RESOLUCIÓN DE ALCALDÍA N.º 472-2024-MDSJL

San Juan de Lurigancho, 02 de diciembre de 2024.

EL ALCALDE DE LA MUNICIPALIDAD DISTRITAL DE SAN JUAN DE LURIGANCHO

VISTOS: El Informe N.°358-2024-MDSJL/GDE-SGRD, de la fecha, del Subgerente de Gestiona del Riesgo de Desastre; el Informe N.°104-2024-MDSJL/OGGDI, de la fecha, del Jefe de la Oficina General de Gobierno Digital e Innovación; el Proveído N.º 985-2024-MDSJL/GM, de la fecha, de Gerencia Municipal; el Informe Legal N.º 306-2024-MDSJL/OGAJ, de la fecha, del Jefe de Oficina General de Asesoría Jurídica; el Proveído N.º 997-2024-MDSJL/GM, de la fecha, de Gerencia Municipal; el Proveído N.°4681-2024-MDSJL/OGSG, de la fecha, de la Jefa de Oficina General de Secretaría General; el Memorando N.°2477-2024-MDSJL/OGSG, de la fecha, del Jefe de Oficina General de Secretaria General; el Informe N.°114-2024-MDSJL/OGGDI, de la fecha, del Jefe de la Oficina General de Gobierno Digital e Innovación; el Proveído N.º 4911-2024-MDSJL/OGSG, de la fecha, de la Jefa de Oficina General de Secretaria General y ;

CONSIDERANDO:

Que, el artículo 194 de la Constitución Política del Perú establece que las municipalidades son órganos de gobierno local, con autonomía política, económica y administrativa en los asuntos de su competencia, lo cual es concordante con lo dispuesto en el artículo II del Título Preliminar de la Ley N.º 27972, Ley Orgánica de Municipalidades y modificatorias, siendo que dicha autonomía radica en la facultad de ejercer actos de gobierno, administrativos y de administración con sujeción al ordenamiento jurídico;

Que, el artículo 2 de la Ley N°28551, Ley que establece la obligación de elaborar y presentar planes de contingencia, define que los planes de contingencia son instrumentos de gestión que definen los objetivos, estrategias y programas que orienten las actividades institucionales para la prevención, la reducción de riesgos, la atención de emergencias y la rehabilitación en casos de desastres permitiendo disminuir o minimizar los daños, victimas y pérdidas que podrían ocurrir a consecuencia de fenómenos naturales, tecnológicos o de la producción industrial, potencialmente dañinos y en su artículo 3 señala que todas las personas naturales y jurídicas de derecho privado o público que conducen y/o administran empresas, instalaciones, edificaciones y recintos tiene la obligación de elaborar y presentar, para su aprobación ante la autoridad competente, planes de contingencia para cada una de las operaciones que desarrolle;

Que, el inciso 1.1. del artículo 1 de la Ley N°27658 Ley Marco de Modernización de la Gestión del Estado, modificado por el Decreto Legislativo 1554, declara al Estado peruano en proceso de modernización en sus diferentes instancias, dependencias, entidades, organizaciones y procedimientos, con la finalidad de mejorar la gestión pública y construir un Estado democrático, descentralizado y al servicio del ciudadano;

Que, mediante Resolución Ministerial N.º 004-2016-PCM, modificada por Resolución Ministerial N.º 166-2017-PCM, se 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;

Que, mediante Resolución Ministerial N.º 320-2021-PCM se apruebo 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";

Que, el literal f., inciso 5.1 del artículo 5 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, define: el Plan de Recuperación de los 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 criticas identificadas, permitiendo una posterior recuperación de las condiciones previas a su ocurrencia;

Que, el inciso 2 del artículo 41 de la Ordenanza N°459-MDSJL, aprueba el Reglamento de Organización y Funciones -ROF, señalando como una de las funcione de la Oficina General de Gobierno Digital e Innovación es "Formular, proponer, ejecutar y evaluar los planes informáticos en concordancia con los objetivos institucionales y necesidades de los órganos de la entidad";

Que, mediante Resolución de Alcaldía N°436-2024-MDSJL, se designó al Gerente Municipal como unidad orgánica responsable de la Gestión de la Continuidad Operativa en la Municipalidad Distrital de San Juan de Lurigancho, debiendo cumplir las funciones establecidas en 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;

Que, con Resolución de Alcaldía N°450-2024-MDSJL, se aprobó la conformación del Grupo de Comando para la Gestión de la Continuidad Operativa de la Municipalidad Distrital de San Juan de Lurigancho;

Que, con informe N°104-2024-MDSJL/OGGDI, el Jefe de la Oficina General de Gobierno Digital e Innovación, presenta la propuesta del Plan de Recuperación de los Servicios Informáticos de la Municipalidad Distrital de San Juan de Lurigancho 2024-2027, tiene como objetivo general, garantizar la continuidad operativa de los sistemas informáticos y la infraestructura tecnológica para el desarrollo de actividades de la Municipalidad Distrital de San Juan de Lurigancho, con el fin de continuar brindando servicios necesarios a la población, ante la ocurrencia de un desastre o evento que produzca una interrupción prolongada de sus operaciones;

Que, mediante Informe Legal N.°306-2024-MDSJL/OGAJ, el jefe de la Oficina General de Asesoría Jurídica señala que la finalidad es establecer un plan de acción operativo en informática, el cual se ejecutará en caso ocurra un evento disruptivo o contingencia que afecte los procesos y servicios municipales que se sustentan en infraestructura y servicios tecnológicos de la Municipalidad Distrital de San Juan de Lurigancho o tercerizados con la finalidad que los procesos y servicios municipales retornen al a situación previa a la ocurrencia del evento disruptivo o contingencia, concluyendo que emite opinión favorable para que se apruebe el Plan de Recuperación de Servicios Informáticos de la Municipalidad Distrital de San Juan de Lurigancho;

Que, mediante Informe N.°114-2024-MDSJL/OGG, el Jefe de la Oficina General de Gobierno Digital e Innovación, realiza las modificaciones del proyecto del Plan de Recuperación de los Servicios Informáticos de la Municipalidad Distrital de San Juan de Lurigancho 2024-2027

Que, estando a lo expuesto y en uso de las atribuciones conferidas por el numeral 6 del artículo 20 de la Ley N°27972- Ley Orgánica de Municipalidades;

RESUELVE:

Artículo 1.- APROBAR el **PLAN DE RECUPERACIÓN DE SERVICIOS INFORMÁTICOS 2024- 2027 DE LA MUNICIPALIDAD DISTRITAL DE SAN JUAN DE LURIGANCHO**, el mismo que como anexo forma parte integrante de la presente Resolución de Alcaldía.

Artículo 2.- ENCARGAR a la Oficina General de Gobierno Digital e Innovación, el cumplimiento de las disposiciones del Plan aprobado mediante la presente Resolución de Alcaldía.

Artículo 3.- ENCARGAR a la Oficina General de Comunicaciones e Imagen Institucional en coordinación con la Oficina General de Gobierno Digital e Innovación realicen la publicación de la presente Resolución en el portal institucional (www.munisjl.gob.pe).

Regístrese, comuníquese y cúmplase.

SAN JUAN DE LURIGANCHO
LIVIA ESTHER FLOREZ FERNANDEZ
JEFA DE OFICINA GENERAL DE SECRETARÍA GENERAL

SAN JUAN DE LURIGANCHO
JESÚS MALDONADO AMAO
ALCALDE

SAN JUAN DE LURIGANCHO
CAMBIA CONTIGO

MUNICIPALIDAD DE SAN JUAN DE LURIGANCHO

PLAN DE RECUPERACIÓN DE SERVICIOS INFORMÁTICOS DE LA MUNICIPALIDAD DISTRITAL DE SAN JUAN DE LURIGANCHO

2024-2027

MUNICIPALIDAD DE SAN JUAN DE LURIGANCHO
V°B°

ÍNDICE

MUNICIPALIDAD DE SAN JUAN DE LURIGANCHO
V°B°

1. INTRODUCCIÓN

El presente documento contiene el "Plan de Recuperación de Servicios Informáticos de la Municipalidad de San Juan de Lurigancho 2024-2027", en adelante "PRESI", elaborado por la Oficina General de Gobierno Digital e Innovación constituye el anexo N°1 del "Plan de Continuidad Operativa" de la Municipalidad de San Juan de Lurigancho, el PRESI está orientado a recuperar los servicios informáticos y de comunicaciones de datos que sustentan las "actividades críticas" contenidas en el Plan de Continuidad Operativa e identificadas por el Grupo Comando. Asimismo, el presente documento contiene los procesos que establece las tareas orientadas a recuperar los servicios informáticos y de comunicaciones de datos que sustentan las actividades municipales que no han sido definidas como "críticas" en el presente plan a fin de restaurar los servicios.

2. FINALIDAD

Establecer un plan de acción operativo en informática, el cual se ejecutará en caso ocurra un evento disruptivo o contingencia que afecte los procesos y servicios municipales que se sustentan en infraestructura y servicios tecnológicos de la Municipalidad de San Juan de Lurigancho o tercerizados con la finalidad que los procesos y servicios municipales retornen a la situación previa a la ocurrencia de evento disruptivo o contingencia.

3. ALCANCE

El Plan de Recuperación de Servicios Informáticos de la Municipalidad de San Juan de Lurigancho 2024-2027 (PRESI) comprende: los servicios informáticos y de comunicaciones de datos que sustentan las actividades críticas identificadas como indispensables por el Grupo Comando en el Plan de Continuidad Operativa de la Municipalidad de San Juan de Lurigancho que han sido afectadas por "evento disruptivo" de gran magnitud son los siguientes:

a. Mantener el comando y control conjuntamente con los órganos de apoyo, órganos de asesoramiento y órganos de línea de la Municipalidad.
b. Continuidad operativa del flujo de información brindado el soporte
c. Programar y organizar los recursos humanos y adquisición de bienes de la municipalidad
d. Emisión de dispositivos legales y respaldo del acervo documentario
e. Servicio de limpieza pública, recojo de residuos sólidos y escombreras.
f. Seguridad ciudadana
g. Velar por el planeamiento urbano público y el Sistema Económico
h. Monitoreo de la emergencia a través del Centro de Operaciones de Emergencia Distrital – COED
i. Servicio social a la población de San Juan de Lurigancho
j. Las actividades no identificadas como críticas por el grupo de comando en el plan de continuidad operativa de la Municipalidad de San Juan de Lurigancho, que han sido afectadas por "evento disruptivo" de gran magnitud.

k. La conectividad de la Municipalidad de San Juan de Lurigancho que ha sido total o parcialmente afectada por evento disruptivo o contingencia que interrumpe temporal o prolongadamente la interconectividad de los procesos y servicios municipales.

4. BASE LEGAL

a. Ley N°29664, Ley que crea el sistema nacional de gestión del riesgo de desastres (SINAGERD).
b. Que, con Ley N°28551, Ley que establece la obligación de elaborar y presentar planes de contingencia.
c. Ley N°27658 Ley Marco de Modernización de la Gestión del Estado, modificado por el Decreto Legislativo 1554.
d. Decreto Supremo N°038-2021-PCM, aprueba la Política Nacional de Gestión del Riesgo de Desastres al 2050.
e. Decreto Supremo N°115-2022-PCM, Decreto Supremo que aprueba la Política Nacional de Gestión del Riesgo de Desastres -PLANAGERD 2022-2030.
f. Resolución Ministerial N°320-2021-PCM, que aprueba los Lineamientos para la Gestión de Continuidad Operativa de las entidades públicas en los tres niveles de Gobierno".
g. Ordenanza N°459-MDSJL, publicada en el diario oficial El Peruano el 24 de enero de 2024, se aprobó el Reglamento de Organización y Funciones -ROF y la Estructura Orgánica de la Municipalidad Distrital de San Juan de Lurigancho y modificatorias
h. Resolución de Alcaldía N°436-2024-MDSJL, designan al Gerente Municipal con la unidad orgánica responsable de la Gestión de la Continuidad Operativa de la Municipalidad Distrital de San Juan de Lurigancho.
i. Resolución de Alcaldía N°450-2024-MDSJL, aprueba la conformación del Grupo de Comando para la Gestión de la Continuidad Operativa de la Municipalidad Distrital de San Juan de Lurigancho.

5. OBJETIVOS

5.1 Objetivo general

El Plan de Recuperación de Servicios Informáticos (PRESI) tiene como objetivo general restaurar o rehabilitar los servicios informáticos y de comunicaciones de datos que sustenten las "actividades críticas" identificadas y contenidas en el "Plan de Continuidad Operativa" de la Municipalidad de San Juan de Lurigancho ante la ocurrencia de un desastre de gran magnitud o un evento disruptivo que detenga prolongadamente los procesos y servicios municipales.
Asimismo, el objetivo general comprende la reincorporación de los servicios informáticos y de comunicaciones de datos de las actividades municipales no consideradas como "críticas" en el "Plan de Continuidad Operativa".

5.2 Objetivos específicos

5.2.1 **Identificar y analizar riesgos** posibles que podrían afectar las operaciones y procesos de los sistemas informáticos de la institución.

5.2.2 **Reincorporar los servicios informáticos y de comunicaciones de datos**, que sustentan las "actividades críticas" en el "Plan de Continuidad Operativa" de la Municipalidad de San Juan de Lurigancho, afectadas por un evento disruptivo de gran magnitud.

5.2.3 **Aperturar una nueva sede provisional o alterna**, que defina el grupo de comando, la red de datos y equipos informáticos destinados al personal de apoyo, supervisor y funcionarios relacionados con las "actividades críticas" establecidas en el "Plan de Continuidad Operativa" de la Municipalidad de San Juan de Lurigancho.

5.2.4 **Recuperar los servicios informáticos y de comunicaciones de datos**, que sustenten las actividades no consideradas "críticas" en el Plan de Continuidad Operativa de la Municipalidad de San Juan de Lurigancho, afectados por un evento disruptivo de gran magnitud.

5.2.5 **Restaurar los servicios informáticos y de comunicaciones de datos**, que sustenten los procesos y servicios de la Municipalidad de San Juan de Lurigancho.

5.2.6 **Restaurar la "red dorsal de fibra óptica"** de la Municipalidad Distrital de San Juan de Lurigancho afectada por un evento disruptivo de gran magnitud que interrumpe la interconectividad de los procesos y servicios municipales.

6. TÉRMINOS DE REFERENCIAS

6.1 Actividades críticas

Están conformadas por actividades que la entidad ha logrado identificar como imprescindibles y que no pueden dejar de operar, conforme a sus competencias indicadas en las normas vigentes sobre la materia.

6.2 Contingencia:

Probabilidad de que un fenómeno, hecho o circunstancia ocurra o se presente, en particular lo no deseado previsto.

6.3 Continuidad operativa

Capacidad de una entidad para mantener de manera prolongada sus funciones principales durante y después de la ocurrencia de un incidente o interrupción.

6.4 Evento

Suceso imprevisto, ocurrencia o eventualidad, hecho imprevisto o cambio de un conjunto particular de circunstancias.

6.5 Evento disruptivo

Suceso que afecta a la actividad de una institución de forma brusca que causa una interrupción de manera significativa en la prestación de determinado servicio por ejemplo la ocurrencia de fenómenos como: tsunami, sismos, inundaciones ataque terroristas entro otros.

6.6 Gestión de incidentes de seguridad digital

Procedimiento que tiene por propósito planificar, preparar, identificar, contener o investigar incidentes de seguridad digital, así como la restauración y determinación de acciones correctivas.

6.7 Mitigación
Implementación de medidas para reducir el impacto de un evento.

6.8 Plan de Continuidad Operativa
Instrumento por el cual se realizará la implementación de la continuidad operativa, va a tener como objetivo garantizar que la entidad ejecute las actividades críticas identificadas anteriormente.

6.9 Peligro
Probabilidad de que un fenómeno físico potencialmente dañino, de origen natural o inducido por acción humana, se presente en un lugar específico con cierta intensidad y en un periodo de tiempo y frecuencia definidos.

6.10 Proveedor
Persona jurídica o natural responsable de abastecer bienes o servicios informáticos de comunicaciones.

6.11 Sede alterna de la entidad pública.
Espacio físico determinado con anterioridad.

7. ORGANIZACIÓN

7.1 Conformación del Equipo de Respuestas ante Incidentes de Seguridad Digital

Los miembros del Equipo de respuesta ante Incidentes de seguridad Digital (en adelante: ERISD) son los siguientes:

a. El Jefe de la Oficina General de Gobierno Digital e Innovación o el que haga sus veces, como líder del ERISD.
b. Oficial de Seguridad y Confianza Digital (Designado por Resolución de Alcaldía).
c. Coordinador de "Redes, Servicios y Seguridad TI" (RESET) o quien haga de sus veces (Denominación referencial: Soporte Técnico).
d. Administrador de Servidores (adscrito a RESET).
e. Administrador de redes y telefonía IP (adscrito a RESET).
f. Especialista del servicio de Soporte Técnico (adscrito a RESET).
g. Especialista en cableado estructurado (adscrito a RESET).

Nota:
La denominación del ERISD está en concordancia con lo establecido en el numeral 4.5 de la Resolución de Secretaría de Gobierno y Transformación Digital N°003-2023-PCM/SGTD.

7.2 **Funciones generales del Equipo de Respuesta ante Incidentes de Seguridad Digital**

a. Realizar las actividades del Plan de Recuperación de Servicios Informáticos.
b. Llevar control de todas las operaciones realizadas al ejecutar el "PRESIC"
c. Hacer seguimiento y coordinación con los proveedores de servicios tecnológicos.
d. Plantear capacitaciones hacia el personal que participa en los procesos críticos de la Municipalidad de San Juan de Lurigancho los cuales deberán actuar en situaciones de contingencia.
e. Tener en cuenta la realización de pruebas y ensayos que aseguren la ejecución del PRESIC.

7.3 **Funciones específicas del Equipo de Respuesta ante Incidentes de Seguridad Digital**.

a. Identificar si existen las condiciones necesarias para restaurar los servicios informáticos y de comunicaciones de datos en la sede principal de la municipalidad (Palacio Municipal – Sede central) y en la sede municipal que alberga los Data Center 01 y 02 (Sede Central y CECOM) ante la ocurrencia de incidente disruptivo.
b. Convocar al Oficial de Seguridad y Confianza Digital (OSCD), a los Coordinadores RESET y PRESET a reunión con carácter de emergencia, comunicando como punto de reunión el "Centro de Operaciones TI (previsto), el día y la hora.
c. Activar el Equipo de Respuesta ante Incidentes de Seguridad Digital (ERISD) ante la ocurrencia de un evento disruptivo. (En la reunión convocada con carácter de emergencia en el "Centro de Operaciones TI" con los miembros del ERISD que se encuentran presentes.
d. Definir la ubicación del "Centro de Operaciones TI" que utilizará el "Equipo de Respuesta ante Incidentes de Seguridad Digital" (ERISD) durante la ejecución de las tareas del "Plan de Recuperación de Servicios Informáticos".
e. Ante una ocurrencia de evento disruptivo, se procederá a comunicarse inmediatamente con:

   - El Oficial de Seguridad y Confianza Digital (OSCD)
   - El Coordinador de Redes, Servicios y Seguridad TI (RESET).
   - Todo tipo de comunicación disponible: Llamada a teléfono fijo, llamada a teléfono móvil (celular), envió de mensaje SMS (Short Message Service) a través de la red de telefonía móvil, envió de mensaje móvil con conexión a internet (WhatsApp-Telegram).

f. Reportar la ubicación del evento disruptivo (Departamento, Provincia y Distrito), nombre y apellido del OSCD, correo electrónico del OSCD, número de celular del OSCD, sector al que pertenece el OSCD (institución pública) y describir el evento disruptivo (en texto máximo de 500 caracteres).

7.4 **Funciones específicas del Oficial de Seguridad y Confianza Digital (OSCD)**

a. Desplegar "Grupos Tácticos" con la misión de restaurar y/o gestionar la operatividad de la data center, gestionar las torres de comunicación todo ello con la finalidad de recuperar los servicios informáticos de las actividades municipales.
b. Informar al Oficial de Seguridad y Confianza Digital (OSCD) el impacto del evento disruptivo (incidente de seguridad digital) en los procesos misionales y servicios que brinda la entidad.
c. Articular con el Oficial de Seguridad y Confianza Digital (OSCD) la implementación de controles de seguridad de la información durante la ejecución del Plan de Recuperación de Servicios Informáticos.

7.5 **Funciones específicas del Coordinador de Redes, Servicios y Seguridad TI (RESET) o quien haga de sus veces**

a. Verificar en los "Servidores Controladores de Dominio" (hardware alojado en el Data Center 01) el normal funcionamiento de los "roles FSMO" (Flexible Single Master Operations) y servicios siguientes:
   - Directorio Activo (Active Directory) PDC (Primary Domain Controller), FSMO roler.
   - Servicio DHCP (Dynamic Host Configuration Protocol.
   - Maestro de Esquemas (Scheme Master), FSMO roler. Maestro de Sistema de Nombres de Dominio (Domain Name Master).
b. Verificar la operatividad de los "Sistemas Hipervisores" y "Máquinas Virtuales" (contiene: sistemas operativos, servicios y aplicaciones requeridos por los sistemas informáticos de la MSJL), en el caso los "Sistemas Hipervisores" y/o "Máquinas Virtuales" estén afectados por el evento disruptivo, procede a configurar y restablecer los mismos o coordina con el proveedor respectivo en el caso que estos componentes estén sujetos a contrato de servicio de soporte.
c. Verificar la operatividad de los "Servicios Web" utilizados en el entorno público o privado (Principalmente: Pagos en línea, Mesa de Partes, Codisec, I.T.S.E., DEMUNA, SGD, SISMULTAS, SATRIM, SISTRAM, Gestión de Citas, Página Web Institucional), en el caso que los "Servicios Web" hayan sido afectados por el evento disruptivo, lo comunica inmediatamente al Administrador Web para que configure y restablezca los "Servicios Web".
d. Verificar la operatividad del "Servicio de Motor de Base de Datos", en el caso este afectado por el evento disruptivo lo comunica inmediatamente al Administrador de Base de Datos para que configure y reestablezca el servicio.
e. Verificar la funcionalidad de los Sistemas Operativos de los Servidores Físicos y Servidores Virtuales, en el caso que algunas funcionalidades estén afectadas por el evento disruptivo, procede a configurar y restablecer las mismas o coordina con el proveedor respectivo en el caso que estas funcionalidades estén sujetas a contrato de servicio de soporte.

f. Verificar la operatividad de los Servidores físicos (Aplicaciones, datos y servicios) y sus componentes de hardware (discos duros, fuente de poder, memorias, microprocesadores, chasis, conexiones, etc.), en el caso que los servidores físicos y/o sus componentes hayan sido afectados por el evento disruptivo, proceder a realizar tareas de mantenimiento correctivo o coordina con el proveedor respectivo en el caso que el servidor físico o componentes estén sujetos a contrato de servicio de soporte.
g. Verificar la operatividad del "Network Attached Storage" (NAS) y si ha sido afectado por el evento disruptivo, procede a reemplazar el componente afectado o coordina con el proveedor respectivo si es que el componente está sujeto a contrato de servicio de soporte.
h. Verificar que el sistema de climatización (aire acondicionado) del Data Center N°01 y N°02 esté operando correctamente, caso contrario realizar las gestiones para la remediación correspondiente.
i. Verificar el normal funcionamiento del servicio de correo electrónico institucional en la "nube".
j. Informar la situación de los servidores, Data Center N°01 y N°02° y servicios asociados al Coordinador de Redes, Servicios y Seguridad TI, después de la ocurrencia del evento disruptivo que generó la activación del Plan de Recuperación de Servicios Informáticos.
k. Verificar la copia de respaldo de datos de la MDSJL en el NAS, en el caso este afectada por el evento disruptivo procede a restaurar los datos desde los sistemas originales.

7.6 **Funciones específicas del administrador de servidores (adscrito al Coordinador RESET)**

a. Verificar la operatividad de los equipos de redes y comunicaciones instalados en los racks de la Data Center N°01 y N°02 (switches, routers, Access points)
b. Verificar la operatividad de la Plataforma de Telefonía IP de la MDSJL (servidores y equipos de telefonía IP), no incluye los terminales IP, en el caso que los componentes se encuentren
c. Verificar los DNS brindados por los proveedores.
d. Verificar las funcionalidades y rendimiento de los servicios de internet.

7.7 **Funciones específicas del administrador del Redes y Telefonía IP (adscrito a RESET)**

a. Verificar que las torres de comunicaciones se encuentren operativa (no haya colapsado) y que cuente con suministro eléctrico; en caso las antenas se encuentren afectadas por el evento disruptivo se ejecutaran las tareas de habilitación temporal con los medios municipales disponibles.
b. Diseñar el plan de “cableado estructurado”, instalación y enrutamiento.
c. Identificar los insumos y recursos que requiere el cableado estructurado.
d. Informar al Coordinador de Red, Servicios y Seguridad TI de los insumos y recursos necesarios y el avance de las tareas de "cableado estructurado".

7.8 **Funciones específicas del especialista de cableado estructurado (Adscrito al RESET)**

a. Conducir y supervisar el "cableado estructurado".
b. Inspeccionar el estado de la infraestructura tecnológica (cableado estructurado, dispositivos de comunicaciones, computadoras, etc.) de los locales municipales de San Juan de Lurigancho, luego de la ocurrencia de un evento disruptivo de gran magnitud (ejemplo: Terremoto 8.5).
c. Elaborar informe de los daños en la infraestructura tecnológica del local municipal asignado como consecuencia del evento disruptivo.
d. Informar los insumos y recursos requeridos para realizar el servicio de soporte técnico durante el proceso de recuperación de los servicios informáticos del local asignado.

7.9 **Funciones específicas del técnico de soporte informático y Help Desk (adscrito al RESET)**

a. Inspeccionar el estado de la infraestructura tecnológica (cableado estructurado y equipos informáticos) de los ambientes (oficinas) asignadas, luego de la ocurrencia de evento disruptivo de gran magnitud (ejemplo: Terremoto 8,5).
b. Informar los insumos y recursos requeridos para realizar el servicio de soporte técnico durante el proceso de recuperación de los servicios informáticos de los ambientes asignados (oficinas).
c. Configurar las computadoras e impresoras reinstaladas, de ser el caso.
d. Crear acceso de los usuarios a la red de datos (de ser el caso) en coordinación con el Administrador de Red.

7.10 **Funciones específicas del administrador de base de datos o quien haga de sus veces**

a. Evaluar e Informar la situación de las bases de datos después de la ocurrencia de evento disruptivo.
b. Restaurar la operatividad de las bases de datos (de ser el caso).
c. Recomendar las medidas de seguridad aplicables a las bases de datos de la municipalidad.

7.11 **Funciones específicas del analista de sistema/programador**

a. Habilitar el "ambiente de producción" del sistema informático asignado en los servidores correspondientes (de ser el caso).
b. Restaurar los servicios informáticos (poner en producción) dirigidos al ciudadano (vecino) y los servicios web funcionales.
c. Restaurar la operatividad las aplicaciones informáticas asignadas
d. Realizar pruebas internas de las aplicaciones informáticas asignadas

7.12 **Funciones específicas del usuario experto del sistema integrado de Administración financiera (SIAF)**

a. Verificar la conexión del SIAF entre la Municipalidad de San Juan de Lurigancho y el Ministerio de Economía y Finanzas (MEF) después de la ocurrencia de evento disruptivo.
b. Coordinar con el área tecnológica del Ministerio de Economía y Finanzas (MEF) en el caso que la conexión del SIAF se haya cortado por la ocurrencia de evento disruptivo.
c. Coordinar con el Administrador de Servidores la verificación de la operatividad del servidor del SIAF.
d. Verificar el estado de los módulos y bases de datos del SIAF
e. Coordinar con las áreas usuarias la atención de incidentes en el SIAF.

7.13 **Funciones específicas del usuario experto del sistema de Información de gestión del estado (SIGA)**

a. Verificar la conexión del SIGA entre la Municipalidad de San Juan de Lurigancho y el Ministerio de Economía y Finanzas (MEF) después de la ocurrencia de evento disruptivo.
b. Coordinar con el área tecnológica del Ministerio de Economía y Finanzas (MEF) en el caso que la conexión del SIGA se haya cortado por la ocurrencia de evento disruptivo.
c. Coordinar con el Administrador de Servidores la verificación de la operatividad del servidor del SIGA.
d. Verificar el estado de los módulos y bases de datos del SIGA.
e. Coordinar con las áreas usuarias la atención de incidentes en el SIGA.

8. PLAN DE RECUPERACION DE SERVICIOS INFORMÁTICOS DE LAS ACTIVIDADES CRÍTICAS DETERMINADAS EN EL PLAN DE CONTINUIDAD DE OPERACIONES DE LA MUNICIPALIDAD DE SAN JUAN DE LURIGANCHO

El "Plan de Recuperación de Servicios Informáticos" de las actividades críticas acordadas en el "Plan de Continuidad de Operaciones" es accionado por el líder del "Equipo de Respuesta ante Incidentes de Seguridad Digital" (ESRID) como consecuencia de la activación del "Plan de Continuidad de Operaciones" por parte del Grupo de comando.

8.1 Condiciones para la ejecución del plan de recuperación de servicios informáticos

Las Condiciones para el inicio y ejecución del plan de recuperación de servicios informáticos de las actividades criticas identificados en el plan de continuidad de operaciones de la Municipalidad de San Juan de Lurigancho por parte del "Equipo de Respuesta ante Incidentes de seguridad Digital" (ERIDS) es necesario contar con las siguientes condiciones:

a. Que el "Grupo de Comando", una vez haya hecho el análisis de la situación a consecuencia del evento disruptivo, determine si va a ser necesario la implementación de la "sede alterna" para la Municipalidad de San Juan de Lurigancho.

b. Que el Grupo de Comando haya finalizado la habilitación de la sede alterna (Instalación de carpa de campaña, mobiliario entre otros) que permita la instalación de equipos informáticos de la red de datos de la "sede temporal".
c. Que el Grupo de Comando haya tenido a bien la realización de coordinaciones que garanticen el total abastecimiento de energía eléctrica, necesario para el normal desarrollo de actividades de la sede alterna.
d. Que el Grupo de Comando, haya hecho las coordinaciones necesarias que permitan tener un sistema de climatización adecuado, que permita el normal funcionamiento de los servidores y equipos de comunicaciones.

8.2 Plan de recuperación de la operatividad del sistema de radio tetra

a. Escenario N°01: Las Torres de Comunicaciones de Radio TETRA de la MSJL ubicadas en 3 módulos diferentes las cuales son Módulo Hirohito, Módulo Electra y en el COED han colapsado por causa de evento disruptivo de gran magnitud (ejemplo: Terremoto grado 8,5).
b. El líder del "Equipo de Respuesta ante Incidentes de Seguridad Digital" (ERISD) activa el "Plan de Recuperación de Servicios Informáticos y Contingencias" e indica al Coordinador de Redes, Servicios y Seguridad TI (RESET) que envié al "Grupo Táctico N°01" a los puntos de ubicación de las Torres de Comunicaciones de Radio TETRA de la MSJL, para evaluar la magnitud de los daños de los equipos instalados en las Torres, identificar si existen o no equipos recuperables (antenas), determinar si disponen o no de suministro de energía eléctrica y si están interconectadas con el "Network Management System" (NMS) instalado en el Data Center N° 1.
c. El "Grupo Táctico N°01" (RESET - GTI) se moviliza al "Módulo Hirohito", "Módulo Electra" y el COED para inspeccionar el estado de las Torres de Comunicaciones de Radio TETRA de la MSJL, de los equipos asociados y la conectividad. Elabora informe situacional en ambos casos.
d. El "Grupo Táctico N°01" (RESET GTI) dotado de los recursos necesarios ejecuta las tareas de instalación y pruebas de antenas alternativas para reestablecer el servicio de comunicaciones de las Torres de Radio TETRA de la MSJL, para respaldar las "actividades críticas" determinadas en el Plan de Continuidad Operativa.
e. El Coordinador de Redes, Servicios y Seguridad TI (RESET -GTI) coordina con el proveedor del servicio TETRA para reforzar la cobertura de las antenas alternativas implementadas con antenas adicionales (del proveedor), con la finalidad de maximizar la cobertura de comunicaciones de Radio TETRA que demandan las "actividades críticas" en un contexto de emergencia generado por evento disruptivo de gran magnitud.

8.3 Plan de Recuperación de Servicios Informáticos de la Actividad Crítica de Serenazgo

El "Equipo de Respuesta ante Incidentes de Seguridad Digital" (ERISD) interviene ante la ocurrencia de evento disruptivo de gran magnitud y si las condiciones descritas en el numeral 8.1 están cumplidas, realizando las siguientes tareas:

a. El líder del "Equipo de Respuesta ante Incidentes de Seguridad Digital" (ERISD) activa el "Plan de Recuperación de Servicios Informáticos y Contingencias" e indica al Coordinador de Redes, Servicios y Seguridad TI (RESET) se sirva:

- Asignar al "Grupo Táctico N°02" (RESET-GTI) la misión de restaurar (si es el caso) la operatividad del Data Center N°02 (dispositivos de comunicaciones, servidores de aplicaciones, servidores de datos), ubicado en CECOM.

- Asignar al "Grupo Táctico N°03" (RESET-GTI) la misión de habilitar la red de datos e instalar los equipos de cómputo en la "Sede Alterna relacionados con la "actividad crítica" de Serenazgo, del personal de seguridad ciudadana de apoyo, supervisión o conductor del servicio de serenazgo (que no realiza trabajo en el campo).

b. El Coordinador de Redes, Servicios y Seguridad TI (RESET) dispone en primer lugar que el "Grupo Táctico N°02" (RESET-GTI) se movilice al Data Center N°01 ubicado en la SEDE CENTRAL e inspecciona la operatividad de los servidores de aplicaciones y de base de datos, de los dispositivos de comunicaciones de la red de datos, del sistema de aire acondicionado, de las conexiones y el suministro de energía eléctrica, que ejecute las medidas correctivas correspondientes (de ser el caso) y elabore un informe situacional.

c. El Coordinador de Redes, Servicios y Seguridad TI (RESET) dispone en segundo lugar que el "Grupo Táctico N°02" (RESET-GTI) se movilice al Data Center N°02 ubicado en CECOM e inspeccione la operatividad de los servidores de aplicaciones y de base de datos, de los dispositivos de comunicaciones de la red de datos, del sistema de aire acondicionado, de las conexiones y el suministro de energía eléctrica, que ejecute las medidas correctivas correspondientes (de ser el caso) y elabore un informe situacional.