Caso simulado

"Diez días para enderezar la casa": Servicio Regional de Obras y Aseo (SROA) – Región de Los Canelos *(ficticio)*

Contexto. El SROA recibe un oficio de la Contralora General solicitando[1], con plazo breve, un reporte integral de controles internos asociados a hechos recientes de probidad y gestión. Se exige clasificar y evidenciar controles preventivos, detectivos y correctivos, detallar fechas, personas involucradas, sumarios y sanciones/medidas.

Tu rol. Eres la/el Directora/Director (estudiante) del SROA. Debes coordinar un informe único y coherente para toda la institución.

La historia

Es lunes, 19 de agosto, 07:42. En tu correo aparece el asunto: *"Requerimiento de información sobre controles internos"*. Tomas café, respiras hondo y abres el mensaje. El oficio pide evidencias concretas. "Sin storytelling vacío, con papeles", piensas. Y vaya que hay material.

Episodio 1: Compras "a la medida"

El Departamento de Abastecimiento tramitó en tres semanas cuatro órdenes de compra de $29,8 millones cada una para "repuestos y mantención de camiones recolectores". El tope para licitar era $30 millones.

- Red flags: Fechas casi correlativas, tres proveedores con representantes que comparten dirección tributaria, y dos cotizaciones con metadatos idénticos (mismo autor PDF).
- WhatsApp filtrado (impreso por un denunciante): "*Mándame la 3ª cotización y cambia el membrete, que quede distinto*".
- Controles existentes (declarados): "Revisión de tres cotizaciones" y "VºBº del Jefe de Abastecimiento".

[1] Tip: leer algunas noticias antes:
https://www.biobiochile.cl/noticias/nacional/chile/2025/08/18/alguien-te-mira-contraloria-ordena-a-todo-el-estado-reportar-controles-internos-ante-corrupcion.shtml

https://www.litoralpress.cl/SimbiuPDF/2025/08/20/6112173.pdf?utm_source=chatgpt.com

- Lo real: No hay matriz de segregación de funciones (el mismo analista arma bases, recibe cotizaciones y propone adjudicación). No hay revisión independiente de fraccionamiento.

Episodio 2: Horas extra fantasma en Operaciones

En Aseo y Barrido, la jefatura reportó picos de horas extra por emergencias climáticas. Pero los GPS de los camiones muestran 30% menos de tiempo en ruta y las planillas de asistencia tienen firmas escaneadas idénticas.

- Bitácoras: Tres días seguidos sin registro de salida de patio, pero con horas extra pagadas.
- Control declarado: “Firma de jefe de turno”.
- Brecha: Sin conciliación cruzada entre asistencia, GPS y partes diarios. Sin alertas automáticas por sobre-umbral de horas.

Episodio 3: TI y la sombra en los logs

El usuario “admin” es compartido por tres personas del área TI. Una auditoría interna anterior ya observó borrados de logs en fines de semana.

- Hecho crítico: Entre 24 y 26 de junio no existen registros del servidor de archivos de Abastecimiento.
- Control declarado: “Respaldo semanal”.
- Brecha: Backups no probados (nadie hace restore test), accesos no segregados, y sin SIEM para correlación de eventos.

Otros condimentos

- Combustible: vales manuales, sin control kilométrico ni consumo estándar por ruta.
- Proveedores repetidos: dos RUT con accionistas parientes de un ex-funcionario.
- Capacitación probidad: última sesión hace 3 años; nadie firmó asistencia.

Lo que te piden (sí o sí en el reporte)

1. Mapa de procesos críticos (Abastecimiento, Operaciones, TI).
2. Riesgos y controles clasificados en preventivo / detectivo / correctivo.
3. Evidencias (documentos, metadatos, logs, actas, reportes GPS, respaldos).

4. Fechas de ocurrencia, personas involucradas, estado de sumarios y medidas.
5. Plan de mejora con plazos (30/60/90 días) + responsables + KPI de control.

Formato recomendado (matriz por proceso)

Proceso	Riesgo	Control (P/D/C)	Dueño	Frecuencia	Evidencia	Test de diseño	Test de operación	Eficacia	Mejora/Plazo	KPI de control

(P = preventivo; D = detectivo; C = correctivo)

Preguntas/Enunciado:

1. Diseña la matriz de controles del proceso de Abastecimiento para mitigar fraccionamiento de compras y colusión, clasificando preventivos, detectivos y correctivos. Indica evidencias, frecuencia, dueños, pruebas de auditoría (diseño/operación) y KPI mínimos.
2. (Gestión del cambio) ¿Cómo implementarías, en 90 días, un plan de remediación que cambie conductas arraigadas (p. ej., “usuario admin compartido”, “vales manuales”), sin paralizar el servicio?
3. (TI & continuidad) Propón un esquema de seguridad y continuidad para logs, respaldos y trazabilidad documental que sea viable con presupuesto municipal.

Respuesta:

Tabla P/D/C – Seguridad TI & Continuidad (Municipal)

Área	Preventivo (P)	Detectivo (D)	Correctivo (C)
Logs de sistemas	- Centralizar logs con software libre (Graylog, Wazuh o syslog Linux). - Definir retención mínima 12 meses en línea y 24 meses en respaldo. - Permisos restringidos de solo escritura.	- Hash semanal SHA-256 para validar integridad. - Reportes mensuales de accesos y errores. - Cruce de logs con asistencia/usuarios.	- Reprocesar logs desde respaldos si hay pérdida. - Apertura de sumario si hay alteraciones. - Notificación a CGR de medidas adoptadas.
Respaldos de datos	- Estrategia 3-2-1: 3 copias (producción, local, nube). - Incrementales diarios y completos semanales. - Copia mensual offsite en disco externo cifrado.	- Verificación automática de respaldo (checksums). - Informe mensual de respaldo correcto. - Ensayo de restauración trimestral.	- Restaurar desde copia más reciente. - Aplicar plan de continuidad (operación manual). - Informe de lección aprendida con plazos de mejora.
Trazabilidad documental	- Uso de gestor documental libre/bajo costo (Nextcloud, Alfresco). - Firma electrónica simple (Ley 19.799). - Metadatos obligatorios (fecha, responsable, etapa).	- Registro de accesos y descargas. - Reportes automáticos de modificaciones y versiones. - Auditoría interna mensual.	- Restaurar versión anterior del documento. - Rectificación con firma y nuevo folio. - Informar y registrar corrección ante unidad jurídica.

Área	Preventivo (P)	Detectivo (D)	Correctivo (C)
Plan de continuidad	- BIA básico: definir procesos críticos. - RTO=48 hrs, RPO=24 hrs. - Manual de continuidad con responsables.	- Simulacros semestrales de caída de sistema y pérdida de respaldo. - Checklist de cumplimiento ISO 22301 light.	- Activar plan manual (Excel + firmas) hasta restauración. - Documentar incidente y acciones. - Ajustar plan de continuidad según hallazgos.

Prof.: Dr. (c) Rafael Paredes Carrasco
Cátedra: Auditoría Gubernamental