CITYBUS
SISTEMA DE TRANSPORTE COLECTIVO METROPOLITANO CITYBUS OAXACA.

Plan de Recuperación ante Desastres (DRP) del Sistema de Transporte Colectivo Metropolitano CityBus Oaxaca

-2025-

CITYBUS
SISTEMA DE TRANSPORTE
COLECTIVO METROPOLITANO
CITYBUS OAXACA.

1. Propósito y Objetivo del DRP

Propósito

Este DRP tiene como objetivo proporcionar un plan detallado para la recuperación y restauración de servicios críticos en caso de un desastre, minimizando el tiempo de inactividad y la pérdida de datos para el Sistema de Transporte Colectivo Metropolitano CityBus Oaxaca. Además, busca asegurar la continuidad operativa del sistema de transporte, garantizando la seguridad de los pasajeros, la integridad de los datos y la funcionalidad de los sistemas tecnológicos clave.

Objetivo

Garantizar la rápida recuperación de los sistemas de transporte y el sistema de videovigilancia, la integridad de los datos de validación de tarjetas y monitoreo de pasajeros, y el restablecimiento de la infraestructura de TI en el site y en los autobuses. Esto incluye:

- Minimizar el tiempo de inactividad de los sistemas críticos.
- Proteger los datos sensibles, como los registros de validación de tarjetas y las grabaciones de videovigilancia.
- Restaurar la conectividad y funcionalidad de los sistemas de GPS, cámaras y validadores en los autobuses.
- Asegurar que los servicios de transporte se reanuden en el menor tiempo posible, manteniendo la confianza de los usuarios.

2. Alcance del DRP

Este plan abarca:

- Infraestructura de TI en el site de la dependencia: Servidores, equipos de cómputo, switches, routers, firewalls y sistemas de almacenamiento.

- Sistema de videovigilancia y DVRs: Cámaras de seguridad, grabadoras digitales y sistemas de monitoreo en tiempo real.
- Infraestructura de red y equipos de conectividad: Routers, switches, firewalls, UPS y sistemas de respaldo de energía.
- Sistemas de transporte: Validadores de tarjetas, sistemas GPS, cámaras en autobuses y pantallas informativas.

Además, el DRP incluye protocolos para la recuperación de datos, la restauración de servicios críticos y la comunicación efectiva durante una emergencia.

3. Análisis de Impacto y Evaluación de Riesgos

3.1 Amenazas potenciales

- Amenazas naturales: Terremotos, incendios, inundaciones y otros fenómenos climáticos.
- Amenazas tecnológicas: Fallas de hardware (discos duros, servidores), pérdida de energía eléctrica, ataques cibernéticos (ransomware, phishing, DDoS).
- Amenazas humanas: Sabotaje interno o externo, errores humanos en la configuración de sistemas o manejo de equipos.

3.2 Evaluación del impacto

- Tiempo de inactividad en red y servidores: Afectaría la operación de cámaras y DVRs, validadores y sistemas GPS, lo que podría resultar en la interrupción del monitoreo de las unidades en el tema de videovigilancia, ubicación geográfica y recaudo electrónico.
- Pérdida de datos: Impactaría los registros de validación de pasajeros y monitoreo de videovigilancia, lo que podría comprometer la seguridad y el recaudo electrónico.

- Interrupción en autobuses: Pérdida de monitoreo en tiempo real y verificación de pago, lo que podría generar problemas en la operatividad y afectar la experiencia del usuario.

4. Inventario y Clasificación de Activos

Activo	Cantidad	Ubicación	Nivel de criticidad
Equipos de cómputo	23	site	Media
Discos duros	10	site	Media
Servidores	8	site	Alta
Rack y patch panel	2	site	Alta
Monitor para cámaras	1	site	Alta
MikroTik, routers, UPS	1 c/u	site	Alta
Switch de 48 puertos	2	site	Alta
Firewall Palo Alto	1	site	Alta
DVRs	3	site	Alta
Pantallas informativas	16	Variado	Media
Autobuses (con equipos)	43	Externos	Alta
Cámaras de videovigilancia	30	Terminal y edificio	Alta

5. Estrategia de Respaldo y Recuperación de Datos

5.1 Frecuencia de Respaldo

- Respaldos diarios: Bases de datos de validación de pago y sistemas de videovigilancia.
- Respaldos semanales: Configuraciones de red, DVR y sistemas GPS.
- Respaldos incrementales: Cada 12 horas para datos críticos, como registros de transacciones y grabaciones de videovigilancia.

5.2 Ubicación de Respaldos

- Local: Discos duros que se encuentran en la dependencia, almacenados en un lugar seguro y protegido contra incendios e inundaciones.

- Remoto: copias de seguridad almacenadas fuera del site, preferiblemente en un centro de datos seguro o en la nube, con encriptación de datos para garantizar la confidencialidad.

5.3 Pruebas de Recuperación de Datos

- Mensual: Pruebas de recuperación de respaldo para verificar la integridad y rapidez de restauración.
- Anual: Simulaciones completas de recuperación ante desastres, incluyendo la restauración de servidores, bases de datos y sistemas de videovigilancia.

6. Plan de Contingencia para Infraestructura de Red y Servidores

6.1 Redundancia de Red

- Configurar el firewall Palo Alto y routers en alta disponibilidad para conmutación automática en caso de fallo.
- Implementar enlaces de red redundantes con proveedores de internet diferentes para garantizar la conectividad.
- Verificar regularmente la operatividad del MikroTik y los switches de 48 puertos mediante monitoreo continuo.

6.2 UPS y Energía de Respaldo

- Configurar el UPS para mantener operativos los equipos de red críticos (routers, firewall, switch) en caso de apagones de corta duración.
- Instalar generadores de respaldo para garantizar la operación continua en caso de cortes prolongados de energía.
- Realizar pruebas trimestrales de los sistemas de respaldo de energía.

- Planificar y probar la recuperación en escenarios de falla total de energía.

6.3 Plan de Recuperación de Servidores

- Servidores de respaldo: Tener servidores de reemplazo rápido en caso de falla del servidor principal.
- Servidor de cámaras: Configurar un servidor de respaldo que pueda tomar el rol en caso de falla, con sincronización automática de datos.

7. Recuperación del Sistema de Videovigilancia y DVRs

7.1 Monitoreo y Mantenimiento Preventivo

- Verificar la funcionalidad de cámaras y DVR semanalmente, incluyendo la revisión de cables, conexiones y almacenamiento.
- Configurar alertas para detectar fallos en tiempo real, como cámaras desconectadas o espacio insuficiente en los DVRs.

7.2 Plan de Respaldo y Restauración de DVRs en Autobuses

- Tener DVR móviles de respaldo listos para cambiar en caso de fallo.
- Realizar respaldo diario de los videos capturados en DVRs del site y almacenarlos en un servidor central seguro.

8. Restauración de Servicios Críticos para Autobuses

8.1 Cámaras, GPS y Validadores de Tarjetas

- Verificación semanal del correcto funcionamiento de cámaras, sensores de aforo, GPS y validadores de tarjetas en cada autobús.

- Mantener un inventario de unidades de respaldo para cambiarlas rápidamente en caso de fallo.

8.2 Plan de Contingencia de Monitoreo en Autobuses

- Desarrollar un protocolo para notificar inmediatamente al personal de soporte técnico cuando un sistema en un autobús presente fallas en tiempo real.
- Implementar un sistema de monitoreo remoto que permita diagnosticar y resolver problemas en la medida de lo posible las fallas que presenten las unidades.

9. Comunicación y Coordinación en Caso de Desastre

9.1 Notificación de Incidentes

- Definir un protocolo de comunicación para informar rápidamente a todo el personal sobre el incidente, utilizando canales como correo electrónico, mensajes de texto.
- Establecer un equipo o enlace de operaciones de emergencia (COE) para coordinar las acciones de recuperación.
- Asegurar que todos los empleados y conductores estén al tanto del plan y sepan cómo actuar en caso de emergencia.

9.2 Responsabilidades y Roles

- Equipo de TI: Responsable de restauración de servicios de red y servidores.
- Equipo de Mantenimiento en Autobuses: Encargado de reparar o sustituir DVRs, GPS y validadores en autobuses.
- Equipo de Comunicación: Informa a los usuarios de la interrupción de servicios si fuera necesario, utilizando redes sociales, pantallas informativas y anuncios en autobuses.

10. Pruebas, Mantenimiento y Actualización del DRP

10.1 Simulaciones de Desastre

- Realizar simulaciones de desastres anuales para evaluar la eficacia del DRP, incluyendo escenarios como cortes de energía, ataques cibernéticos y fallos de hardware.

10.2 Documentación y Actualización

- Revisar y actualizar el DRP cada seis meses o cuando haya cambios en la infraestructura de TI.
- Mantener documentado cada cambio en los equipos y el inventario actualizado de recursos.

10.3 Entrenamiento del Personal

- Capacitar al equipo de TI y al personal de soporte en el uso del DRP, incluyendo procedimientos de recuperación y manejo de emergencias.
- Informar a todo el personal de las medidas de emergencia para garantizar que el DRP sea efectivo.
- Se desarrollarán programas de capacitación en seguridad de TICs que incluyan módulos de concientización sobre amenazas cibernéticas y buenas prácticas de seguridad.

Tabla 2. Potenciales escenarios de aplicación

Tipo	Nivel de riesgo	Consecuencias	Modo de Recuperación
Incendio	Grave	- Pérdida total o parcial del inmueble y su contenido, incluyendo equipos de cómputo,	- Adquisición de nuevo equipo de cómputo (servidores, PCs, switches, routers, etc.). - Restauración de la

		servidores, DVRs y dispositivos de red. - Daño a la infraestructura eléctrica y de comunicaciones. - Pérdida de datos	infraestructura eléctrica y de comunicaciones. - Uso del último respaldo de información, obtenido por medio físico o del servicio en la nube. - Reubicación temporal de operaciones en un site alterno si el inmueble principal no es habitable.
Sismo	Medio	- Daños físicos a equipos y estructuras, dependiendo de la intensidad del sismo. - Posible interrupción de servicios eléctricos y de comunicaciones. - Riesgo de pérdida parcial de datos, en caso de daño directo en los discos	- Evaluación de daños en equipos y estructuras. - Adquisición de nuevo equipo de cómputo (servidores, PCs, etc.) en caso de daños irreparables. - Uso del último respaldo de información, obtenido por medio físico o del servicio en la nube. - Restablecimiento de servicios eléctricos y de comunicaciones.
Robo	Bajo	- Pérdida de equipos de cómputo, servidores, dispositivos de red y otros activos tecnológicos. - Interrupción temporal de servicios críticos. - Riesgo de	- Adquisición de nuevo equipo de cómputo (servidores, PCs, etc.). - Uso del último respaldo de información, obtenido por medio físico o del servicio en la nube. - Refuerzo de medidas de seguridad física,

		exposición de datos sensibles. (Sólo en caso de que no estén encriptados los datos)	como cámaras de vigilancia, controles de acceso y sistemas de alarma. - Notificación a autoridades y seguimiento del caso.
Virus	Grave	- Infección de sistemas críticos, como servidores, bases de datos y dispositivos de red. - Pérdida de datos si el virus es del tipo ransomware. - Interrupción de servicios debido a la inoperabilidad de los sistemas afectados. - Posible filtración de datos sensibles si el virus incluye componentes de spyware.	- Aislamiento inmediato de los sistemas infectados para evitar la propagación. - Uso de antivirus o antimalware para eliminar la amenaza. - Restauración de sistemas a partir del último respaldo de información, obtenido por medio físico o del servicio en la nube. - Revisión y actualización de políticas de seguridad para prevenir futuros ataques.
Inundación	Grave	- Daños severos a equipos eléctricos y de cómputo debido al contacto con agua. - Pérdida total o parcial de infraestructura física. - Interrupción prolongada de servicios críticos.	- Evaluación de daños en equipos y estructuras. - Adquisición de nuevo equipo de cómputo (servidores, PCs, etc.) en caso de daños irreparables. - Uso del último respaldo de información, obtenido por medio físico o del servicio en la nube. - Implementación de medidas preventivas,

			como sistemas de drenaje y elevación de equipos críticos.
Corte de energía	Medio	- Interrupción temporal de servicios críticos, como sistemas de videovigilancia, validadores de tarjetas y monitoreo de autobuses. - Posible corrupción de datos si los sistemas no se apagan correctamente.	- Uso de sistemas de alimentación ininterrumpida (UPS) para mantener operativos los equipos críticos durante cortes breves. - Activación de generadores de respaldo en caso de cortes prolongados. - Verificación de la integridad de los datos y sistemas después de restablecer la energía.
Ciberataque (DDoS)	Alto	- Saturación de la red, resultando en la inaccesibilidad de servicios críticos. - Interrupción del monitoreo en tiempo real y sistemas de pago. - Posible pérdida de confianza por parte de los usuarios.	- Implementación de firewalls y sistemas de detección de intrusos (IDS/IPS) para mitigar el ataque. - Colaboración con el proveedor de servicios de internet para filtrar el tráfico malicioso. - Restauración de servicios una vez que el ataque haya sido neutralizado.
Error humano	Medio	- Eliminación accidental de datos o configuraciones incorrectas. - Interrupción temporal de servicios debido a errores en la	- Restauración de datos a partir del último respaldo de información. - Revisión y corrección de configuraciones incorrectas. - Capacitación del

		operación de sistemas.	personal para evitar futuros errores.

11. Conclusiones

El Plan de Recuperación de Desastres de TI del Sistema de Transporte Colectivo Metropolitano CityBus Oaxaca es una herramienta estratégica esencial para garantizar la continuidad operativa ante situaciones imprevistas. Su correcta implementación permitirá minimizar el impacto de fallos tecnológicos, proteger la integridad de los datos y reducir los tiempos de inactividad.

Además, el plan establece procedimientos claros para la recuperación eficiente de los sistemas críticos, asegurando la seguridad, confiabilidad y estabilidad del servicio. Su constante revisión y actualización será clave para mantener su efectividad ante nuevos riesgos tecnológicos.

ELABORÓ

C. IVÁN SALAS PÉREZ
JEFE DE UNIDAD DE ESTADÍSTICA Y SEGUIMIENTO

AUTORIZÓ

CITYBUS OAXACA

C.P. KARINA GÓMEZ ESTEBAN
DIRECTORA GENERAL DEL SISTEMA DE TRANSPORTE COLECTIVO METROPOLITANO CITYBUS OAXACA