

Plan de Mejoras Contra Incidentes en el Período Nocturno

Documento Interno – Patito EC

Elaborado por: Luciana Santamaría, Jefa de Continuidad Operativa y Gestión de Riesgos

Fecha: 8 de abril de 2025

1. Introducción

El presente documento, titulado “**Plan de Mejoras Contra Incidentes en el Período Nocturno**”, tiene como objetivo establecer un conjunto integral de acciones preventivas, correctivas y estructurales para reducir la probabilidad de incidentes críticos durante los turnos nocturnos en Patito EC.

El incidente ocurrido el **6 de abril de 2025**, que provocó la caída del sitio VentadePatos.com, puso en evidencia deficiencias en los sistemas de monitoreo, en la supervisión humana, en la configuración de alertas, en el flujo de comunicación y en la redundancia operativa.

Este plan se basa en un principio fundamental:

No se trata solo de reaccionar a tiempo; se trata de prevenir para no depender de la reacción.

2. Objetivos del Plan

2.1 Objetivo General

Reducir a cero la ocurrencia de incidentes no detectados en horarios nocturnos mediante un sistema híbrido de prevención, supervisión técnica y redundancia funcional.

2.2 Objetivos Específicos

1. Implementar mecanismos redundantes de alerta que no dependan de un único operador.

2. Asegurar supervisión activa por medio de tecnología predictiva e IA.
 3. Reformar la estructura de turnos nocturnos para disminuir la fatiga y mejorar la capacidad de respuesta.
 4. Garantizar que el personal cuente con herramientas confiables y procedimientos claros.
 5. Crear protocolos automatizados de verificación y auditoría continua.
 6. Fortalecer la comunicación interna durante el período nocturno.
-

3. Diagnóstico del Problema

El análisis del incidente reveló los siguientes factores clave:

3.1 Dependencia excesiva de un único operador

El monitoreo recayó completamente sobre el encargado de turno, sin mecanismos que permitieran detectar su inactividad.

3.2 Falta de redundancia en el sistema de alertas

El sistema actual envía notificaciones a un solo dispositivo y no realiza escalamiento si no hay respuesta.

3.3 Ausencia de supervisión externa durante la madrugada

No existía ningún supervisor o mecanismo automático que validara la actividad del operador.

3.4 Procesos desactualizados de verificación

El procedimiento de revisión nocturna carece de pasos obligatorios automatizados que aseguren que el operador está activo.

3.5 Señales previas ignoradas

Durante dos semanas antes del incidente, se registraron micro-fallos de memoria sin intervención.

4. Plan de Acción Integral

A continuación, se detalla el conjunto de acciones divididas en cinco pilares estratégicos.

4.1 Pilar A – Monitoreo Inteligente y Redundante

4.1.1 Sistema de Alertas Redundantes

Implementación del sistema **TriplexAlert**, con tres canales simultáneos:

- Notificación push a dispositivo móvil.
- Llamada automatizada.
- Activación de alarma sonora en estación de trabajo.

Si el operador no responde dentro de 90 segundos:

- Se activa escalamiento automático al supervisor nocturno.
- Si tampoco responde el supervisor, escalamiento a Luciana Santamaría y al equipo de contingencia.

4.1.2 IA Predictiva "Ave Fénix"

Integración del módulo IA propuesto en la "Operación Ave Fénix":

- Monitoreo continuo de patrones anómalos.
- Predicción de picos de RAM, CPU y saturación de red con 2 a 15 minutos de anticipación.
- Recomendaciones automáticas de acción.
- Intervenciones preventivas sin requerir aprobación humana (cuando el riesgo sea menor y controlado).

4.1.3 Auditorías automatizadas

Cada 30 minutos se enviarán señales de actividad al sistema central. Si el operador no confirma en 3 minutos:

- Se envía alerta inmediata.
- Se activa protocolo de verificación.

4.2 Pilar B – Mejora en Supervisión Humana

4.2.1 Supervisión Nocturna en Capas

Nueva estructura de vigilancia:

1. **Operador Nocturno Primario** (encargado directo del monitoreo).
2. **Supervisor Nocturno** (responsable de validar actividad y apoyar decisiones).
3. **Responsable de Continuidad** (guardia pasiva, disponible para escalamiento).

4.2.2 Revisión en Tiempos Específicos

El supervisor nocturno deberá:

- Realizar check-ins obligatorios cada 45 minutos.
- Llevar un registro digital de cada verificación.
- Confirmar funcionamiento del módulo IA.

4.2.3 Sistema Anti-Somnolencia

Para reducir el riesgo de dormirse durante turno:

- Alarmas ambientales cada 45 minutos.
- Iluminación LED fría en estaciones nocturnas.
- Pausas activas obligatorias.
- Verificación de estado del operador mediante sensores de actividad (teclado/mouse).

4.3 Pilar C – Prevención Operativa

4.3.1 Automatización de Respuestas

Los siguientes procesos serán automatizados:

- Limpieza de memoria en picos sostenidos.
- Reinicio controlado de servicios secundarios.
- Envío de advertencias tempranas a administradores.

4.3.2 Detección anticipada de saturación

La herramienta IA debe notificar:

- Crecimiento acelerado de RAM.
- Procesos corruptos en base de datos.

- Riesgo de caída de servicios.

4.3.3 Simulacros de Incidentes

Se realizarán cada 2 semanas:

- Simulacro de caída de base de datos.
 - Simulacro de picos de memoria.
 - Evaluación de tiempos de reacción.
-

4.4 Pilar D – Bienestar y Desempeño Humano

4.4.1 Evaluación de Fatiga

Implementación de un registro semanal para operadores nocturnos:

- Horas dormidas.
- Estado físico.
- Nivel de alerta.

4.4.2 Rotación de Turnos

Para evitar dependencia constante de un solo operador:

- Rotación semanal.
- Entrenamiento cruzado.

4.4.3 Capacitación Especializada

El personal nocturno recibirá:

- Curso avanzado de respuesta a incidentes.
 - Capacitación en manejo de sistemas críticos.
 - Entrenamiento para interpretación del módulo IA.
-

4.5 Pilar E – Mejoras Estructurales y Tecnológicas

4.5.1 Eliminación de Dependencias Críticas

Se reducirá:

- Dependencia de un solo sistema de alarmas.
- Dependencia de un solo operador.

4.5.2 Plataforma Unificada de Contingencia

El proyecto **VentadeGansos.com** será descartado como solución improvisada. Se desarrollará en su lugar:

- Una plataforma espejo de VentadePatos.com.
- Replicación instantánea de datos.
- Failover automático.

4.5.3 Revisión Completa de Configuraciones de Servidores

Se auditará:

- Configuración de memoria.
- Procesos corruptos.
- Scripts de mantenimiento.
- Actualizaciones recientes.

5. Indicadores de Éxito

El plan será considerado exitoso si se cumplen los siguientes criterios:

1. **Cero incidentes críticos nocturnos en 90 días.**
2. Respuesta a alertas menor a 2 minutos.
3. Cumplimiento del 100% de auditorías automatizadas.
4. Reducción del 80% en micro-fallos detectados.
5. Evaluaciones positivas de desempeño del personal nocturno.

6. Cronograma de Implementación

Fase 1 – Primeras 48 horas

- Activación de auditorías automáticas.
- Implementación de alertas redundantes provisionales.

Fase 2 – Primera semana

- Entrenamiento inicial del personal nocturno.
- Nuevas reglas de supervisión.
- Instalación de alarmas ambientales.

Fase 3 – Primer mes

- Activación completa del módulo IA Ave Fénix.
- Inicio de simulacros quincenales.
- Rotación de turnos.

Fase 4 – Primer trimestre

- Plataforma espejo para failover.
- Revisión total de infraestructura.
- Informe final de resultados.

7. Conclusión

Este plan representa un cambio profundo en la cultura operativa de Patito EC. La meta no es únicamente mejorar la reacción ante incidentes, sino construir un sistema donde los incidentes graves sean prácticamente imposibles.

La prevención es la forma más elevada de protección.

Firmado:

Luciana Santamaría

Jefa de Continuidad Operativa y Gestión de Riesgos

Patito EC