Manual de Mantenimiento, Respaldo y Recuperación

Sistema Integral de Gestión para Procesos de Automatización

(SIGPA)

INTRODUCCIÓN

Propósito de este Manual

Este documento establece los procedimientos técnicos y las mejores prácticas para el mantenimiento, respaldo (backup) y recuperación (restore) del Sistema Integral de Gestión (SIGPA). El objetivo es asegurar la integridad de los datos, la disponibilidad del servicio y la continuidad operativa de la plataforma.

Roles y Responsabilidades

Administrador de Sistemas / Personal de TI: Responsable de ejecutar todos los procedimientos descritos en este manual, incluyendo mantenimientos, backups, restauraciones y monitoreo del sistema.

Administrador de Base de Datos (DBA): Supervisa la salud de la base de datos MySQL, optimiza consultas y lidera los esfuerzos de respaldo y recuperación de datos.

Usuarios Finales: Responsables de reportar cualquier anomalía o lentitud en el sistema al equipo de TI.

Componentes Críticos del Sistema

El SIGPA se compone de tres elementos clave que deben ser mantenidos y respaldados:

Aplicación Frontend (React): Los archivos estáticos que componen la interfaz de usuario.

Aplicación Backend (Laravel/PHP): El código fuente que contiene la lógica de negocio y las APIs.

Base de Datos (MySQL): El componente más crítico, donde se almacena toda la información operativa (fallas, mantenimientos, usuarios, etc.).

Procedimientos de Mantenimiento Preventivo

Mantenimiento Diario (Automatizado)

Verificación de Backups Automáticos: Confirmar que el script de backup nocturno se ejecutó correctamente y que el archivo de respaldo fue creado y almacenado en la ubicación designada.

Revisión de Logs del Sistema: Analizar los logs del servidor, de la aplicación (Laravel) y de la base de datos (MySQL) en busca de errores críticos o advertencias recurrentes.

Monitoreo de Recursos del Servidor: Revisar el uso de CPU, memoria RAM y espacio en disco para detectar tendencias anómalas.

Mantenimiento Semanal

Optimización de la Base de Datos: Ejecutar comandos de optimización en las tablas de MySQL para mejorar el rendimiento y recuperar espacio no utilizado.

Revisión de la Seguridad: Analizar los logs de acceso en busca de intentos de inicio de sesión fallidos o actividad sospechosa

Prueba de Integridad del Backup más Reciente: Realizar una restauración de prueba del último backup completo en un entorno de ensayo (staging) para garantizar que el respaldo es válido y recuperable.

Mantenimiento Mensual

Rotación y Archivado de Logs: Comprimir y archivar los logs antiguos para liberar espacio en disco, manteniendo un histórico según las políticas de la empresa (ej. 90 días).

Revisión de Actualizaciones de Seguridad: Verificar la existencia de parches de seguridad, el servidor web, PHP, Laravel y MySQL. Planificar su aplicación.

Limpieza de Datos Temporales: Eliminar archivos temporales, sesiones expiradas y otros datos residuales de la aplicación.

Mantenimiento Bajo Demanda (Actualizaciones)

Aplicación de Parches y Actualizaciones:

Notificar a los usuarios sobre una ventana de mantenimiento programada.

Realizar un backup completo del sistema justo antes de iniciar.

Aplicar las actualizaciones en un entorno de pruebas primero.

Si las pruebas son exitosas, aplicar las actualizaciones en el servidor de producción.

Realizar pruebas de humo (smoke tests) en producción para verificar que las funciones clave operan correctamente.

Notificar a los usuarios la finalización del mantenimiento.

Estrategia de Respaldo (Backup)

Qué Respaldar: Datos y Aplicación

Base de Datos MySQL: El volcado completo (dump) de la base de datos sigpa_db. Esta es la máxima prioridad.

Código Fuente de la Aplicación: La carpeta completa del proyecto Laravel/PHP y la carpeta del build de React. Esto incluye archivos de configuración (.env).

Frecuencia y Tipos de Backup

Backups Completos Diarios (Automatizados): Realizar un backup completo de la base de datos cada noche durante horas de bajo tráfico (ej. 2:00 AM).

Backups Semanales de la Aplicación: Realizar un backup completo del código fuente de la aplicación una vez por semana (ej. domingos), ya que cambia con menos frecuencia que los datos.

Backups Manuales: Realizar un backup completo manual de la base de datos y la aplicación antes y después de cualquier cambio significativo en el sistema (actualizaciones, migraciones, etc.).

Herramientas Recomendadas

Para la Aplicación: tar o zip (para comprimir los directorios del código).

Almacenamiento y Retención de Backups

Regla 3-2-1:

3 copias de los datos.

En 2 tipos de medios diferentes (ej. disco local del servidor y almacenamiento en red).

1 copia off-site (fuera de las instalaciones, ej. en otro centro de datos o en la nube).

Retención:

Backups semanales: Retener por 4 semanas.

Backups mensuales: Retener por 6 meses.

Backups anuales: Retener por 1-3 años, según las políticas de auditoría de la empresa.

Monitoreo y Alertas

Indicadores Clave de Rendimiento (KPIs) a Monitorear

Disponibilidad del Sistema (Uptime): Objetivo > 99.5%.

Tiempo de Respuesta del Servidor: Debe ser inferior a 500ms.

Uso de CPU/RAM: Picos sostenidos por encima del 85% requieren investigación.

Espacio en Disco: Alertas cuando el uso supere el 80%.

Errores de Aplicación (HTTP 5xx): La tasa de errores debe ser cercana a cero.

Configuración de Alertas

Utilizar herramientas de monitoreo (ej. Nagios, Zabbix, Prometheus/Grafana, o servicios en la nube) para configurar alertas automáticas por correo electrónico o SMS al equipo de TI cuando cualquiera de los KPIs anteriores exceda sus umbrales definidos.