AdviceGroup
LATAM

LOS 10 ERRORES OPERACIONALES MÁS COMUNES

Programa: Liderazgo y Estrategia

Serie: Automatización con IA - Optimización de procesos

Prevenir errores operacionales comunes no es solo una buena práctica: es una necesidad crítica **para garantizar la continuidad del negocio, la seguridad de los datos y la eficiencia operativa.**

Incluso, los errores más pequeños, como una mala configuración, una actualización no planificada o una omisión en los respaldos, pueden escalar rápidamente en fallas costosas. ncia entre una administración de TI deficiente y una gestión optimizada como los múltiples beneficios para el negocio.

> **Según un estudio de Gartner, el 80% de las interrupciones no planificadas en los servicios de TI son causadas por errores humanos.**

Tomar conciencia de las fallas más comunes descritas a continuación **y cómo prevenirlas,** puede hacer la diferencia entre una administración de TI deficiente y una gestión optimizada como los múltiples beneficios para el negocio.

1. Errores humanos

Pueden ocurrir debido a **configuraciones hechas de manera incorrecta**, cambios no autorizados o mal ejecutados en la configuración de los sistemas, redes o aplicaciones, lo que suele generar vulnerabilidad o fallas.

También pueden deberse a la **manipulación manual de procesos críticos** o introducción de errores mientras se realizan procesos de mantenimiento o actualización.

¿Cómo evitarlos?

Identifica los procedimientos que pueden ser estandarizados mediante runbooks y scripts. **Implementa soluciones de automatización para la gestión de TI** en procesos frecuentes, que requieran grandes volúmenes de datos o con más riesgo de error.

Establecer políticas de revisión por pares en tareas críticas es una excelente medida, que debe acompañarse de **capacitación continua del personal técnico y operativo para garantizar la eficiencia del equipo.** Además, puedes implementar controles de cambio con aprobación y doble validación.

2. Falta de actualizaciones o parcheo

El desarrollo de amenazas en la internet obliga a **aplicar actualizaciones de seguridad o parches** para no exponer a los sistemas a vulnerabilidades de ninguna clase, especialmente aquellas para las que ya existen defensas comprobadas.

¿Cómo evitarlos?

Implementa un calendario de mantenimiento y parcheo regular para llevar a cabo esta gestión. Aún mejor, **automatiza el despliegue de parcheos** no disruptivos y usa herramientas de gestión de vulnerabilidades. Realiza pruebas en entornos de prueba antes del pase a producción.

3. Problemas en la gestión del cambio

Al hacer cambios en los sistemas, siempre **es recomendable hacer pruebas**, en algunos casos exhaustivas para establecer que todo quede funcionando bien, sin riesgos de interrupciones o comportamientos inesperados. **La mala coordinación entre equipos humanos al hacer cambios da lugar a vulnerabilidades** que pueden volverse críticas, generar conflictos o incoherencias en los sistemas.

¿Cómo evitarlos?

Adopta un modelo formal de gestión del cambio (ITIL). **Asegúrate de que la comunicación del cambio sea clara,** respondiendo a preguntas específicas como “quién es responsable”, “de qué es responsable”, “cuándo es responsable”, “cómo es responsable”, “por qué es responsable”.

4. Errores en la automatización

La configuración errónea de scripts y herramientas de automatización puede resultar en la **ejecución incorrecta de tareas, pérdida de datos o inactividad del servicio**. También pueden ocurrir fallos en la integración de las herramientas automatizadas, lo que deriva en interrupciones de procesos interconectados.

¿Cómo evitarlos?

Recuerda **no automatizar procesos no estandarizados** o inestables. Valida y prueba los scripts/bots exhaustivamente antes de desplegar. **Monitorea los resultados de procesos automatizados** y establece alertas ante fallos. Mantén trazabilidad y **logs detallados** de las ejecuciones, implementando soluciones con IA.

5. Problemas de seguridad

Los errores en la gestión de permisos y automatizaciones provocan que haya **accesos indebidos o malintencionados que pueden causar daños incalculables a los sistemas**, pues la información sensible queda expuesta a personas malintencionadas que aprovechan las brechas en los sistemas de seguridad.

¿Cómo evitarlos?

Aplica políticas de **mínimo privilegio** (Zero Trust Security). Implementa **autenticación multifactor** (MFA). Realiza **auditorías de seguridad periódicas** y capacita a los equipos en ciberseguridad y ciberresiliencia.

6. Fallas en la gestión de backups y recuperación

La información de respaldo o **backup puede ser alcanzada por fallas de seguridad**, lo que pone en riesgo la información y la posibilidad de recuperarla ante un fallo del sistema. En caso de un incidente, la falta de pruebas periódicas de los planes de recuperación, puede causar períodos prolongados de inactividad y graves pérdidas.

¿Cómo evitarlos?

Implementa soluciones con automatización de copias de seguridad y funciones de ciberseguridad, pero recuerda verificar siempre su ejecución. Haz pruebas periódicas de los procesos de restauración. Y sigue la regla 3-2-1: 3 copias, en 2 medios diferentes, 1 fuera del sitio.

7. Monitoreo y alertas deficientes

La **falta de monitoreo adecuado** dificulta la detección de anomalías que empeoran los problemas que pueden ocurrir.

¿Cómo evitarlos?

Utiliza plataformas centralizadas de **monitoreo para la gestión de TI**. **Configura alertas precisas y priorizadas por nivel de criticidad**. Establece umbrales realistas y alertas por anomalías, no solo por fallas. **Es importante capacitar al equipo** para interpretar y actuar ante alertas, lo cual evitará falsos avisos y apatía.

8. Fallas en la documentación y procedimientos

La falta de instrucciones precisas y actualizadas puede permitir **acciones erróneas durante la operación o mantenimiento del sistema.** Cuando no hay protocolos claros para la ejecución de tareas críticas, aumenta la posibilidad de que ocurran errores.

¿Cómo evitarlos?

Crea y mantén actualizada la **documentación técnica y operativa, fijando revisiones periódicas** para asegurar la calidad de la información. Usa wikis o sistemas de gestión del conocimiento accesibles a todos para saber cómo proceder ante un incidente.

9. Dependencia de sistemas legados

El uso de tecnologías que ya dejaron de funcionar puede generar **incompatibilidades, brechas de seguridad** y dificultades para integrar nuevas soluciones.

¿Cómo evitarlos?

Mapea riesgos y costos asociados a sistemas legacy. **Planifica migraciones progresivas** y uso de APIs para integraciones temporales. Es muy importante **aislar los sistemas heredados y aplicar controles de seguridad estrictos**. Involucra a colaboradores con experiencia en el legado, para que aporten con su conocimiento en el proceso de modernización.

10. Errores de comunicación y coordinación

La falta de comunicación y coordinación **entre equipos de la empresa y de proveedores externos** es un riesgo para que ocurran malentendidos y ejecución errónea de procesos en momentos críticos.

¿Cómo evitarlos?

Establece canales formales de comunicación con acceso fácil e inmediato en el que participen usuarios clave. **Realiza reuniones de seguimiento operativas** periódicas para evaluación de procesos. Implementa **herramientas de trabajo colaborativo** y establece procedimientos con roles específicos.

En **AdviceGroup LATAM**, empresa de Corporación MS, **impulsamos la transformación digital de Latinoamérica** brindando soluciones innovadoras que mejoran la eficiencia operativa para adaptar los negocios a las demandas del mercado.

Si necesitas **apoyo para la gestión de TI** o asesoría para implementar soluciones que te ayuden a prevenir estos errores mediante la automatización, **ponte en contacto.**

Siempre tenemos **un asesor y una demo para apoyarte** a tomar una decisión informada en la optimización de procesos.

AdviceGroup
LATAM