PERÚ | Ministerio de Energía y Minas

PLAN DE RECUPERACIÓN DE LOS SERVICIOS INFORMÁTICOS

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN

2024

CONTENIDO

PLAN DE RECUPERACIÓN DE LOS SERVICIOS INFORMÁTICOS DEL MINISTERIO DE ENERGÍA Y MINAS

INTRODUCCIÓN

El Plan de Recuperación de los Servicios Informáticos se define como el proceso continuo de planificación, desarrollo, pruebas e implementación de procedimientos para la recuperación de los servicios críticos de la entidad ante un posible evento o siniestro que pueda afectar su normal funcionamiento. Este plan define las acciones para asegurar la reanudación eficiente y efectiva de los servicios y operaciones de tecnologías de la información del Ministerio de Energía y Minas.

PLAN DE RECUPERACIÓN DE LOS SERVICIOS INFORMÁTICOS DEL MINISTERIO DE ENERGÍA Y MINAS

I. OBJETIVOS

1.1 General

Garantizar la restauración de los servicios de tecnología de la información del Ministerio de Energía y Minas (MINEM), ante eventos que podrían alterar el normal funcionamiento de dichos servicios, a fin de minimizar el impacto y responder de forma inmediata hacia la recuperación de las actividades normales, minimizando el tiempo de disponibilidad de los servicios tecnológicos.

1.2 Específicos

- Identificar los servicios críticos de tecnologías de la información del MINEM.
- Identificar y analizar los posibles riesgos que pueden afectar el correcto funcionamiento de los servicios informáticos del MINEM.
- Establecer e implementar las estrategias adecuadas para asegurar la continuidad de los servicios críticos ante alguna interrupción, que permita restablecer los mismos en el menor tiempo posible.
- Contar con documentación actualizada que garantice al MINEM la continuidad de los servicios tecnológicos críticos sin sufrir interrupciones o pérdidas de información.
- Contar con personal debidamente capacitado para afrontar adecuadamente las incidencias que puedan presentarse en los servicios informáticos del MINEM.

1.3 Vinculación con los Planes Institucionales

El Objetivo General y los Objetivos Específicos, del Plan de recuperación de los servicios informáticos del MINEM, se encuentran vinculados al Plan Estratégico Institucional (PEI) 2020 – 2027 ampliado del MINEM; aprobado mediante Resolución Ministerial N° 119-2024-MINEM/DM, en los Objetivos y Acciones Estratégicas Institucionales:

- ✓ **O.E.I.06: Fortalecer la Gestión Institucional**

  A.E.I. 06.01: Gestión Institucional moderna, eficiente y eficaz.

- ✓ **O.E. 07: Implementar la Gestión del Riesgo**

  A.E.I.07.02: Plan de Continuidad Operativa de la Institución implementado.

Asimismo, se vincula en el Plan Operativo Institucional (POI) Anual del MINEM consistente con el (PIA) 2024, aprobado por Resolución Ministerial N° 523-2023-MINEM/DM, a la siguiente Actividad Operativa de la Oficina de Tecnologías de la Información:

A.O 15 Elaboración y/o evaluación de planes estratégicos relacionados a tecnologías de la información.

1.4 Presupuesto requerido

El Plan de Recuperación de los Servicios Informáticos del MINEM, se ejecutará mediante la renovación de infraestructura tecnológica, lo cual se encuentra presupuestado dentro del Plan de Gobierno Digital 2023 – 2026 del MINEM como parte de la infraestructura tecnológica; y, en lo que

respecta al personal (recurso humano), se ejecutará considerando al personal con el que cuenta la Oficina de Tecnologías de la Información (Nombrados y CAS Indeterminados).

II. ALCANCE

El Plan de Recuperación de Servicios Informáticos del MINEM abarca todos los componentes relacionados con las aplicaciones, soluciones tecnológicas, servicios, infraestructura tecnológica, personal, y otros recursos que son gestionados por la Oficina de Tecnologías de la Información. Su propósito es minimizar los posibles riesgos ante situaciones adversas que puedan afectar el funcionamiento de los servicios informáticos del MINEM.

III. BASE LEGAL

- Ley N° 28716, Ley de Control Interno de las Entidades del Estado.
- 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.
- Ley Nº 30705, Ley de Organización y Funciones del Ministerio de Energía y Minas.
- Decreto Legislativo Nº 1412, Ley de Gobierno Digital.
- Decreto Supremo Nº 031-2007-EM, Reglamento de Organización y Funciones del Ministerio de Energía y Minas y sus modificatorias.
- Decreto Supremo N° 029-2021-PCM, Decreto Supremo que aprueba el Reglamento del Decreto Legislativo Nº 1412, Decreto Legislativo que aprueba la Ley de Gobierno Digital, y establece disposiciones sobre las condiciones, requisitos y uso de las tecnologías y medios electrónicos en el procedimiento administrativo.
- Decreto Supremo N° 118-2018-PCM, declaran de Interés Nacional el desarrollo del gobierno digital, la innovación y la economía digital con enfoque territorial.
- Resolución Ministerial Nº 004-2016-PCM, que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2da 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 Ministerial N° 030-2021-PCM, Resolución Ministerial que aprueba los "Lineamientos para la Gestión de la Continuidad Operativa y la Formulación de los Planes de Continuidad Operativa de las entidades públicas en los tres niveles de Gobierno".
- Resolución Ministerial N° 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 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 Jefatural N° 076-95-INEI, que aprueba la Directiva Normas Técnicas para la seguridad e integridad de la información que se procese en la Administración Pública.
- Resolución Jefatural N° 090-95-INEI, que aprueba las recomendaciones técnicas para la protección física de los equipos y medios de procesamiento de la información en la Administración Pública.
- Resolución Jefatural N° 140-95-INEI, que aprueba las recomendaciones técnicas para la organización y gestión de los servicios informáticos para la Administración Pública.
- Resolución Jefatural Nº 386-2002-INEI, que aprueba la Directiva Nº 016-2002- INEI/DTNP, "Normas Técnicas para el Almacenamiento y Respaldo de la información Procesada por las Entidades de la Administración Pública".

Las referidas normas incluyen sus respectivas disposiciones ampliatorias, modificatorias y conexas, de ser el caso.

IV. GLOSARIO DE TÉRMINOS Y DEFINICIONES

4.1 Acceso: Es el resultado positivo de una autenticación a un equipo informático, sistema, aplicación, red o algún otro dispositivo. Los accesos pueden ser de diferentes niveles de acuerdo a la función o cargo del usuario.

4.2 Activo de Información: Cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización, pueden ser procesos de negocio, datos, aplicaciones, equipos informáticos, personal, soportes de información, redes, equipamiento auxiliar o instalaciones. Es susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización.

4.3 Amenazas de los activos: Probabilidad de que ocurra un incidente porque se aprovecha una vulnerabilidad del activo del sistema; éstas pueden provocar daños o pérdidas de todo tipo en la organización y se puede materializar desde el interior de la organización o del exterior.
Las amenazas se originan a partir de la presencia de una vulnerabilidad, que por un lado puede ser aprovechada por personas externas para hacer daño o por otro lado sin intención de daño pero que pueden poner en riesgo los activos de información.

4.4 Aplicaciones: Son los archivos y programas con sus correspondientes manuales de usuario y/o técnicos desarrollados o adquiridos por la Entidad.

4.5 Ataque: Es el término general usado para cualquier acción o evento que intente interferir con el funcionamiento adecuado de un sistema informático o el intento de obtener de modo no autorizado la información confiada a un computador.

4.6 Base de Datos: Son conjunto de datos relacionados que se almacenan de forma que se pueda acceder a ellos de manera sencilla, con la posibilidad de relacionarlos, ordenarlos en base a diferentes criterios de selección.

4.7 Centro de Datos: Es un centro de procesamiento para obtener información, en el cual se albergan los sistemas de información, hardware, componentes asociados, como telecomunicaciones y sistemas de almacenamiento.

4.8 Cortafuego (Firewall): Es un dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de normas y otros criterios y pueden ser implementados en hardware o software, o en una combinación de ambos.

4.9 Datos: Se consideran datos a todos aquellos elementos por medio de los cuales es posible la generación de información. Tales elementos pueden ser estructurados (base de datos) o no estructurados (correos electrónicos) y se presentan en forma de imágenes, sonidos o colección de bits.

4.10 Disponibilidad: Propiedad de la seguridad de la información que garantiza que la información esté disponible y pueda ser accedida por las personas autorizadas en el momento que ellas lo requieran.

4.11 Evento de Contingencia: Es una experiencia inesperada e incontrolable que afecta de manera intensa la sensación de seguridad y autoconfianza del individuo provocando intensas

reacciones de vulnerabilidad y temor hacia el entorno.

4.12 Gestión de riesgos: Selección e implantación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados.

4.13 Impacto: Conjunto de consecuencias provocadas por un hecho o actuación que afecta a un entorno o ambiente social o natural.

4.14 Incidencia: Denominamos incidencia al hecho que se puede presentar en cualquier momento, bajo una probabilidad de ocurrencia.

4.15 Incidente: En este contexto será entendido como la interrupción de las condiciones normales de operación en cualquier proceso informático del MINEM.

4.16 Integridad: Es uno de los pilares de la seguridad de la información y se refiere a asegurar que la información no sea manipulada, destruida o corrompida por accidentes o acciones intencionadas. Ello incluye los elementos que garantizan su procedencia o autenticidad.

4.17 Método Delphi: Es una técnica de comunicación estructurada, desarrollada como un método de predicción sistemático interactivo, basado en el consenso de un grupo de expertos, de forma anónima y realizando una retroalimentación controlada, ya que el grupo consultado sólo es conocido por un coordinador que será el responsable de centralizar el trabajo de un grupo participante que no se conocerá ni se reunirá.

4.18 Plan de Recuperación de Servicios Informáticos: Plan que forma parte del Plan de Continuidad Operativa, el cual busca, inicialmente, restaurar los servicios de tecnología de información necesarios para ejecutar las actividades críticas identificadas, permitiendo una posterior recuperación de las condiciones previas a su ocurrencia. Para su desarrollo se toma en cuenta la Norma Técnica Peruana NTP ISO/IEC 27001:2014.

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

4.20 Punto de restauración objetivo – RPO (Recovery Objetive Point): Se refiere al volumen de datos en riesgo de pérdida que la organización considera tolerable. El RPO determina el objetivo de posible pérdida máxima de datos introducidos desde el último backup, hasta la caída del sistema, y no depende del tiempo de recuperación.

4.21 Riesgo: Probabilidad de que se produzca un evento adverso que genere pérdidas ya sea de carácter físico, digital, económico o de otra índole en particular que afecte a la organización.

4.22 Seguridad: Son las medidas que aplica el MINEM con el objeto de preservar la integridad de sus datos o información procurando que no sean modificados, destruidos o divulgados ya sea en forma accidental, no autorizado e intencional. En el caso de los datos e información contenidos en los sistemas de información del MINEM, la privacidad y la seguridad guardan estrecha relación entre sí, aunque la diferencia entre ellas radica en que la primera se refiere a la distribución autorizada de información y la segunda al acceso no autorizado.

4.23 Sistemas de Información: Es el conjunto de elementos relacionados entre sí con un objetivo en común, en el cual se almacenan datos y se genera información relacionada a un tema en

particular, para ponerlos a disposición de sus usuarios. Pueden ser registros simples como archivos de Word y Excel, o pueden ser complejos como una aplicación de software con base de datos.

4.24 Tiempo de Recuperación Objetivo – RTO (Recovery Time Objetive): Expresa el tiempo durante el cual una organización pueda tolerar la falta de funcionamiento de sus aplicaciones y la caída de nivel de servicio asociada, sin afectar a la continuidad del negocio.

4.25 Vulnerabilidad: Debilidad que puede ser explotada por una amenaza; en otras palabras, son los puntos débiles que se encuentran en un sistema informático y que pueden ser por un lado aprovechados por Hackers o por otro lado ocurrir un daño en el sistema de información a causa de las debilidades.

4.26 TI: Tecnología de la Información.

V. MARCO TEÓRICO

A continuación, se desarrolla el marco teórico necesario para elaborar el Plan de recuperación de servicios de TI.

5.1 Gestión del Riesgo

Es evidente que, debido a consideraciones de costo y practicidad, resulta inviable implementar procedimientos de respuesta a contingencias para todos los activos (recursos, procesos, personas, tecnología) empleados por una organización en la prestación de sus servicios. Por consiguiente, se hace imperativo identificar los activos críticos, aquellos que se encuentran más expuestos a riesgos que podrían afectar su disponibilidad. Para llevar a cabo esta identificación, se recurre a la gestión de riesgos, la cual puede resumirse en tres procesos fundamentales: identificación, análisis, respuesta y control de los riesgos.

5.1.1 Identificación de Riesgos: Se realiza una evaluación exhaustiva de todos los activos y procesos involucrados en las operaciones de la organización para identificar posibles amenazas y vulnerabilidades.

5.1.2 Análisis de Riesgos: Una vez identificados los riesgos, lo siguiente es análisis de riesgos propiamente dichos, maneja tres factores: a) La probabilidad de ocurrencia del riesgo; b) El impacto que dicho riesgo ocasionaría si se presentase; y c) 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.

a) **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:

Nivel de Probabilidad	1	2	3	4	5
	Muy Bajo	Bajo	Medio	Alto	Muy Alto
Nivel de frecuencia	1 vez cada 2 años	1 vez al año	2 a 3 veces al año	4 o 5 veces al año	De 6 a más veces al año
Nivel de Controles Actuales (*)	81 – 100%	61 – 80 %	41 – 60 %	21 – 40%	0 – 20%
Criterio	El riesgo se ha presentado una sola vez en el último año. Es muy poco probable que ocurra y no se tienen controles.	El riesgo se ha presentado una sola vez en el último año. Es muy poco probable que ocurra y no se tienen controles.	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	Es extremadamente probable que ocurra y no se tiene ningún control o los que existen son insuficientes. 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.	El riesgo puede ser inminente.

Tabla 1: Probabilidad de ocurrencia de riesgos.

b) 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.

Nivel de Impacto	1	2	3	4	5
	Muy Bajo	Bajo	Medio	Alto	Muy Alto
Criterio	Riesgo que puede tener un pequeño efecto en la entidad, sobre todo en el orden interno.	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	Riesgo cuya materialización causaría 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	Riesgo cuya materialización dañaría medianamente el patrimonio o imagen de la Entidad. 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.	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.

Tabla 2: Determinación del impacto del riesgo.

c) Nivel de exposición del Riesgo (VR).

El valor del riesgo 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.

Nivel de Riesgo	Valor del riesgo (VR)	Interpretación
	10-25	La indisponibilidad del servicio ofrecido por la OTI puede tener repercusiones graves en la operación y servicio del MINEM. Esta situación podría ocasionar una paralización prolongada de las operaciones, sobrepasando los límites de tiempo tolerables. Además, conlleva pérdidas económicas significativas y daños considerables a la reputación y la imagen del MINEM.

Alto	4-9	La afectación de los niveles de operación y servicio de la OTI puede resultar en el incumplimiento de los objetivos estratégicos del MINEM, así como en pérdidas económicas significativas.
Bajo	1-3	El problema de servicio de la OTI puede tener un impacto mínimo en el cumplimiento de un objetivo estratégico o servicio funcional del MINEM

Tabla 3: Determinación del impacto del riesgo.

5.1.3 Respuesta y Control de Riesgos.

En el numeral VI se especifica que la respuesta y Control de Riesgos está en función del desarrollo del Plan de recuperación de los servicios informáticos del MINEM.

5.1.4 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.

MATRIZ DE NIVEL DE RIESGO			VALOR DE 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

Tabla 4: Matriz de probabilidad - impacto

VI. DESARROLLO DEL PLAN DE RECUPERACIÓN DE LOS SERVICIOS INFORMÁTICOS DEL MINEM

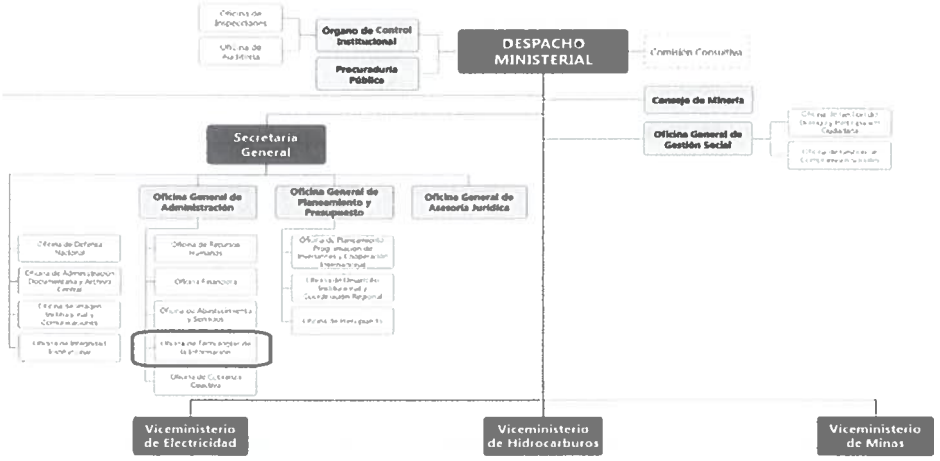
El Plan de recuperación de servicios informáticos del MINEM se ha dividido en las siguientes fases:

- Organización.
- Identificación de los activos críticos de la OTI.
- Identificación, análisis y priorización de riesgos.
- Procedimientos de respuesta y recuperación de servicios.

6.1 ORGANIZACIÓN

De acuerdo al Reglamento de Organización y Funciones del MINEM, aprobado por Decreto Supremo N° 031-2007-EM y sus modificatorias, la Oficina de Tecnologías de la Información depende de la Oficina General de Administración, tal como se muestra en el siguiente gráfico:

Gráfico Nº 1: Organigrama de ubicación de la Oficina de Tecnologías de la Información



El Plan de recuperación de servicios informáticos del MINEM, es un documento que reúne un conjunto de procedimientos que contempla los tres momentos por lo que pasa todo evento de contingencia.

- **Antes de la contingencia**, como acciones dentro de un esquema de prevención para mitigar los incidentes (procedimientos de operación, monitoreo y control desarrollados).
- **Durante la contingencia**, como acciones orientadas a la recuperación de incidentes, en el menor tiempo posible y con la funcionalidad completa, (procedimientos ante contingencias y plan de emergencia)
- **Después de la contingencia**, como acciones de retorno a la operación normal una vez superado el incidente para regresar al estado normal de operación. (Plan de Recuperación).

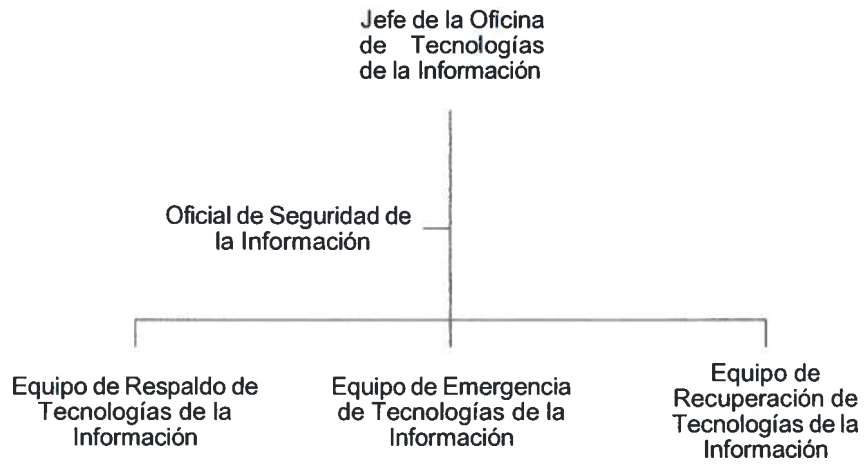
Los procedimientos de contingencia están enfocados en retornar el funcionamiento de los servicios críticos relacionados a Tecnologías de la Información y Comunicaciones - TICs del MINEM, cuando estos servicios han sufrido algún incidente que afecta su disponibilidad.

El plan de recuperación de servicios informáticos permite minimizar las consecuencias en caso de incidente, con el fin de reanudar las operaciones en el menor tiempo posible en forma eficiente y oportuna.

La validación de la funcionalidad y efectividad relacionada a los procedimientos establecidos en el plan de recuperación de servicios informáticos se ejecutará al menos una vez al año, por personal asignado de la Oficina de Tecnologías de la Información, con el fin de evaluar la efectividad y acortar los tiempos de recuperación ante la ocurrencia de un riesgo y/o incidencia, así como de realizar las mejoras necesarias a los procedimientos de contingencia establecidos.

Por ello se ha considerado tres (3) equipos de trabajo, los cuales implementarán las estrategias de respaldo, emergencia y recuperación del presente Plan, teniendo en cuenta los tres (3) momentos descritos, lo cual se organiza de la siguiente manera:

Gráfico N° 02: Organización del Equipo de Recuperación de servicios informáticos



El equipo de recuperación de servicios informáticos está liderado por el Jefe de la Oficina de Tecnologías de la Información que, en coordinación con el Oficial de Seguridad de la Información, tendrán a cargo las siguientes funciones y roles:

- Responsable de la coordinación para la ejecución del plan de recuperación de servicios informáticos, cuando se presenten los eventos que lo activan.
- Velar que el personal se encuentre debidamente capacitado y preparado para ejecutar el Plan de recuperación de servicios informáticos.
- Coordinar la ejecución de las actividades del Plan de pruebas y registrar los resultados de las mismas en la Bitácora de Pruebas de Recuperación.
- Determinar las prioridades y plazos de recuperación de los diferentes servicios que pudieran verse afectados.

Equipo de Respaldo de Tecnologías de la Información

Este equipo es el encargado de ejecutar las acciones preventivas, antes de que ocurra un incidente, su finalidad es evitar su materialización y en caso ocurriese, tener todo lo requerido para realizar la recuperación de los servicios informáticos del MINEM en el menor tiempo posible.

Equipo de Emergencia de Tecnologías de la Información

Equipo encargado de ejecutar acciones requeridas durante la materialización del incidente, su finalidad es reducir el impacto sobre la infraestructura tecnológica y la información del MINEM, tratando de salvaguardar su pérdida o deterioro.

Equipo de Recuperación de Tecnologías de la Información

Equipo encargado de ejecutar las acciones necesarias luego que el incidente esté controlado, su finalidad es restituir en el menor tiempo posible el funcionamiento de la infraestructura tecnológica y recuperar el estado de los servicios informáticos del MINEM de manera conjunta con los miembros titulares y suplentes del Grupo de Comando de Continuidad Operativa del MINEM.

Los equipos no ejecutarán sus actividades de forma paralela, el orden de operación debe ser como se indica:

Los miembros de cada uno de los tres (3) equipos se detallan a continuación:

Equipo de Respaldo de Tecnologías de la Información	• Coordinador de Infraestructura Tecnológica, es el responsable del Equipo de Respaldo de Tecnologías de la Información (Titular y Alterno) • Coordinador de Desarrollo de Aplicaciones (Titular y Alterno) • Administrador de Base de Datos
Equipo de Emergencia de Tecnologías de la Información	• Coordinador de Infraestructura Tecnológica, es el responsable del Equipo de Emergencia de Tecnologías de la Información (Titular y Alterno) • Coordinador de Desarrollo de Aplicaciones (Titular y Alterno) • Administrador de Base de Datos (Titular y Alterno) • Soporte Técnico (Titular y Alterno)
Equipo de Recuperación de Tecnologías de la Información	• Coordinador de Infraestructura Tecnológica, es el responsable del equipo de Recuperación de Tecnologías de la Información (Titular y Alterno) • Coordinador de Desarrollo de Aplicaciones (Titular y Alterno) • Administrador de Base de Datos (Titular y Alterno) • Soporte Técnico (Titular y Alterno)

Se contará con una relación de los datos del personal de la Oficina de Tecnologías de la Información, la cual podrá ser requerida en el momento de la contingencia.

Para el registro de la información en el formato debe considerarse lo siguiente:

- Los responsables mencionados deben tener permanentemente operativo el dispositivo móvil asignado por el MINEM para las comunicaciones pertinentes y al menos uno debe contar con línea abierta disponible, en caso debe comunicarse con proveedores externos y/o especializados.
- Se debe registrar en adicional al correo electrónico institucional, un alternativo de servicios gratuitos, el cual pueda ser utilizado en caso haya indisponibilidad de comunicación vía correo institucional proporcionado por el MINEM.
- Los registros contenidos en el formato deben ser actualizados de manera permanente y deben ser remitidos al siguiente personal:
  - Jefe de la Oficina de Tecnologías de la Información.
  - Oficial de Seguridad de la Información.
  - Alta Dirección del MINEM.
  - Responsable asignado por el Servicio de Seguridad Física y Vigilancia en las Sedes de la Entidad.

Las funciones que desempeña cada uno de los roles definidos en los equipos de trabajo (titulares y alternos) son las siguientes:

a) <u>Equipo de Respaldo de Tecnologías de la Información</u>

i. **Coordinador de Infraestructura Tecnológica**

- ✓ Es el responsable del Equipo de Respaldo de Tecnologías de la información.
- ✓ Programar y/o realizar el mantenimiento preventivo de los equipos de comunicaciones y de los equipos componentes que forman parte de la infraestructura tecnológica, considerando el tiempo de vida útil y garantía de los mismos.
- ✓ Llevar un control detallado del mantenimiento realizado a cada componente del Centro de Datos
- ✓ Llevar un control detallado del mantenimiento realizado a cada equipo de la Infraestructura Tecnológica del Centro de Datos

- ✓ Notificar al Jefe de la Oficina de Tecnologías de la Información y al Oficial de Seguridad de la Información o a quien haga sus veces las acciones del Equipo de Respaldo.
- ✓ Elaborar informes técnicos de conformidad, luego de cada mantenimiento efectuado, así como elaborar informes periódicos del funcionamiento del Centro de Datos.
- ✓ Realizar las pruebas previas de recuperación y registrarlas en la Bitácora de Pruebas de Contingencia.

ii. Coordinador de Desarrollo y Aplicaciones

- ✓ Gestionar que se ejecuten las copias de respaldo de las aplicaciones y sistemas existentes del MINEM.
- ✓ Verificar que las copias de respaldo de las aplicaciones y sistemas se almacenen en un ambiente y con las condiciones adecuadas.
- ✓ Realizar las pruebas previas de restauración y registrarlas en la Bitácora de Pruebas de Contingencia.

iii. Administrador de Base de Datos

- ✓ Gestionar que se ejecuten las copias de respaldo de las bases de datos de los aplicativos y sistemas del MINEM.
- ✓ Verificar que las copias de respaldo de las bases de datos se almacenen en un ambiente y con las condiciones adecuadas.
- ✓ Realizar las pruebas previas de restauración y registrarlas en la Bitácora de Pruebas de Contingencia.
- ✓ Revisar que las copias de respaldo de las bases de datos, se encuentren clasificadas por el tipo de motor de base de datos, aplicaciones y sistemas.

Cabe resaltar que se realizan copias de respaldo de los archivos que se encuentran dentro del File Server, en las carpetas compartidas que cada dirección, oficina o dependencia tiene asignada, cuyo contenido es administrado por lo miembros de cada uno de los grupos asignados.

b) <u>Equipo de Emergencia de Tecnologías de la Información</u>

i. Coordinador de Infraestructura Tecnológica

- ✓ Es el responsable del Equipo de Emergencia de Tecnologías de la Información.
- ✓ Notificar el incidente al Jefe de la Oficina de Tecnologías de la Información y al Oficial de Seguridad de la Información o a quien haga sus veces.
- ✓ Ejecutar las acciones de emergencia en los equipos informáticos instalados en el Centro de Datos del MINEM.
- ✓ Ejecutar las acciones de emergencia en los componentes de la Infraestructura Tecnológica del MINEM.
- ✓ Realizar la evaluación de las condiciones de los equipos de comunicaciones, los equipos y componentes que forman parte de la Infraestructura Tecnológica.
- ✓ Notificar al Jefe de la Oficina de Tecnologías de la Información y al Oficial de Seguridad de la Información o a quien haga sus veces las acciones de emergencia ejecutadas.
- ✓ Elaborar un informe técnico de conformidad que incluya la evaluación de condiciones de los equipos y componentes de la Infraestructura Tecnológica del MINEM.

ii. Coordinador de Desarrollo y Aplicaciones

- ✓ Ejecutar las acciones de emergencia definidas para las aplicaciones informáticas y sistemas del MINEM.
- ✓ Realizar la evaluación del estado y las condiciones de los aplicativos informáticas y sistemas del MINEM.

- ✓ Elaborar un informe técnico que incluya la evaluación de condiciones de las aplicaciones y sistemas de información del MINEM.

iii. Administrador de Base de Datos

- ✓ Ejecutar las acciones de emergencia definidas para los datos y la información almacenada en las distintas bases de datos.
- ✓ Realizar la evaluación de las condiciones de los datos e información que se encuentra en las distintas bases de datos del MINEM, durante la emergencia.
- ✓ Elaborar un informe técnico que incluya la evaluación de condiciones de los datos e información del MINEM.

iv. Soporte Técnico

- ✓ Ejecutar las acciones de emergencia definidas para atender los requerimientos de los usuarios del MINEM.
- ✓ Notificar de los casos críticos, que afecten la funcionalidad de los equipos informáticos y/o pérdida de información de los usuarios.
- ✓ Elaborar un informe técnico que resuma las condiciones de los equipos informáticos y la información.

c) <u>Equipo de Recuperación de Tecnologías de la Información</u>

i. Coordinador de Infraestructura Tecnológica

- ✓ Es el responsable del Equipo de Recuperación de Tecnologías de la Información.
- ✓ Iniciar el proceso de recuperación, efectuando pruebas de funcionamiento de los equipos y componentes afectados de la infraestructura tecnológica del MINEM.
- ✓ Efectuar la restauración de los equipos afectados de la infraestructura tecnológica que impacten en los servicios informáticos.
- ✓ Notificar de las acciones realizadas al Jefe de la Oficina de Tecnologías de la Información y al Oficial de Seguridad de la Información o a quien haga sus veces.
- ✓ Elaborar un informe técnico de conformidad que las acciones de recuperación de los equipos y componentes de la Infraestructura Tecnológica del MINEM.

ii. Coordinador de Desarrollo y Aplicaciones

- ✓ Verificar el estado del funcionamiento de los sistemas y aplicaciones del MINEM.
- ✓ Desplegar y/o reinstalar los sistemas y aplicativos informáticos en caso donde sea requerido ya sea por afectación o corrección de fallo.
- ✓ Elaborar un informe técnico que incluya la evaluación de condiciones de las aplicaciones y sistemas de información del MINEM.

iii. Administrador de Base de Datos

- ✓ Verificar el funcionamiento de las bases de datos de los sistemas y aplicaciones del MINEM.
- ✓ En caso aplique coordinar la restauración de las copias de respaldo de las bases de datos, que pudieran haber resultado afectadas.
- ✓ Ejecutar pruebas de funcionamiento en caso se haya realizado restauración de bases de datos.
- ✓ Elaborar un informe técnico que incluya la evaluación de condiciones de los datos e información del MINEM, luego de efectuada la recuperación.

iv. Soporte Técnico

- ✓ Verificar el funcionamiento de los equipos de los usuarios en las sedes del MINEM, para lo cual debe distribuir la carga de trabajo.
- ✓ Resolver los problemas de conexión y funcionamiento de los equipos de

usuarios, impresoras, escáner u otros.

- ✓ Elaborar un informe técnico que incluya la evaluación de condiciones de los equipos de los usuarios del MINEM, luego de efectuada la recuperación.

La OTI debe participar como miembro en el "Grupo de comando" en el Plan de Continuidad Operativa para el MINEM.

6.2 SOBRE LA IMPLEMENTACIÓN DE LA SEDE ALTERNA DEL MINEM

El plan de recuperación de servicios informáticos se alineará con las futuras iniciativas de la organización en materia de continuidad operativa, una vez que éstas sean establecidas. Se considerará la integración de los objetivos y procedimientos del plan de recuperación con las medidas y directrices que surjan del plan de continuidad operativa, asegurando así una gestión efectiva ante posibles contingencias.

La implementación del Centro de Datos Alterno del MINEM, considera contar con 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 MINEM y a los usuarios externos.

El responsable del equipo de trabajo de Infraestructura Tecnológica se encarga del desarrollo de dicho proyecto, estableciendo los requisitos mínimos que debe cumplir dicha implementación de un centro de datos alterno para el MINEM.

La Infraestructura física del Centro de Datos Alterno – MINEM

La Infraestructura física del Centro de Datos Alterno – MINEM, 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:

Entidad Certificadora: TIA – 942 / Uptime Institute / ICREA

Nivel: Rated-2 / Tier II / Nivel 2

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

- Disponibilidad de suministro eléctrico redundante para garantizar la continuidad del servicio.
  - Transformador de aislamiento.
  - Dispositivo protector de sobretensiones.
  - Grupo electrógeno.
  - Tablero de Transferencia Automática.
  - Tableros de distribución.
  - Circuitos y distribución eléctrica.
- Sistema de climatización adecuado para mantener una temperatura estable y controlada en el ambiente del centro de datos.
- Sistema de detección y extinción de incendios que cumpla con los estándares de seguridad establecidos.
- Acceso seguro y controlado al centro de datos, con medidas de seguridad física y de vigilancia.
- Capacidad de conexión redundante a las redes de comunicación, asegurando la disponibilidad de las conexiones de red.
- Sistema de respaldo de energía (UPS) para mantener la operatividad en caso de interrupción del suministro eléctrico.
- Espacio y disposición adecuados para la instalación de servidores, equipos de red y otros componentes de infraestructura tecnológica.
- Sistema de monitoreo y gestión remota para supervisar el funcionamiento del centro de datos y responder rápidamente ante cualquier incidente.

De la modalidad para la implementación del Centro de Datos Alterno MINEM

La implementación del Centro de Datos Alterno - MINEM, considera las opciones existentes en el 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 MINEM, 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 MINEM, 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 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:

Equipamiento de comunicaciones para el centro de datos alternos	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
Enlace para acceso a internet 200 Mbps	01
Enlace para replicación de conectividad 10 Gbps	03
Enlace para acceso a otras entidades	01
Servidor para telefonía 1TB de almacenamiento 32GB de RAM y 16 vCPU	01

Fuente: elaboración propia.

Equipamiento para seguridad digital	Cantidad
Solución DDoS cloud	01
Firewall perimetral	01
Firewall WAM	01
Firewall de aplicaciones web	01
Solución de e-mail security gateway	01

Fuente: elaboración propia.

Equipamiento para servidores	Cantidad
Switch 10 MXL 10/40Gb – Force (Red SAN)	01
Switch Power Connect (Red SAN)	01
Switch Force S4810 (Red SAN)	01
Servidores Blade	06
Servidores de Base de datos	01
Chasis blade	02
Servidores rackeable	03
Unidad de almacenamiento 200TB	01

6.3 IDENTIFICACIÓN DE LOS ACTIVOS CRÍTICOS DE LA OTI

La misión de la OTI es gestionar servicios de tecnologías de información y comunicaciones (TIC) para el MINEM, utilizando las buenas prácticas de gestión de procesos TIC, personal competente, estándares internacionales y el debido cumplimiento de la normativa de transformación y gobierno digital del Estado Peruano; 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 MINEM, para ello identificamos los servicios funcionales críticos del MINEM.

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

a) **Servicios o aplicaciones críticas del MINEM**:
Son los servicios web o aplicaciones considerados críticos que son usados por los ciudadanos a nivel nacional y/o por los usuarios del MINEM (ANEXO N° 1: INVENTARIO DE SISTEMAS Y APLICACIONES)

b) **Activos de hardware y software críticos del MINEM**
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 MINEM a nivel nacional (ANEXO 2: INVENTARIO DE LA INFRAESTRUCTURA TECNOLÓGICA).

6.4 IDENTIFICACIÓN, ANÁLISIS Y PRIORIZACIÓN DE RIESGOS

La identificación, análisis y priorización de riesgos se ha realizado en base al numeral V "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 crítico existe uno o más riesgos identificados que deben ser evaluados, cuyo 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 6.2, considerando los siguientes peligros:

N°	Categorización del origen del peligro	Peligro	Posibilidad de Ocurrencia
1	Naturales	Sismo de gran magnitud en Lima y Callao	3
2	Instalaciones	Incendio en sede principal	3
3		Atentado o explosión	1
4		Grave alteración del orden público	1
5	Tecnologías	Ataque informático	3

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

Área 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
	RSG-SGSI-048	Incendio del cuarto de UPS por capacitación de seguridad insuficiente	4	4	Extremo
	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
		Mal funcionamiento del equipo del sistema de aire			

	RSG-SGSI-029	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 mantenimiento insuficiente	4	4	
	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	
	RSG-SGSI-051	Incendio del cuarto de UPS por falta de técnicas apropiadas para controlar algún evento catastrófico	4	4	
	RSG-SGSI-052	Inundación del cuarto de UPS por ubicaciones en un área susceptible a las inundaciones	4	4	
	RSG-SGSI-053	Inundación del cuarto de UPS por falta de técnicas apropiadas para controlar algun evento catastrófico	4	4	
	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	
Acumuladores de Energía (UPS)	RSG-SGSI-055	Polvo, corrosión, congelación, sobrecalentamiento de acumuladores de energía (UPS) por mantenimiento insuficiente	4	4	
	RSG-SGSI-056	Polvo, corrosión, congelación, sobrecalentamiento de acumuladores de energía (UPS) por susceptibilidad a la humedad, al polvo y a la suciedad	4	4	
	RSG-SGSI-057	Mal funcionamiento del equipo de acumuladores de energía (UPS) por mantenimiento insuficiente	4	4	

	RSG-SGSI-058	Mal funcionamiento del equipo de acumuladores de energia (UPS) por susceptibilidad a la humedad, al polvo y a la suciedad	4	4	Extremo
	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

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 equipo no exige el cambio periódico de contraseña	4	3	Alto

ACTIVO	CODIGO RIESGO	NOMBRE_RIESGO	IMPACTO	PROBABILIDAD	NIVEL DEL RIESGO
Switch de Distribución	RSG-SGSI-148	Polvo, corrosión, congelación, sobrecalentamiento del switch de distribución por mantenimiento Insuficiente	4	4	
	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	
	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	
	RSG-SGSI-156	Mal funcionamiento del switch de distribución por obsolescencia tecnológica	4	4	
	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
	RSG-SGSI-178	Mal funcionamiento del switch de borde por obsolescencia tecnológica	3	4	Alto
	RSG-SGSI-560	Interrupción del servicio del internet por inexistencia o insuficiencia de acuerdo sobre el nivel de servicio	5	2	Alto

Internet	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	
	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	
	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	
	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	Indisponibilidad por falta de mantenimiento	4	3	**Alto**
Controlador de WIFI	RSG-SGSI-192	Polvo, corrosión, congelación, sobrecalentamiento del controlador de WIFI por mantenimiento insuficiente	4	4	
	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	

	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	
	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

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	
	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

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**

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**
		Fuga de información del			

	RSG-SGSI-455	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

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	
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
	RSG-SGSI-658	Fuga de información del correo electrónico por error humano	5	2	Alto
	RSG-SGSI-659	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	
	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	
	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 mala administración de la contraseña	5	2	Alto
	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

6.5 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 N° 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 especialista de Base de datos de la OTI, se encarga de configurar los respaldos de las bases de datos, dichos respaldos son almacenados temporalmente en el servidor de origen o en una unidad compartida y luego son grabadas en cinta magnética de tipo LTO.

La OTI cuenta con una matriz en Excel para dar seguimiento a los respaldos de las bases de datos en la siguiente ruta:

Y:\INF\2.Infraestructura\Documentacion\Backup\Proyecto Procedimientos Backup

6.6 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)	
- 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), 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.	

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.

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.

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.

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

MINISTERIO DE ENERGÍA Y MINAS
Tecnología de la Información
VºBº

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 Respaldo de Tecnologías de la Información.

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 equipo de emergencia de tecnología de la información.

c) Personal encargado
El equipo de recuperación de tecnología de la información.

d) 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

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

3. Plan de evaluación (después)

a) Personal Encargado

El equipo de Infraestructura Tecnológica, luego de validar la corrección del problema del equipo informará a los jefes y/o directores de las unidades orgánicas para la reanudación de las operaciones de los servicios afectados en el equipo averiado.

b) Descripción de actividades

El plan de recuperación de servicios está 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:

- 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 MINEM informando la reanudación de los servicios.

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

c) Mecanismos de Comprobación

El/La coordinador/a de Infraestructura Tecnológica, presentará un informe a el/la Jefe/a de OTI, explicando que parte del servicio u operaciones se han visto afectadas, y cuáles son las acciones tomadas.

d) Desactivación del Plan

Con el aviso de el/la coordinador/a de continuidad de TI, se desactivará el presente Plan.

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

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 Respaldo de Tecnologías de la Información

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 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 equipos 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

Equipo de Emergencia de Tecnologías de la Información.

c) Personal Encargado

Equipo de Recuperación de Tecnologías de la Información.

d) 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.

e) Duración

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

3. Plan de evaluación (después)

a) Personal Encargado

El Equipo de Infraestructura Tecnológica, luego de validar la corrección del problema del equipo informará a los Jefes y/o Directores de las unidades orgánicas 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 la instalación 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 MINEM informando la reanudación de los servicios.

En función a esto, se tomarán las medidas preventivas del caso.

c) Mecanismos de Comprobación

El/La coordinador/a de Infraestructura tecnológica, presentará un informe al el/la jefe/a de la OTI, explicando que parte del servicio u operaciones se han visto afectadas, y cuáles son las acciones tomadas.

d) Desactivación del Plan

Con el aviso de el/la Jefe/a de Tecnologías de la Información, 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 OTI, 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 MINEM, 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 equipo de respaldo de tecnologías de la información, 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 infraestructura tecnológica 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 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
Equipo de emergencia de tecnologías de la información

c) Personal Encargado
Equipo de recuperación de tecnologías de la información.

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.

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 OTI, 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 MINEM, 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 equipo de respaldo de tecnologías de la información, 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 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 respaldo 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.

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

Equipo de Emergencia de Tecnologías de la Información.

c) Personal Encargado

Equipo de Recuperación de Tecnologías de la Información.

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.

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

MINISTERIO DE ENERGÍA Y MINAS
Oficina General de Tecnologías de la Información

MINISTERIO DE ENERGÍA Y MINAS
V°B°
Tecnologías de la Información

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 MINEM.

c) Entorno

Este evento puede afectar los sistemas, servicios de red y autenticación de los usuarios internos y externos del MINEM.

d) Personal Encargado

El Jefe de la OTI, 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 respaldo de Tecnologías de la Información 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 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 respaldo 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.

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
Equipo de Emergencia de Tecnologías de la Información

c) Personal Encargado
Equipo de Recuperación de Tecnologías de la Información

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

a) Acciones post evento

- 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 MINEM.

d) Personal Encargado

El Jefe de TI, 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 Respaldo de Tecnologías de la Información 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

- 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 Respaldo 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
Equipo de Emergencia de Tecnologías de la Información

c) Personal Encargado
Equipo de Recuperación de Tecnologías de la Información.

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.

Código:	FRS-12
Activo crítico:	UPS
Evento:	Falla de equipo UPS

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, los riesgos que podrían interrumpir la continuidad de las operaciones en el MINEM, se identifican cinco peligros que podrían ocasionar la interrupción de operaciones y funcionamiento del MINEM.

Cuadro N ° 3: Riesgos con posibilidad de ocurrencia

N°	Categorización del origen del peligro	Peligro	Posibilidad de Ocurrencia
1	Naturales	Sismo de gran magnitud en Lima y Callao	3
2	Instalaciones	Incendio en sede principal	3
3		Atentado o explosión	1
4		Grave alteración del orden público	1
5	Tecnologías	Ataque informático	3

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

No	Activo Crítico afectado	Sismo de gran magnitud en Lima	Incendio en la sede principal	Ataque informático.
01	Equipo Firewall		X	X
02	Software Antivirus		X	X
03	Equipo Antispam		X	X
04	Equipo Filtro de Contenido Web		X	X
05	Switch Core	X	X	
06	Switch de Distribución		X	
07	Routers (acceso a Internet)	X	X	X
08	Balanceador de Enlaces Internet		X	X

09	Balanceador de Aplicaciones		X	X
10	Servidores Blade	X	X	
11	Servidores Rack	X	X	
12	Chassis de Servidores	X	X	
13	Solución de Almacenamiento	X	X	
14	Software de Base de Datos ORACLE			X
15	Software de Virtualización			X
16	Central Telefónica	X	X	
17	Equipos UPS	X	X	
18	Sistema de Extinción de Incendios		X	
19	Generador Eléctrico	X	X	
20	Sistema de Aire Acondicionado		X	

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 MINEM:

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 Oficina de Tecnologías 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 – MINEM, sin exponer la seguridad de las personas.

c) Entorno

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

d) Personal Encargado

El/la Jefe/a de Tecnologías de la Información, 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 Respaldo 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 MINEM, 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 - MINEM.
- Mantenimiento del orden y limpieza de la Sala de UPS y los ambientes del Centro de Datos – MINEM.
- Inspecciones de seguridad internas y externas de los ambientes del Centro de Datos – MINEM.
- Realización de simulacros internos en horarios que no afecten las actividades.

g) Acciones del Equipo de Respaldo 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 – MINEM, 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

Equipo de Emergencia de Tecnologías de la Información

c) Personal Encargado
Equipo de Recuperación de Tecnologías de la Información

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.).
- 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 MINEM, 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.).

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 equipo de emergencia de tecnologías de la información y el equipo de recuperación de tecnologías de la información, cuyo rol principal es asegurar el normal

desarrollo de los servicios y operaciones de TI del MINEM.

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 – MINEM.
- 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 – MINEM.
- 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 de Recuperación Tecnologías de la Información, 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 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 Jefe/a de Tecnologías de la Información, 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 Jefe/a de Tecnologías de la Información desactivará el Plan de Recuperación Informático una vez que se haya tomado las acciones descritas en el presente, 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 Jefe de Tecnologías de la Información, 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 Oficina de Tecnologías 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 – MINEM, sin exponer la seguridad de las personas.

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

d) Personal Encargado
El/la Jefe/a de Tecnologías de la Información, 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 Respaldo de Tecnologías de la Información 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 – MINEM.
- 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 - MINEM.
- Mantenimiento del orden y limpieza de las Salas de Comunicaciones, Sala de Servidores y sala de UPS del Centro de Datos – MINEM.
- Inspecciones de seguridad internas y externas de los ambientes del Centro de Datos – MINEM.
- 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 – MINEM, 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 – MINEM, 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 – MINEM.
El proceso de contingencia se activará inmediatamente después de ocurrir el evento.

b) Personal que autoriza la contingencia informática

El equipo de emergencia de tecnologías de la información

c) Personal Encargado

El equipo de recuperación de tecnologías de la información

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.).
- 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 MINEM, 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 Jefe de Tecnologías de la Información, cuyo rol principal es asegurar el normal desarrollo de los servicios y operaciones de TI del MINEM.

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 – MINEM.
- 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 – MINEM y mantener informado al Equipo de Recuperación de Tecnologías de la Información.
- 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 de Recuperación de Tecnologías de la Información, 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 – MINEM, 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 Jefe/a de Tecnologías de la Información, 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 Jefe/a de Tecnologías de la Información desactivará el Plan de Recuperación Informático una vez que se haya tomado las acciones descritas en el presente, 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 Jefe/a de Tecnologías de la Información, luego del cual se determinará las acciones a tomar.

MINISTERIO DE ENERGÍA Y MINAS – Tecnologías de la Información – V°B°

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 Oficina de Tecnologías 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 del MINEM, sin exponer la seguridad de las personas.

c) Entorno

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

d) Personal Encargado

El Jefe/a de la Oficina de Tecnologías de la Información, 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 Respaldo de Tecnologías de la Información debe realizar las

MINISTERIO DE ENERGÍA Y MINAS
Tecnologías de la Información
VoBo

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 del MINEM.
- 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 del MINEM.
- Mantenimiento del orden y limpieza de la sala de comunicaciones, sala de servidores, sala de UPS y los ambientes conexos al Centro de Datos del MINEM.
- Inspecciones de seguridad internas y externas de los ambientes y equipos del sistema de aire acondicionado del Centro de Datos del MINEM.
- Realización de simulacros internos en horarios que no afecten las actividades.

g) Acciones del Equipo de Respaldo de TI
- Validar la operatividad del sistema de aire acondicionado del Centro de Datos del MINEM, así como la restauración de servicio de los mismos.
- Programar y supervisar el mantenimiento preventivo al sistema de aire acondicionado del Centro de Datos del MINEM, 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 sismo que afecte la operatividad del Centro de Datos del MINEM.
El proceso de contingencia se activará inmediatamente después de ocurrir el evento.

b) Personal que autoriza la contingencia informática
El equipo de emergencia de tecnologías de la información

c) Personal Encargado
Equipo de recuperación de tecnologías de la información

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.).
- 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.
- 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 MINEM, 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 sismo, la probabilidad de reinicio y daños que pudiera afectar la infraestructura

3. Plan de evaluación

a) Personal Encargado
El/la coordinador/a de infraestructura tecnológica

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 aire acondicionado del Centro de Datos del MINEM.
- 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 del MINEM y mantener informado al Equipo de Recuperación de Servicios Informáticos.
- 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 de Recuperación Tecnologías de la Información, 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 del MINEM, 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 del MINEM.
  - 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

c) Mecanismos de Comprobación
El/la Jefe/a de Tecnologías de la Información remite 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 Jefe/a de Tecnologías de la Información 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 Jefe/a de Tecnologías de la Información, 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 MINEM, 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 OTI cuenta con manuales y procedimientos, los cuales mencionamos a continuación:

2. Plan o procedimiento de Recuperación (durante)

- ✓ Dependiendo de los daños ocasionados, se determinará junto al Grupo Especializado de Continuidad Operativa el tiempo en que el personal acudirá a las instalaciones de la OTI, 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 infraestructura tecnológica, 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 del MINEM, sin exponer la seguridad de las personas.

c) Entorno

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

d) Personal Encargado

El/la Jefe/a de Tecnologías de la Información, 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 Respaldo de Tecnologías de la Información 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 MINEM, el mismo que debe ser de conocimiento de todo el personal que labora en el Centro de Datos del MINEM y sus ambientes conexos.
c. Realización de prácticas de uso de extintores con la participación del personal que labora en el Centro de Datos del MINEM 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 del MINEM.
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 del MINEM.
b. Mantenimiento del orden y limpieza de la Sala de UPS y los ambientes del Centro de Datos del MINEM.
c. Inspecciones de seguridad internas y externas de los ambientes del Centro de Datos del MINEM.
d. Realización de simulacros internos en horarios que no afecten las actividades.

g) Acciones del Equipo de Respaldo de Tecnologías de la Información

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 del MINEM, 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.
b. 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 Jefe/a de Tecnologías de la Información.

c) Personal Encargado
Equipo de Emergencia de Tecnologías de la Información.

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.).
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 MINEM, 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

a. El proceso de evacuación del personal del área se realizará de modo calmado y demorar 5 minutos como máximo.
b. 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 Equipo de Infraestructura Tecnológica, cuyo rol de la Entidad es asegurar el normal desarrollo de los servicios y operaciones de TI del MINEM.

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 del MINEM.
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 del MINEM y mantener informado al Equipo de Recuperación de Tecnologías de la Información.

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 de Recuperación Tecnologías de la Información, 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

El/la Jefe/a de Tecnologías de la Información remitirá 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 Jefe/a de Tecnologías de la Información desactivará el Plan de Recuperación 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 Jefe/a de Tecnologías de la Información, 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 del MINEM, sin exponer la seguridad de las personas.

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

d) Personal Encargado
El/la Jefe/a de Tecnologías de la Información, 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 Respaldo 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 del MINEM.
- 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 del MINEM.
- Mantenimiento del orden y limpieza de las Salas de Comunicaciones, Sala de Servidores, sala de UPS y los ambientes conexos al Centro de Datos.
- Inspecciones de seguridad internas y externas de los ambientes del Centro de Datos.
- Realización de simulacros internos en horarios que no afecten las actividades.

g) Acciones del Equipo de Respaldo de Tecnologías de la Información
- Establecer, organizar, ejecutar y supervisar procedimientos de prueba y esfuerzo del sistema de extinción de incendios del Centro de Datos del MINEM, 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 del MINEM, 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 Incendio que afecte la operatividad del Centro de Datos del MINEM.
El proceso de contingencia se activará inmediatamente después de ocurrir el evento.

b) Personal que autoriza la contingencia informática

El/la Jefe/a de Tecnologías de la Información

c) Personal Encargado
Equipo de Emergencia de Tecnologías de la Información.

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.).
   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 MINEM, 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
   a. El proceso de evacuación del personal del área se realizará de modo calmado y demorar 5 minutos como máximo.
   b. 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 equipo de infraestructura tecnológica y el equipo de recuperación de tecnologías de la información, cuyo rol de la Entidad es asegurar el normal desarrollo de los servicios y operaciones de TI del MINEM.

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 del MINEM.
   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 – MINEM y mantener informado al Equipo de Recuperación de Tecnologías de la Información.
   d. Validar la operatividad del sistema de extinción de incendio del Centro de Datos y el restablecimiento de operación.
   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 de Recuperación de Tecnologías de la Información, 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, 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 Jefe/a de Tecnologías de la Información, 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 Jefe/a de Tecnologías de la Información, desactivará el Plan de Recuperación 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 Jefe/a de Tecnologías de la Información, luego del cual se determinará las acciones a tomar.

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:

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, sin exponer la seguridad de las personas.

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

d) Personal Encargado
El/la Jefe/a de Tecnologías de la Información, 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 Respaldo de Tecnologías de la Información 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.
- 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.
- Mantenimiento del orden y limpieza de las Salas de Comunicaciones, Sala de Servidores, sala de UPS y los ambientes conexos al Centro de Datos.
- Inspecciones de seguridad internas y externas de los ambientes y equipos del sistema de aire acondicionado del Centro de Datos.
- Realización de simulacros internos en horarios que no afecten las actividades.

g) Acciones del Equipo de Respaldo de TI
- Validar la operatividad del sistema de aire acondicionado del Centro de Datos, así como la restauración de servicio de los mismos.
- Programar y supervisar el mantenimiento preventivo al sistema de aire acondicionado del Centro de Datos, 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.
El proceso de contingencia se activará inmediatamente después de ocurrir el evento.

b) Personal que autoriza la contingencia informática

El/La Jefe/a de Tecnologías de la Información.

c) Personal Encargado
Equipo de Emergencia de Tecnologías de la Información.

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.).
- Verificar que el personal que labora en el área se encuentre bien.
- 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.).
- 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 Incendio. En todo momento se coordinará con el personal de mantenimiento del MINEM, 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 Equipo de Infraestructura Tecnológica y el Equipo de Recuperación de Tecnologías de la Información, cuyo rol de la Entidad es asegurar el normal desarrollo de los servicios y operaciones de TI del MINEM.

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 aire acondicionado del Centro de Datos.
  - ✓ 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 y mantener informado al Equipo de Recuperación de Tecnologías de la Información.
  - ✓ 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 de Recuperación de Tecnologías de la Información, 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, 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.
    - 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

c) Mecanismos de Comprobación

El/la Jefe/a de Tecnologías de la Información, 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 Jefe/a de Tecnologías de la Información desactivará el Plan de Recuperación 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 Jefe/a de Tecnologías de la Información, 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 Infraestructura Tecnológica 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
El/la Jefe/a de Tecnologías de la Información y el/la Oficial de Seguridad de la

Información pueden activar la contingencia.

Personal Encargado
Equipo de Infraestructura tecnológica.

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 recuperación de TI, luego de restaurar el correcto funcionamiento del servidor, estación de trabajo (PC, laptop), sistemas de información y portales web, coordinará con el/la Jefe/a de Tecnologías de la Información para reanudar las labores de trabajo con el equipo o sistema que fue afectado.

b) Descripción de actividades

Se informará a el/la Jefe/a de Tecnologías de la Información, 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 MINEM.
El evento será evaluado y registrado de ser necesario en el formato de ocurrencia de incidentes de seguridad informática.

c) Mecanismos de Comprobación

El personal de Infraestructura Tecnológica, según sea el caso, presentará un informe a el/la Jefe/a de la Oficina de Tecnologías de la Información, explicando que parte del servicio u operaciones se han visto afectadas, y cuáles son las acciones tomadas.
Se llenará el formato de incidentes de seguridad digital y se informará al Comité de Gobierno Digital.

d) Desactivación del plan de recuperación

Con el aviso de el/la Jefe/a de Tecnologías de la Información se desactivará el presente plan.

Código:	**FRS – 25**
Activo crítico:	**Firewall**
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.

b) Personal que autoriza la contingencia

El/La Jefe/a de Tecnologías de la Información y el/la Oficial de Seguridad de la Información pueden activar la contingencia.

c) Personal Encargado

Equipo de Emergencia de Tecnologías de la Información

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 recuperación de TI, luego de restaurar el correcto funcionamiento del servidor, estación de trabajo (PC, laptop), sistemas de información y portales web, coordinará con el/la Jefe/a de Tecnologías de la Información para reanudar las labores de trabajo con el equipo o sistema que fue afectado.

b) Descripción de actividades

Se informará a el/la jefe/a de Tecnologías de la Información 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).
- 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 preventivas del caso enviando una alerta vía correo al personal del MINEM.

El evento será evaluado y registrado de ser necesario en el formato de ocurrencia de incidentes de seguridad informática.

a) Mecanismos de Comprobación

El personal de Infraestructura Tecnológica, según sea el caso, presentará un informe a el/la jefe/a de la Oficina de Tecnologías de la Información, explicando que parte del servicio u operaciones se han visto afectadas, y cuáles son las acciones tomadas.

Se llenará el formato de incidentes de seguridad digital y se informará al Comité de Gobierno Digital.

b) Desactivación del plan de recuperación

Con el aviso de el/la Jefe/a de Tecnologías de la Información se desactivará el presente plan.

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 Infraestructura Tecnológica 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 Jefe/a de Tecnologías de la Información y el/la Oficial de Seguridad de la Información pueden activar 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

2. PLAN DE RECUPERACIÓN

a) Personal Encargado
El equipo de recuperación de TI, luego de restaurar el correcto funcionamiento del servidor, estación de trabajo (PC, laptop), sistemas de información y portales web, coordinará con el/la Jefe/a de Tecnologías de la Información para reanudar las labores de trabajo con el equipo o sistema que fue afectado.

b) Descripción de actividades
Se informará a el/la Jefe/a de Tecnologías de la Información 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.

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 MINEM.
El evento será evaluado y registrado de ser necesario en el formato de ocurrencia de incidentes de seguridad informática.

b) Mecanismos de Comprobación
El personal de Infraestructura Tecnológica, según sea el caso, presentará un informe a el/la Jefe/a de la Oficina de Tecnologías de la Información, explicando que parte del servicio u operaciones se han visto afectadas, y cuáles son las acciones tomadas.

Se llenará el formato de incidentes de seguridad digital y se informará al Comité de Gobierno Digital.

c) Desactivación del plan de Recuperación
Con el aviso de el/la Jefe de Tecnologías de la Información se desactivará el presente plan.

Código:	**FRS – 27**
Activo crítico:	**Antispam**
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 Infraestructura Tecnológica 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 Jefe/a de Tecnologías de la Información y el/la Oficial de Seguridad de la Información pueden activar la contingencia.

c) Personal Encargado
Equipo Emergencia de Tecnologías ed la Información

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 recuperación de TI, luego de restaurar el correcto funcionamiento del servidor, estación de trabajo (PC, laptop), sistemas de información y portales web, coordinará con el/la Jefe/a de Tecnologías de la Información para reanudar las labores de trabajo con el equipo o sistema que fue afectado.

b) Descripción de actividades
Se informará a el/la J efe/a de Tecnologías de la Información 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.

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 MINEM.
El evento será evaluado y registrado de ser necesario en el formato de ocurrencia de incidentes de seguridad informática.

c) Mecanismos de Comprobación
El personal de Infraestructura Tecnológica, según sea el caso, presentará un informe a el/la Jefe/a de la Oficina de Tecnologías de la Información, explicando que parte del servicio u operaciones se han visto afectadas, y cuáles son las acciones tomadas.
Se llenará el formato de incidentes de seguridad digital y se informará al Comité de Gobierno Digital.

d) Desactivación del plan de Recuperación

Con el aviso de el/la Jefe de Tecnologías de la Información se desactivará el presente plan.

ANEXOS

ANEXO N° 1: INVENTARIO DE SISTEMAS Y APLICACIONES

SISTEMA	SIGLAS	DESCRIPCIÓN	UO	LENGUAJE
Sistema de Evaluación Ambiental en Línea	SEAL	Sistema de registro, consulta y evaluación de los estudios ambientales que solicitan los titulares Mineros.	DGAAM	plone - javasript - python
Sistema Ambiental Minero Energético	SIA	Sistema para el registro, control y seguimiento de los instrumentos de gestión ambiental.	DGAAM / DGAAE / DGAAH	Power Builder
Sistema de Pago de Aportes de las Empresas Eléctricas	APORTES	Sistema para la declaración de autoliquidación de aportes de las empresas eléctricas	DGE	.Net
Sistema de Concesiones Eléctricas de la DGE	SISCE	El sistema SISCE está diseñado para registrar toda la información requerida sobre concesiones eléctricas y hacer seguimiento de proceso de trámite de concesiones.	DGE	.Net
Sistema Acreditación de Pequeño Productor Minero / Productor Minero Artesanal	REPPMA	También cuenta con opciones de reportes y consultas, donde el usuario podrá crear sus consultas personalizadas y descargar su resultado en formato Excel y CSV.	DGFM	plone - javasript - python
Sistema de Ventanilla Única para Proceso de Formalización Minera	VUPC	Sistema para el registro de usuarios por región, registro de los requisitos físicos y evaluación del registro de los requisitos físicos.	DGFM	.Net
Sistema de Declaración Anual Consolidada	DAC	Sistema de declaración de todas las actividades que han realizado en un año cada titular minero en las concesiones que han sido otorgadas por INGEMMET.	DGM	plone - javasript - python
Sistema para la solicitud del Certificado de Operación Minera Excepcional	COMEX	Sistema de evaluación de los certificados de operación minera a los Titulares Mineros en el proceso de formalización.	DGM	plone - javasript - python
Registro Especial de Comercializadores y Procesadores de Oro	RCOM	Sistema donde se registran los comercializadores de Oro a nivel nacional.	DGM	plone - javasript - python
Inventarios Pasivos de Ambientales Mineros	IPA	Sistema donde se registran y actualizan los pasivos Ambientales Mineros, se evalúan y se da prioridad de rango.	DGM	plone - javasript - python
Garantía Plan de Cierre de Minas	GAR	Sistema donde se registran las garantías de plan de cierre.	DGM	plone - javasript - python
Concesiones y Autorizaciones de Beneficio	CAB	Sistema de evaluación de concesión y autorización de beneficio de los Titulares Mineros donde se autorizan por etapas el tratamiento del mineral obtenido.	DGM	plone - javasript - python
Sistema de Devolución de IGV	DIGV	Sistema de registro de solicitudes de devolución del impuesto general a las ventas, para luego ser evaluado.	DGM	plone - javasript - python

Aviso de Accidentes Mortales e Incidentes Peligrosos	MORTAL	Sistema donde declaran los accidentes mortales e incidentes peligrosos registrados en las	DGM	.Net
SISTEMA	**SIGLAS**	**DESCRIPCIÓN**	**UO**	**LENGUAJE**
		concesiones mineras por titular minero.		
Sistema de Autorización de Explotación - Plan de Minado	MINADO	Sistemas de evaluación y consulta de los planes de minado de los titulares mineros, aquí se otorgan Resolución Directoral para los permisos.	DGM	plone - javasript - python
Sistema de Autorización de Exploración	EXPLORA	Sistemas de evaluación y consulta de las solicitudes de inicio de actividades de exploración los titulares mineros, aquí se otorga Resolución Directoral para los permisos.	DGM	plone - javasript - python
Sistema de Contratistas Mineros	SISCO	Sistema web que permite a las empresas realizar el procedimiento de solicitud de inscripción de contratistas minera, las cuales serán revisadas por la Dirección General de Minería para su evaluación y aprobación respectiva.	DGM	.Net
Sistema de Fiscalización Minera	SIFIM	Sistema que permite registrar y hacer seguimiento de las inspecciones mineras encargadas a la DGM	DGM	.Net
Sistema Estadística Mensual Minera	ESTAMIN	Sistema de declaración mensual de la actividad que han realizado cada titular minero en las concesiones que han sido otorgadas por INGEMMET.	DGM	.Net
Sistema de información para la Gestión de Información, Medición, Reporte y Verificación	SISMRV	Plataforma MRV del sector energía el cual cada institución, pública o privada puede implementar en la medida de sus posibilidades cualquiera de las medidas de mitigación y hacer que las mismas aporten a las Contribuciones Nacionalmente Determinadas.	DGEE	.Net
Sistema de Información de Inventarios de Servidumbres de las Empresas Operadoras de la DGH	SERVIDUMBRE	Inventario de Servidumbres de los siguientes recursos: Baterías, Ductos, Locaciones y Instalaciones, para la actividad de hidrocarburos	DGH	.Net
Sistema de Seguimiento de Casos y Compromisos Sociales	SSCCS	Registro de los conflictos sociales de los compromisos social, del sector minero-energético	OGGS	plone - javasript - python
Sistema para el Programa Minero de Solidaridad con el Pueblo	PMSP	Registro del seguimiento de proyectos del sector mineros, convenios con 39 empresas por 5 años (Empresas-Gobierno-Población)	OGGS	plone - javasript - python

Sistema de Fondo Social	FS	Registro del seguimiento de fondo sociales del sector minero - energético, licitaciones que realiza pro inversión (7 empresas)	OGGS	plone - javasript - python
SISTEMA	**SIGLAS**	**DESCRIPCIÓN**	**UO**	**LENGUAJE**
Seguimiento de Asuntos Sociales - Mesa de Diálogo	SSAS	Sistema para gestionar la información de los asuntos sociales del sector, con el fin de prevenir casos de conflicto, a través del registro de compromisos y hechos, para el seguimiento de su cumplimiento.	OGGS	.Net
Sistema de Declaración de Compromisos Sociales Mineros	DCSM	Registro del seguimiento y avances de los compromisos sociales del sector minero. Según el EIA existe dos compromisos sociales Obligatorio y Voluntario	OGGS	.Net
Sistema GIS de consulta geoespacial del MINEM	GIS	Sistema web que permite consultas de información geoespacial, de acuerdo a cada tema ya sea de datos de energía eólica, hidroeléctrico, minero entre otros que tiene disponible el Minem.	DGE , DGER, DGM	.Net - javascript
Sistema de Visitas	VISITAS	Registro de sistemas de Visitas de usuarios que ingresan al Ministerio a las diferentes áreas.	IMAGEN	plone - javasript - python
Sistema de Tramite Documentario	SITRADOC	Sistema para el registro, control y seguimiento de los documentos externos (mesa de partes) e internos.	OADAC	Power Builder
Sistema de Gestion Documentaria	SIGED	Sistema para el seguimiento y control de los documentos ingresados por Ventanilla Virtual y Acceso a la Información Pública.	OADAC	.Net
Sistema de Ventanilla Virtual	VV	Sistema para facilitar a los administrados el registro de la solicitud de expedientes para la tramitación de un Procedimiento Administrativo TUPA o NO TUPA.	OADAC	.Net
Sistema Transparencia de Acceso a la Información Pública	SAIP	Sistema para el registro y control de solicitudes de acceso de información pública.	OADAC	.Net
Sistema de Control del Proceso de Digitalización	SIDIG	Sistema para el control de la digitalización de expedientes físicos que ingresan por mesa de partes.	OADAC	.Net
Sistema de Atención de Tickets	CERO-COVID	Aplicativo para el registro de solicitud de atención de mesa de partes.	OADAC	.Net
Sistema de Mesa de Ayuda	SMA	Sistema para el registro, control y seguimiento de las solicitudes de mesa de ayuda que recibe la Oficina de Tecnologías de la Información	MINEM	.Net
Sistema de Inventario de Control de Archivos	SICA	Sistema para el control de documentos ingresados al archivo central del ministerio.	OADAC	.Net

Sistema de Biblioteca Virtual y Consulta	BLIDMEM	Sistema que emite registrar y publicar los documentos al portal Institucional o a la Intranet del MINEM y administrar, controlar el registro y publicación de los documentos de las diferentes direcciones generales.	OGA	.Net
Sistema de Convocatorias CAS	CONVOCAS	Sistema de gestión para el soporte del ciclo de vida de las convocatorias CAS	ORH	.Net

SISTEMA	SIGLAS	DESCRIPCIÓN	UO	LENGUAJE
Sistema Integrado de Gestión Administrativo	EL GESTOR	Sistema para la gestión administrativa del MINEM, a nivel de OGA y oficinas dependientes.	OGA	Power Builder
Sistema Integrado de Gestión Administrativo - El Gestor Web	GESTOR WEB	Sistema para la gestión administrativa del MINEM, a nivel de usuarios y oficinas solicitantes.	OGA	.Net
Sistema de Denuncias por Actos de Corrupción	SIDE	Sistema de registro, control y seguimiento de las denuncias respecto a actos de corrupción.	OADAC	.Net
Sistema de Personal	SISPER	Sistema que brinda soporte al registro de papeletas de asistencia y vacaciones (programación, reprogramación)	ORH	.Net
Sistema de registro, control y seguimiento de recomendaciones	MOREC	Sistema para el registro y seguimiento de recomendaciones de la OCI.	OII	.Net
Sistema de Cobranza Coactiva y Multas	SISCC	Sistema de cobranza coactivas y multas del sector minero y energía administrador por la Oficina de Cobranza Coactiva y Financiera	OFIN	.Net
Plataforma de Gestión Proyecta MINEM	PROYECTA	Sistema para el registro y consulta de los principales proyectos mineros	ALTA DIRECCIÓN	.Net
Canon Minero	CANON	Sistema para el registro de importe de ventas de las empresas del canon minero	DGM	.Net

ANEXO N° 2: INVENTARIO DE LA INFRAESTRUCTURA TECNOLÓGICA

1. Inventario de Servidores:

Detalle de Máquinas Virtuales	Total
CentOS 4/5 or later (64-bit)	2
CentOS 4/5/6/7 (64-bit)	6
CentOS 8 (64-bit)	2
Microsoft Windows Server 2003 Standard (32-bit)	2
Microsoft Windows Server 2008 R2 (64-bit)	19
Microsoft Windows Server 2012 (64-bit)	71
Microsoft Windows Server 2016 (64-bit)	17
Microsoft Windows Server 2019(64-bit)	16
Microsoft Windows Server 2022(64-bit)	26
Red Hat Enterprise Linux 6 (64-bit)	1
Red Hat Enterprise Linux 8 (64-bit)	6
Ubuntu Linux (64-bit)	1
Total general	169

Sistema Operativo de Máquinas Virtuales	Total
Linux	18
Windows Server	151
Total general	169

2. Inventario de Base de Datos Oracle:

Virtual Machine	Sistema Operativo	Virtualizado con	Memoria GB	Procesador	Capacidad GB	Detalle
MEM7	Oracle Linux version 7.9	Oracle Linux Virtualization Manager 4.4	64	16	6519.6	Servidor de Base de datos Oracle 19.0 - RAC
MEM9	Oracle Linux version 7.9	Oracle Linux Virtualization Manager 4.4	32	16	1885.68	Servidor de Base de datos Oracle 10.0 - RAC
WEBMEM	Oracle Linux version 7.9	Oracle Linux Virtualization Manager 4.4	16	8	1390	Servidor de Base de datos Oracle 19.0 - RAC
MEMSPFISE01	Oracle Linux 8 (64-bit)	VMWare - esxi	8	4	250	Servidor FISE - Web FISE - Publicaciones

3. Inventario Storage:

Storage	Detalle	TB
Storage VNX-5400	VMWare	100
Storage Unity 450F	VMWare	50
Storage Unity 450F	Oracle	27
Storage PowerStore 500t	VMWare	7

4. Inventario de Equipo de Seguridad Perimetral:

Hardware	Marca	Modelo
Router (Principal)	Mikrotik	CCR1009-7G-1C-1S
Router (Secundario)		
Firewall (Principal)	Palo Alto	PAN-PA-3220
Firewall (Secundario)		
AntiDDoS (Principal)	Fortinet	FortiDDoS-200F
AntiDDoS (Secundario)		
Filtro Web (Principal)	Barracuda	WSG610
Filtro Web (Secundario)		
Gestor Ancho de Banda	Exinda	4062 Series
AntiSpam (Principal)	FortiMail	Fortimail-400F
AntiSpam (Secundario)		
WAF (Principal)	FortiWeb	FortiWeb-600E
WAF (Secundario)		

5. Inventario de Equipos de Comunicaciones:

Switch	Orden	Modelo	Detalle
SW_CORE_MEM	SW-STACK	WS-C4500X-32	cat4500e-universalk9.SPA.03.08.01.E.152-4.E1.bin
	SW-STACK	WS-C4500X-32	cat4500e-universalk9.SPA.03.08.01.E.152-4.E1.bin
SW-DATACENTER	SW-MASTER	WS-C3850-48T	cat3k_caa-universalk9
	SW-STACK	WS-C3850-48T	cat3k_caa-universalk9
SW-DMZ-PUBLICO	ÚNICO	WS-C2960S-24PS-L	C2960S-UNIVERSALK9-M
SW-WAF-IMPERVA	ÚNICO	WS-C2960S-24PS-L	C2960S-UNIVERSALK9-M

6. Inventario de Switch Capa 2

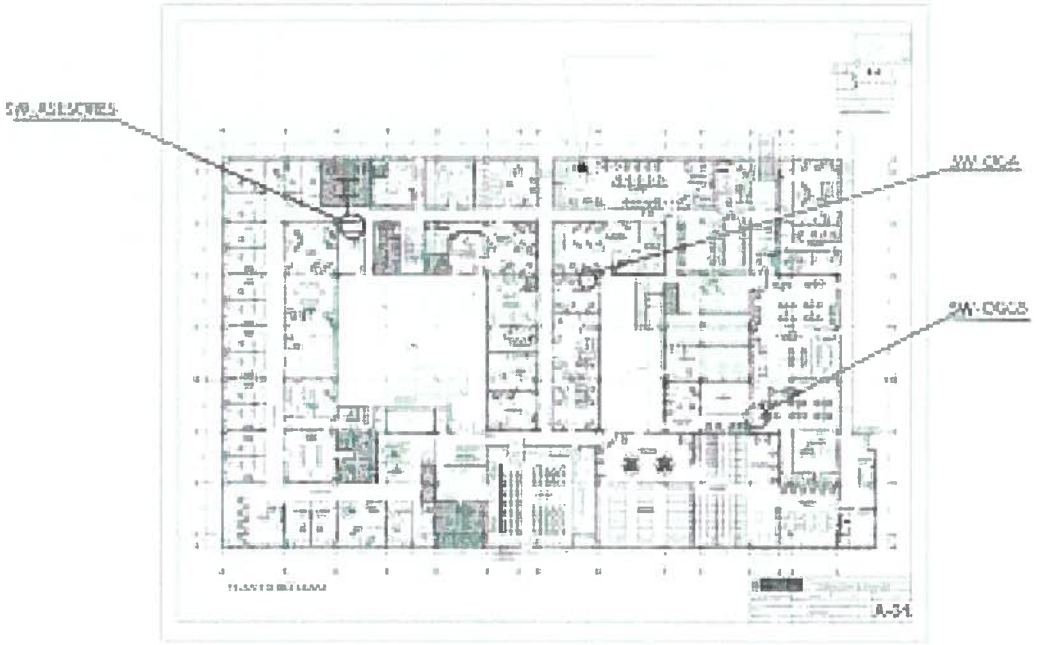
UBICACIÓN	MODELO	ORDEN	Total	Libres	Ocupados
OGA	WS-C2960X-48LPD-L	SW-MASTER	48	7	41
	WS-C2960X-48LPD-L	SW-STACK	48	28	20
	WS-C2960X-48LPD-L	SW-STACK	48	3	45
	WS-C2960X-48LPD-L	SW-STACK	48	16	32
	WS-C2960X-48LPD-L	SW-STACK	48	0	48
ASESORES	WS-C2960X-48LPD-L	SW-MASTER	48	0	48
	WS-C2960X-48LPD-L	SW-STACK	48	2	46
	WS-C2960X-48LPD-L	SW-STACK	48	18	30
CASA ALQUILADA	WS-C2960L-48PS-LL	CASCADA POR RADIO ENLANCE	48	4	44
SJM	WS-C2960S-24PS-L	CASCADA POR RADIO ENLANCE	24	0	24
CARELEC	WS-C2960X-48LPD-L	SW-MASTER	48	28	20
	WS-C2960X-48LPD-L	SW-STACK	48	39	9

UBICACIÓN	MODELO	ORDEN	Total	Libres	Ocupados
	WS-C2960X-48LPD-L	SW-STACK	48	15	33
DESPACHO MINISTERIAL	WS-C2960X-48LPD-L	SW-STACK	48	3	45
	WS-C2960X-48LPD-L	SW-STACK	48	9	39
OADAC - EXPEDIENTES	WS-C2960X-48LPD-L	SW-MASTER	48	2	46
	WS-C2960X-48LPD-L	SW-STACK	48	21	27
DGAAM	WS-C2960X-48LPD-L	SW-MASTER	48	0	48
	WS-C2960X-48LPD-L	SW-STACK	48	0	48
	WS-C2960X-48LPD-L	SW-STACK	48	0	48
DGE	WS-C2960X-48LPD-L	SW-MASTER	48	15	33
	WS-C2960X-48LPD-L	SW-STACK	48	30	18
DGH	WS-C2960X-48LPD-L	SW-STACK	48	18	30
	WS-C2960X-48LPD-L	SW-MASTER	48	5	43
	WS-C2960X-48LPD-L	SW-STACK	48	18	30
DGM	WS-C2960X-48LPD-L	SW-MASTER	48	13	35
	WS-C2960X-48LPD-L	SW-STACK	48	14	34
	WS-C2960X-48LPD-L	SW-STACK	48	28	20
	WS-C2960X-48LPD-L	SW-STACK	48	14	34
DGAAE	WS-C2960X-48LPD-L	ÚNICO	48	0	48
	WS-C2960G-48TC-L	SW-CASCADA (SW-DGAAE-I)	48	12	36
OADAC	WS-C2960X-48LPD-L	SW-MASTER	48	9	39
	WS-C2960X-48LPD-L	SW-STACK	48	10	38
DGEE	WS-C2960X-48LPD-L	SW-MASTER	48	1	47
	WS-C2960X-48LPD-L	SW-STACK	48	1	47
OGGS	WS-C2960X-48LPD-L	ÚNICO	48	4	44
	WS-C2960S-48LPS-L	CASCADA (SW-OGGS-I)	48	20	28
	WS-C2960S-48FPD-L	CASCADA (SW-OGGS-II)	48	18	30
OTI	WS-C2960X-48LPD-L	SW-MASTER	48	11	37
	WS-C2960X-48LPD-L	SW-STACK	48	3	45
	WS-C2960X-48LPD-L	SW-STACK	48	2	46
YANACOTO	WS-C2960S-48FPD-L	ÚNICO	48	44	4
SJM	SG350X-24 24-Port	CASCADA (SW-ARCHIVO-SJM)	24	23	1

7. Ubicación de Gabinetes

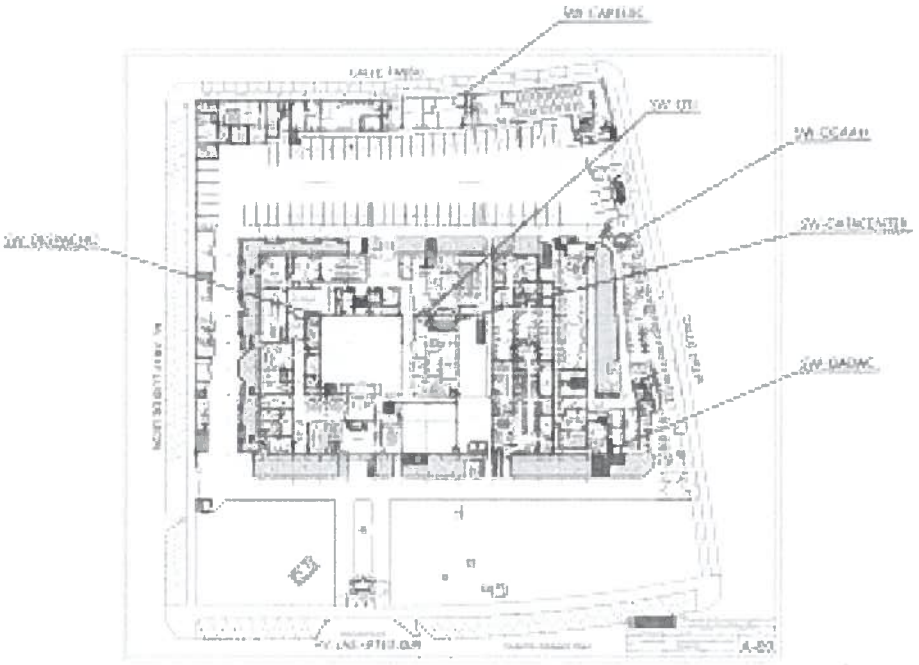
7.1 Plano 01

Ubicación	:	Av. Las Artes 260
Distrito	:	San Borja
Provincia	:	Lima
Departamento	:	Lima
Plano	:	Sótano
Escala	:	1:100



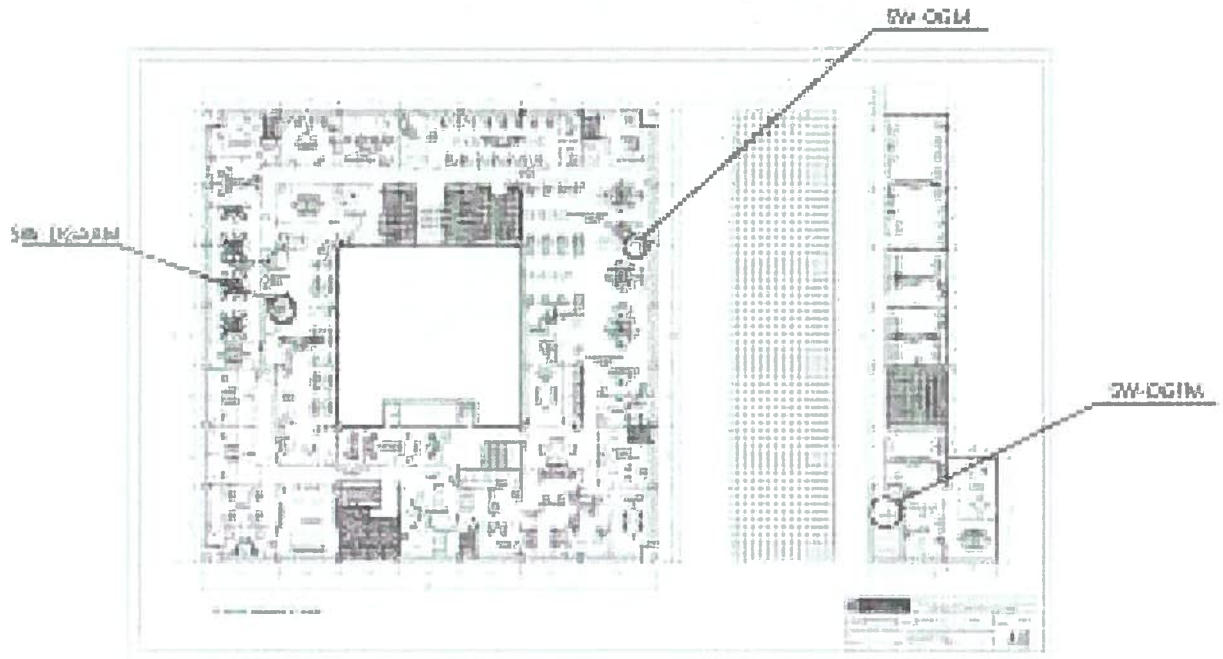
7.2 Plano 02

Ubicación	:	Av. Las Artes 260
Distrito	:	San Borja
Provincia	:	Lima
Departamento	:	Lima
Plano	:	Primer Piso
Escala	:	1:100



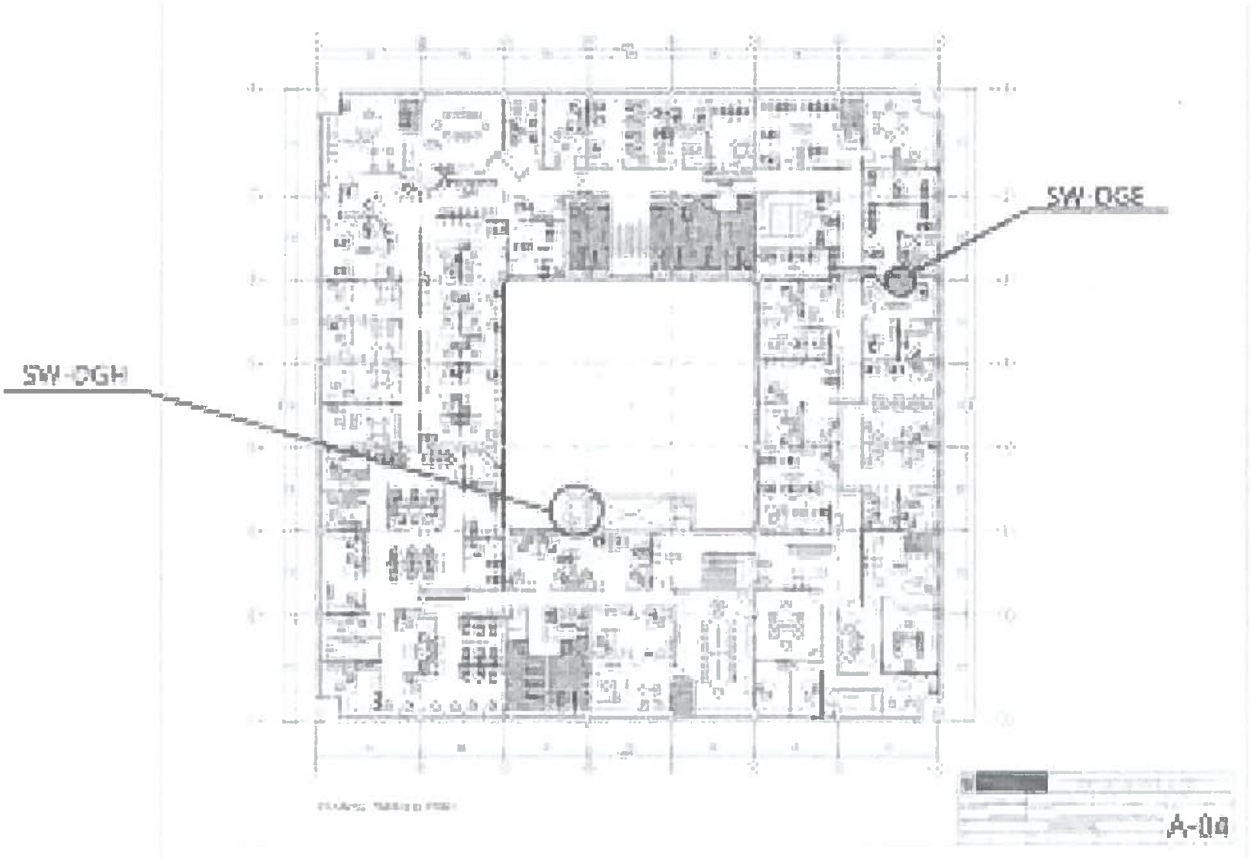
7.3 Plano 03

Ubicación	:	Av. Las Artes 260
Distrito	:	San Borja
Provincia	:	Lima
Departamento	:	Lima
Plano	:	Segundo Piso
Escala	:	1:100



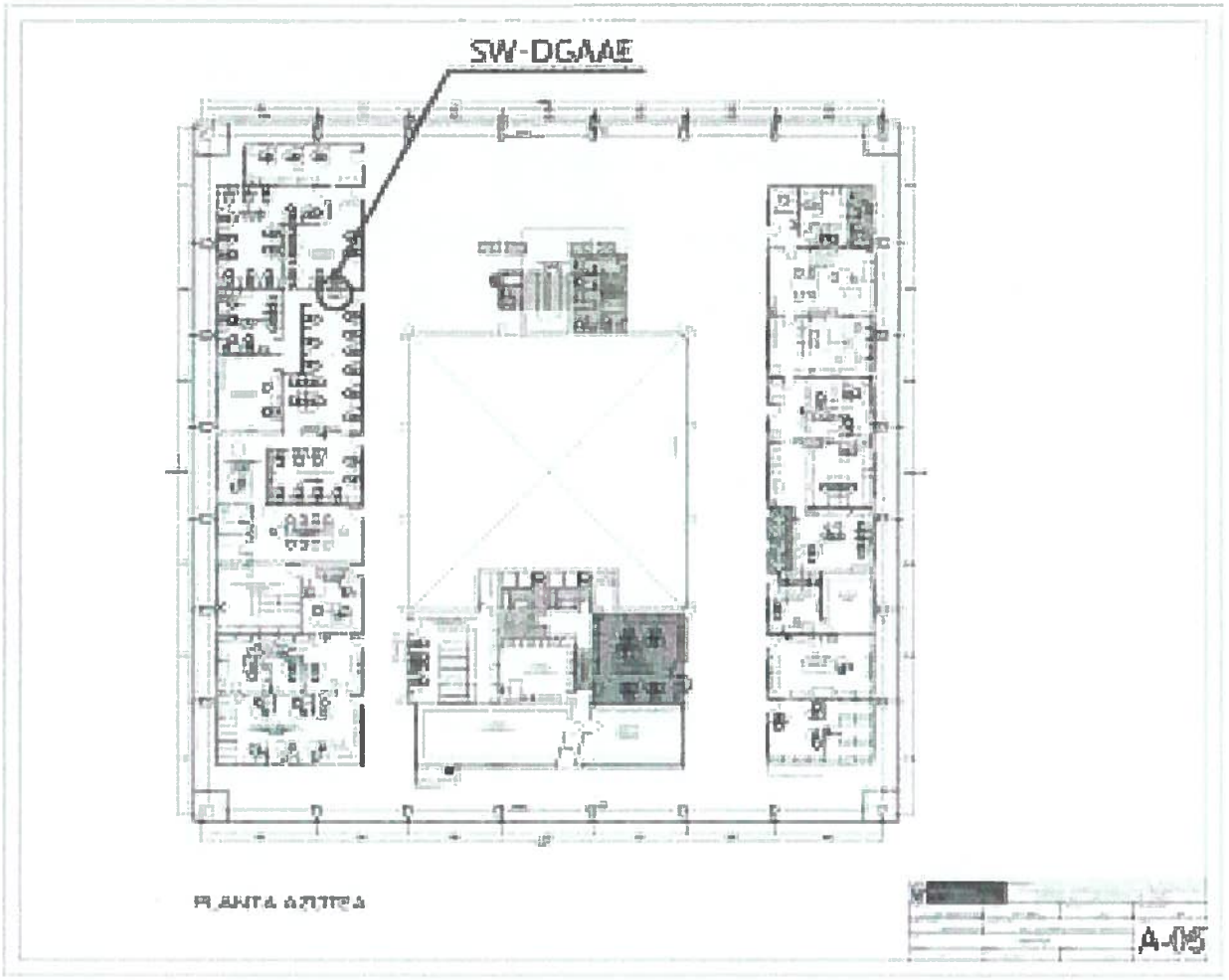
7.4 Plano 04

Ubicación	:	Av. Las Aries 260
Distrito	:	San Borja
Provincia	:	Lima
Departamento	:	Lima
Plano	:	Tercer Piso
Escala	:	1:100

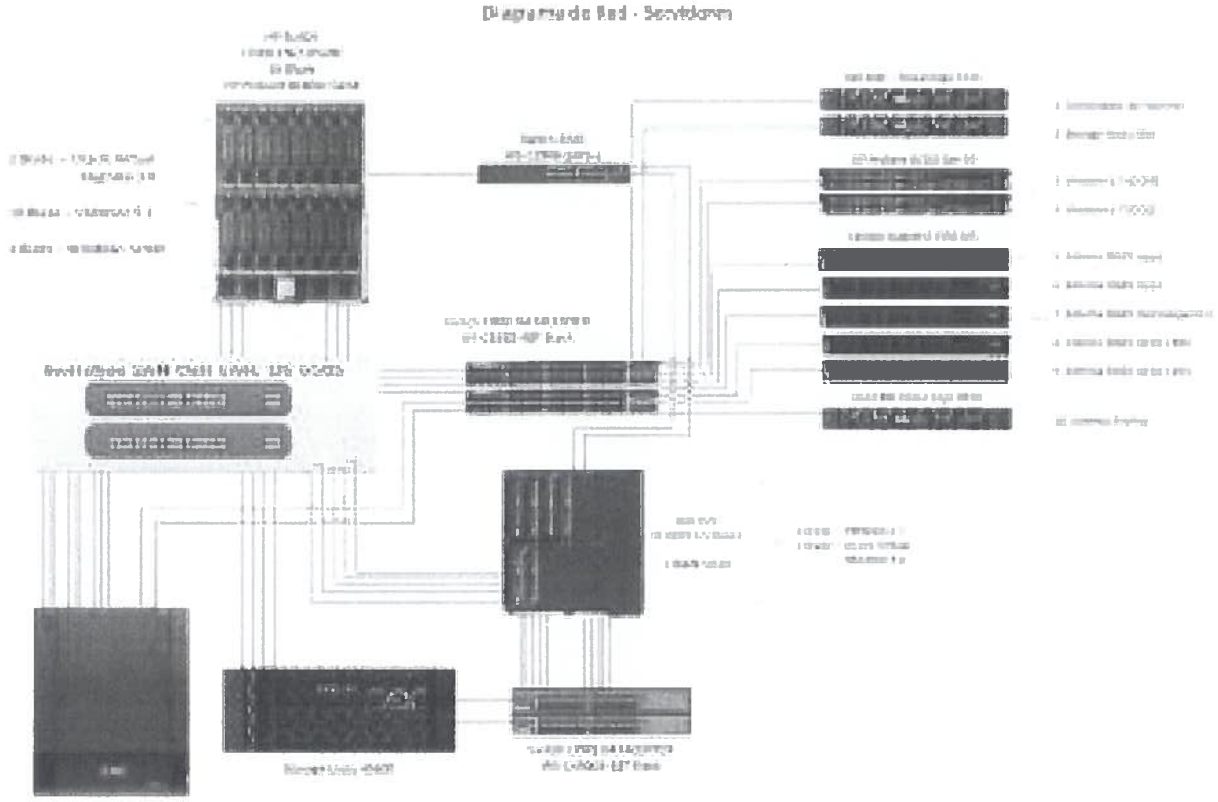


7.6 Plano 06

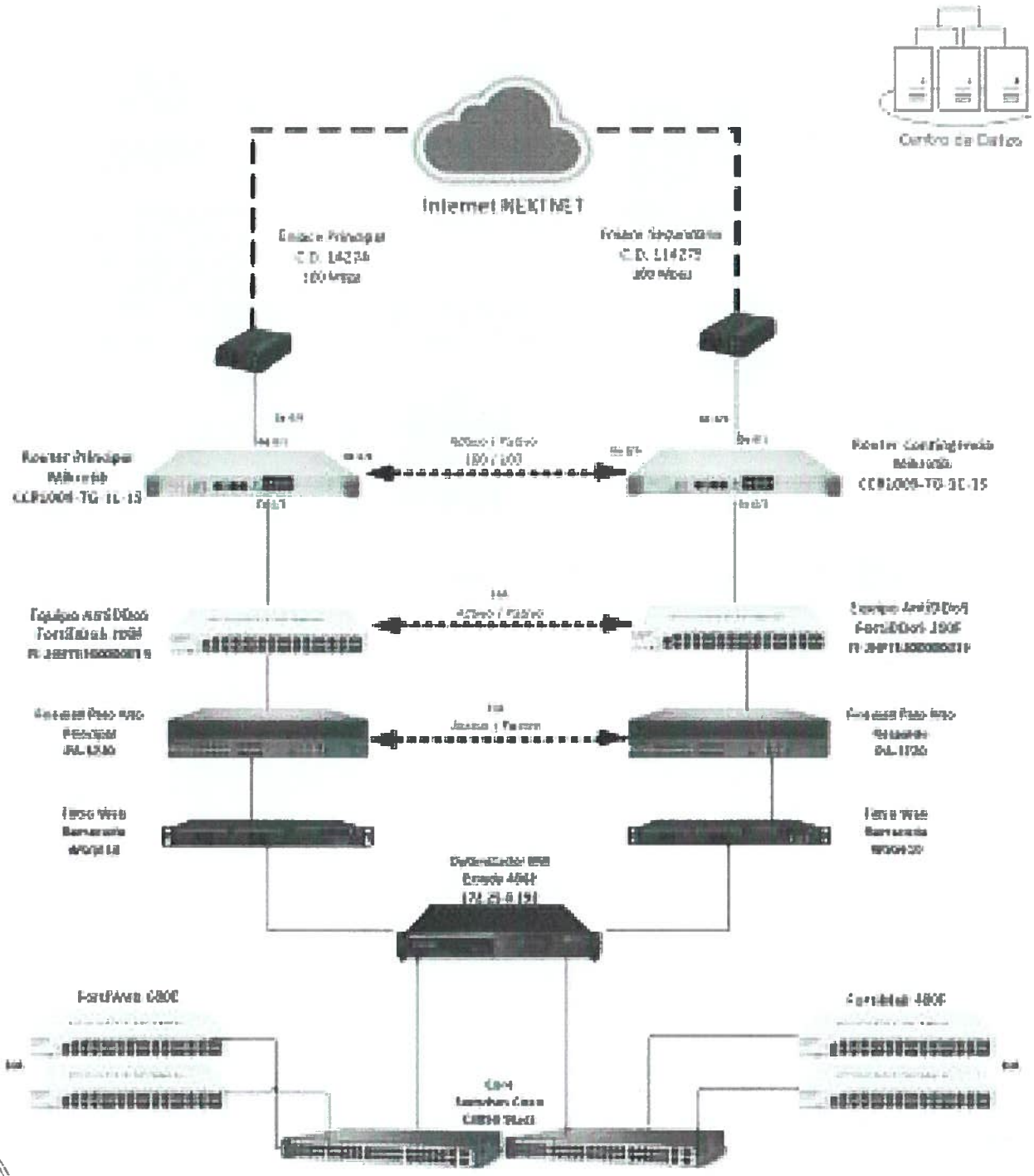
Ubicación	:	Av. Las Artes 260
Distrito	:	San Borja
Provincia	:	Lima
Departamento	:	Lima
Plano	:	Azotea
Escala	:	1:100



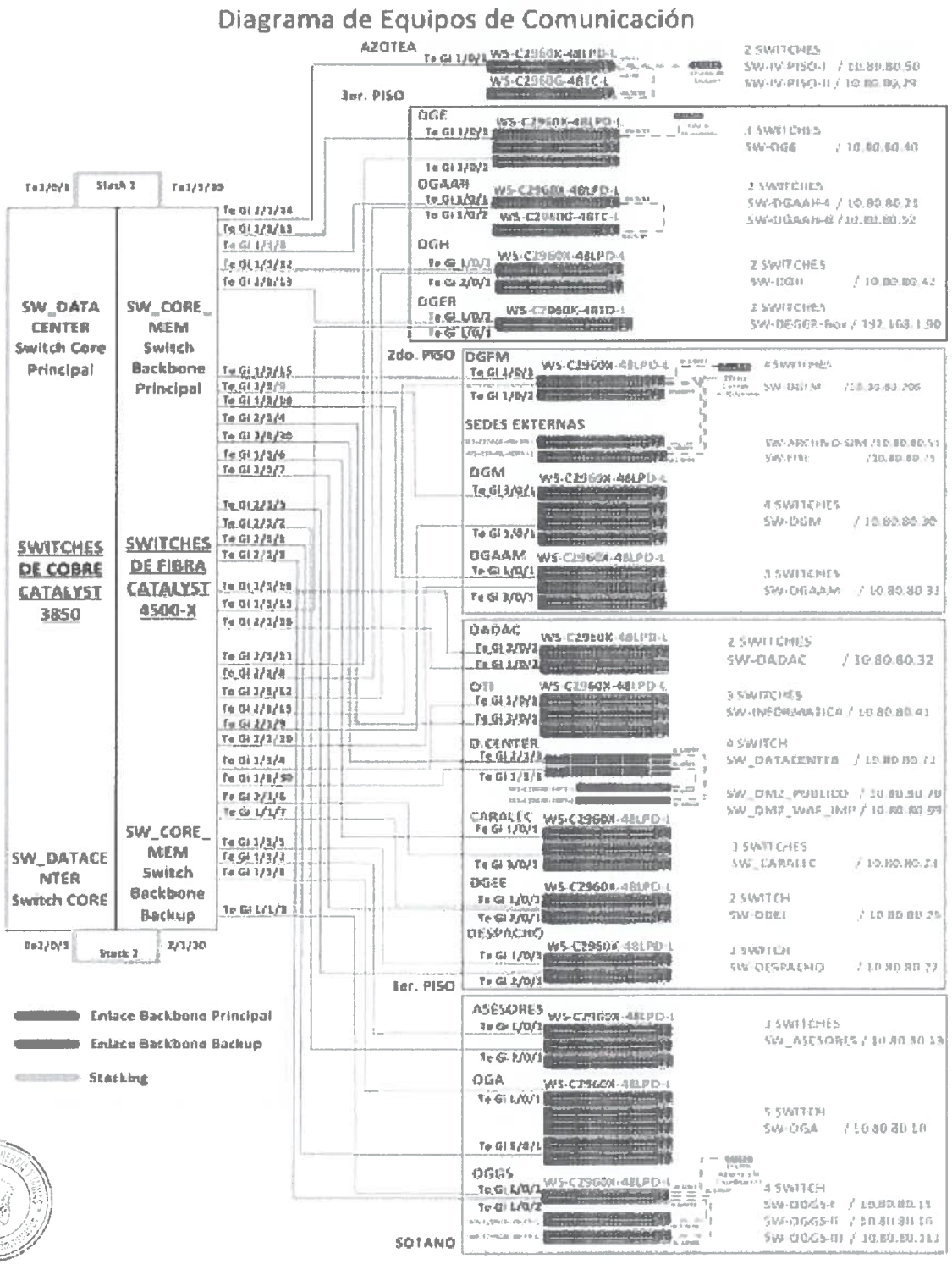
8. Diagrama de Servidores



9. Diagrama de Equipos de Seguridad Perimetral



0. Diagrama de Equipos de Comunicación



ANEXO 3: GESTIÓN DE PROVEEDORES

GESTION DE PROVEEDOR OTI				
Empresa	Servicio	Móvil	correo	Nombre Contacto
Smart Global	Firewall	080071770 01-6418341	nsoc@smartglobal.pe	Operador de 1er y 2do Nivel
Smart Global	Firewall	954386249	mariela.mamani@smartglobal.pe	Mariela Mamani Díaz
Bigsecure	FiltroWeb Barracuda	942235084	jvasquez@bigsecure.net	Jhosman Vasquez
NextNet	Internet	9487715866	mfulleda@nextnet.pe	Milena Fulleda Bravo
Fravatel	Telefonía	986681333 510 0000 / Anexo 209	noc@fravatel.com.pe	Jean Piers Montero P.
Fravatel	Telefonía	908823673 510 0000 / Anexo 204	noc@fravatel.com.pe	Rodrigo Antonio Aranda Ybañez
Consultoria data	Base de Datos Oracle	984126262	econde@consultoriadata.com	Eduardo Conde
Consultoria data	Base de Datos Oracle	----------	proyectos@consultoriadata.com	----------
Consultoria data	Base de Datos Oracle	----------	aquivio@consultoriadata.com	Alba Quivio
Softline International Perú SAC	Microsoft (Windows Server - Exchange Server)	980702614 6371200 ext. 395	Dorliska.garcia@softline.com	Dorliska García Meléndez
Softline International Perú SAC	Microsoft (Windows Server - Exchange Server)	981473996	Juan.Ureta@softline.com	Juan Diego Ureta Valdez
Softline International Perú SAC	Microsoft (Windows Server - Exchange Server)	922748450	Emmanuel.Mateo@softline.com	Emmanuel Mateo
Polysistemas	Laserfiche	962772500	carlos.asto@polysistemas.com	Carlos Asto
Zenware	Backup - Networker	956285137	soporte@zenware-la.com	Rodrigo Huerta
Zenware	Storage Dell	920369702	soporte@zenware-la.com	Chalks Alvino
Zenware	WMWARE 6.7	920369702	soporte@zenware-la.com	Chalks Alvino
BigSecure	Waf-Antispam	942235084	jvasquez@bigsecure.net	Jhosman Vasquez
BigSecure	Waf-Antispam	988 963 695	apuicon@bigsecure.net	Anggie Puicon
BigSecure	Waf-Antispam	985 317 593	knima@bigsecure.net	Kacelly Nima
BigSecure	Waf-Antispam	----------	soporte@bigsecure.net	Soporte de Casos Escalados
Vecodata	FortiMail	994274098	jcjaves@vecodata.pe	Juan Javes Sanchez
Vecodata	FortiDDoS	994274098	jcjaves@vecodata.pe	Juan Javes Sanchez
Vecodata	FortiWeb	994274098	jcjaves@vecodata.pe	Juan Javes Sanchez
EXXODA	Antivirus	947637435	luis.ayala@exxoda.com	Luis Ayala
EXXODA	Antivirus	951347624	alonso.rodriguez@exxoda.com	Alonso Rodriguez
EXXODA	Antivirus	928748574	jesus.palacios@exxoda.com	Jesus Palacios
EXXODA	Antivirus	967762316	vicente.pisco@exxoda.com	Vicente Pisco
EXXODA	Antivirus	967762316	luis.cardenas@exxoda.com	Luis Cardenas
EXXODA	Antivirus	987277247	manuel.pena@exxoda.com	Manuel Peña

ANEXO 4: CONTINGENCIA

Disaster Recovery

El Plan de Recuperación de Sistemas Informáticos tiene por finalidad; mantener un inventario de hardware (servidores, computadoras, portátiles, equipos de comunicación, otros), aplicaciones de software y datos que nos permitan desarrollar estrategias que garantice ante un evento la realización de respaldos de toda la información crítica y la puesta en funcionamiento de los servicios que el Ministerio de Energía y Minas brinda a la ciudadanía.

La OTI para tal efecto ha identificado datos de los servidores de red (configuraciones y sistemas), computadoras de escritorio, computadoras portátiles y dispositivos de los cuales es necesario hacer copias de seguridad. El plan de recuperación incluye copias de seguridad programadas regularmente a un dispositivo de almacenamiento de alta capacidad conectado a una red que permitirá a los usuarios autorizados gestionar el almacenamiento y recuperar datos a una infraestructura similar que nos permita poner en funcionamiento los servicios informáticos resguardados.

La lista de verificación de DRP consiste en:

- Identificación de redes y sistemas informáticos críticos (aquellos que son vitales para que el MINEM pueda seguir operando).
- Definición del RPO (objetivo del punto de recuperación, es decir, cada cuánto tiempo se realiza una copia de seguridad de los datos y sistemas críticos de la empresa) y del RTO (objetivo del tiempo de recuperación, es decir, el tiempo de inactividad permitido hasta la recuperación de la normalidad).
- Las acciones necesarias para reiniciar, reconfigurar y recuperar sistemas, datos y redes.

Además, el plan de recuperación de Sistemas Informáticos debe ser difundido a todos los colaboradores del MINEM, con la finalidad que tengan conocimiento de las acciones ante un incidente o brecha de seguridad que pueda poner en riesgo la continuidad del servicio informático y de sistemas.

Relación de Aplicaciones críticas de TI

En el Anexo N° 01 está especificado las aplicaciones críticas, estas aplicaciones de servicios críticos son componentes básicos para el funcionamiento de los procesos críticos del MINEM cuya paralización haría que no se pueda brindar los servicios a nivel nacional.

En el Anexo 02, se muestra el inventario de la Infraestructura Tecnológica con que cuenta la OTI, estos recursos están expuestos a amenazas. Las amenazas identificadas son: terremoto, inundación y aniego, incendio, delitos informáticos, debilidad estructural, falla en la energía eléctrica, pandemia, ataque terrorista, disturbios sociales, actividad criminal, falla en las

telecomunicaciones, caída de internet y lluvias.

Se han determinado controles los cuales permiten determinar qué tan protegidos se encuentran los recursos críticos frente a la ocurrencia de una amenaza. Los controles con los que actualmente cuenta la OTI son los siguientes:

Recurso Crítico	Control Existente
Servidores • Servidores de base de datos • Servidores de la plataforma de virtualización • Servidores raqueables **Sistema de Almacenamiento** **Librerías de respaldo**[1] **Equipos de comunicación**[2] **Firewall**	**Datacenter** • Cámaras de videovigilancia en el Interio del Centro de Datos • UPS dentro del centro de datos • Mantenimiento del Aire Acondicionado • Sistema Contra Incendios en el Centro de Datos • Política de Backup
Internet	Contrato Vigente con proveedor de Internet
Servicios Informáticos • SIAF • SIGA • Portal MINEM • Ventanilla Electrónica • Correo Electrónico • Controlador de Dominio	• Política de Backup

Para determinar el nivel de riesgo, la OTI utilizó la metodología de evaluación de riesgos descrita en

el numeral 5.1.4 del presente documento, obteniéndose el siguiente resultado:

[1] Se debe tener en cuenta que los equipos de respaldo ya no cuentan con soporte ni garantía de la marca esto se indica en el informe técnico N° 013-2023-MINEM-OGA-OTI/FP donde se solicita su reemplazo

[2] Los equipos de comunicaciones ya no cuentan con soporte ni garantía de la marca, esto se indica en el informe técnico N° 001-2021- MINEM-OGA-OTI/FP donde se solicita su reemplazo.

RECURSO CRITICO	Terremoto	Inundación y Anlego	Incendio	Delitos Informáticos	Debilidad Estructural	Falla de Energía Eléctrica	Pandemia o Epidemia	Ataque Terrorista	Disturbios Sociales	Actividad Criminasl	Fallas en las Telco	Caída de Internet/Sistemas	Prensa Amarilla	Lluvias
Servidores • Servidores de Base de datos • Servidores para plataforma de virtualización • Servidores Raqueables Sistema de Almacenamiento Librerías de respaldo Equipos de comunicación Firewall														
Internet														
Servicios informáticos • SIAF • SIGA • Portal MINEM • Ventanilla Electrónica • Correo electrónico Controlador de dominio														

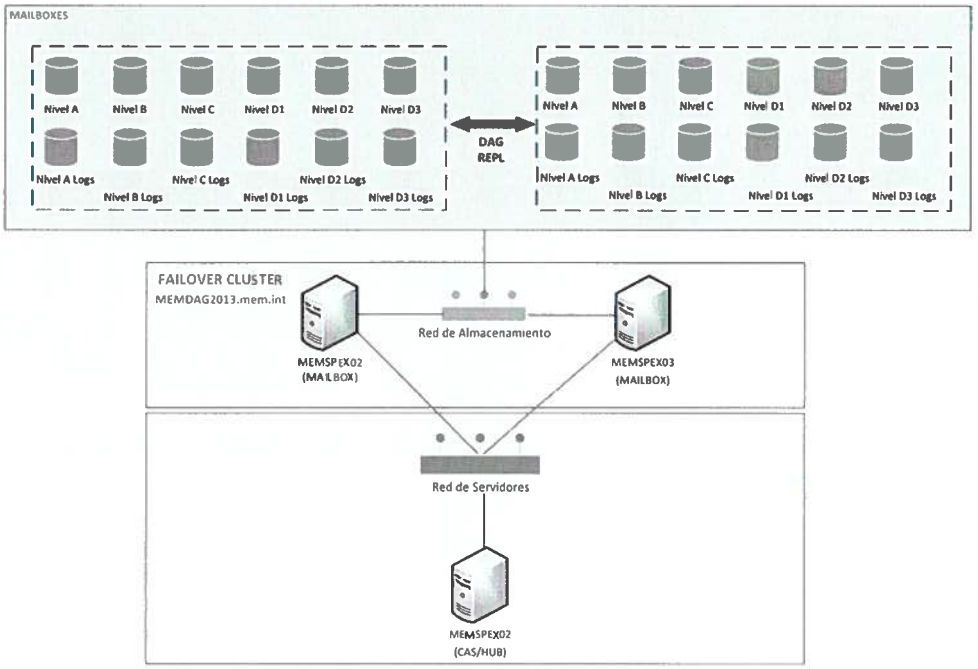
ANEXO N° 5: ESTRATEGIA PARA CORREO ELECTRÓNICO

1. Situación Actual

Actualmente el MINEM cuenta con un servidor de correos ONPREMISSE Microsoft Exchange Server 2013 - Versión 15.0 Build 1497.2, con 1780 buzones de correo.

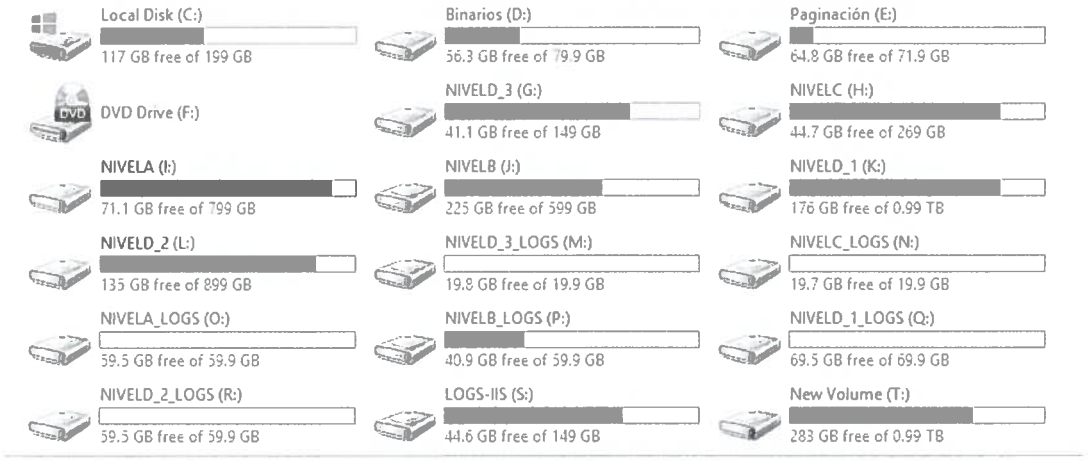
1.1 Topología de la infraestructura del Correo Electrónico Actual

Topología de la Infraestructura de Correo Electronico



1.2 Consumo de disco

- Espacio total asignado 5.42TB
- Espacio libre 1.45TB
- Espacio ocupado 3.97TB


Local Disk (C:)
117 GB free of 199 GB
Binarios (D:)
56.3 GB free of 79.9 GB
Paginación (E:)
64.8 GB free of 71.9 GB
DVD Drive (F:)
NIVELD_3 (G:)
41.1 GB free of 149 GB
NIVELC (H:)
44.7 GB free of 269 GB
NIVELA (I:)
71.1 GB free of 799 GB
NIVELB (J:)
225 GB free of 599 GB
NIVELD_1 (K:)
176 GB free of 0.99 TB
NIVELD_2 (L:)
135 GB free of 899 GB
NIVELD_3_LOGS (M:)
19.8 GB free of 19.9 GB
NIVELC_LOGS (N:)
19.7 GB free of 19.9 GB
NIVELA_LOGS (O:)
59.5 GB free of 59.9 GB
NIVELB_LOGS (P:)
40.9 GB free of 59.9 GB
NIVELD_1_LOGS (Q:)
69.5 GB free of 69.9 GB
NIVELD_2_LOGS (R:)
59.5 GB free of 59.9 GB
LOGS-IIS (S:)
44.6 GB free of 149 GB
New Volume (T:)
283 GB free of 0.99 TB

ANEXO N° 6: ESTRATEGIA PARA BASE DE DATOS

1. Situación Actual

Actualmente el MINEM cuenta con diferentes versiones de la base de datos Oracle, y a continuación las mencionamos:

- Servidor Oracle 11c Express Edition
- Servidor Oracle 12.1 Express Edition
- Servidor de Base de datos Oracle 19 Enterprise Edition
- Servidor de Base de datos Oracle 19 Enterprise Edition

1.1 Distribución de los Servidores Oracle

MARCA	VM	SO OVM	Virtualizador
DELL PowerEdge M640 RAM: 384 GB 2CPU Intel Xeon Gold 6142 2.6 GHz	DGM01	Oracle Linux versión 7.6	Oracle Virtual Machine Versión 3.4
	MEMSPBDCAT	Oracle Linux versión 7.6	
	RMEM71	Oracle Linux versión 7.6	
	RMEM91	Oracle Linux versión 7.6	
	RWEBMEM1	Oracle Linux versión 7.6	
	EM13	----	
DELL PowerEdge M640 RAM: 384 GB 2CPU Intel Xeon Gold 6142 2.6 GHz	RMEM72	Oracle Linux versión 7.6	
	RMEM92	Oracle Linux versión 7.6	
	RWEBMEM2	Oracle Linux versión 7.6	
HP Proliant BL460C Gen8 2 proc 128 GB RAM	MEMLISDBPING	VMware 5.1	VMWARE 5.1
	MEMLISDBGIS01		
	MEMSPFISEDB		

1.2 Arquitectura Oracle