo de Emergencia de TI.

d) Descripción de las actividades después de activar la contingencia
- Evacuar las oficinas de acuerdo a las disposiciones de los Brigadistas de Evacuación, utilizando las rutas establecidas durante los simulacros. (considerar las escaleras de emergencia, señalización de rutas, zonas de agrupamiento del personal, etc.), no se debe utilizar los ascensores.
- Verificar que el personal que labora en el área se encuentre bien.
- Alejarse de las lunas (ventanas) para evitar sufrir cortes por roturas y/o desprendimiento de trozos de vidrio.
- Evaluación de los daños ocasionados por el sismo sobre las instalaciones físicas, ambientes de trabajo, estanterías, instalaciones eléctricas, documentos, etc.
- Inventario general de documentación, personal, equipos, etc. y/o recursos afectados,indicando el estado de operatividad de los mismos.
- Limpieza de las áreas afectadas por el sismo. En todo momento se coordinará con el personal de mantenimiento del MTC, para las acciones que corresponda ser efectuadas por ellos.
- Verificar que el equipo UPS redundante haya asumido la totalidad de carga.
- Validar el estado y niveles de operación del equipo (nivel de carga de baterías, carga eléctrica, voltaje, frecuencia, estado del equipo, etc.).

Código:	**FR - 17**
Activo crítico:	**Equipos UPS**
Evento:	**Terremoto / Sismo**

e) Duración
- El proceso de evacuación del personal del área se realizará de modo calmado y demorar 5 minutos como máximo.
- La duración total del evento dependerá del grado del sismo, la probabilidad de réplicas o daños que pudiera afectar la infraestructura.

3. Plan de evaluación

a) Personal Encargado

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

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 son: manuales técnicos de instalación y operación de los equipos UPS del Centro de Datos – MTC.
- Establecer contacto con los proveedores clave y terceros para proporcionar instrucciones inmediatas y/o notificarles cualquier requisito de ayuda sobre la operación y/o recuperación de los equipos.
- Supervisar el progreso de las actividades de recuperación y operación de los equipos UPS del Centro de Datos – MTC y mantener informado al Grupo Especializado de Recuperación de TI.
- Validar la operatividad del equipo afectado y el restablecimiento de modo de operación en paralelo – redundante.
- Monitorear la operación de los equipos (nivel de desempeño y eventos de los equipos por un mínimo de cinco (05) horas).
- Coordinar bajo responsabilidad la ejecución de pruebas de esfuerzo y forzar la contingencia para validar si los tiempos de recuperación se mantienen.
- El Equipo Especializado de Recuperación TI, restaurará el espacio de trabajo para permitir que el personal crítico de la oficina pueda operar, para lo cual deberán:
  - Ejecutar los procedimientos de recuperación de la plataforma tecnológica.
  - Verificar que las aplicaciones críticas se hayan recuperado y estén funcionandocorrectamente.
  - Verificar que las funcionalidades de comunicación están funcionando correctamente.
  - Asegurar que el ambiente del área de trabajo, las aplicaciones y las telecomunicaciones están funcionando una vez concluida la emergencia o siniestro.
  - Si no es posible acceder remotamente equipo, conectarse vía consola o directamente con laptop y verificar su configuración.
  - Reiniciar equipo principal.
  - Contactar con el soporte técnico y/o fabricante para recibir apoyo en la solución del inconveniente presentado.

c) Mecanismos de Comprobación

El/La Coordinador/a de Continuidad de TI, presentará un informe al Grupo Especializado de Continuidad Operativa, explicando qué equipos y/o

Firmado digitalmente por: REQUENA CASTRO Jesus Nicanor FAU 20131379944 soft
Motivo: Doy V° B°
Fecha: 29/09/2022 11:09:45-0500

Código:	**FR - 17**
Activo crítico:	**Equipos UPS**
Evento:	**Terremoto / Sismo**

actividades y/o operaciones de tecnología de la información se han visto afectadas y cuáles son las acciones tomadas.

d) Desactivación del Plan de Contingencia
El/La Coordinador/a de Continuidad de TI desactivará el Plan de Contingencia Informático una vez que se haya tomado las acciones descritas en el presente Plan de Recuperación, mediante una comunicación electrónica al Grupo Especializado de Continuidad Operativa.

e) Proceso de Actualización
El proceso de actualización será en base al informe presentado por el/la Coordinador/a de Continuidad de TI, luego del cual se determinará las acciones a tomar.

Código:	**FR - 18**
Activo crítico:	**Sistema de extinción de incendios**
Evento:	**Terremoto / Sismo**

1. Plan de prevención

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

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

Infraestructura:
- Oficinas y/o Centro de Datos Principal

Recursos Humanos
- Personal de la entidad.

b) Objetivo
Establecer las acciones que se ejecutarán ante un sismo a fin de minimizar el tiempo de interrupción de las operaciones del Centro de Datos – MTC, sin exponer la seguridad de las personas.

c) Entorno
Este evento puede afectar las instalaciones de la Sede Central del Ministerio de Transportes y Comunicaciones y al Centro de Datos de la entidad, el cual se ubica al interior de la misma.

d) Personal Encargado
El Grupo Especializado de la Oficina de Infraestructura Tecnológica y Seguridad Informática (OITSI) de la Oficina General de Tecnología de la Información del MTC, es quien debe dar los lineamientos y dar cumplimiento a las Condiciones de Prevención de Riesgo del presente Plan.
Por su parte, el Equipo de Prevención de TI debe realizar las acciones descritas en el punto f).

Código:	**FR - 18**
Activo crítico:	**Sistema de extinción de incendios**
Evento:	**Terremoto / Sismo**

e) Condiciones de Prevención de Riesgo
- Inspecciones de seguridad realizadas periódicamente.
- Contar con un plan de mantenimiento del sistema de extinción de incendios del Centro de Datos – MTC.
- Realización de mantenimientos periódicos del sistema de extinción de incendios.
- Conformación de las brigadas de emergencia, y capacitarlas semestralmente.
- Mantenimiento de las áreas y ambientes 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.

f) Procesos Relacionados antes del evento
- Tener el inventario actualizado de los equipos que se albergan en el Centro de Datos - MTC.
- Mantenimiento del orden y limpieza de las Salas de Comunicaciones, Sala de Servidores, sala de UPS y los ambientes conexos al Centro de Datos – MTC.
- Inspecciones de seguridad internas y externas de los ambientes del Centro de Datos – MTC.
- Realización de simulacros internos en horarios que no afecten las actividades.

g) Acciones del Equipo de Prevención de TI
- Establecer, organizar, ejecutar y supervisar procedimientos de prueba y esfuerzo del sistema de extinción de incendios del Centro de Datos – MTC, así como la restauración de servicio de los mismos.
- Programar y supervisar el mantenimiento preventivo al sistema de extinción de incendios del Centro de Datos – MTC, en coordinación con el soporte técnico contratado.
- Realizar monitoreo continuo del estado de operación del sistema (nivel de carga de cilindro de agente extintor, lectura de alertas en panel, voltaje, frecuencia, estado del equipo, etc.).
- Verificación visual de componentes del sistema (panel central, sensores, ductos de aspiración, filtros, etc.).
- Tener a la mano los teléfonos de contacto del personal o soporte técnico del proveedor.

2. Plan de ejecución

a) Eventos que activan la contingencia
La contingencia se activará ante la ocurrencia de un sismo que afecte la operatividad del Centro de Datos – MTC.
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 de TI.

c) Personal Encargado
Equipo de Emergencia de TI.

d) Descripción de las actividades después de activar la contingencia

Código:	**FR - 18**
Activo crítico:	**Sistema de extinción de incendios**
Evento:	**Terremoto / Sismo**

- Validar la existencia real de un incidente al interior del Centro de Datos
- Evacuar los ambientes y oficinas de acuerdo a las disposiciones de los Brigadistas de Evacuación, utilizando las rutas establecidas durante los simulacros. (considerar las escaleras de emergencia, señalización de rutas, zonas de agrupamiento del personal, etc.), no se debe utilizar los ascensores.
- Verificar que el personal que labora en el área se encuentre bien.
- Evaluación de los daños ocasionados por algún incidente a raíz del sismo sobre las instalaciones físicas del centro de Datos (gabinetes, equipos, instalaciones eléctricas, etc.).
- Inventario general de la documentación, personal, equipos, etc. y/o recursos afectados,indicando el estado de operatividad de los mismos.
- Limpieza de las áreas afectadas por el sismo. En todo momento se coordinará con el personal de mantenimiento del MTC, para las acciones que corresponda ser efectuadas por ellos.
- Validar el estado y niveles de operación del equipo (nivel de carga de baterías, carga eléctrica, voltaje, frecuencia, estado del equipo, etc.).

e) Duración

- El proceso de evacuación del personal del área se realizará de modo calmado y demorar 5 minutos como máximo.

La duración total del evento dependerá del grado o magnitud del incendio, la probabilidad de reinicio y daños que pudiera afectar la infraestructura

3. Plan de evaluación

a) Personal Encargado

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

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 son: manuales técnicos de instalación y operación del sistema de extinción de incendios del Centro de Datos – MTC.
- Establecer contacto con los proveedores clave y terceros para proporcionar instrucciones inmediatas y/o notificarles cualquier requisito de ayuda sobre la operación y/o recuperación del sistema de extinción de incendio del Centro de Datos y su equipamiento.
- Supervisar el progreso de las actividades de recuperación y restauración de operatividad del sistema de extinción de incendios del Centro de Datos – MTC y mantener informado al Grupo Especializado de Recuperación de TI.
- Validar la operatividad del sistema de extinción de incendio del Centro de Datos y el restablecimiento de operación.
- Monitorear la operación del sistema de extinción de incendio del Centro de Datos por un mínimo de cinco (05) horas.
- Coordinar bajo responsabilidad la ejecución de pruebas de esfuerzo y operatividad para validar si los tiempos de recuperación se mantienen.
- El Equipo Especializado de Recuperación TI, restaurará el espacio de

Código:	**FR - 18**
Activo crítico:	**Sistema de extinción de incendios**
Evento:	**Terremoto / Sismo**

trabajo para permitir que el personal crítico de la oficina pueda operar, para lo cual deberán:

- Ejecutar los procedimientos de recuperación del sistema de extinción de incendio del Centro de Datos
- Asegurar que las áreas y ambientes del Centro de Datos – MTC, se encuentren limpios una vez concluido el sismo a fin de reiniciar las actividades.
- Coordinar bajo responsabilidad, el servicio de mantenimiento y recarga del sistema de extinción de incendios.
- Contactar con el soporte técnico y/o fabricante para recibir apoyo en la solución del inconveniente presentado.
- Validar la operatividad del sistema y estado de operación del sistema (nivel de carga de cilindro de agente extintor, verificación de alertas en panel, voltaje, frecuencia, estado del equipo, etc.).
- Documentar y registrar

c) Mecanismos de Comprobación

El/La Coordinador/a de Continuidad de TI, presentará un informe al Grupo Especializado de Continuidad Operativa, explicando qué áreas, ambientes y equipos de tecnología de la información se han visto afectadas y cuáles son las acciones tomadas.

d) Desactivación del Plan de Contingencia

El/La Coordinador/a de Continuidad de TI desactivará el Plan de Contingencia Informático una vez que se haya tomado las acciones descritas en el presente Plan de Recuperación, mediante una comunicación electrónica al Grupo Especializado de Continuidad Operativa.

e) Proceso de Actualización

El proceso de actualización será en base al informe presentado por el/la Coordinador/a de Continuidad de TI, luego del cual se determinará las acciones a tomar.

Firmado digitalmente por: REQUENA CASTRO Jesus Nicanor FAU 20131379944 soft
Motivo: Doy V° B°
Fecha: 29/09/2022 11:09:14-0500

Código:	**FR - 19**
Activo crítico:	**Sistema de aire acondicionado**
Evento:	**Terremoto / Sismo**

1. Plan de prevención

a) Descripción del evento

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

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

Infraestructura:

- Oficinas y/o Centro de Datos Principal

Recursos Humanos

- Personal de la entidad.

Jirón Zorritos 1203 – Lima - Perú
Central telefónica. (511) 615-7800
www.gob.pe/mtc

Código:	**FR - 19**
Activo crítico:	**Sistema de aire acondicionado**
Evento:	**Terremoto / Sismo**

b) Objetivo

Establecer las acciones que se ejecutarán ante un sismo a fin de minimizar el tiempo de interrupción de las operaciones del Centro de Datos – MTC, sin exponer la seguridad de las personas.

c) Entorno

Este evento puede afectar las instalaciones de la Sede Central del Ministerio de Transportes y Comunicaciones y al Centro de Datos de la entidad, el cual se ubica al interior de la misma.

d) Personal Encargado

El Grupo Especializado de la Oficina de Infraestructura Tecnológica y Seguridad Informática (OITSI) de la Oficina General de Tecnología de la Información del MTC, es quien debe dar los lineamientos y dar cumplimiento a las Condiciones de Prevención de Riesgo del presente Plan.
Por su parte, el Equipo de Prevención de TI debe realizar las acciones descritas en el punto f).

e) Condiciones de Prevención de Riesgo

- Inspecciones de seguridad realizadas periódicamente.
- Contar con un plan de mantenimiento del sistema de aire acondicionado del Centro de Datos – MTC.
- Realización de mantenimientos periódicos del sistema de aire acondicionado.
- Conformación de las brigadas de emergencia, y capacitarlas semestralmente.
- Mantenimiento de las áreas y ambientes 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.

f) Procesos Relacionados antes del evento

- Tener el inventario actualizado de los equipos que conforman el sistema de aire acondicionado del Centro de Datos - MTC.
- Mantenimiento del orden y limpieza de las Salas de Comunicaciones, Sala de Servidores, sala de UPS y los ambientes conexos al Centro de Datos – MTC.
- Inspecciones de seguridad internas y externas de los ambientes y equipos del sistema de aire acondicionado del Centro de Datos – MTC.
- Realización de simulacros internos en horarios que no afecten las actividades.

g) Acciones del Equipo de Prevención de TI

- Validar la operatividad del sistema de aire acondicionado del Centro de Datos – MTC, así como la restauración de servicio de los mismos.
- Programar y supervisar el mantenimiento preventivo al sistema de aire acondicionado del Centro de Datos – MTC, en coordinación con el soporte técnico contratado.
- Realizar monitoreo continuo del estado de operación del sistema (lectura de alertas en panel, voltaje, frecuencia, estado del equipo, etc.).
- Verificación visual del funcionamiento y estado de componentes del sistema (unidad condensadora y unidad evaporadora, etc.).

Código:	**FR - 19**
Activo crítico:	**Sistema de aire acondicionado**
Evento:	**Terremoto / Sismo**

- Tener a la mano los teléfonos de contacto del personal o soporte técnico del proveedor.

2. Plan de ejecución

a) Eventos que activan la contingencia

La contingencia se activará ante la ocurrencia de un sismo que afecte la operatividad del Centro de Datos – MTC.

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 de TI.

c) Personal Encargado

Equipo de Emergencia de TI.

d) Descripción de las actividades después de activar la contingencia

- Validar la existencia real de un incidente al interior del Centro de Datos
- Evacuar los ambientes y oficinas de acuerdo a las disposiciones de los Brigadistas de Evacuación, utilizando las rutas establecidas durante los simulacros. (considerar las escaleras de emergencia, señalización de rutas, zonas de agrupamiento del personal, etc.), no se debe utilizar los ascensores.
- Verificar que el personal que labora en el área se encuentre bien.
- Evaluación de los daños ocasionados por algún incidente a raíz del sismo sobre las instalaciones físicas del centro de Datos (gabinetes de unidades evaporadoras, unidades compresoras, etc.).
- Inventario general de la documentación, personal, equipos, etc. y/o recursos afectados,indicando el estado de operatividad de los mismos.
- Limpieza de las áreas afectadas por el sismo. En todo momento se coordinará con el personal de mantenimiento del MTC, para las acciones que corresponda ser efectuadas por ellos.
- Verificar la conmutación de estado de los equipos de estado Stanby – Running.
- Validar el estado y niveles de operación de los equipos (lectura de alertas en panel, voltaje, frecuencia, estado del equipo, etc.).

e) Duración

- El proceso de evacuación del personal del área se realizará de modo calmado y demorar 5 minutos como máximo.

La duración total del evento dependerá del grado o magnitud del incendio, la probabilidad de reinicio y daños que pudiera afectar la infraestructura

3. Plan de evaluación

a) Personal Encargado

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

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.

Código:	**FR - 19**
Activo crítico:	**Sistema de aire acondicionado**
Evento:	**Terremoto / Sismo**

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

- Verificar la disponibilidad de recursos para la contingencia como son: manuales técnicos de instalación y operación del sistema de aire acondicionado del Centro de Datos – MTC.
- Establecer contacto con los proveedores clave y terceros para proporcionar instrucciones inmediatas y/o notificarles cualquier requisito de ayuda sobre la operación y/o recuperación del sistema de aire acondicionado del Centro de Datos y su equipamiento.
- Supervisar el progreso de las actividades de recuperación y restauración de operatividad del sistema de aire acondicionado del Centro de Datos – MTC y mantener informado al Grupo Especializado de Recuperación de TI.
- Validar la operatividad del sistema de aire acondicionado del Centro de Datos y el restablecimiento de operación.
- Monitorear la operación del sistema de aire acondicionado del Centro de Datos por un mínimo de cinco (05) horas.
- Coordinar bajo responsabilidad la ejecución de pruebas de esfuerzo y operatividad para validar si los tiempos de recuperación se mantienen.
- El Equipo Especializado de Recuperación TI, restaurará el espacio de trabajo para permitir que el personal crítico de la oficina pueda operar, para lo cual deberán:
  - Ejecutar los procedimientos de recuperación del sistema de aire acondicionado del Centro de Datos
  - Asegurar que las áreas y ambientes del Centro de Datos – MTC, se encuentren limpios una vez concluido el sismo a fin de reiniciar las actividades.
  - Coordinar bajo responsabilidad, el servicio de mantenimiento y recarga del sistema de aire acondicionado del Centro de Datos - MTC.
  - Contactar con el soporte técnico y/o fabricante para recibir apoyo en la solución del inconveniente presentado.
  - Validar la operatividad y estado de operación del sistema (nivel de carga de gas refrigerante, verificación de alertas en panel, voltaje, frecuencia, estado del equipo, etc.).
  - Documentar y registrar

Firmado digitalmente por: REQUENA CASTRO Jesus Nicanor FAU 20131379944 soft
Motivo: Doy V° B°
Fecha: 29/09/2022 11:08:44-0500

c) <u>Mecanismos de Comprobación</u>

El/La Coordinador/a de Continuidad de TI, presentará un informe al Grupo Especializado de Continuidad Operativa, explicando qué áreas, ambientes y equipos de tecnología de la información se han visto afectadas y cuáles son las acciones tomadas.

d) <u>Desactivación del Plan de Contingencia</u>

El/La Coordinador/a de Continuidad de TI desactivará el Plan de Contingencia Informático una vez que se haya tomado las acciones descritas en el presente Plan de Recuperación, mediante una comunicación electrónica al Grupo Especializado de Continuidad Operativa.

e) <u>Proceso de Actualización</u>

El proceso de actualización será en base al informe presentado por el/la Coordinador/a de Continuidad de TI, luego del cual se determinará las acciones a tomar.

Código:	**FRS-20**
Activo crítico:	**Servidores Físicos o Virtuales**
Evento:	**Sismo / Terremoto**

1. Plan de prevención (antes)

- ✓ Es necesario tener acceso a los diagramas actualizados de la arquitectura de cada uno de los sistemas. Con estos diagramas se pueden hacer seguimiento del flujo de información, y visualizar en que puntos se está teniendo inconvenientes.
- ✓ "Levantamiento de Información de la Plataforma de Virtualización" esta información tiene como objetivo documentar la infraestructura existente a nivel de hardware y software donde se soportan los sistemas críticos del MTC, así como también especificar los procedimientos requeridos para proceder a un correcto apagado, desmontaje, movimiento (mudanza), montaje y encendido que permita garantizar la continuidad de los servicios. La OGTI cuenta con manuales y procedimientos, los cuales mencionamos a continuación:
  - Procedimiento de Cambio y Relevo de Turno en el Centro de Cómputo.
  - Procedimiento de Normas y Políticas de Gestión del Centro de Cómputo.
  - Procedimiento de Atención de Problemas en el Centro de Cómputo.
  - Procedimiento para el Respaldo de la Información en Medios Magnéticos.
  - Procedimiento para el Mantenimiento de Servidores en Producción.
  - Procedimiento para el Registro de Evento en los Servidores.
  - Procedimiento de Apago y Encendido de los Servidores del Centro de Cómputo.
  - Procedimiento Servicio de Traslado y Custodia de Medios Magnéticos. El tiempo promedio del traslado de medio magnético a la OGTI, de 04 horas.
  - Procedimiento Ejecución y Restauración de Backup.

2. Plan o procedimiento de Recuperación (durante)

- ✓ Dependiendo de los daños ocasionados, el comité de contingencia determinará el tiempo en que el personal acudirá a las instalaciones de la OGTI, en caso se encuentren fuera de la entidad, o si pueden retornar a sus puestos de trabajo en caso se encuentren dentro de la entidad.
- ✓ Verificar que los servidores no se encuentren dañados por el movimiento telúrico y que los sistemas informáticos críticos se encuentren operativos y si hay comunicación verificar remotamente los servicios, si no hay comunicaciones verificar in situ.
- ✓ Realizar el check list de los servicios afectados, backup, diagramas de arquitectura de sistemas críticos y hacer seguimiento del flujo de información, ver qué puntos está teniendo inconvenientes y realizar un listado del estado interno de los equipos en el Centro de Datos.

3. Plan de evaluación (después)

- ✓ Luego de validar que los servidores se encuentren operando y de no ser así, se procede a la instalación y configuración del sistema operativo, parches de seguridad y restauración de información para aquellos equipos que lo requieran.
- ✓ Realizar las configuraciones de las aplicaciones comprometidas y su conectividad con la base de datos de acuerdo a la arquitectura de aplicaciones.
- ✓ El equipo de operaciones de la OITSI, deberá realizar las pruebas de integridad de la data restaurada y el correcto acceso a los sistemas críticos restablecidos.
- ✓ Realizar informes de evaluación de daños ocasionados por el sismo y las medidas correctivas que se han asumido para proceder a la retroalimentación del plan.

Código:	**FRS-21**
Activo crítico:	**Equipos UPS**
Evento:	**Incendio**

1. Plan de prevención

a) Descripción del evento

Un Incendio, es un fuego de grandes proporciones que arde de forma fortuita o provocada y destruye cosas que no están destinadas a quemarse, pudiendo propagarse de modo agresivo y alcanzar niveles incontrolables.

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

Infraestructura:

a. Oficinas y/o Centro de Datos de la Entidad

Recursos Humanos

b. 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 del Centro de Datos – MTC, sin exponer la seguridad de las personas.

c) Entorno

Este evento puede afectar las instalaciones de la Sede Central del Ministerio de Transportes y Comunicaciones y al Centro de Datos de la Entidad, el cual se ubica al interior de la misma.

d) Personal Encargado

El Grupo Especializado de la Oficina de Infraestructura Tecnológica y Seguridad Informática (OITSI) de la Oficina General de Tecnología de la Información del MTC, es quien debe dar los lineamientos y dar cumplimiento a las Condiciones de Prevención de Riesgo del presente Plan.
Por su parte, el Equipo de Prevención de TI debe realizar las acciones descritas en el punto f).

e) Condiciones de Prevención de Riesgo

a. Inspecciones de seguridad realizadas periódicamente.
b. Contar con un plan de evacuación de las instalaciones del MTC, el mismo que debe ser de conocimiento de todo el personal que labora en el Centro de Datos – MTC y sus ambientes conexos.
c. Realización de prácticas de uso de extintores con la participación del personal que labora en el Centro de Datos – MTC y sus ambientes conexos.
d. Conformación de las brigadas de emergencia, y capacitarlas semestralmente.
e. Mantenimiento de las salidas libres de obstáculos.
f. Señalización de las zonas seguras y las salidas de emergencia.
g. Funcionamiento del sistema de extinción de incendios del Centro de Datos - MTC.
h. Definición de los puntos de reunión en caso de evacuación.

f) Procesos Relacionados antes del evento

a. Tener el inventario actualizado de los equipos UPS del Centro de Datos - MTC.

Código:	**FRS-21**
Activo crítico:	**Equipos UPS**
Evento:	**Incendio**

b. Mantenimiento del orden y limpieza de la Sala de UPS y los ambientes del Centro de Datos – MTC.
c. Inspecciones de seguridad internas y externas de los ambientes del Centro de Datos – MTC.
d. Realización de simulacros internos en horarios que no afecten las actividades.

g) Acciones del Equipo de Prevención de TI
a. Establecer, organizar, ejecutar y supervisar procedimientos de prueba y esfuerzo de los equipos UPS, así como la restauración de servicio de los mismos.
b. Programar y supervisar el mantenimiento preventivo a los equipos UPS del Centro de Datos – MTC, en coordinación con el soporte técnico contratado.
c. Realizar monitoreo continuo del estado de operación de los equipos UPS del Centro de Datos (nivel de carga de baterías, carga eléctrica, voltaje, frecuencia, estado del equipo, etc.).
d. Verificar la operación de los equipos en paralelo – redundante.
e. Tener a la mano los teléfonos de contacto del personal o soporte técnico del proveedor.

2. Plan de ejecución

a) Eventos que activan la contingencia
La contingencia se activará ante la ocurrencia de 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 de TI.

c) Personal Encargado
Equipo de Emergencia de TI.

d) Descripción de las actividades después de activar la contingencia
a. Evacuar las oficinas de acuerdo a las disposiciones de los Brigadistas de Evacuación, utilizando las rutas establecidas durante los simulacros. (considerar las escaleras de emergencia, señalización de rutas, zonas de agrupamiento del personal, etc.), no se debe utilizar los ascensores.
b. Verificar que el personal que labora en el área se encuentre bien.
c. Evaluación de los daños ocasionados por el Incendio sobre las instalaciones físicas, ambientes de trabajo, estanterías, instalaciones eléctricas, documentos, equipos, etc.
d. Inventario general de documentación, personal, equipos, etc. y/o recursos afectados,indicando el estado de operatividad de los mismos.
e. Limpieza de las áreas afectadas por el Incendio. En todo momento se coordinará con el personal de mantenimiento del MTC, para las acciones que corresponda ser efectuadas por ellos.
f. Verificar que los equipos UPS´s no se hayan visto comprometidos o afectados de modo que afecten su operación.
g. Validar el estado físico y lógico del equipo (nivel de carga de baterías, carga eléctrica, voltaje, frecuencia, estado del equipo, etc.).

e) Duración

Código:	**FRS-21**
Activo crítico:	**Equipos UPS**
Evento:	**Incendio**

h. El proceso de evacuación del personal del área se realizará de modo calmado y demorar 5 minutos como máximo.
i. La duración total del evento dependerá del grado o magnitud del Incendio, dificultad de control o probabilidad de reinicio y daños que pudiera afectar la infraestructura.

3. Plan de evaluación

a) Personal Encargado

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

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:

a. Verificar la disponibilidad de recursos para la contingencia como son: manuales técnicos de instalación y operación de los equipos UPS del Centro de Datos – MTC.
b. Establecer contacto con los proveedores clave y terceros para proporcionar instrucciones inmediatas y/o notificarles cualquier requisito de ayuda sobre la operación y/o recuperación de los equipos.
c. Supervisar el progreso de las actividades de recuperación y operación de los equipos UPS del Centro de Datos – MTC y mantener informado al Grupo Especializado de Recuperación de TI.
d. Validar la operatividad del equipo afectado y el restablecimiento de modo de operación en paralelo – redundante.
e. Monitorear la operación de los equipos (nivel de desempeño y eventos de los equipos por un mínimo de cinco (05) horas).
f. Coordinar bajo responsabilidad la ejecución de pruebas de esfuerzo y forzar la contingencia para validar si los tiempos de recuperación se mantienen.
g. El Equipo Especializado de Recuperación TI, restaurará el espacio de trabajo para permitir que el personal crítico de la oficina pueda operar, para lo cual deberán:
   - Ejecutar los procedimientos de recuperación de la plataforma tecnológica.
   - Verificar que las aplicaciones críticas se hayan recuperado y estén funcionando correctamente.
   - Verificar que las funcionalidades de comunicación están funcionando correctamente.
   - Asegurar que el ambiente del área de trabajo, las aplicaciones y las telecomunicaciones están funcionando una vez concluido el siniestro.
   - Si no es posible acceder remotamente a los equipos, conectarse vía consola o directamente con laptop y verificar su configuración.
   - Reiniciar los equipos de la Entidad.
   - Contactar con el soporte técnico y/o fabricante para recibir apoyo en la solución del inconveniente presentado.

c) Mecanismos de Comprobación

Firmado digitalmente por: REQUENA CASTRO Jesus Nicanor FAU 20131379944 soft
Motivo: Doy V° B°
Fecha: 29/09/2022 11:08:02-0500

Código:	**FRS-21**
Activo crítico:	**Equipos UPS**
Evento:	**Incendio**

El/La Coordinador/a de Continuidad de TI, presentará un informe al Grupo Especializado de Continuidad Operativa, explicando qué equipos y/o actividades y/o operaciones de tecnología de la información se han visto afectadas y cuáles son las acciones tomadas.

d) Desactivación del Plan de Contingencia
El/La Coordinador/a de Continuidad de TI desactivará el Plan de Contingencia Informático una vez que se haya tomado las acciones descritas en el presente Plan de Recuperación, mediante una comunicación electrónica al Grupo Especializado de Continuidad Operativa.

e) Proceso de Actualización
El proceso de actualización será en base al informe presentado por el/la Coordinador/a de Continuidad de TI, luego del cual se determinará las acciones a tomar.

Código:	**FRS-22**
Activo crítico:	**Sistema de extinción de incendios**
Evento:	**Incendio**

1. Plan de prevención

a) Descripción del evento
Un Incendio, es un fuego de grandes proporciones que arde de forma fortuita o provocada y destruye cosas que no están destinadas a quemarse, pudiendo propagarse de modo agresivo y alcanzar niveles incontrolables.

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

Infraestructura:
- Oficinas y/o Centro de Datos de la Entidad

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 del Centro de Datos – MTC, sin exponer la seguridad de las personas.

c) Entorno
Este evento puede afectar las instalaciones de la Sede Central del Ministerio de Transportes y Comunicaciones y al Centro de Datos de la entidad, el cual se ubica al interior de la misma.

d) Personal Encargado
El Grupo Especializado de la Oficina de Infraestructura Tecnológica y Seguridad Informática (OITSI) de la Oficina General de Tecnología de la Información del MTC, es quien debe dar los lineamientos y dar cumplimiento a las Condiciones de Prevención de Riesgo del presente Plan.

Código:	**FRS-22**
Activo crítico:	**Sistema de extinción de incendios**
Evento:	**Incendio**

Por su parte, el Equipo de Prevención de TI debe realizar las acciones descritas en el punto f).

e) Condiciones de Prevención de Riesgo
- Inspecciones de seguridad realizadas periódicamente.
- Contar con un plan de mantenimiento del sistema de extinción de incendios del Centro de Datos – MTC.
- Realización de mantenimientos periódicos del sistema de extinción de incendios.
- Conformación de las brigadas de emergencia, y capacitarlas semestralmente.
- Mantenimiento de las áreas y ambientes 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.

f) Procesos Relacionados antes del evento
- Tener el inventario actualizado de los equipos que se albergan en el Centro de Datos - MTC.
- Mantenimiento del orden y limpieza de las Salas de Comunicaciones, Sala de Servidores, sala de UPS y los ambientes conexos al Centro de Datos – MTC.
- Inspecciones de seguridad internas y externas de los ambientes del Centro de Datos – MTC.
- Realización de simulacros internos en horarios que no afecten las actividades.

g) Acciones del Equipo de Prevención de TI
- Establecer, organizar, ejecutar y supervisar procedimientos de prueba y esfuerzo del sistema de extinción de incendios del Centro de Datos – MTC, así como la restauración de servicio de los mismos.
- Programar y supervisar el mantenimiento preventivo al sistema de extinción de incendios del Centro de Datos – MTC, en coordinación con el soporte técnico contratado.
- Realizar monitoreo continuo del estado de operación del sistema (nivel de carga de cilindro de agente extintor, lectura de alertas en panel, voltaje, frecuencia, estado del equipo, etc.).
- Verificación visual de componentes del sistema (panel central, sensores, ductos de aspiración, filtros, etc.).
- Tener a la mano los teléfonos de contacto del personal o soporte técnico del proveedor.

Firmado digitalmente por: REQUENA CASTRO Jesus Nicanor FAU 20131379944 soft
Motivo: Doy V° B°
Fecha: 29/09/2022 11:07:43-0500

2. Plan de ejecución

a) Eventos que activan la contingencia

La contingencia se activará ante la ocurrencia de un Incendio que afecte la operatividad del Centro de Datos – MTC.
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 de TI.

c) Personal Encargado

Código:	**FRS-22**
Activo crítico:	**Sistema de extinción de incendios**
Evento:	**Incendio**

Equipo de Emergencia de TI.

d) Descripción de las actividades después de activar la contingencia

a. Validar la existencia real de un incidente al interior del Centro de Datos.
b. Evacuar los ambientes y oficinas de acuerdo a las disposiciones de los Brigadistas de Evacuación, utilizando las rutas establecidas durante los simulacros. (considerar las escaleras de emergencia, señalización de rutas, zonas de agrupamiento del personal, etc.), no se debe utilizar los ascensores.
c. Verificar que el personal que labora en el área se encuentre bien.
d. Verificar si el sistema de extensión de incendios se activó o no.
e. Evaluación de los daños ocasionados por el Incendio sobre las instalaciones físicas del centro de Datos (gabinetes, equipos, instalaciones eléctricas, etc.).
f. Inventario general de la documentación, personal, equipos, etc. y/o recursos afectados,indicando el estado de operatividad de los mismos.
g. Limpieza de las áreas afectadas por el Incendio. En todo momento se coordinará con el personal de mantenimiento del MTC, para las acciones que corresponda ser efectuadas por ellos.
h. Validar el estado y niveles de operación de los equipos afectados y del sistema contra incendios (nivel de carga de baterías, carga eléctrica, voltaje, frecuencia, estado del equipo, etc.).

e) Duración

i. El proceso de evacuación del personal del área se realizará de modo calmado y demorar 5 minutos como máximo.

La duración total del evento dependerá del grado o magnitud del incendio, la probabilidad de reinicio y daños que pudiera afectar la infraestructura.

Firmado digitalmente por: REQUENA CASTRO Jesus Nicanor FAU 20131379944 soft
Motivo: Doy V° B°
Fecha: 29/09/2022 11:07:30-0500

3. Plan de evaluación

a) Personal Encargado

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

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:

a. Verificar la disponibilidad de recursos para la contingencia como son: manuales técnicos de instalación y operación del sistema de extinción de incendios del Centro de Datos – MTC.
b. Establecer contacto con los proveedores clave y terceros para proporcionar instrucciones inmediatas y/o notificarles cualquier requisito de ayuda sobre la operación y/o recuperación del sistema de extinción de incendio del Centro de Datos y su equipamiento.
c. Supervisar el progreso de las actividades de recuperación y restauración de operatividad de los equipos afectados, así también del sistema de extinción de incendios del Centro de Datos – MTC y mantener informado al Grupo Especializado de Recuperación de TI.
d. Validar la operatividad del sistema de extinción de incendio del Centro de Datos y el restablecimiento de operación.

Código:	**FRS-22**
Activo crítico:	**Sistema de extinción de incendios**
Evento:	**Incendio**

e. Monitorear la operación del sistema de extinción de incendio del Centro de Datos por un mínimo de cinco (05) horas.
f. Coordinar bajo responsabilidad la ejecución de pruebas de esfuerzo y operatividad para validar si los tiempos de recuperación se mantienen.
g. El Equipo Especializado de Recuperación TI, restaurará el espacio de trabajo para permitir que el personal crítico de la oficina pueda operar, para lo cual deberán:

- Ejecutar los procedimientos de recuperación del sistema de extinción de incendio del Centro de Datos
- Asegurar que las áreas y ambientes del Centro de Datos – MTC, se encuentren limpios una vez concluido el Incendio a fin de reiniciar las actividades.
- Coordinar bajo responsabilidad, el servicio de mantenimiento y recarga del sistema de extinción de incendios.
- Contactar con el soporte técnico y/o fabricante para recibir apoyo en la solución del inconveniente presentado.
- Validar la operatividad del sistema y estado de operación del sistema (nivel de carga de cilindro de agente extintor, verificación de alertas en panel, voltaje, frecuencia, estado del equipo, etc.).
- Documentar y registrar

c) Mecanismos de Comprobación
El/La Coordinador/a de Continuidad de TI, presentará un informe al Grupo Especializado de Continuidad Operativa, explicando qué áreas, ambientes y equipos de tecnología de la información se han visto afectadas y cuáles son las acciones tomadas.

d) Desactivación del Plan de Contingencia
El/La Coordinador/a de Continuidad de TI desactivará el Plan de Contingencia Informático una vez que se haya tomado las acciones descritas en el presente Plan de Recuperación, mediante una comunicación electrónica al Grupo Especializado de Continuidad Operativa.

e) Proceso de Actualización
El proceso de actualización será en base al informe presentado por el/la Coordinador/a de Continuidad de TI, luego del cual se determinará las acciones a tomar.

Firmado digitalmente por: REQUENA CASTRO Jesus Nicanor FAU 20131379944 soft
Motivo: Doy V° B°
Fecha: 29/09/2022 11:06:46-0500

Código:	**FRS-23**
Activo crítico:	**Sistema de aire acondicionado**
Evento:	**Incendio**

1. Plan de prevención

a) Descripción del evento
Un Incendio, es un fuego de grandes proporciones que arde de forma fortuita o provocada y destruye cosas que no están destinadas a quemarse, pudiendo propagarse de modo agresivo y alcanzar niveles incontrolables.

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

Código:	**FRS-23**
Activo crítico:	**Sistema de aire acondicionado**
Evento:	**Incendio**

Infraestructura:
- Oficinas y/o Centro de Datos De la Entidad

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 del Centro de Datos – MTC, sin exponer la seguridad de las personas.

c) Entorno
Este evento puede afectar las instalaciones de la Sede Central del Ministerio de Transportes y Comunicaciones y al Centro de Datos de la entidad, el cual se ubica al interior de la misma.

d) Personal Encargado
El Grupo Especializado de la Oficina de Infraestructura Tecnológica y Seguridad Informática (OITSI) de la Oficina General de Tecnología de la Información del MTC, es quien debe dar los lineamientos y dar cumplimiento a las Condiciones de Prevención de Riesgo del presente Plan.
Por su parte, el Equipo de Prevención de TI debe realizar las acciones descritas en el punto f).

e) Condiciones de Prevención de Riesgo
- Inspecciones de seguridad realizadas periódicamente.
- Contar con un plan de mantenimiento del sistema de aire acondicionado del Centro de Datos – MTC.
- Realización de mantenimientos periódicos del sistema de aire acondicionado.
- Conformación de las brigadas de emergencia, y capacitarlas semestralmente.
- Mantenimiento de las áreas y ambientes 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.

f) Procesos Relacionados antes del evento
- Tener el inventario actualizado de los equipos que conforman el sistema de aire acondicionado del Centro de Datos - MTC.
- Mantenimiento del orden y limpieza de las Salas de Comunicaciones, Sala de Servidores, sala de UPS y los ambientes conexos al Centro de Datos – MTC.
- Inspecciones de seguridad internas y externas de los ambientes y equipos del sistema de aire acondicionado del Centro de Datos – MTC.
- Realización de simulacros internos en horarios que no afecten las actividades.

g) Acciones del Equipo de Prevención de TI
- Validar la operatividad del sistema de aire acondicionado del Centro de Datos – MTC, así como la restauración de servicio de los mismos.
- Programar y supervisar el mantenimiento preventivo al sistema de aire

Código:	**FRS-23**
Activo crítico:	**Sistema de aire acondicionado**
Evento:	**Incendio**

acondicionado del Centro de Datos – MTC, en coordinación con el soporte técnico contratado.

- Realizar monitoreo continuo del estado de operación del sistema (lectura de alertas en panel, voltaje, frecuencia, estado del equipo, etc.).
- Verificación visual del funcionamiento y estado de componentes del sistema (unidad condensadora y unidad evaporadora, etc.).
- Tener a la mano los teléfonos de contacto del personal o soporte técnico del proveedor.

2. Plan de ejecución

a) Eventos que activan la contingencia

La contingencia se activará ante la ocurrencia de un Incendio que afecte la operatividad del Centro de Datos – MTC.

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 de TI.

c) Personal Encargado

Equipo de Emergencia de TI.

d) Descripción de las actividades después de activar la contingencia

h. Validar la existencia real de un incidente al interior del Centro de Datos
i. Evacuar los ambientes y oficinas de acuerdo a las disposiciones de los Brigadistas de Evacuación, utilizando las rutas establecidas durante los simulacros. (considerar las escaleras de emergencia, señalización de rutas, zonas de agrupamiento del personal, etc.), no se debe utilizar los ascensores.
j. Verificar que el personal que labora en el área se encuentre bien.
k. Evaluación de los daños ocasionados por algún incidente a raíz del Incendio sobre las instalaciones físicas del centro de Datos (gabinetes de unidades evaporadoras, unidades compresoras, etc.).
l. Inventario general de la documentación, personal, equipos, etc. y/o recursos afectados, indicando el estado de operatividad de los mismos.
m. Limpieza de las áreas afectadas por el Incendio. En todo momento se coordinará con el personal de mantenimiento del MTC, para las acciones que corresponda ser efectuadas por ellos.
n. Verificar la conmutación de estado de los equipos de estado Stanby – Running.
o. Validar el estado y niveles de operación de los equipos (lectura de alertas en panel, voltaje, frecuencia, estado del equipo, etc.).

e) Duración

p. El proceso de evacuación del personal del área se realizará de modo calmado y demorar 5 minutos como máximo.

La duración total del evento dependerá del grado o magnitud del incendio, la probabilidad de reinicio y daños que pudiera afectar la infraestructura

3. Plan de evaluación

1. Personal Encargado

Firmado digitalmente por: REQUENA CASTRO Jesus Nicanor FAU 20131379944 soft
Motivo: Doy V° B°
Fecha: 29/09/2022 11:06:11-0500

Código:	**FRS-23**
Activo crítico:	**Sistema de aire acondicionado**
Evento:	**Incendio**

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

2. 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:

q. Verificar la disponibilidad de recursos para la contingencia como son: manuales técnicos de instalación y operación del sistema de aire acondicionado del Centro de Datos – MTC.
r. Establecer contacto con los proveedores clave y terceros para proporcionar instrucciones inmediatas y/o notificarles cualquier requisito de ayuda sobre la operación y/o recuperación del sistema de aire acondicionado del Centro de Datos y su equipamiento.
s. Supervisar el progreso de las actividades de recuperación y restauración de operatividad del sistema de aire acondicionado del Centro de Datos – MTC y mantener informado al Grupo Especializado de Recuperación de TI.
t. Validar la operatividad del sistema de aire acondicionado del Centro de Datos y el restablecimiento de operación.
u. Monitorear la operación del sistema de aire acondicionado del Centro de Datos por un mínimo de cinco (05) horas).
v. Coordinar bajo responsabilidad la ejecución de pruebas de esfuerzo y operatividad para validar si los tiempos de recuperación se mantienen.
w. El Equipo Especializado de Recuperación TI, restaurará el espacio de trabajo para permitir que el personal crítico de la oficina pueda operar, para lo cual deberán:

- Ejecutar los procedimientos de recuperación del sistema de aire acondicionado del Centro de Datos
- Asegurar que las áreas y ambientes del Centro de Datos – MTC, se encuentren limpios una vez concluido el Incendio a fin de reiniciar las actividades.
- Coordinar bajo responsabilidad, el servicio de mantenimiento preventivo o correctivo y recarga del sistema de aire acondicionado del Centro de Datos - MTC.
- Contactar con el soporte técnico y/o fabricante para recibir apoyo en la solución del inconveniente presentado.
- Validar la operatividad y estado de operación del sistema (nivel de carga de gas refrigerante, verificación de alertas en panel, voltaje, frecuencia, estado del equipo, etc.).
- Documentar y registrar

3. Mecanismos de Comprobación

El/La Coordinador/a de Continuidad de TI, presentará un informe al Grupo Especializado de Continuidad Operativa, explicando qué áreas, ambientes y equipos de tecnología de la información se han visto afectadas y cuáles son las acciones tomadas.

4. Desactivación del Plan de Contingencia

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

Firmado digitalmente por: REQUENA CASTRO Jesus Nicanor FAU 20131379944 soft
Motivo: Doy V° B°
Fecha: 29/09/2022 11:05:59-0500

Código:	**FRS-23**
Activo crítico:	**Sistema de aire acondicionado**
Evento:	**Incendio**

Informático una vez que se haya tomado las acciones descritas en el presente Plan de Recuperación, mediante una comunicación electrónica al Grupo Especializado de Continuidad Operativa.

5. Proceso de Actualización

El proceso de actualización será en base al informe presentado por el/la Coordinador/a de Continuidad de TI, luego del cual se determinará las acciones a tomar.

Código:	**FRS – 24**
Activo crítico:	**Firewall Perimetral**
Evento:	**Delito Informático**

1. PLAN DE PREVENCIÓN

a) Descripción del evento

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

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

b) Objetivo

Restaurar la operatividad del equipo de seguridad informática después de eliminar los malware o contrarrestar el ataque cibernético.

c) Entorno

Este evento se puede dar en cualquier equipo de seguridad informática que no cuente con firmas actualizadas de los módulos de prevención de amenazas.

d) Personal Encargado

El Equipo de Seguridad Informática es el responsable del correcto funcionamiento de los equipos de la plataforma de seguridad TI.

e) Condiciones de Prevención de Riesgo

- Establecimiento de políticas de seguridad para prevenir intrusiones o accesos no autorizados.
- Ejecución de ataques de Hacking Ético por terceros especializados.
- Mantener actualizada las licencias de los módulos de seguridad y contar con las últimas versiones recomendadas por el fabricante.

2. PLAN DE EJECUCIÓN

a) Eventos que activan la Contingencia

- Mensajes de error durante la ejecución de compilado de la base de datos para guardar cambios.
- Perdida de acceso a la consola de gestión.
- Lentitud en el acceso a la consola de gestión.
- Degradación del rendimiento del equipo.

Código:	**FRS – 24**
Activo crítico:	**Firewall Perimetral**
Evento:	**Delito Informático**

b) Personal que autoriza la contingencia

El/La Coordinador/a de Continuidad de TI y el/la Oficial de Seguridad de la Información pueden activar la contingencia.

Personal Encargado

Equipo Especializado de Seguridad Informática.

c) Descripción de las actividades después de activar la contingencia

- Denegar demasiadas conexiones simultáneas con la misma IP de origen.
- Rastrear de ser necesario el origen de la infección u ataque (archivo infectado, correo electrónico, hacking, etc.)
- Guardar la muestra del virus detectado y remitirlo al proveedor del antivirus utilizado. En el caso de hacking a aplicaciones, se debe guardar el archivo modificado.
- Eliminar el agente causante de la infección, es decir, remover el malware/virus del sistema.

3. PLAN DE RECUPERACIÓN

a) Personal Encargado

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

b) Descripción de actividades

Se informará a el/la Director/a de OGTI del MTC el tipo de malware/virus, o tipo de ataque encontrado y el procedimiento usado para removerlo.

Estas actividades deben contemplar como mínimo:

a. Realización de la restauración de la base de datos con la última copia de seguridad disponible (Restore).
b. Efectuar las pruebas necesarias de acceso a los servicios.
c. Probar el funcionamiento del HA.
d. Comunicar el restablecimiento del servicio.
e. Si no es posible acceder remotamente equipo, conectarse vía consola o directamente con laptop y verificar su configuración.
f. Reiniciar equipo principal.
g. Contactar con el soporte técnico y/o fabricante para recibir apoyo en la solución del inconveniente presentado.

En función a esto, el/la Oficial de Seguridad de la Información, tomará las medidas preventivas del caso enviando una alerta vía correo al personal del MTC.
El evento será evaluado y registrado de ser necesario en el formato de ocurrencia de incidentes de seguridad informática.

c) Mecanismos de Comprobación

Se llenará el formato de incidentes de seguridad de la información y se informará al Comité de Gestión de Seguridad de la Información.
El personal de Técnico de Soporte y/o Especialista en Redes y Comunicaciones, según sea el caso, presentará un informe a el/la Director/a de OGTI, explicando que parte del servicio u operaciones se han visto afectadas, y cuáles son las acciones

Firmado digitalmente por: REQUENA CASTRO Jesus Nicanor FAU 20131379944 soft
Motivo: Doy V° B°
Fecha: 29/09/2022 11:05:32-0500

Código:	**FRS – 24**
Activo crítico:	**Firewall Perimetral**
Evento:	**Delito Informático**

tomadas.

d) Desactivación del plan de Contingencia

Con el aviso de el/la Coordinador/a de Continuidad de TI del MTC se desactivará el presente plan.

Código:	**FRS – 25**
Activo crítico:	**Firewall WAN**
Evento:	**Delito Informático**

1. PLAN DE PREVENCIÓN

a) Descripción del evento

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

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

b) Objetivo

Restaurar la operatividad del equipo de seguridad informática después de eliminar los malware o contrarrestar el ataque cibernético.

c) Entorno

Este evento se puede dar en cualquier equipo de seguridad informática que no cuente con firmas actualizadas de los módulos de prevención de amenazas.

d) Personal Encargado

El Equipo de Seguridad Informática es el responsable del correcto funcionamiento de los equipos de la plataforma de seguridad TI.

e) Condiciones de Prevención de Riesgo

- Establecimiento de políticas de seguridad para prevenir intrusiones o accesos no autorizados.
- Ejecución de ataques de Hacking Ético por terceros especializados.
- Mantener actualizada las licencias de los módulos de seguridad y contar con las últimas versiones recomendadas por el fabricante.

2. PLAN DE EJECUCIÓN

a) Eventos que activan la Contingencia

- Mensajes de error durante la ejecución de compilado de la base de datos para guardar cambios.
- Perdida de acceso a la consola de gestión.
- Lentitud en el acceso a la consola de gestión.
- Degradación del rendimiento del equipo.

b) Personal que autoriza la contingencia

Código:	**FRS – 25**
Activo crítico:	**Firewall WAN**
Evento:	**Delito Informático**

El/La Coordinador/a de Continuidad de TI y el/la Oficial de Seguridad de la Información puedenactivar la contingencia.

c) Personal Encargado
Equipo Especializado de Seguridad Informática.

d) Descripción de las actividades después de activar la contingencia
- Denegar demasiadas conexiones simultáneas con la misma IP de origen.
- Rastrear de ser necesario el origen de la infección u ataque (archivo infectado, correo electrónico, hacking, etc.)
- Guardar la muestra del virus detectado y remitirlo al proveedor del antivirus utilizado. En el caso de hacking a aplicaciones, se debe guardar el archivo modificado.
- Eliminar el agente causante de la infección, es decir, remover el malware/virus del sistema.

3. PLAN DE RECUPERACIÓN

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

b) Descripción de actividades
Se informará a el/la Director/a de OGTI del MTC el tipo de malware/virus, o tipo de ataqueencontrado y el procedimiento usado para removerlo.
Estas actividades deben contemplar como mínimo:
- Realización de la restauración de la base de datos con la última copia de seguridad disponible(Restore).
- Si no es posible acceder remotamente equipo, conectarse vía consola o directamente con laptop y verificar su configuración.
- Efectuar las pruebas necesarias de acceso a los servicios.
- Comunicar el restablecimiento del servicio.

En función a esto, el/la Oficial de Seguridad de la Información, tomará las medidas preventivasdel caso enviando una alerta vía correo al personal del MTC.
El evento será evaluado y registrado de ser necesario en el formato de ocurrencia de incidentesde seguridad informática.

a) Mecanismos de Comprobación
Se llenará el formato de incidentes de seguridad de la información y se informará al Comité de Gestión de Seguridad de la Información.
El personal de Técnico de Soporte y/o Especialista en Redes y Comunicaciones, según sea el caso,presentará un informe a el/la Director/a de OGTI, explicando que parte del servicio u operacionesse han visto afectadas, y cuáles son las acciones tomadas.

b) Desactivación del plan de Contingencia
Con el aviso de el/la Coordinador/a de Continuidad de TI del MTC se desactivará el presente plan.

Firmado digitalmente por: REQUENA CASTRO Jesus Nicanor FAU 20131379944 soft
Motivo: Doy V° B°
Fecha: 29/09/2022 11:05:09-0500

Código:	**FRS – 26**
Activo crítico:	**Filtro de Contenido Web**
Evento:	**Delito Informático**

1. PLAN DE PREVENCIÓN

a) Descripción del evento

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

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

b) Objetivo

Restaurar la operatividad del equipo de seguridad informática después de eliminar los malware o contrarrestar el ataque cibernético.

c) Entorno

Este evento se puede dar en cualquier equipo de seguridad informática que no cuente con licencia actualizada de los módulos de seguridad.

d) Personal Encargado

El Equipo de Seguridad Informática es el responsable del correcto funcionamiento de los equipos de la plataforma de seguridad TI.

e) Condiciones de Prevención de Riesgo

- Establecimiento de políticas de seguridad para prevenir intrusiones o accesos no autorizados.
- Ejecución de ataques de Hacking Ético por terceros especializados.
- Mantener actualizada las licencias de los módulos de seguridad y contar con las últimas versiones recomendadas por el fabricante.

2. PLAN DE EJECUCIÓN

a) Eventos que activan la Contingencia

- Mensajes de error durante la ejecución de compilado de la base de datos para guardar cambios.
- Perdida de acceso a la consola de gestión.
- Lentitud en el acceso a la consola de gestión.
- Degradación del rendimiento del equipo.
- Imposibilidad de navegación en Internet.

b) Personal que autoriza la contingencia

El/La Coordinador/a de Continuidad de TI y el/la Oficial de Seguridad de la Información puedenactivar la contingencia.

c) Personal Encargado

Equipo Especializado de Seguridad Informática.

d) Descripción de las actividades después de activar la contingencia

- Denegar demasiadas conexiones simultáneas con la misma IP de origen.
- Rastrear de ser necesario el origen de la infección u ataque (archivo infectado, correo

Código:	**FRS – 26**
Activo crítico:	**Filtro de Contenido Web**
Evento:	**Delito Informático**

electrónico, hacking, etc.)
- Guardar la muestra del virus detectado y remitirlo al proveedor del antivirus utilizado. En el caso de hacking a aplicaciones, se debe guardar el archivo modificado.
- Eliminar el agente causante de la infección, es decir, remover el malware/virus del sistema.

3. PLAN DE RECUPERACIÓN

a) Personal Encargado

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

b) Descripción de actividades

Se informará a el/la Director/a de OGTI del MTC el tipo de malware/virus, o tipo de ataque encontrado y el procedimiento usado para removerlo.
Estas actividades deben contemplar como mínimo:

- Realización de la restauración de la base de datos con la última copia de seguridad disponible(Restore).
- Efectuar las pruebas necesarias de acceso a los servicios.
- Probar el funcionamiento del equipo.

e) Comunicar el restablecimiento del servicio

f) Si no es posible acceder remotamente equipo, conectarse vía consola o directamente con laptop y verificar su configuración.

g) Contactar con el soporte técnico y/o fabricante para recibir apoyo en la solución del inconveniente presentado.

Firmado digitalmente por: REQUENA CASTRO Jesus Nicanor FAU 20131379944 soft
Motivo: Doy V° B°
Fecha: 29/09/2022 11:03:44-0500

En función a esto, el/la Oficial de Seguridad de la Información, tomará las medidas preventivasdel caso enviando una alerta vía correo al personal del MTC.
El evento será evaluado y registrado de ser necesario en el formato de ocurrencia de incidentesde seguridad informática.

b) Mecanismos de Comprobación

Se llenará el formato de incidentes de seguridad de la información y se informará al Comité de Gestión de Seguridad de la Información.
El personal de Técnico de Soporte y/o Especialista en Redes y Comunicaciones, según sea el caso,presentará un informe a el/la Director/a de OGTI, explicando que parte del servicio u operacionesse han visto afectadas, y cuáles son las acciones tomadas.

c) Desactivación del plan de Contingencia

Con el aviso de el/la Coordinador/a de Continuidad de TI del MTC se desactivará el presente plan.

Código:	**FRS – 27**
Activo crítico:	**Antispam**
Evento:	**Delito Informático**

1. PLAN DE PREVENCIÓN

a) Descripción del evento

Jirón Zorritos 1203 – Lima - Perú
Central telefónica. (511) 615-7800
www.gob.pe/mtc

Código:	**FRS – 27**
Activo crítico:	**Antispam**
Evento:	**Delito Informático**

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

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

b) Objetivo
Restaurar la operatividad del equipo de seguridad informática después de eliminar los malware o contrarrestar el ataque cibernético.

c) Entorno
Este evento se puede dar en cualquier equipo de seguridad informática que no cuente con firmas actualizadas de los módulos de prevención de amenazas.

d) Personal Encargado
El Equipo de Seguridad Informática es el responsable del correcto funcionamiento de los equipos de la plataforma de seguridad TI.

e) Condiciones de Prevención de Riesgo
- Establecimiento de políticas de seguridad para prevenir intrusiones o accesos no autorizados.
- Ejecución de ataques de Hacking Ético por terceros especializados.
- Mantener actualizada las licencias de los módulos de seguridad y contar con las últimas versiones recomendadas por el fabricante.

2. PLAN DE EJECUCIÓN

a) Eventos que activan la Contingencia
- Mensajes de error durante la ejecución del proceso de guardar cambios.
- Perdida de acceso a la consola de gestión.
- Lentitud en el acceso a la consola de gestión.
- Degradación del rendimiento del equipo.
- Imposibilidad de recibir correos.

b) Personal que autoriza la contingencia
El/La Coordinador/a de Continuidad de TI y el/la Oficial de Seguridad de la Información puedenactivar la contingencia.

c) Personal Encargado
Equipo Especializado de Seguridad Informática.

d) Descripción de las actividades después de activar la contingencia
- Denegar demasiadas conexiones simultáneas con la misma IP de origen.
- Rastrear de ser necesario el origen de la infección u ataque (archivo infectado, correo electrónico, hacking, etc.)
- Guardar la muestra del virus detectado y remitirlo al proveedor del antivirus utilizado. En el caso de hacking a aplicaciones, se debe guardar el archivo modificado.
- Eliminar el agente causante de la infección, es decir, remover el malware/virus del sistema.

Código:	**FRS – 27**
Activo crítico:	**Antispam**
Evento:	**Delito Informático**

3. PLAN DE RECUPERACIÓN

a) Personal Encargado

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

b) Descripción de actividades

Se informará a el/la Director/a de OGTI del MTC el tipo de malware/virus, o tipo de ataque encontrado y el procedimiento usado para removerlo.
Estas actividades deben contemplar como mínimo:

- Realización de la restauración de la base de datos con la última copia de seguridad disponible(Restore).
- Efectuar las pruebas necesarias de acceso a los servicios.
- Probar el funcionamiento del HA.

h) Comunicar el restablecimiento del servicio

- Si no es posible acceder remotamente equipo, conectarse vía consola o directamente con laptop y verificar su configuración.
- Reiniciar equipo principal.
- Contactar con el soporte técnico y/o fabricante para recibir apoyo en la solución del inconveniente presentado.

Firmado digitalmente por: REQUENA CASTRO Jesus Nicanor FAU 20131379944 soft
Motivo: Doy V° B°
Fecha: 29/09/2022 11:03:21-0500

En función a esto, el/la Oficial de Seguridad de la Información, tomará las medidas preventivasdel caso enviando una alerta vía correo al personal del MTC.
El evento será evaluado y registrado de ser necesario en el formato de ocurrencia de incidentesde seguridad informática.

c) Mecanismos de Comprobación

Se llenará el formato de incidentes de seguridad de la información y se informará al Comité de Gestión de Seguridad de la Información.
El personal de Técnico de Soporte y/o Especialista en Redes y Comunicaciones, según sea el caso,presentará un informe a el/la Director/a de OGTI, explicando que parte del servicio u operacionesse han visto afectadas, y cuáles son las acciones tomadas.

d) Desactivación del plan de Contingencia

Con el aviso de el/la Coordinador/a de Continuidad de TI del MTC se desactivará el presente plan.

Jirón Zorritos 1203 – Lima - Perú
Central telefónica. (511) 615-7800
www.gob.pe/mtc

ANEXO 01 - Identificación de Activos Críticos del MTC

Servicios o aplicaciones críticas del MTC								
Ítem	**Descripción**	**Funciones críticas**	**Oficina o Dirección Usuaria**	**Responsable OGTI**	**Usuario final**	**Servidor APP**	**Repositorio**	**Servidor BD**
1	Sistema Nacional de Conductores - SNC	Emisión de licencias de conducir	DGPPT	Director ODTD / Jefe Proyectos OGTI	Ciudadanos a nivel nacional	Windows Server IIS 10 + Java	MS Team Foundation	Oracle 11g
2	Sistema Nacional de Sanciones - SNS	Registrar, procesar y controlar toda la información relacionada con las sanciones impuestas a los conductores/administrados que infrinjan las normas de tránsito.	DGATR	Director ODTD / Jefe Proyectos OGTI	SUNAT, entre otras entidades publicas	Windows Server 2012	MS Team Foundation	Oracle 11g
3	Sistema de Mesa de Partes Virtual - MPV	Administrado presenta documentos ante este ministerio. Registro de solicitudes TUPA y no TUPA de los administrados. Subsanación de observaciones a las solicitudes. Seguimiento del estado de la solicitud.	OACGD	Director ODTD / Jefe Proyectos OGTI	Ciudadanos a nivel nacional	Windows Server 2012 IIS 10	Alfresco	Oracle 11g

Firmado digitalmente por: REQUENA CASTRO Jesus Nicanor FAU 20131379944 soft
Motivo: Doy V° B°
Fecha: 29/09/2022 11:03:13-0500

Jirón Zorritos 1203 – Lima - Perú
Central telefónica. (511) 615-7800
www.gob.pe/mtc

Servicios o aplicaciones críticas del MTC								
Ítem	**Descripción**	**Funciones críticas**	**Oficina o Dirección Usuaria**	**Responsable OGTI**	**Usuario final**	**Servidor APP**	**Repositorio**	**Servidor BD**
4	Casilla Electrónica MTC	Notificación al administrado mediante una plataforma electrónica	OACGD	Director ODTD / Jefe Proyectos OGTI	Ciudadanos a nivel nacional	Windows Server 2012 IIS 10	MS Team Foundation	MS SQL Server
5	TUPA Digital	Administrados puedan registrar sus requisitos para realizar los procedimientos administrativos del TUPA. Registro de solicitudes de procedimientos TUPA. Consulta de estado de trámites del ADMINISTRADO	OACGD /OGPP-ODM	Director ODTD / Jefe Proyectos OGTI	Ciudadanos a nivel nacional	Servidores con Windows Server 2008/ 2012/2016 (IIS)	MS Team Foundation	Oracle 11g
6	Sistema de Trámite Documentario - STD	Recepción, registro, derivación, seguimiento y control de los documentos internos que se transmiten en el Ministerio	OACGD	Director ODTD / Jefe Proyectos OGTI	Personal del MTC	Red Hat Enterprise Linux 6 JBOSS	Alfresco + Share Point	Oracle 11g
7	Registro Nacional de Transporte Terrestre - RENAT	Registro de autorizaciones de transportista, habilitación de vehículos de transporte terrestre e impresión de constancias y certificados de habilitación.	DGATR	Director ODTD / Jefe Proyectos OGTI	Ciudadanos a nivel nacional	Windows Server 2012 R2	MS Team Foundation	Oracle 11g
8	Correo Electrónico	Envió y recepción de correos electrónicos entre los funcionarios del MTC y con el exterior	OGTI	Director OITSI	Personal del MTC	MS Exchange 2013	MS Exchange 2013	---

Jirón Zorritos 1203 – Lima - Perú
Central telefónica. (511) 615-7800
www.gob.pe/mtc

Servicios o aplicaciones críticas del MTC								
Ítem	**Descripción**	**Funciones críticas**	**Oficina o Dirección Usuaria**	**Responsable OGTI**	**Usuario final**	**Servidor APP**	**Repositorio**	**Servidor BD**
9	SIGA WEB	Soporte administrativo a la gestión de personal y logística del MTC	OGA	Director ODTD / Jefe Proyectos OGTI	Personal del MTC	Windows Server 2008	https://sigaweb.mtc.gob.pe	Oracle 11g
10	SIGA- Personal	Soporte administrativo a la gestión Administrativa de Recursos Humanos permite la emisión de planillas de pagos de Pensionista, Nombrados y CAS	OGA	Director ODTD / Jefe Proyectos OGTI	Personal del MTC	Cliente Servidor	No aplica	Oracle 11g
11	SIGA- Finanzas	Soporte administrativo a la gestión de ingreso y egresos del MTC, permite el registro de ingresos y emite documentos de pago electrónico.	OGA	Director ODTD / Jefe Proyectos OGTI	Personal del MTC	Cliente Servidor	No aplica	Oracle 11g
12	Ellipse	consultas y reportes de los expedientes de los servicios privados, radiodifusión y públicos, certificados de internamiento de equipos, homologación, reportes estadísticos de rendimiento laboral, notificaciones y finalización de documentos	DGAT	Director ODTD / Jefe Proyectos OGTI	Viceministerio de Comunicaciones - VMC	Windows Server 2003	No aplica	Oracle Solaris SPARC
13	Sistema Integrado de Información DTA	Aplicativo que se encarga del control del parque naviero en el Perú, supervisa los permisos de póliza, fletamentos, control de rutas Empresas Navieras.	DTA	Director ODTD / Jefe Proyectos OGTI	VMT	Linux Red Hat / wildfly-10.1.0.Final	MS Team Foundation	Oracle 11g

Firmado digitalmente por: REQUENA CASTRO Jesus Nicanor FAU 20131379844 soft
Motivo: Doy V° B°
Fecha: 29/09/2022 11:02:56-0500

Jirón Zorritos 1203 – Lima - Perú
Central telefónica. (511) 615-7800
www.gob.pe/mtc

Servicios o aplicaciones críticas del MTC								
Ítem	**Descripción**	**Funciones críticas**	**Oficina o Dirección Usuaria**	**Responsable OGTI**	**Usuario final**	**Servidor APP**	**Repositorio**	**Servidor BD**
14	Sistema Integrado de la Dirección General de Aeronáutica Civil	Permite la gestión de empresas aéreas del rubro Aeronáutica, gestión de Licencias para personal aeronáutico, control y supervisión de empresas Aérea clasificados en sus distintas RAP's	DGAT	Director ODTD / Jefe Proyectos OGTI	VMT	Windows Server 2008-IIS 7.5.0/MVC 4 .net	MS Team Foundation	Oracle 11g

Activos de hardware y software críticos del MTC								
Ítem	**Descripción**	**Ubicación**	**Cantidad**	**Función**	**Oficina o Dirección**	**Responsable**	**Estado actual (agosto 2022)**	**Año de adquisición**
1	Equipo Firewall WAN	Centro de Datos MTC	1	Control de tráfico a nivel LAN/WAN	OITSI	Especialista en Seguridad Informática	Operativo	2007

Jirón Zorritos 1203 – Lima - Perú
Central telefónica. (511) 615-7800
www.gob.pe/mtc

Activos de hardware y software críticos del MTC								
Ítem	**Descripción**	**Ubicación**	**Cantidad**	**Función**	**Oficina o Dirección**	**Responsable**	**Estado actual (agosto 2022)**	**Año de adquisición**
2	Equipo Firewall Internet	Centro de Datos MTC	2	Seguridad perimetral	OITSI	Especialista en Seguridad Informática	Operativo	2018
3	Software Antivirus	Centro de Datos MTC	4000 Licencias	Protección a los endpoint (PCs) contra código malicioso.	OITSI	Especialista en Seguridad Informática	Operativo y con soporte vigente.	2020
4	Equipo Antispam	Centro de Datos MTC	2	Protección frente a correo malicioso.	OITSI	Especialista en Seguridad Informática	Operativo y con soporte vigente.	2015
5	Equipo Filtro de Contenido Web	Centro de Datos MTC	1	Navegación segura a Internet.	OITSI	Especialista en Seguridad Informática	Operativo y con soporte vigente.	2015
6	Switch Core	Centro de Datos MTC	2	Administración de red en el Centro de Datos	OITSI	Administrador de Red	Operativo	2014
7	Switch de Distribución	Centro de Datos MTC	2	Administración de red en el Centro de Datos	OITSI	Administrador de Red	Operativo	2014

Jirón Zorritos 1203 – Lima - Perú
Central telefónica. (511) 615-7800
www.gob.pe/mtc

Activos de hardware y software críticos del MTC								
Ítem	**Descripción**	**Ubicación**	**Cantidad**	**Función**	**Oficina o Dirección**	**Responsable**	**Estado actual (agosto 2022)**	**Año de adquisición**
8	Routers	Centro de Datos MTC	2	Interconexión a Internet del Operador	Proveedor del Servicio de Internet / OITSI	Administrador de Red	Operativo	2020
9	Balanceador de Enlaces Internet	Centro de Datos MTC	2	Balacear o distribuir el tráfico de red entrante de Internet en el MTC	Proveedor del Servicio de Internet / OITSI	Administrador de Red	Operativo	2020
10	Balanceador de Aplicaciones	Centro de Datos MTC	2	Balancear o distribuir el tráfico de red entrante a servidores de aplicaciones del MTC	Proveedor del Servicio de Internet / OITSI	Administrador de Red	Operativo	2020
11	Servidores Blade	Centro de Datos MTC	34	Procesamiento de datos de aplicaciones y servicios.	OITSI	Administracion de Servidores	Operativos	2014 / 2018
12	Servidores Raqueable	Centro de Datos MTC	15	Procesamiento de datos de aplicaciones y servicios.	OITSI	Administracion de Servidores	Operativos	2014 / 2018
13	Chassis de Servidores	Centro de Datos MTC	4	Soporte y conectividad de los servidores blade	OITSI	Administracion de Servidores	Operativos	2014 / 2018

Jirón Zorritos 1203 – Lima - Perú
Central telefónica. (511) 615-7800
www.gob.pe/mtc

Activos de hardware y software críticos del MTC								
Ítem	**Descripción**	**Ubicación**	**Cantidad**	**Función**	**Oficina o Dirección**	**Responsable**	**Estado actual (agosto 2022)**	**Año de adquisición**
14	Solución de Almacenamiento	Centro de Datos MTC	3	Sistemas de almacenamiento de información.	OITSI	Administracion de Servidores	Operativos	2014 / 2018
15	Software de Base de Datos POSTGRESQL	Centro de Datos MTC	1	Servicios de Base de Datos	OITSI	Asistente técnico en Base de Datos	Operativo	-
16	Software de Base de Datos MYSQL	Centro de Datos MTC	1	Servicios de Base de Datos	OITSI	Asistente técnico en Base de Datos	Operativo	-
17	Software de Base de Datos MS SQL	Centro de Datos MTC	1	Servicios de Base de Datos	OITSI	Asistente técnico en Base de Datos	Operativo.	2013
18	Software de Base de Datos Oracle	Centro de Datos MTC	2	Servicios de Base de Datos	OITSI	Asistente técnico en Base de Datos	Operativo, con soporte vigente (hasta junio 2024)	2018

Jirón Zorritos 1203 – Lima - Perú
Central telefónica. (511) 615-7800
www.gob.pe/mtc

Activos de hardware y software críticos del MTC								
Ítem	**Descripción**	**Ubicación**	**Cantidad**	**Función**	**Oficina o Dirección**	**Responsable**	**Estado actual (agosto 2022)**	**Año de adquisición**
19	Software de Virtualización	Centro de Datos MTC	1	Herramienta de administración de la infraestructura virtual de servidores que soporta los servicios y sistemas del MTC.	OITSI	Administracion de Servidores	Operativo, con soporte vigente (hasta noviembre 2023)	2014
20	Central Telefónica	Sala de Telefonía / Centro de Datos MTC	1	Telefonía y comunicaciones	OITSI	Especialista en Telefonía y comunicaciones	Operativo, con soporte vigente.	UPGRADE 2019
21	Equipos UPS	Centro de Datos MTC	2	Provisión de energía eléctrica temporal y de contingencia eléctrica al Centro de Datos - MTC	OITSI	Técnico de Centro de Datos	Operativo.	2011
22	Sistema de Extinción de Incendios	Centro de Datos MTC	1	Mitigar eventos relacionados con el fuego al interior del Centro de Datos - MTC	OITSI	Técnico de Centro de Datos	Operativo	2015

Firmado digitalmente por: REQUENA CASTRO Jesus Nicanor FAU 20131379944 soft
Motivo: Doy V° B°
Fecha: 29/09/2022 11:00:09-0500

Jirón Zorritos 1203 – Lima - Perú
Central telefónica. (511) 615-7800
www.gob.pe/mtc

Activos de hardware y software críticos del MTC								
Ítem	**Descripción**	**Ubicación**	**Cantidad**	**Función**	**Oficina o Dirección**	**Responsable**	**Estado actual (agosto 2022)**	**Año de adquisición**
23	Generador Eléctrico	Centro de Datos MTC	1	Provisión de energía eléctrica de sustento ante ausencia de fluido eléctrico del proveedor - ENEL	Oficina de Abastecimeinto - OGA	Sub Oficina de Servicios Generales - OABAST	Operativo	----
24	Sistema de Aire Acondicionado	Centro de Datos MTC	1	Control de temperatura y humedad al interior del Centro de Datos	OITSI	Técnico de Centro de Datos	Operativo	2015

Firmado digitalmente por:
REQUENA CASTRO Jesus
Nicanor FAU 20131379944 soft
Motivo: Doy V° B°
Fecha: 29/09/2022 11:01:56-0500

Jirón Zorritos 1203 – Lima - Perú
Central telefónica. (511) 615-7800
www.gob.pe/mtc