	colapso parcial. La estructura no es segura para su uso continuo.		• Atención de personal afectado y control de emergencias internas. • Recuperación y aseguramiento de equipamiento crítico. • Autorización de "liberar" al personal no esencial.
Muy grave	Sede institucional con daño severo, destruida o en condición de colapso inminente. Inaccesible o altamente riesgosa.	Afectación severa: personal lesionado, recursos destruidos o desaparecidos, pérdida de capacidad operativa.	• Acceso restringido únicamente para equipos de intervención autorizados. • Registro de daños críticos y evaluación especializada. • Apoyo psicológico y atención al personal afectado. • Proyección de requerimientos operativos y costos de recuperación. • Activación total de la sede alterna y movilización del personal crítico.

Nota: Elaborado por el Grupo de comando de la Municipalidad distrital de Lurigancho – Costos estimamos al 2025

Fuente: Guía Metodológica para la elaboración del Plan de Continuidad Operativa en entidades públicas de los tres niveles de gobierno", INDECI.

f) Procedimientos Operativos para la Continuidad por Instancia Municipal

Para asegurar la continuidad institucional ante un evento disruptivo, todas las unidades orgánicas de la Municipalidad Distrital de Lurigancho actúan bajo la dirección del Grupo de Comando, desarrollando sus funciones esenciales conforme a sus competencias, procedimientos internos y responsabilidades definidas en el presente Plan. Cada jefe de unidad es responsable de mantener operativas las actividades críticas asignadas, informando oportunamente sobre avances, limitaciones y cualquier requerimiento adicional que pueda afectar la prestación de los servicios municipales.

El personal identificado como esencial para la continuidad debe estar disponible para ser movilizado de manera inmediata hacia la sede alterna, según las disposiciones del Grupo de Comando. Para ello, cada unidad orgánica mantiene actualizado su listado de personal crítico, las funciones específicas que desempeñará durante la activación del PCO, así como la sucesión de mando y los turnos operativos. Paralelamente, los materiales, equipos y recursos institucionales asignados deben ser verificados, trasladados y habilitados en la sede alterna, garantizando su adecuada custodia, registro y funcionamiento. La Gerencia de Gestión del Riesgo de Desastres supervisa que los recursos movilizados respondan efectivamente a las necesidades reales de la continuidad operativa.

Durante el periodo de restablecimiento, todas las unidades orgánicas mantienen comunicación constante con el Grupo de Comando, informando necesidades, restricciones operativas, riesgos emergentes y avances de implementación. Asimismo, ajustan sus procedimientos conforme evolucione la emergencia y brindan apoyo interáreas cuando sea necesario para asegurar la continuidad de las actividades fundamentales. El Grupo de Comando consolida los requerimientos institucionales y gestiona su priorización y viabilidad operativa, garantizando que la respuesta municipal se mantenga ordenada, sostenible y alineada con las capacidades disponibles.

5.8 ACTIVACIÓN Y DESACTIVACIÓN DE LA SEDE ALTERNA

La activación de la sede alterna se inicia con la movilización inmediata dispuesta por el Grupo de Comando, quien organiza el traslado del personal esencial, los equipos críticos, la documentación prioritaria y los recursos operativos hacia el local designado. Este proceso incluye la preparación de rutas seguras, la asignación de vehículos y la coordinación logística para el carguío y descarga de bienes, asegurando la integridad del material trasladado. Paralelamente, un Equipo de Avanzada verifica las condiciones de seguridad, accesibilidad, servicios disponibles y operatividad básica del espacio, emitiendo un reporte que autoriza el ingreso del personal restante y el inicio de las actividades.

Una vez habilitada la sede alterna, se procede a la activación de las líneas vitales, comunicaciones y tecnologías de la información indispensables para asegurar la continuidad institucional. Se restablecen los servicios de energía, agua y comunicaciones; se instalan radios VHF, equipos informáticos, puntos de acceso inalámbrico, servidores y sistemas administrativos digitales; y se implementan conexiones de respaldo que permitan mantener operativos los sistemas esenciales. El Grupo de Comando se instala en un ambiente estratégico de la sede alterna, desde donde coordina el funcionamiento institucional, emite directrices, organiza los espacios de trabajo y mantiene comunicación permanente con las unidades orgánicas y la Gerencia de Gestión del Riesgo de Desastres.

Durante todo el periodo de funcionamiento de la sede alterna, el Grupo de Comando gestiona la crisis institucional, coordinando con entidades externas, resolviendo emergencias del personal y supervisando la continuidad de las actividades fundamentales. Cada unidad orgánica reporta sus avances, limitaciones y necesidades operativas, permitiendo al Grupo de Comando consolidar la información y gestionar oportunamente los recursos, equipamiento e insumos que sean necesarios para sostener la continuidad operativa mientras dure la contingencia.

5.8.1 Recuperación de sedes y servicios

La recuperación de sedes y servicios constituye la etapa destinada a restablecer la operatividad institucional luego de una emergencia. Este proceso es conducido y supervisado por el Grupo de Comando, en estrecha articulación con las unidades orgánicas involucradas. La primera prioridad consiste en la atención y verificación del estado del personal. Para ello, la Gerencia de Administración, a través del área de Recursos Humanos, coordina con todas las unidades la identificación de trabajadores afectados, la disponibilidad de personal esencial y la necesidad de reubicación de recursos humanos. Asimismo, se implementan acciones de soporte emocional y asistencia básica para los trabajadores desplazados a la sede alterna y, de ser necesario, para sus familias. Además, se habilitan mecanismos administrativos que permitan mitigar el impacto del evento en la fuerza laboral, priorizando la continuidad de los servicios esenciales.

Posteriormente, el Grupo de Comando dispone la ejecución de una inspección técnica exhaustiva de la infraestructura institucional, la cual debe realizarse dentro de las 48 horas posteriores a la emergencia. Esta evaluación es liderada por profesionales internos o externos acreditados, quienes determinan la condición real de la sede principal y de las sedes alternas, definiendo niveles de riesgo, daños en componentes estructurales y no estructurales, y proponiendo alternativas para el restablecimiento seguro de actividades. El

informe definitivo, con conclusiones y recomendaciones, debe emitirse en un plazo máximo de cinco días. Paralelamente, se realiza una inspección detallada de los servicios básicos energía eléctrica, agua potable, desagüe, comunicaciones y telefonía con participación de personal técnico operativo y equipos de servicios generales. Este diagnóstico permite establecer una hoja de ruta para la recuperación inmediata de servicios, articulando con entidades externas del Gobierno Regional, Gobierno Central o proveedores especializados.

Un proceso similar se aplica a los servicios de Tecnologías de la Información y Comunicaciones (TIC). Dentro de las 48 horas posteriores al evento, el Grupo de Comando dispone evaluaciones especializadas que permitan identificar daños, interrupciones o vulnerabilidades en sistemas informáticos, servidores, plataformas digitales y redes institucionales. Con los resultados, se elabora un informe técnico que incluye recomendaciones y el plan de acción correspondiente, el cual debe presentarse en un plazo máximo de cinco días. A partir de estas evaluaciones se activan los procedimientos de adquisición de bienes y servicios necesarios para el reacondicionamiento estructural, la reposición de equipamiento crítico, la restauración de líneas vitales y la recuperación de plataformas tecnológicas. La Gerencia de Administración designa un equipo especializado para atender exclusivamente los requerimientos emergentes vinculados a la adecuación de ambientes, adquisiciones urgentes y logística de restablecimiento.

5.8.2 Desactivación de la sede alterna y desmovilización institucional

Una vez que la sede principal recupera condiciones seguras para operar, el Grupo de Comando inicia el proceso de desactivación de la sede alterna. Para ello, el área de Control Patrimonial, junto con Administración, debe contar con un catálogo de posibles locales temporales y proveedores que faciliten la reubicación progresiva de unidades si fuese necesario. Esta información se contrasta con la evaluación de infraestructura y con los lineamientos de Planeamiento y Presupuesto para adecuar el POI y reprogramar actividades que, por razones de continuidad operativa, deban ser suspendidas o reemplazadas temporalmente. Cuando se confirme que la sede principal puede volver a funcionar, se organiza el retorno ordenado del personal esencial, el traslado de documentación, mobiliario crítico y equipamiento técnico, asegurando el seguimiento de inventarios y la reposición de materiales utilizados durante la contingencia.

En esta etapa también se aborda la recuperación de la información generada en contingencia. Las unidades orgánicas son responsables de consolidar y resguardar la documentación producida durante la emergencia, tanto en formato digital como físico, asegurando copias para efectos administrativos y de control. El Grupo de Comando instruye

al equipo de Gobierno Digital para brindar soporte técnico y asegurar la integridad, respaldo y custodia de la información generada. Finalmente, la Oficina de Administración comunica la disponibilidad de los ambientes recuperados y coordina la ocupación progresiva de las áreas asignadas, considerando que, mientras persista la emergencia, se podrán mantener modalidades temporales como el trabajo remoto o el uso de locales alternos. Cuando el retorno total sea viable, el Grupo de Comando dispone la desmovilización completa de la sede alterna, la desinstalación de módulos, la devolución de equipos, el cierre de contratos temporales y la culminación formal de la respuesta, en coordinación con la Gerencia de Gestión del Riesgo de Desastres. Este proceso finaliza con un informe institucional que recoge las acciones ejecutadas, los costos asociados y las lecciones aprendidas para fortalecer futuras capacidades de respuesta y continuidad operativa.

5.9 DESARROLLO DE LAS ACTIVIDADES CRÍTICAS

Las actividades críticas identificadas corresponden a aquellas funciones que, por su naturaleza, impacto y necesidad operativa, deben mantenerse activas de manera ininterrumpida durante y después de una emergencia. Estas actividades aseguran la continuidad mínima indispensable de la gestión municipal, garantizando la prestación de servicios esenciales, la respuesta inmediata ante contingencias y el sostenimiento de los procesos administrativos indispensables para la operatividad institucional.

Tabla 25.-*Actividades Críticas Identificadas*

N°	Unidad Orgánica	Actividad Critica Priorizada
1	Gerencia de Gestión del Riesgo de Desastres	**001.** Responsable de la gestión Operativa de la Municipalidad **002.** Operatividad del Centro de Operaciones de Emergencia Distrital - COED **003.** Evaluación de daños y análisis de necesidades **004.** Atención con Bienes de Ayuda Humanitaria **005.** Evaluación de daños de edificaciones esenciales
2	Oficina General de Administración y Finanzas	**001.** Asegurar la provisión oportuna de bienes, materiales y equipos necesarios para la continuidad operativa. **002.** Gestionar la contratación de servicios esenciales durante situaciones de emergencia.

		003. Supervisar el abastecimiento y control del inventario institucional.
3	Oficina General de Planeamiento y Presupuesto	**001.** Coordinar la priorización presupuestal para la ejecución del PCO. **002.** Monitorear la implementación de las acciones de continuidad operativa. **003.** Elaborar reportes técnicos de seguimiento y evaluación del plan.
4	Gerencia de Desarrollo Urbano	**001.** Verificar el estado estructural de la infraestructura municipal y servicios básicos. **002.** Ejecutar acciones de reparación o refuerzo en edificaciones afectadas. **003.** Supervisar la habitabilidad de locales municipales para garantizar la continuidad operativa.
5	Gerencia de Servicios Públicos y Gestión Ambiental	**001.** Asegurar la recolección, transporte y disposición final de residuos sólidos. **002.** Mantener la operatividad de las rutas críticas de limpieza durante emergencias. **003.** Coordinar con entidades externas el manejo de residuos sólidos.
6	Gerencia de Seguridad Ciudadana	**001.** Garantizar la difusión de mensajes institucionales en emergencias. **002.** Promover la sensibilización y capacitación del personal en continuidad operativa. **003.** Implementar mecanismos de comunicación interna ante interrupciones del servicio.
		001. Ejecutar acciones de resguardo y control de accesos en instalaciones municipales. 002. Coordinar la evacuación del personal durante eventos críticos. 003. Mantener la comunicación operativa con el COED Distrital.

6. CRONOGRAMA DE EJERCICIOS DEL PLAN DE CONTINUIDAD OPERATIVA

ACTIVIDAD	PERIODO DE EJECUCIÓN ESTIMADO	DOCUMENTOS DE SUSTENTO
1. Validación operativa de la Matriz de Continuidad y verificación del cumplimiento de actividades críticas. Incluye ejercicios internos de activación, revisión de indicadores y simulaciones funcionales.	I y II Semestre	- Informe del Grupo de Comando- Registro de evaluación de continuidad
2. Confirmación y ensayo de la operatividad de las sedes alternas oficiales (Estadio Solís García, Base Ñaña y Base Campiña). Comprende pruebas de ocupación, accesibilidad, comunicaciones y funcionamiento básico.	I Semestre	- Acta del Grupo de Comando- Reporte de inspección GGRD
3. Actualización técnica del Plan de Continuidad Operativa. Incluye la revisión de actividades críticas, análisis de riesgos operativos, ajustes organizacionales y validación de capacidades institucionales.	I y II Semestre	- Informe técnico GGRD- Acta del Grupo de Comando
4. Protección, inventario y resguardo del acervo documental y de los repositorios digitales institucionales. Ensayos de respaldo y recuperación realizados por Gobierno Digital.	I y II Semestre	- Informe de Gobierno Digital- Registro de resguardo documental

5. Identificación y confirmación del personal esencial para la continuidad operativa. Coordinación con Recursos Humanos y asignación formal de responsabilidades.	I Semestre	- Reporte de Recursos Humanos- Acta del Grupo de Comando
6. Identificación de recursos tecnológicos esenciales y validación de su disponibilidad y funcionamiento. Revisión de equipos, sistemas, accesos, plataformas y conectividad.	I Semestre	- Informe OGD- Acta del Grupo de Comando
7. Determinación de recursos logísticos y físicos indispensables para la continuidad. Incluye fichas de recursos, pruebas de uso y disponibilidad institucional.	I y II Semestre	- Reporte logístico- Acta del Grupo de Comando
8. Ejecución de ensayos, pruebas integrales y simulacros internos de continuidad. Evaluación del desempeño de cada unidad orgánica y de la efectividad de los procedimientos definidos.	I y II Semestre	- Informes de evaluación- Actas del Grupo de Comando

7. ANEXOS

a) PLAN DE RECUPERACIÓN DE LOS SERVICIOS INFORMÁTICOS.

En concordancia con lo establecido en los Lineamientos para la Gestión de la Continuidad Operativa y la Formulación de los Planes de Continuidad de las Entidades Públicas de los tres niveles de gobierno, el Plan de Recuperación de los Servicios Informáticos constituye un instrumento técnico complementario al Plan de Continuidad Operativa, orientado a asegurar la restauración progresiva y oportuna de los servicios de tecnologías de la información necesarios para la ejecución de las actividades críticas institucionales.

El presente Plan ha sido elaborado por la Oficina de Gestión de Gobierno Digital, adscrita a la Oficina General de Planeamiento y Presupuesto, y si bien no cuenta a la fecha con Resolución de aprobación, se encuentra formalmente sustentado mediante el Informe N.° 000845-2025-MDL/OGPP-OGGD, a través del cual se adjunta la Versión Preliminar Consolidada del Marco de Recuperación, en la que se establecen los lineamientos técnicos, procedimientos y responsabilidades para la recuperación de los sistemas informáticos ante escenarios de interrupción.

En tal sentido, y considerando su naturaleza de instrumento técnico específico e independiente, el Plan de Recuperación de los Servicios Informáticos se adjunta en la parte final de los anexos del Plan de Continuidad Operativa institucional, manteniendo articulación funcional y operativa con los objetivos, actividades críticas y estrategias de continuidad definidas a nivel institucional.

b) PROCEDIMIENTO PARA LA CONVOCATORIA DEL PERSONAL INVOLUCRADO EN LA EJECUCIÓN DE LAS ACTIVIDADES CRÍTICAS.

– INTEGRANTES DEL GRUPO DE COMANDO Y ACTIVIDADES CRÍTICAS PRIORIZADAS

El Grupo de Comando del Plan de Continuidad Operativa (PCO) constituye la instancia responsable de dirigir, coordinar y supervisar las acciones destinadas a asegurar la continuidad de los servicios esenciales de la Municipalidad Distrital de Lurigancho (MDL) ante la ocurrencia de eventos disruptivos. Está integrado por las unidades orgánicas de mayor capacidad decisoria y operativa, las cuales ejecutan actividades críticas catalogadas como indispensables para mantener la funcionalidad mínima del gobierno local. La identificación de estas unidades responde a criterios de impacto institucional, necesidad operativa, interdependencia entre procesos y obligatoriedad en la prestación de servicios de carácter público.

La Gerencia de Gestión del Riesgo de Desastres (GGRD), como presidencia del Grupo de Comando, es la responsable de conducir la gestión operativa de la municipalidad durante una emergencia, activar los mecanismos de respuesta institucional y garantizar la operatividad del Centro de Operaciones de Emergencia Distrital (COED). Esta gerencia desarrolla actividades críticas relacionadas a la evaluación de daños y análisis de necesidades, la coordinación para la entrega de bienes de ayuda humanitaria y la inspección de edificaciones esenciales posterior a un evento adverso. Su participación resulta determinante para la toma de decisiones informadas, la coordinación intersectorial y la gestión de recursos de respuesta, por lo que su personal debe ser convocado sin demora.

La Oficina General de Administración y Finanzas (OGAF) contribuye directamente a la sostenibilidad operativa de la municipalidad mediante actividades críticas vinculadas con la provisión de bienes, materiales y equipos imprescindibles para continuar con las funciones mínimas institucionales. Además, es la responsable de agilizar los mecanismos de contratación de servicios esenciales, supervisar el abastecimiento y controlar los inventarios estratégicos. Su rol es decisivo para garantizar el flujo logístico en situaciones de emergencia, permitiendo que la municipalidad mantenga la capacidad de operación incluso en condiciones limitadas.

La Oficina General de Planeamiento y Presupuesto (OGPP) tiene la responsabilidad de asegurar el soporte técnico y presupuestal del PCO. Sus actividades críticas incluyen

coordinar la priorización de recursos, monitorear la ejecución de las acciones de continuidad y elaborar reportes técnicos de avance y evaluación del plan. Esta unidad asegura que los procesos administrativos y financieros de la continuidad operativa se formulen, registren y monitoreen adecuadamente, evitando retrasos en la asignación presupuestal o limitaciones técnicas durante la activación del plan.

Por su parte, la **Gerencia de Desarrollo Urbano (GDU)** cumple funciones críticas relacionadas a la verificación del estado estructural de las instalaciones municipales tras un evento disruptivo, así como a la planificación y ejecución de acciones correctivas o de refuerzo que garanticen el uso seguro de los locales institucionales. Asimismo, supervisa la habitabilidad de los espacios designados como sedes alternas, temporales o de contingencia. Su intervención inmediata es fundamental para evitar la ocupación de edificaciones en riesgo y para facilitar la continuidad operativa en ambientes seguros.

La Gerencia de Servicios Públicos y Gestión Ambiental (GSPGA) desarrolla actividades críticas orientadas a mantener operativa la limpieza pública del distrito, garantizar la recolección y disposición final de los residuos sólidos, y coordinar de manera oportuna con entidades externas para manejo adecuado de residuos durante la emergencia. La continuidad de estos servicios previene la acumulación de desechos, la proliferación de vectores y la generación de riesgos sanitarios, aspectos determinantes para asegurar condiciones mínimas de seguridad y salud pública en escenarios de emergencia.

La Gerencia de Educación y Desarrollo Humano (GEDH) tiene como responsabilidad asegurar la difusión oficial de mensajes institucionales, promover acciones de sensibilización del personal sobre el PCO y garantizar mecanismos de comunicación interna adecuados ante fallas tecnológicas o interrupciones administrativas. La labor de esta gerencia es esencial para asegurar que la información fluya adecuadamente entre las unidades administrativas, los funcionarios y la población, evitando la desinformación y fortaleciendo la capacidad de coordinación institucional.

Finalmente, **la Gerencia de Seguridad Ciudadana (GSC)** ejecuta actividades críticas relacionadas al resguardo y vigilancia de instalaciones municipales, control de acceso, evaluación del entorno de seguridad y coordinación de movimientos de evacuación del personal. Además, mantiene comunicación directa con el COED para informar incidentes internos o externos que puedan afectar la continuidad operativa. Su intervención permite preservar el orden, la integridad del personal y la protección de los activos institucionales.

– ACTIVACIÓN DE LA CADENA DE LLAMADAS

La activación de la cadena de llamadas constituye el mecanismo inicial y fundamental para movilizar en el menor tiempo posible al personal responsable de ejecutar las actividades críticas. Este proceso es liderado por la Gerencia de Gestión del Riesgo de Desastres o por la autoridad correspondiente de acuerdo con la cadena de sucesión establecida en el PCO, garantizando que las decisiones no se detengan ante la ausencia de un funcionario titular. La activación se ejecuta inmediatamente después de identificarse un evento disruptivo que impacta o amenaza con afectar la continuidad de los servicios municipales, tales como desastres naturales, fallas críticas de infraestructura, interrupciones tecnológicas, entre otros.

Para asegurar la efectividad de este proceso, cada unidad orgánica debe mantener actualizado un directorio de personal crítico que incluya datos de contacto primarios y alternos, así como mecanismos de comunicación redundantes (llamadas telefónicas, mensajes de texto, radios VHF, correos institucionales y aplicaciones de mensajería). La disponibilidad de canales múltiples permite mantener operativa la comunicación aun cuando una parte de la infraestructura tecnológica se encuentre comprometida. El uso de mensajería digital permite la transmisión de documentos, procedimientos u orientaciones en tiempo real, lo cual agiliza la toma de decisiones.

Este proceso debe efectuarse de manera estructurada, siguiendo un orden de prioridad basado en la criticidad de las funciones y la urgencia de ejecución. Por ejemplo, si el incidente genera daños en edificios municipales, la Gerencia de Desarrollo Urbano debe ser activada de inmediato; si afecta el suministro de bienes esenciales, la Oficina General de Administración y Finanzas debe estar entre las primeras convocadas. El objetivo es evitar retrasos que puedan comprometer la eficiencia de las intervenciones.

– SECUENCIA DEL FLUJO DE LLAMADAS

El flujo de comunicación se inicia desde el COED, entidad que actúa como el núcleo operativo del sistema municipal de respuesta y continuidad operativa. Este centro evalúa la gravedad del evento, determina la necesidad de activar el PCO y establece la prioridad de convocatoria del personal según la naturaleza del incidente. Una vez realizada la activación, el COED notifica de inmediato a los titulares de las unidades orgánicas integrantes del Grupo de Comando, quienes a su vez activan sus propias cadenas internas de llamadas para convocar al personal crítico.

Este proceso debe ejecutarse siguiendo un esquema de jerarquía y redundancia para asegurar su eficacia. El funcionario convocado debe confirmar la recepción del mensaje mediante los mecanismos establecidos; en caso de no obtenerse respuesta en un tiempo razonable, se procederá a contactar al responsable alterno designado en el cuadro de sucesión de cada unidad orgánica. Esta estrategia permite asegurar la disponibilidad permanente del recurso humano necesario para atender la emergencia.

Además, el flujo de llamadas debe documentarse de manera rigurosa, registrando la fecha, hora, persona contactada, medio utilizado y respuesta obtenida. Este registro no solo permite evaluar la efectividad del proceso de convocatoria, sino que constituye un insumo fundamental para auditorías, actualizaciones del PCO y evaluaciones post-evento. Asimismo, permite identificar oportunidades de mejora en materia de comunicación interna y disponibilidad del personal.

– CONVOCATORIA ALINEADA A LAS ACTIVIDADES CRÍTICAS

La convocatoria del personal debe efectuarse de manera diferenciada y estratégica, alineando la disponibilidad del recurso humano con la naturaleza operativa de las actividades críticas que cada unidad orgánica tiene bajo su responsabilidad. Este enfoque permite movilizar exactamente al equipo necesario, optimizando tiempos, recursos y acciones de respuesta.

En el caso de la Gerencia de Gestión del Riesgo de Desastres, la convocatoria se dirige prioritariamente al equipo técnico del COED, a los especialistas en evaluación de daños y análisis de necesidades, y al personal encargado de la gestión de bienes de ayuda humanitaria. La naturaleza de estas actividades exige conocimientos específicos que permitan ejecutar diagnósticos rápidos, coordinar eficientemente con entidades externas y activar mecanismos de soporte inmediato a la población afectada.

Para la Oficina General de Administración y Finanzas, la convocatoria prioriza al personal de logística y abastecimiento, enfatizando en los responsables de procesos de adquisición, control de inventarios y distribución de bienes críticos. La capacidad de activar oportunamente la cadena logística determina la continuidad de funciones institucionales básicas, tales como movilidad, comunicaciones y operaciones de campo.

La Oficina General de Planeamiento y Presupuesto convoca a sus especialistas técnicos responsables de análisis presupuestal, programación y seguimiento del PCO. La disponibilidad de estos profesionales garantiza la viabilidad presupuestal de las acciones

inmediatas y evita interrupciones en la ejecución de actividades críticas que requieren soporte financiero.

La Gerencia de Desarrollo Urbano convoca a ingenieros, inspectores y especialistas encargados de diagnósticos estructurales, quienes deben evaluar daños en edificaciones municipales, identificar zonas seguras y determinar si los locales institucionales se encuentran en condiciones de operar. Estos análisis son indispensables para decidir el uso de sedes alternas o la reubicación temporal de servicios.

La Gerencia de Servicios Públicos y Gestión Ambiental convoca al personal de limpieza pública, supervisores de rutas y operadores de vehículos, asegurando la continuidad de las actividades de recolección de residuos. En escenarios de emergencia, el incremento de residuos y su acumulación puede generar problemas sanitarios graves, por lo cual su activación rápida es esencial.

La Gerencia de Educación y Desarrollo Humano convoca a los comunicadores institucionales y encargados de estrategias educativas internas, responsables de difundir alertas, comunicados y procedimientos que permitan mantener informados al personal y al público. Su papel es crucial para evitar rumores, desinformación o confusión durante la emergencia.

Finalmente, la Gerencia de Seguridad Ciudadana convoca a sus jefes de turno, supervisores y serenos encargados del resguardo de instalaciones y control perimetral. Su presencia garantiza condiciones de orden y seguridad que permiten al resto de unidades desarrollar sus actividades críticas sin interferencias o riesgos adicionales.

PRESENTACIÓN DEL PERSONAL CONVOCADO

Todo servidor convocado para la ejecución de actividades críticas deberá presentarse de inmediato en la sede institucional o en la sede alterna establecida en el PCO, de acuerdo con las instrucciones emitidas durante la cadena de llamadas. Esta obligación es inherente a la función pública, especialmente en situaciones de emergencia donde la permanencia y capacidad operativa del municipio pueden verse comprometidas.

La presentación del personal debe realizarse en condiciones que garanticen su disponibilidad para ejecutar las funciones asignadas. En caso de que algún funcionario o servidor presente un impedimento de fuerza mayor, deberá informarlo de inmediato a su jefe de unidad orgánica, quien activará la sucesión correspondiente convocando al profesional

alterno previamente registrado. El incumplimiento injustificado podrá ser considerado una falta administrativa conforme a la normativa vigente.

En circunstancias específicas, determinadas actividades críticas pueden ser desempeñadas bajo modalidad remota (cuando la infraestructura tecnológica no se encuentre comprometida), lo que permite reducir tiempos de respuesta y garantizar continuidad en tareas administrativas, presupuestales o de coordinación externa. No obstante, actividades de campo como inspecciones, operatividad del COED o resguardo físico requieren presencia obligatoria del personal convocado.

- **REGISTRO DE LA ACTIVACIÓN**

Todo el proceso de activación debe quedar registrado en los formatos oficiales del PCO, constituyendo un instrumento técnico de control institucional. El registro incluye la identificación del evento, fecha y hora de activación, responsable de emitir la convocatoria, medios utilizados, funcionarios convocados, tiempos de respuesta y confirmación efectiva de presentación. Esta información es consolidada por la Gerencia de Gestión del Riesgo de Desastres a través del COED y constituye evidencia para auditorías, fiscalización, revisión de desempeño y actualizaciones del PCO.

El registro sistemático de la activación permite analizar patrones de disponibilidad del personal, identificar brechas en la comunicación interna y mejorar los tiempos de respuesta institucional. Asimismo, facilita la retroalimentación posterior al evento, ayudando a fortalecer capacidades, ajustar procedimientos y optimizar la operatividad del PCO ante futuras emergencias.

c) DIRECTORIO DEL GRUPO DE COMANDO

N°	UNIDAD ORGANICA	Anexo (01)510-1856	Sedes
1	GERENTE DE GESTIÓN DE RIESGO Y DESASTRE	3007	Carmela Estrella
2	OFICINA GENERAL DE ADMINISTRACIÓN Y FINANZAS	2016	Casa de la Mujer
3	JEFE (E) DE LA OFICINA GENERAL DE PLANEAMIENTO Y PRESUPUESTO	2029	Casa de la Mujer
4	GERENTE DE DESARROLLO URBANO	2037	Casa de la Mujer
5	GERENTE DE SERVICIOS PÚBLICOS Y GESTIÓN AMBIENTAL	2031	Casa de la Mujer
6	GERENTE (E) EDUCACIÓN Y DESARROLLO HUMANO	3001	Casa de la Mujer
	GERENTE DE SEGURIDAD CIUDADANA	2041	Leoncio Prado

d) ORGANIZACIÓN PARA EL DESARROLLO DE LAS ACTIVIDADES CRÍTICAS

1. DESASTRE

↓

2. CENTRO DE OPERACIONES DE EMERGENCIA DISTRITAL – COED

Monitorea, verifica y comunica

↓

3. GERENCIA DE GESTIÓN DEL RIESGO DE DESASTRES – GGRD

Brinda información oficial al alcalde

↓

4. ALCALDE DE LA MUNICIPALIDAD DISTRITAL DE LURIGANCHO

Toma decisiones estratégicas

↓

5. GERENCIA DE GESTIÓN DEL RIESGO DE DESASTRES – GGRD

- Lidera el Grupo de Comando
- Ejecuta activación del proceso de llamadas
- Moviliza al personal crítico
- Coordina ejecución de actividades críticas

ORGANIZACIÓN PARA LA EJECUCIÓN DE ACTIVIDADES CRÍTICAS

Gerencia de Gestión del Riesgo de Desastres	Oficina General de Administración y Finanzas	Gerencia de Desarrollo Urbano	Gerencia de Servicios Públicos y Gestión Ambiental	Gerencia de Educación y Desarrollo Humano	Gerencia de Seguridad Ciudadana

Cada área actúa mediante su personal crítico:

- **Equipos técnicos**
- **Supervisores operativos**
- **Responsables alternos y suplentes**

e) SISTEMA DE COMUNICACIONES DE EMERGENCIA.

1. FINALIDAD DEL SISTEMA DE COMUNICACIONES DE EMERGENCIA

1.1. El Sistema de Comunicaciones de Emergencia tiene como finalidad asegurar la continuidad del mando, control, coordinación y toma de decisiones institucionales ante la ocurrencia de una emergencia o desastre que afecte la operatividad de la Municipalidad Distrital de Lurigancho.

1.2. El sistema permite mantener el flujo permanente y ordenado de información crítica, garantizando que las decisiones adoptadas por el Grupo de Comando se transmitan oportunamente a los niveles táctico y operativo, evitando duplicidad de funciones, retrasos o contradicciones en la respuesta institucional.

1.3. Asimismo, el sistema contribuye a la reducción del tiempo de respuesta, a la adecuada asignación de recursos y a la protección del personal municipal y de la población, en concordancia con los objetivos del Plan de Continuidad Operativa.

2. MARCO DE AUTORIDAD Y DIRECCIÓN DEL SISTEMA

2.1. El Sistema de Comunicaciones de Emergencia se encuentra bajo la dirección del Grupo de Comando del Plan de Continuidad Operativa, órgano encargado de conducir la respuesta institucional ante situaciones críticas.

2.2. De conformidad con la Resolución de Alcaldía N.º 232-2025/MDL, el Grupo de Comando es presidido por la Gerencia de Gestión del Riesgo de Desastres, la cual asume la responsabilidad de dirigir, coordinar y supervisar el funcionamiento integral del sistema de comunicaciones durante la emergencia.

2.3. Toda comunicación estratégica, tanto interna como externa, debe ser canalizada, validada y autorizada por el Grupo de Comando, a fin de asegurar coherencia institucional y evitar la difusión de información no confirmada.

3. COMPONENTES DEL SISTEMA DE COMUNICACIONES

3.1 COMPONENTE ORGANIZACIONAL

3.1.1. El componente organizacional define los niveles de responsabilidad y coordinación, asegurando una estructura clara de mando y control.

3.1.2. Está conformado por el Grupo de Comando, el Centro de Operaciones de Emergencia Distrital (COED) y las gerencias y unidades orgánicas responsables de actividades críticas.

3.1.3. Cada nivel cumple funciones diferenciadas pero articuladas, lo que permite una respuesta integrada y eficiente.

3.2 COMPONENTE TECNOLÓGICO

3.2.1. Este componente comprende los **medios y equipos de telecomunicación** necesarios para asegurar la conectividad institucional durante la emergencia.

3.2.2. Incluye telefonía móvil institucional, radios portátiles VHF/UHF, sistemas informáticos, plataformas digitales y equipos de energía de respaldo.

3.2.3. La disponibilidad y operatividad de estos medios es fundamental para garantizar la continuidad de las comunicaciones incluso ante fallas parciales o totales de los servicios convencionales.

3.3 COMPONENTE PROCEDIMENTAL

3.3.1. El componente procedimental establece los **protocolos y flujos de comunicación**, definiendo cómo, cuándo y por quién se emite la información.

3.3.2. Estos procedimientos aseguran que los reportes de situación, daños y necesidades sigan un orden jerárquico, facilitando la toma de decisiones.

3.3.3. Su correcta aplicación permite mantener la trazabilidad de la información durante toda la emergencia.

4. ESTRUCTURA FUNCIONAL DEL SISTEMA

4.1 NIVEL ESTRATÉGICO – DIRECCIÓN DEL SISTEMA

4.1.1. El nivel estratégico está a cargo de la Gerencia de Gestión del Riesgo de Desastres, en su calidad de presidencia del Grupo de Comando.

4.1.2. Este nivel tiene la función de activar el sistema, definir prioridades, emitir directivas estratégicas y coordinar con entidades externas como INDECI, la Policía Nacional del Perú y los organismos de primera respuesta.

4.1.3. Asimismo, valida la información oficial que será difundida a nivel institucional y a la población.

4.2 NIVEL TÁCTICO – COORDINACIÓN OPERATIVA

4.2.1. El nivel táctico es ejercido por el Centro de Operaciones de Emergencia Distrital (COED), como órgano de coordinación y control.

4.2.2. El COED recepciona los reportes de las unidades orgánicas, consolida la información situacional y la remite al Grupo de Comando para la toma de decisiones.

4.2.3. Además, transmite las instrucciones estratégicas hacia los niveles operativos, asegurando su correcta ejecución.

4.3 NIVEL OPERATIVO – EJECUCIÓN

4.3.1. El nivel operativo está conformado por las gerencias y subgerencias responsables de la ejecución de las actividades críticas priorizadas en el PCO.

4.3.2. Estas unidades tienen la obligación de reportar de manera permanente y oportuna el estado de su operatividad, los daños identificados y las necesidades de recursos.

4.3.3. La comunicación constante con el COED permite ajustar las acciones de respuesta en tiempo real.

5. MEDIOS DE COMUNICACIÓN DEL SISTEMA

5.1 MEDIOS PRIMARIOS

5.1.1. La telefonía móvil institucional constituye el principal medio de comunicación directa entre los integrantes del Grupo de Comando, el COED y las unidades orgánicas.

5.1.2. Los radios portátiles VHF/UHF aseguran la comunicación en campo, especialmente en escenarios donde la red móvil se encuentre afectada.

5.1.3. Los sistemas informáticos institucionales permiten el intercambio de información documentada y reportes digitales.

5.2 MEDIOS ALTERNOS

5.2.1. La telefonía fija y la mensajería digital institucional se emplean como medios alternos en caso de fallas parciales de los sistemas primarios.

5.2.2. Las redes sociales oficiales de la municipalidad se utilizan para la difusión de información a la población, siempre bajo autorización expresa del Grupo de Comando.

5.3 MEDIOS DE RESPALDO

5.3.1. Los equipos de energía de respaldo, *como* baterías externas y grupos electrógenos, garantizan la operatividad continua del sistema.

5.3.2. En escenarios de colapso total de telecomunicaciones, se activa la comunicación presencial mediante mensajeros institucionales.

6. PROTOCOLO DE ACTIVACIÓN DEL SISTEMA

6.1. El Sistema de Comunicaciones de Emergencia se activa automáticamente ante la ocurrencia de una emergencia o desastre que afecte la continuidad operativa.

6.2. La activación formal es dispuesta por el Grupo de Comando, presidido por la Gerencia de Gestión del Riesgo de Desastres.

6.3. Una vez activado, todas las unidades orgánicas deben mantener comunicación permanente con el COED.

7. FLUJO DE COMUNICACIONES

7.1. Las unidades orgánicas remiten sus reportes iniciales al COED.

7.2. El COED consolida la información y la eleva al Grupo de Comando.

7.3. El Grupo de Comando adopta decisiones y emite directivas.

7.4. Las directivas son difundidas por el COED a los niveles operativos y entidades externas.

8. TIPOLOGÍA DE COMUNICACIONES

8.1. Comunicación de alerta: aviso inmediato ante eventos adversos.

8.2. Comunicación operativa: coordinación de acciones y recursos.

8.3. Comunicación de situación: reportes periódicos de estado.

8.4. Comunicación institucional: información oficial validada.

9. MANTENIMIENTO Y MEJORA DEL SISTEMA

9.1. El sistema es evaluado y actualizado de manera semestral.

9.2. Se realizan pruebas periódicas de los medios de comunicación.

9.3. Se desarrollan simulacros de comunicaciones integrados al PCO.

10. RESULTADO OPERATIVO ESPERADO

10.1. Continuidad del mando y control institucional.

10.2. Reducción del tiempo de respuesta ante emergencias.

10.3. Información confiable, centralizada y oportuna.

11. DISPOSICIÓN FINAL

El presente Sistema de Comunicaciones de Emergencia es de aplicación obligatoria para todas las unidades orgánicas de la Municipalidad Distrital de Lurigancho y forma parte integrante del Plan de Continuidad Operativa.

f) CRONOGRAMA DE IMPLEMENTACIÓN DE LA GESTIÓN DE LA CONTINUIDAD OPERATIVA

N.°	Componente de gestión	Actividad	Frecuencia	2026	2027	2028	2029	2030
1	Evaluación del grado de conocimiento sobre la gestión de la continuidad	Aplicación de encuestas al personal municipal para evaluar el nivel de conocimiento del PCO y sus procedimientos	Semestral	Mar / Oct	Mar / Oct	Mar / Oct	Mar / Oct	Mar / Oct
2	Desarrollo y mejora de la cultura de continuidad operativa	Charlas, capacitaciones y acciones de concientización dirigidas a funcionarios y servidores municipales	Trimestral	Mar / Jun / Sep / Dic	Mar / Jun / Sep / Dic	Mar / Jun / Sep / Dic	Mar / Jun / Sep / Dic	Mar / Jun / Sep / Dic
3	Monitoreo permanente del Plan de Continuidad Operativa	Inspecciones y verificaciones de la operatividad de los procesos críticos y recursos institucionales	Bimestral	Ene / Mar / May / Jul / Sep / Nov	Ene / Mar / May / Jul / Sep / Nov	Ene / Mar / May / Jul / Sep / Nov	Ene / Mar / May / Jul / Sep / Nov	Ene / Mar / May / Jul / Sep / Nov

4	Discusión colegiada de la evolución de la gestión de la continuidad	Análisis de lecciones aprendidas al término de simulacros, ejercicios o eventos reales	Semestral	Jun / Dic	Jun / Dic	Jun / Dic	Jun / Dic	Jun / Dic

Plan de Continuidad Operativa y Recuperación ante Desastres de TI

Municipalidad Distrital de Lurigancho - Chosica

MDL-OGPP-OGGD-01-V4

Versión 4.0

Fecha de Actualización: 14 de agosto de 2025

Control de Versiones

Versión	Fecha	Autor de la Modificación	Descripción del Cambio	Aprobado por
1.0 - 3.0	04/04/2023	Peter A. Chirinos N.	Versiones iniciales y expansión básica.	
4.0	14/08/2025	Peter A. Chirinos N.	Adecuación a la normativa nacional (Ley de Gobierno Digital, D.U. 007-2020), la Guía Nacional de CSIRT y los estándares ISO.	

Tabla de Contenido

CAPÍTULO I: GENERALIDADES

1. Finalidad

El presente documento tiene como finalidad establecer el marco de gobernanza, táctico y operativo para asegurar la continuidad de los servicios de tecnología de la información y comunicaciones (TIC) de la Municipalidad Distrital de Lurigancho - Chosica, en cumplimiento con el marco normativo nacional y las mejores prácticas internacionales, para proteger los activos de información y garantizar la prestación de servicios al ciudadano ante la ocurrencia de incidentes disruptivos.

2. Objetivos

2.1. Objetivo General

Implementar un Sistema de Gestión de Continuidad de TI resiliente, capaz de anticipar, responder, recuperar y adaptarse a las interrupciones, minimizando el impacto adverso sobre los procesos críticos de la Municipalidad y fortaleciendo la confianza digital.

2.2. Objetivos Específicos

- Cumplir con las disposiciones de la Ley de Gobierno Digital y el Marco de Confianza Digital del Estado Peruano.
- Establecer y formalizar el Equipo de Respuesta ante Incidentes de Seguridad Digital (CSIRT-MDLC).
- Definir, documentar y probar los planes de recuperación para los activos de información y sistemas críticos.
- Garantizar que las decisiones durante una crisis se tomen de manera informada, estructurada y oportuna.
- Fomentar una cultura de prevención y preparación en el personal de TI y en toda la organización.

3. Alcance

Este plan abarca la totalidad de la infraestructura tecnológica, sistemas de información, datos y

personal de TI que soportan los procesos operativos y administrativos de la Municipalidad, con especial énfasis en los activos alojados en el Datacenter del Palacio Municipal. Es de cumplimiento obligatorio para todo el personal de la Oficina de Gestión de Gobierno Digital (OGGD) y los miembros del CSIRT-MDLC.

4. Base Legal y Normativa de Referencia

Este plan se alinea y se sustenta en el siguiente marco normativo:

- **Decreto Legislativo N° 1412:** Ley de Gobierno Digital.
- **Decreto de Urgencia N° 007-2020:** Aprueba el Marco de Confianza Digital y crea el Centro Nacional de Seguridad Digital (CNSD).
- **Decreto Supremo N° 029-2021-PCM:** Reglamento del D.L. N° 1412, que establece la obligatoriedad de conformar un Equipo de Respuesta ante Incidentes de Seguridad Digital.
- **Guía para la Conformación e Implementación de Equipos de Respuestas ante Incidentes de Seguridad Digital** de la Presidencia del Consejo de Ministros (PCM).
- **NTP-ISO/IEC 27001:2014:** Norma Técnica Peruana para Sistemas de Gestión de Seguridad de la Información.
- **ISO/IEC 27035:** Estándar internacional para la Gestión de Incidentes de Seguridad de la Información.
- **ISO 22301:** Estándar internacional para Sistemas de Gestión de Continuidad del Negocio.

CAPÍTULO II: MARCO CONCEPTUAL Y ESTRATÉGICO

5. Glosario de Términos Clave

- **Activo de Información:** Cualquier recurso (datos, hardware, software, personas) que tiene valor para la organización.
- **CSIRT (Computer Security Incident Response Team):** Equipo de Respuesta ante Incidentes de Seguridad Informática. Para fines de este plan, se utiliza el término oficial "Equipo de Respuesta ante Incidentes de Seguridad Digital".
- **Incidente de Seguridad Digital:** Evento o serie de eventos adversos, inesperados o no deseados, con una probabilidad significativa de comprometer las operaciones del negocio y

amenazar la seguridad de la información.

- **SGSI (Sistema de Gestión de Seguridad de la Información):** Enfoque sistemático para gestionar la información sensible de la empresa para que permanezca segura. Incluye personas, procesos y sistemas de TI.
- **(Otras definiciones relevantes de la normativa)**

6. Política de Continuidad Operativa

La Municipalidad Distrital de Lurigancho - Chosica se compromete a mantener un alto nivel de disponibilidad y resiliencia en sus servicios de TIC. La continuidad operativa es una responsabilidad de la alta dirección y se gestionará a través de un ciclo de mejora continua, asignando los recursos necesarios para la implementación, prueba y mantenimiento de los planes y capacidades descritos en este documento.

7. Alineamiento con el Sistema de Gestión de Seguridad de la Información (SGSI)

Este Plan de Continuidad es un componente integral del SGSI de la Municipalidad. La gestión de incidentes y la continuidad operativa son controles esenciales para cumplir con los principios de **Disponibilidad, Integridad y Confidencialidad** de la información. Los riesgos de interrupción identificados en el BIA retroalimentan el proceso de apreciación de riesgos del SGSI.

8. Ciclo de Vida de la Gestión de Continuidad (PHVA)

La gestión de la continuidad se basa en el ciclo de Deming o PHVA (Planificar, Hacer, Verificar, Actuar), un modelo iterativo para la mejora continua de procesos y servicios.

- **Planificar (Plan):** Identificar riesgos, realizar el BIA, definir estrategias y desarrollar los planes (este documento).
- **Hacer (Do):** Implementar las estrategias, adquirir recursos, formar al CSIRT y capacitar al personal.
- **Verificar (Check):** Realizar pruebas y simulacros, auditar los planes y medir indicadores de desempeño.
- **Actuar (Act):** Analizar los resultados de las pruebas, implementar acciones correctivas y actualizar el plan.

CAPÍTULO III: GOBERNANZA DE LA CONTINUIDAD Y SEGURIDAD DIGITAL

9. Estructura Organizativa para la Gestión de Incidentes

La gestión de incidentes se estructura en tres niveles jerárquicos para asegurar una respuesta coordinada y eficaz.

- **Nivel Estratégico (Comité de Crisis):** Compuesto por la Alta Dirección (Gerencia Municipal, Gerencia de Planificación). Se activa en incidentes de nivel CRÍTICO. Sus funciones son la toma de decisiones de alto nivel, aprobación de recursos extraordinarios y la gestión de la comunicación externa y el impacto reputacional.
- **Nivel Táctico (Coordinador del CSIRT):** Rol asumido por el Jefe de la OGGD. Dirige la respuesta general al incidente, coordina los equipos operativos, centraliza la información y actúa como nexo con el Nivel Estratégico.
- **Nivel Operativo (Equipos Técnicos del CSIRT):** Conformado por los especialistas de TI que ejecutan los procedimientos técnicos de diagnóstico, contención, erradicación y recuperación descritos en los playbooks.

10. Equipo de Respuesta ante Incidentes de Seguridad Digital (CSIRT-MDLC)

En cumplimiento con el D.S. N° 029-2021-PCM, se conforma el **CSIRT-MDLC**, responsable de la gestión centralizada de incidentes de seguridad y continuidad. Su propósito es la coordinación de las acciones necesarias para la protección de los activos de información frente a amenazas que comprometan la seguridad y disponibilidad.

11. Roles y Responsabilidades Detalladas

El CSIRT-MDLC estará conformado por los siguientes roles, según la guía de la PCM:

- **Coordinador del CSIRT (Jefe de OGGD):** Lidera el equipo, es el punto de contacto con la dirección y el CNSD.
- **Gestor de Incidentes (Especialista en Seguridad):** Responsable del triaje, análisis, contención y seguimiento de los incidentes.
- **Gestor de Redes y Comunicaciones (Jefe de Infraestructura):** Responsable de la seguridad y recuperación de la infraestructura de red.

- **Gestor de Infraestructuras Digitales (Administrador de Servidores):** Responsable de la seguridad y recuperación de servidores y almacenamiento.
- **Oficial de Seguridad y Confianza Digital:** Participa como miembro de apoyo y articulador con el SGSI.
- **(Otros roles que la institución determine)**

12. Articulación con el Centro Nacional de Seguridad Digital (CNSD)

El CSIRT-MDLC es el único punto de contacto oficial de la Municipalidad con el CNSD. De acuerdo al D.U. N° 007-2020, es **obligatorio notificar al CNSD todo incidente de seguridad digital** a través de los canales oficiales (incidentes@cnsd.gob.pe). El Coordinador del CSIRT es responsable de asegurar esta comunicación.

CAPÍTULO IV: GESTIÓN DE RIESGOS Y ANÁLISIS DE IMPACTO

13. Metodología de Evaluación de Riesgos de TI

Se adopta una metodología de evaluación de riesgos basada en la identificación de **Amenazas** (ej. ransomware, sismo) y **Vulnerabilidades** (ej. software sin parchar, falta de UPS) que podrían impactar los **Activos de Información**. El riesgo se cuantifica utilizando una matriz que cruza la **Probabilidad** de ocurrencia con el **Impacto** potencial en la operación.

14. Análisis de Impacto al Negocio (BIA)

El BIA es el proceso formal para identificar las funciones y procesos críticos de la Municipalidad y determinar el impacto que una interrupción tendría sobre ellos a lo largo del tiempo. El BIA es la base para definir las prioridades de recuperación.

15. Identificación de Procesos y Activos Críticos

Basado en el BIA, se han identificado los siguientes procesos como críticos:

1. Recaudación Tributaria y Gestión de Rentas (Soportado por SIGET).
2. Gestión Documental y Trámite Administrativo (Soportado por SGD).
3. Atención al Ciudadano y Pagos en Línea (Soportado por Pagos en Línea).

16. Establecimiento de RTO y RPO

(La tabla de la versión anterior se presenta aquí, con una justificación más detallada por cada sistema)

Sistema / Servicio	Criticidad	RTO (Tiempo Objetivo de Recuperación)	RPO (Punto Objetivo de Recuperación)	Justificación del Impacto
SIGET (Sistema de Gestión Tributaria)	**ALTA**	4 horas	1 hora	Impacto financiero directo por cada hora de inactividad en cajas y en la gestión de cuentas corrientes.
SGD (Sistema de Gestión Documental)	**ALTA**	4 horas	1 hora	Paraliza todo el flujo administrativo y la atención de expedientes, afectando los plazos legales y la operación interna.
Pagos en Línea	ALTA	6 horas	30 minutos	Afecta directamente la recaudación y la experiencia del contribuyente. La pérdida de transacciones (RPO bajo) es inaceptable.
Servidor de Archivos (SRV-FILES)	MEDIA	8 horas	24 horas	Afecta la productividad de todas las áreas al impedir el acceso a documentos de trabajo. El RPO se

				alinea con el respaldo nocturno.
Licencias (LIC-A / LIC-I)	MEDIA	12 horas	24 horas	Proceso importante para el desarrollo económico. Puede tolerar una interrupción de una jornada laboral sin impacto crítico.
PCT (Plataforma de Control Territorial)	MEDIA	12 horas	24 horas	Relevante para la seguridad y fiscalización, pero no es un sistema transaccional en tiempo real que requiera recuperación inmediata.
SISFOH (Empadronamiento)	MEDIA	24 horas	24 horas	Importante para programas sociales. Su interrupción puede afectar la atención planificada a poblaciones vulnerables.
Participación Ciudadana (PART-A / PART-I)	MEDIA	24 horas	24 horas	Afecta la interacción con el ciudadano en procesos no transaccionales, pero no detiene operaciones críticas internas.
GLPI (Gestión de Incidencias TI)	BAJA	48 horas	24 horas	Herramienta interna de TI. Su

				caída afecta la gestión formal de tickets, pero no los servicios al ciudadano. La atención se puede coordinar por otros medios temporalmente.
Otros Sistemas de Baja Criticidad (CTIS, CUPON, VISITAS, CPTE, RIT, etc.)	BAJA	72 horas	48 horas	Son sistemas de apoyo, consulta o de nicho cuya interrupción no tiene un impacto significativo e inmediato en los procesos misionales.

CAPÍTULO V: ESTRATEGIAS DE CONTINUIDAD Y RECUPERACIÓN

17. Estrategia de Resiliencia Tecnológica

Se implementan medidas proactivas para aumentar la resiliencia, incluyendo:

- **Redundancia:** Fuentes de poder y conexiones de red redundantes en servidores críticos.
- **Virtualización:** Uso extensivo del host **VE-ANDROMEDA** para flexibilizar la recuperación y reducir la dependencia de hardware específico.
- **Monitoreo Proactivo:** Uso de Zabbix, PRTG y Uptime Kuma para la detección temprana de anomalías.

18. Estrategia de Respaldo y Restauración de Datos

Se aplica la regla "3-2-1" para garantizar la recuperabilidad de los datos:

- **Política de Respaldo:**
  - **Frecuencia:** Backups incrementales diarios y completos semanales para sistemas críticos.
  - **Destinos:** (1) Servidor local TrueNAS para recuperaciones rápidas. (2) Nube de Acronis

como copia off-site. (3) Discos externos para copias offline de archivo.

- **Política de Verificación:** Se realizarán pruebas de restauración trimestrales para validar la integridad de las copias de seguridad.
- **Política de Retención:** Las copias diarias se retienen por 15 días, las semanales por 1 mes y las mensuales por 1 año.

19. Estrategia de Recuperación de Infraestructura y Comunicaciones

- **Sitio de Recuperación:** El Datacenter del Palacio Municipal es el sitio primario y de recuperación (recuperación in-situ).
- **Hardware:** Se priorizará la recuperación en máquinas virtuales sobre el host VE-ANDROMEDA. Se mantendrá un stock mínimo de componentes de hardware de reemplazo.
- **Comunicaciones:** El enlace de Fibertel es el primario. Se evaluará la contratación de un enlace de respaldo de otro proveedor.

CAPÍTULO VI: PLAN DE GESTIÓN DE INCIDENTES

20. Fases del Manejo de Incidentes (Ciclo de Vida ISO 27035)

Se adopta el ciclo de vida de gestión de incidentes basado en la norma ISO/IEC 27035, que estructura la respuesta en fases claras y definidas.

- **Fase 1: Preparación (Plan and Prepare):** Esta fase proactiva incluye todas las actividades que preparan a la organización para responder a incidentes: desarrollo y mantenimiento de este plan, implementación de herramientas, capacitación del CSIRT-MDLC y realización de simulacros.
- **Fase 2: Detección y Reporte (Detection and Reporting):** Se inicia cuando se identifica un posible incidente a través de alertas o reportes.

Fase 3: Evaluación y Decisión (Assessment and Decision): El Gestor de Incidentes utiliza el Anexo G para evaluar, clasificar y priorizar el evento, decidiendo si se activa formalmente el plan.

- **Fase 4: Respuesta (Respond):** Incluye las acciones de **Contención** (aislar el problema), **Erradicación** (eliminar la causa raíz) y **Recuperación** (restaurar los servicios).

Fase 5: Lecciones Aprendidas (Lessons Learnt): Análisis post-incidente para identificar mejoras, actualizar la documentación y fortalecer las defensas para prevenir la recurrencia.

21. Sistema de Clasificación y Priorización de Incidentes

Nivel	Severidad	Descripción	Ejemplo
4	CRÍTICO	Interrupción total de servicios críticos. Fuga masiva de datos sensibles.	Caída del servidor de base de datos URANO. Ataque de ransomware exitoso.
3	ALTO	Degradación severa de servicios críticos. Interrupción de servicios de criticidad media.	Falla del host de virtualización VE-ANDROMEDA.
2	MEDIO	Interrupción de servicios de baja criticidad. Funcionamiento anómalo de un sistema importante.	Caída del servidor de archivos SRV-FILES.
1	BAJO	Incidente que afecta a un solo usuario o a un servicio no esencial.	Falla en la PC de un usuario.

CAPÍTULO VII: PLANES DE ACCIÓN Y PROCEDIMIENTOS ESPECÍFICOS (PLAYBOOKS)

22. Procedimientos Operativos por Escenario de Contingencia

A continuación, se detallan los playbooks granulares para cada escenario.

22.1. Escenario A: Falla Crítica de Servidor de Base de Datos (URANO)

Fase	Paso	Acción Detallada	Responsable
Detección y Análisis	A-01	Alerta recibida de Zabbix indicando que el host URANO no responde.	W. Cubas / G. Doria
	A-02	Intentar conexión vía Ping y RDP. Registrar si hay respuesta.	P. Chirinos
	A-03	Revisión física en Datacenter: Verificar LEDs de estado de discos, fuentes y red. Conectar monitor local.	G. Doria
	A-04	Clasificar la falla: ¿Es SO, servicio de BD o hardware? Llenar Anexo G.	G. Doria / P. Chirinos
Contención	A-05	Comunicar a Mesa de Ayuda la caída de los sistemas SIGET, SGD y relacionados para que informen a usuarios.	Coordinador CSIRT
Erradicación y Recuperación	A-06	**SI es falla de SO/Servicio:** Intentar reiniciar el servicio de SQL Server. Si no responde, reiniciar el SO.	P. Chirinos

	A-07	**SI es falla de Hardware (Disco/Fuente):** Iniciar el procedimiento de reemplazo de la pieza.	G. Doria
	A-08	**SI la falla es mayor o la recuperación tomará >1h:** Iniciar el Plan de Recuperación Completa. Provisionar una nueva VM en VE-ANDROMEDA con las mismas specs que URANO.	G. Doria
	A-09	Conectar la nueva VM a la red de servidores y configurar IP.	P. Chirinos
	A-10	Iniciar la restauración del backup completo más reciente desde TrueNAS a la nueva VM.	P. Chirinos
	A-11	Aplicar los backups diferenciales/transaccionales posteriores al completo.	P. Chirinos
Post-Incidente	A-12	El equipo de sistemas valida la integridad de la BD restaurada y reconecta las aplicaciones.	W. Cubas
	A-13	Un usuario clave de Rentas realiza una	Usuario Clave

		prueba funcional en SIGET.	
	A-14	Comunicar la restauración del servicio. Monitorear el rendimiento por 24h.	Coordinador CSIRT

(Se aplica un nivel de detalle similar para todos los demás escenarios)

CAPÍTULO VIII: PLAN DE COMUNICACIONES

23. Protocolos de Comunicación Interna y Externa

- **Interna:** Se utilizará el correo electrónico institucional como canal formal y grupos de mensajería instantánea designados para coordinación operativa rápida.
- **Externa:** Toda comunicación a la prensa o al público general será gestionada exclusivamente por la Oficina de Comunicaciones e Imagen Institucional, previa validación del Comité de Crisis.

24. Matriz de Comunicaciones

¿Qué comunicar?	¿A quién?	¿Quién comunica?	¿Cuándo?	¿Cómo?
Inicio de la contingencia	Alta Dirección	Coordinador de TI	Al activar el plan	Correo / Llamada
Estado de los servicios	Jefes de Área	Coordinador de TI	Cada 60 minutos	Correo electrónico
Instrucciones a usuarios	Todos los usuarios	Mesa de Ayuda	Al inicio y al final	Correo masivo
Detalles técnicos	Proveedores (si	Equipo Técnico	Según necesidad	Llamada / Ticket

	aplica)			

25. Uso del Protocolo de Semáforo (Traffic Light Protocol - TLP)

Para el intercambio de información sensible sobre incidentes con el CNSD u otros CSIRTs, se utilizará el TLP para clasificar la información:

- **TLP:RED:** No compartir fuera de la reunión/conversación.
- **TLP:AMBER:** Compartir solo con miembros de la propia organización que necesiten saber.
- **TLP:GREEN:** Compartir con organizaciones aliadas, pero no en canales públicos.
- **TLP:WHITE:** Información pública, sin restricciones.

CAPÍTULO IX: PLAN DE PRUEBAS Y MEJORA CONTINUA

26. Estrategia y Tipos de Pruebas

- **Prueba de Escritorio (Anual):** Reunión del comité para discutir un escenario hipotético y revisar los procedimientos en papel.
- **Prueba de Restauración Parcial (Semestral):** Restaurar una base de datos o VM específica en el entorno de pruebas (SVR-SATURN) para validar la integridad de los backups.
- **Simulacro Completo (Bianual):** Apagado controlado de un sistema no crítico para ejecutar el procedimiento de recuperación de principio a fin.

27. Cronograma Anual de Pruebas

- **Enero:** Prueba de Escritorio (Escenario Ransomware).
- **Junio:** Prueba de Restauración (Base de Datos SIGET).
- **Diciembre:** Prueba de Restauración (Servidor de Archivos).

28. Proceso de Revisión y Actualización del Plan

Este plan será revisado y, si es necesario, actualizado en las siguientes circunstancias:

- Anualmente, como parte del ciclo de mejora continua.
- Después de un incidente real de nivel Alto o Crítico.
- Después de una prueba o simulacro que revele deficiencias significativas.

- Cuando ocurran cambios mayores en la infraestructura tecnológica o en los procesos de negocio.

29. Medición de la Madurez (Referencia SIM3)

Como parte del proceso de mejora continua, se realizarán autoevaluaciones anuales utilizando como referencia el modelo **SIM3 (Security Incident Management Maturity Model)**, promovido por la comunidad internacional y referenciado en la guía de la PCM. El objetivo es medir la madurez del CSIRT-MDLC en sus procesos, herramientas y personal, para identificar brechas y planificar mejoras.