

El Error de los Compliance Officers: Independencia, Criterio y Gobernanza Digital

Presentación del tema

En la práctica organizacional, uno de los riesgos más profundos dentro de las organizaciones no es el error técnico ni la falta de conocimiento normativo, sino algo más sutil: la adaptación excesiva del responsable de cumplimiento para “encajar” en la dinámica organizacional. Esta observación revela una tensión estructural entre el rol técnico del compliance y las presiones culturales, comerciales y políticas que existen dentro de cualquier organización.

El compliance —cumplimiento normativo— no puede entenderse únicamente como un conjunto de normas, controles o manuales. Es un sistema de gobierno interno cuya eficacia depende, en gran medida, de la independencia, la claridad de criterio y la credibilidad de quienes lo ejecutan. El problema comienza cuando el rol deja de sostener criterio para priorizar aceptación: allí se erosiona la función preventiva y protectora que justifica su existencia. Esta reflexión adquiere especial relevancia en el ámbito de las Tecnologías de la Información (IT), donde los sistemas digitales concentran datos, poder de decisión y procesos críticos.

El fenómeno de la adaptación progresiva

El problema no comienza con actos abiertamente irregulares, sino con pequeños ajustes discursivos: “Lo podemos manejar después”, “No seamos tan rígidos”, “Busquemos un punto medio”. Estas expresiones representan micro-decisiones que, acumuladas, generan una pendiente resbaladiza organizacional. No se trata de corrupción manifiesta, sino de una erosión gradual del estándar profesional.

En un entorno tecnológico, el compliance no solo revisa contratos o documentos: supervisa procesos digitales, controles automatizados, trazabilidad de datos, segregación de funciones y auditoría de sistemas. Cuando el criterio se flexibiliza excesivamente, se

Se autoriza la reproducción total o parcial del presente material con fines educativos, siempre que se cite adecuadamente la fuente, indicando autor, título del documento y sitio web de origen.

relajan controles de acceso, se permiten excepciones sin trazabilidad, se postergan mitigaciones de riesgos tecnológicos y se toleran brechas en seguridad o protección de datos. El impacto no es inmediato, pero sí acumulativo.

La presión invisible en entornos organizacionales

El oficial de cumplimiento enfrenta presiones concretas: metas comerciales que demandan velocidad, urgencias operativas que priorizan continuidad sobre control, relaciones personales que generan expectativas de reciprocidad, y el miedo a perder legitimidad ante la organización.

Estas presiones son especialmente intensas en proyectos tecnológicos: el área comercial presiona para lanzar antes del cierre trimestral; el área operativa prioriza continuidad sobre control; los equipos técnicos buscan flexibilidad para cumplir plazos; la dirección espera resultados rápidos. El compliance se encuentra en un punto de fricción permanente entre eficiencia y control, entre objetivos de corto plazo —rentabilidad, velocidad— y objetivos de largo plazo —sostenibilidad, mitigación de riesgo—.

Identidad profesional y pérdida de credibilidad

La identidad profesional del compliance se construye sobre independencia técnica, criterio fundamentado, capacidad de sostener decisiones impopulares y coherencia entre discurso y práctica. Cuando el responsable comienza a negociar lo que no debería negociar, ocurren cuatro pérdidas progresivas: de claridad, de independencia, de autoridad y de credibilidad.

La credibilidad es el capital intangible del compliance. Sin ella, ningún sistema de control funciona: las alertas de seguridad dejan de priorizarse, los hallazgos de auditoría se minimizan, los reportes de incidentes pierden urgencia y las recomendaciones se transforman en sugerencias opcionales. El resultado es la desactivación del sistema preventivo completo.

Compliance como función incómoda y necesaria

El rol no existe para encajar, sino para incomodar cuando es necesario. En administración estratégica, esto puede interpretarse como una función de contrapeso institucional. En proyectos tecnológicos, el compliance puede frenar un despliegue si no se cumplieron pruebas de seguridad, exigir controles adicionales antes de integrar datos sensibles, rechazar configuraciones que violen la segregación de funciones o solicitar documentación antes de aprobar procesos automatizados. Estas decisiones generan fricción inmediata pero previenen costos reputacionales, regulatorios y financieros futuros.

Dos ejemplos ilustran el fenómeno: una empresa implementa un módulo financiero sin validar la segregación de funciones, permitiendo que una misma persona cree y apruebe pagos. El sistema opera técnicamente, pero el riesgo de control interno es crítico. En otro caso, se habilita acceso remoto sin autenticación robusta para cumplir una urgencia operativa; la decisión parece pragmática, pero incrementa la exposición a ciberataques. En ambos casos, el problema no fue la tecnología, sino la adaptación excesiva del criterio.

Implicancias para la formación profesional

Para los estudiantes de la Licenciatura en Administración, la enseñanza es estratégica: la gestión moderna no solo requiere conocimiento técnico, sino fortaleza institucional y coherencia ética. En el contexto de digitalización acelerada, automatización e inteligencia artificial, la función de cumplimiento adquiere mayor relevancia. Cuanto más complejo es el sistema, mayor debe ser la claridad de criterio. La adaptación excesiva puede generar aceptación temporal; la integridad sostenida construye legitimidad duradera.

Conceptos clave

- El mayor riesgo del compliance no es el error técnico, sino la erosión silenciosa del criterio.
- La adaptación progresiva como pendiente resbaladiza organizacional.

Se autoriza la reproducción total o parcial del presente material con fines educativos, siempre que se cite adecuadamente la fuente, indicando autor, título del documento y sitio web de origen.

- La credibilidad como capital intangible del compliance.
- Cuatro pérdidas progresivas ante la pérdida de independencia: claridad, autonomía, autoridad y credibilidad.
- El compliance como función de contrapeso necesaria en la gobernanza digital.
- La integridad no se negocia parcialmente en contextos tecnológicos complejos.

Preguntas de repaso del tema

1. ¿Por qué la pérdida de credibilidad del compliance impacta en la eficacia de los sistemas de información?
2. ¿Cómo pueden las metas comerciales afectar la independencia del responsable de cumplimiento en proyectos tecnológicos?
3. ¿Qué relación existe entre identidad profesional y gobernanza digital?
4. ¿Qué riesgos sistémicos pueden generarse cuando se flexibilizan controles tecnológicos por urgencia operativa?
5. ¿Por qué la integridad no puede negociarse parcialmente en contextos organizacionales complejos?
6. ¿Por qué las micro-decisiones de adaptación son más peligrosas que los actos irregulares evidentes?
7. ¿Qué relación existe entre la credibilidad del compliance y la efectividad de los controles técnicos?
8. ¿Cómo puede el diseño organizacional respaldar la independencia del compliance frente a presiones internas?
9. ¿Qué ejemplos concretos ilustran la tensión entre eficiencia operativa y control en proyectos de TI?

Se autoriza la reproducción total o parcial del presente material con fines educativos, siempre que se cite adecuadamente la fuente, indicando autor, título del documento y sitio web de origen.

10. ¿Por qué la función de compliance adquiere mayor importancia en entornos de alta complejidad tecnológica?