

Deloitte.



Cumplimiento institucional
en hospitales
Un imperativo vital

Introducción

En la industria de hospitales, el cumplimiento normativo no solo se asocia con regulaciones financieras fiscales, legales o administrativas, como cualquier otra industria. Por una parte, los hospitales enfrentan una creciente complejidad regulatoria que abarca desde la seguridad clínica, hasta el manejo de datos sensibles, pasando por la ética médica y la administración de fármacos. Incumplir estas dimensiones no solo conlleva sanciones legales o reputacionales, también puede suponer daños irreparables a la salud y a la dignidad de las personas.

Por otra parte, algunos hospitales están optando por certificaciones y acreditaciones tanto locales como internacionales, para demostrar su compromiso con la excelencia en atención médica. Obtener una certificación hospitalaria de prestigio —como las otorgadas por *Joint Commission International (JCI)*, *Accreditation Canada* o los estándares *ISO*— representa mucho más que el cumplimiento de requisitos: es una decisión estratégica que impulsa la transformación institucional. Entre sus principales beneficios, destacamos los siguientes:

- Mejora continua de la calidad y la seguridad del paciente, a través de procesos clínicos estandarizados, auditables y basados en evidencia.
- Fortalecimiento de la gobernanza hospitalaria, al establecer responsabilidades claras, sistemas de monitoreo y rendición de cuentas.
- Mayor confianza de pacientes, aseguradoras, inversionistas y aliados estratégicos, gracias a un reconocimiento que trasciende fronteras.
- Posicionamiento competitivo en *rankings* nacionales e internacionales, facilitando convenios, atracción de talento y acceso a nuevos mercados.
- Cultura institucional centrada en la excelencia, la eficiencia y la humanización del servicio, reforzando tanto la experiencia del paciente como la del personal clínico.

Certificarse no es un fin en sí mismo, sino una plataforma para alcanzar estándares superiores de desempeño, con impacto real en la salud, la reputación y la sostenibilidad del hospital.



Importancia de un programa institucional de cumplimiento en una **organización hospitalaria**

El cumplimiento en el entorno hospitalario no es una formalidad administrativa: es una función crítica que sostiene la integridad, la seguridad y la legitimidad de toda la operación clínica. Su alcance abarca una serie de principios y controles fundamentales que protegen tanto al paciente como a la institución.



En conjunto, estos elementos no solo mitigan riesgos legales y operativos, sino que consolidan una cultura de responsabilidad, transparencia y mejora continua, indispensable para cualquier hospital que aspire a brindar atención de excelencia y sostener la confianza de sus pacientes, profesionales y aliados.

Seguridad del paciente

Los marcos regulatorios en materia de seguridad del paciente, como el *Plan de acción mundial para la seguridad del paciente* emitido por la Organización Mundial de la Salud (OMS), o las agencias sanitarias locales, exigen protocolos estrictos de identificación, trazabilidad, higiene, administración de tratamientos y monitoreo de eventos adversos (pandemias).

Su cumplimiento no debe verse como una tarea técnica, sino como una manifestación ética del compromiso del hospital con la vida humana. La omisión o el cumplimiento superficial de estas disposiciones ha derivado históricamente en tragedias evitables: desde cirugías erróneas hasta infecciones nosocomiales fatales. La dirección hospitalaria tiene la responsabilidad indelegable de garantizar que estos estándares se cumplan y, sobre todo, que formen parte de la cultura operativa cotidiana.



Ética médica

La ética médica es el conjunto de principios, valores y normas que guían el comportamiento profesional de los médicos y demás personal de salud en el ejercicio de su práctica. No se limita a cumplir alguna ley o a seguir protocolos clínicos, implica tomar decisiones responsables que equilibren el bienestar del paciente, los derechos humanos, las obligaciones profesionales y las implicaciones sociales del acto médico.

Un hospital debiera contar con un comité ético funcional, independiente y multidisciplinario, capaz de emitir juicios objetivos ante dilemas clínicos complejos. Se debe promover la formación continua en ética para todo el personal, pues cumplir con la ética no solo protege a los pacientes, sino también a los médicos ante decisiones difíciles.

Protección de datos sensibles

La información médica de los pacientes es uno de los activos más importantes y sensibles que gestiona un hospital. Normativas como la *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados en México*, o el *Reglamento General de Protección de Datos de la Unión Europea (GDPR)*, por sus siglas en inglés, imponen obligaciones claras en materia de confidencialidad, acceso restringido, encriptación, trazabilidad de accesos y consentimiento informado.

La fuga de un expediente, la filtración de diagnósticos o el uso indebido de imágenes clínicas, además de representar una violación legal, representa una fractura ética que puede destruir la confianza en la institución. Por ello, la dirección del hospital debe asegurar que los sistemas informáticos tengan capas de ciberseguridad avanzadas, que el personal esté capacitado para actuar con plena conciencia en el uso ético de la gestión de la información y que existan sanciones efectivas ante faltas graves.





Control de medicamentos

El cumplimiento en el manejo de medicamentos requiere sistemas robustos para evitar errores de prescripción, abuso en la utilización de ciertos medicamentos, pérdida de trazabilidad, robo hormiga o uso de fármacos caducados. El mal manejo de medicamentos es una de las principales causas de eventos adversos graves, hospitalizaciones innecesarias y gastos evitables.

La dirección debe garantizar que el sistema hospitalario incorpore controles automatizados para la administración de medicamentos, alertas de interacciones peligrosas, inventarios cerrados por zonas y acceso restringido por niveles de responsabilidad. Esto incluye, también, el cumplimiento con regulaciones farmacológicas vigentes, por lo que, en este contexto, el cumplimiento normativo protege tanto al paciente como al hospital frente a posibles litigios por negligencia.

Atención clínica

Finalmente, la atención clínica debe cumplir con protocolos médicos estandarizados, guías clínicas nacionales e internacionales, y criterios de calidad validados por entidades externas. El cumplimiento en esta dimensión no es un fin burocrático, es una herramienta para homogeneizar buenas prácticas, reducir la variabilidad injustificada en la atención y asegurar resultados clínicos medibles.

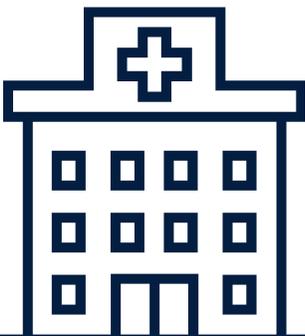
La dirección debe propiciar auditorías clínicas periódicas, programas de mejora continua, comités de calidad y sistemas de monitoreo de desempeño profesional. Cada médico y cada enfermera deben saber que su práctica está sujeta al juicio clínico y, principalmente, al marco normativo que da coherencia a toda la organización.



Regulaciones no clínicas

Además de las regulaciones directamente vinculadas a la atención médica, los hospitales deben cumplir con un conjunto complejo de regulaciones no clínicas que son igual de obligatorias y críticas para su operación. Estas normas abarcan ámbitos empresariales, laborales, ambientales, financieros y de seguridad patrimonial, las cuales son:

- Normatividad laboral y de seguridad social.
- Regulación fiscal y contable.
- Protección civil, infraestructura y seguridad patrimonial.
- Normativa ambiental y de sostenibilidad.
- Regulación contractual, corporativa y de transparencia.
- Normas de tecnología y ciberseguridad.
- Cumplimiento financiero, lavado de dinero y seguros.
- Derechos humanos, inclusión y equidad.



Implementar un **programa de cumplimiento** robusto e institucional no es opcional, es estratégico y necesario

La regulación es un conjunto de criterios mínimos éticos para garantizar condiciones seguras de cumplimiento. Las instituciones de salud operan en un entorno de alta complejidad, donde confluyen la atención al paciente, el manejo de información sensible, la operación con recursos públicos o privados y una estricta regulación sanitaria.

Un hospital que solo actúa “cuando lo obliga la autoridad” opera día a día de forma arriesgada o crítica; por el contrario, un hospital que interioriza el cumplimiento como un acto de respeto hacia la vida y la dignidad humana, construye reputación, sostenibilidad y liderazgo ético.

La carencia de un programa de cumplimiento institucional vuelve a cualquier hospital una entidad expuesta, frágil y mal preparada para crecer o afrontar una crisis. En cambio, la implementación de un programa robusto, permite alinear la operación con las exigencias normativas, proteger a los pacientes y profesionales de la salud, así como fortalecer la imagen y sostenibilidad de la organización.

Se debe asegurar que todas las operaciones se realicen de manera ética, legal, segura y alineada con los valores institucionales, generando confianza sostenible con pacientes, autoridades, empleados y la sociedad en general. Este objetivo se traduce en seis líneas de impacto estratégico:

- Protección de la continuidad operativa.
- Fortalecimiento de la confianza institucional.
- Toma de decisiones oportunas y transparentes.
- Prevención de riesgos clave.
- Agilidad operativa con marcos normativos claros.
- Creación de valor institucional y reputacional.

Contar con un sólido programa de cumplimiento, vuelve al hospital más atractivo para inversionistas, alianzas estratégicas, aseguradoras, talento médico y autoridades.



Riesgos, control interno y cumplimiento: *tres líneas* que no pueden caminar por separado

Un programa institucional de cumplimiento eficaz no puede operar de forma aislada; debe estar estrechamente vinculado con la administración de riesgos y el sistema de control interno. En el entorno hospitalario, donde cada decisión puede afectar la vida o, peor aún, causar la muerte de una persona, esta sinergia no es opcional, es vital.

Identificar para *prevenir*

El primer paso del cumplimiento es saber dónde están los riesgos. Un hospital que no identifica sus puntos vulnerables —por ejemplo, en la trazabilidad de expedientes, en la cadena de suministro de medicamentos o en el consentimiento informado— siempre estará reaccionando tarde. La administración de riesgos en hospitales debe contemplar lo siguiente:

- Riesgos clínicos: omisión de protocolos, errores en la atención.
- Riesgos regulatorios: incumplimiento de normas de la Comisión Federal para la Protección contra Riesgos Sanitarios (COFEPRIS), Normas Oficiales Mexicanas (NOM), leyes de protección de datos.
- Riesgos de corrupción: compras no transparentes, relaciones indebidas con proveedores.
- Riesgos reputacionales: eventos adversos ocultos o mal gestionados.

Un mapa de riesgos bien construido permite al área de cumplimiento actuar con foco, prioridad y contundencia.

Control interno: ejecutar con *confianza*

El sistema de control interno hospitalario es el andamiaje operativo que permite ejecutar los procesos con integridad, precisión y eficiencia. Cada política clínica, autorización, segregación de funciones y monitoreo interno fortalecen la credibilidad del hospital y dan sustento al cumplimiento. A continuación, algunos ejemplos clave:

- Protocolos documentados para la administración de medicamentos controlados.
- Accesos auditados a expedientes clínicos digitales.
- Validaciones cruzadas en la facturación a aseguradoras.
- Evaluación de proveedores con criterios éticos, técnicos y financieros.

Sin control interno, el cumplimiento es aspiracional. Sin cumplimiento, el control interno no tiene brújula.

Una triada de *protección* institucional

Riesgos, controles y cumplimiento deben hablar el mismo idioma, esto se traduce en las siguientes características:

- Gobernanza unificada: comités que supervisan los tres temas en conjunto.
- Sistemas integrados: tecnología que detecta anomalías, dispara alertas y permite trazabilidad.
- Cultura organizacional: el personal clínico y administrativo entiende su rol en protección del paciente y de la organización.

Con estas tres características alineadas, un hospital opera con transparencia, minimiza errores, previene sanciones y gana la confianza del entorno.

En la industria de hospitales, el cumplimiento no puede tratarse como un simple requisito normativo, es una función estratégica, transversal y crítica para la sostenibilidad operativa, la calidad clínica y la confianza institucional. Sin ello, los riesgos se desbordan, los controles se debilitan y los errores se vuelven inevitables. No obstante, cuando el cumplimiento se institucionaliza, cuando se conecta con la gestión de riesgos y se apoya en un control interno robusto, se convierte en una fortaleza competitiva y moral.

El **rol estratégico** de Auditoría Interna en el fortalecimiento del programa de cumplimiento

En un hospital —donde la confianza es un activo intangible y la exposición al riesgo regulatorio es permanente—, la función de Auditoría Interna debe dejar de ser vista como un mero verificador de hechos pasados para posicionarse como un socio estratégico del programa de cumplimiento. Su valor radica en su capacidad para evaluar objetivamente, anticipar desviaciones y fortalecer la cultura de integridad, en un entorno donde los errores no solo cuestan dinero, sino vidas.

El programa de cumplimiento en un hospital no se limita a verificar normativas médicas; como se menciona anteriormente, abarca una compleja red de regulaciones que incluyen protección de datos, prácticas laborales, uso de recursos públicos o donativos, ética en la contratación, transparencia financiera y responsabilidad socioambiental. En este contexto, Auditoría Interna actúa como el principal mecanismo de aseguramiento independiente, garantizando que los controles del programa de cumplimiento estén no solo diseñados, sino que realmente operen con eficacia en la práctica clínica, administrativa y financiera.

Su rol también implica identificar vacíos normativos, evaluar la eficacia de las líneas de denuncia, verificar la integridad de los procesos críticos (como la adquisición de insumos o la facturación), y emitir recomendaciones que corrijan la raíz de los incumplimientos, no solo sus síntomas. Esto es particularmente relevante en instituciones que enfrentan presiones reputacionales, auditorías externas o acreditaciones sanitarias.

Además, cuando Auditoría Interna trabaja de forma coordinada con el área de cumplimiento —pero conservando su independencia— se crea un modelo de defensa robusto, que combina monitoreo continuo, evaluaciones temáticas, uso de analítica de datos y pruebas de eficacia que brindan certeza al consejo directivo sobre el verdadero estado del cumplimiento institucional.

Auditoría Interna es el puente entre el diseño normativo y la realidad operativa del hospital. Es el radar que detecta zonas grises, el escudo contra sanciones inesperadas y el motor de una mejora continua basada en evidencia objetiva. Ignorar o subutilizar esta función es dejar el cumplimiento a merced de la intuición. Integrarla, en cambio, es transformar el riesgo en gobernabilidad.

Tecnología

La tecnología se ha convertido en el principal habilitador para institucionalizar y escalar un programa de cumplimiento. Su papel no es accesorio, es estructural. La digitalización permite automatizar controles, generar alertas tempranas, fortalecer la auditoría continua y, en tiempo real, dar visibilidad a los riesgos clínicos y administrativos.

En México, múltiples hospitales han comenzado a integrar soluciones tecnológicas como parte de su estrategia de cumplimiento, especialmente, en áreas críticas como el expediente clínico, la cadena de suministro y la relación con terceros. Por ejemplo, plataformas de expediente clínico electrónico certificadas por la *NOM-004-SSA3-2012* permiten documentar cada intervención, firmar digitalmente órdenes médicas y auditar accesos a la información del paciente, lo cual, no solo mejora la atención, sino que mitiga riesgos legales por omisiones o alteraciones. Algunas soluciones tecnológicas, al estar integradas con módulos de gestión hospitalaria, permiten establecer alertas automáticas en caso de faltar consentimientos informados según el tipo de procedimiento, si se rompe la cadena de frío de un medicamento o si hay una sobredosis registrada.

La analítica avanzada también se está utilizando para prevenir incumplimientos antes de que ocurran. Algunos hospitales exploran la aplicabilidad de modelos de *machine learning* (aprendizaje automático) sobre sus datos operativos para detectar patrones inusuales, como prescripciones fuera del estándar, rotación anormal de personal en ciertas áreas o pacientes con reingresos recurrentes sin causa clínica clara. Esta capacidad predictiva convierte al cumplimiento en una función proactiva, más cercana a la prevención de incidentes que a la corrección de fallas.

Conclusiones

Contar con un programa de cumplimiento sólido ya no es una opción para los hospitales, es una exigencia ética, legal y estratégica. La creciente complejidad regulatoria, los riesgos clínicos y operativos, así como la presión social por brindar servicios seguros y transparentes, obligan a replantear cómo se gestiona el cumplimiento dentro de las instituciones de salud.

Pero no basta con tener políticas o comités: la verdadera diferencia radica en qué tan maduro y eficaz es el programa. De ahí la necesidad de plantearse lo siguiente: el programa ¿está alineado con los riesgos reales del hospital?, ¿es comprendido y aplicado por el personal clínico y administrativo?, ¿está preparado para responder ante incidentes críticos o auditorías regulatorias?

Una forma de responder estas preguntas con objetividad es medir el nivel de madurez del programa de cumplimiento para identificar brechas, reconocer fortalezas y construir una hoja de ruta hacia un cumplimiento verdaderamente institucionalizado.



Contactos

Israel Zagal

Socio de Asesoría y Consultoría
Deloitte México
izagal@deloittemx.com

Miguel Hernández

Socio de Asesoría y Consultoría
Deloitte México
mihernandez@deloittemx.com

Alexandro Arias

Socio Líder de Ciencias de la Vida y Cuidado de la Salud
Deloitte Spanish Latin America
alarias@deloittemx.com

Deloitte.

Deloitte se refiere a una o más entidades de Deloitte Touche Tohmatsu Limited (“DTTL”), su red global de firmas miembro y sus sociedades afiliadas a una firma miembro (en adelante “Entidades Relacionadas”) (colectivamente, la “organización Deloitte”). DTTL (también denominada como “Deloitte Global”) así como cada una de sus firmas miembro y sus Entidades Relacionadas son entidades legalmente separadas e independientes, que no pueden obligarse ni vincularse entre sí con respecto a terceros. DTTL y cada firma miembro de DTTL y su Entidad Relacionada es responsable únicamente de sus propios actos y omisiones, y no de los de las demás. DTTL no provee servicios a clientes. Consulte www.deloitte.com/mx/conozcanos para obtener más información.

Deloitte presta servicios profesionales líderes de auditoría y assurance, impuestos y servicios legales, consultoría, asesoría financiera y asesoría en riesgos, a casi el 90% de las empresas Fortune Global 500® y a miles de empresas privadas. Nuestros profesionales brindan resultados medibles y duraderos que ayudan a reforzar la confianza pública en los mercados de capital, permiten a los clientes transformarse y prosperar, y liderar el camino hacia una economía más fuerte, una sociedad más equitativa y un mundo sostenible. Sobre la base de su historia de más de 175 años, Deloitte abarca más de 150 países y territorios. Conozca cómo los aproximadamente 460,000 profesionales de Deloitte en todo el mundo crean un impacto significativo en www.deloitte.com.

Tal y como se usa en este documento, Galaz, Yamazaki, Ruiz Urquiza, S.C., tiene el derecho legal exclusivo de involucrarse en, y limita sus negocios a, la prestación de servicios de auditoría y otros servicios profesionales bajo el nombre de “Deloitte”. Deloitte Impuestos y Servicios Legales, S.C., tiene el derecho legal exclusivo de involucrarse en, y limita sus negocios a, la prestación de servicios de consultoría fiscal, asesoría legal y otros servicios profesionales bajo el nombre de “Deloitte”. Deloitte Audit Delivery Center, S.C. (antes Deloitte Auditoría, S.C.), tiene el derecho legal exclusivo de involucrarse en, y limita sus negocios a, la prestación de servicios de auditoría y otros servicios profesionales bajo el nombre de “Deloitte”. Deloitte Asesoría en Riesgos, S.C., tiene el derecho legal exclusivo de involucrarse en, y limita sus negocios a, la prestación de servicios de asesoría en riesgos y otros servicios profesionales bajo el nombre de “Deloitte”. Deloitte Asesoría Financiera, S.C., tiene el derecho legal exclusivo de involucrarse en, y limita sus negocios a, la prestación de servicios de asesoría financiera y otros servicios profesionales bajo el nombre de “Deloitte”. Y Deloitte Consulting Group, S.C., tiene el derecho legal exclusivo de involucrarse en, y limita sus negocios a, la prestación de servicios de consultoría y otros servicios profesionales bajo el nombre de “Deloitte”.

Esta comunicación contiene solamente información general y ni Touche Tohmatsu Limited (“DTTL”), su red global de firmas miembro o sus Entidades Relacionadas (colectivamente, la “organización Deloitte”) está, por medio de esta comunicación, prestando asesoramiento profesional o servicio alguno. Antes de tomar cualquier decisión o tomar cualquier medida que pueda afectar sus finanzas o su negocio, debe consultar a un asesor profesional calificado.

No se proporciona ninguna representación, garantía o promesa (ni explícita ni implícita) sobre la veracidad ni la integridad de la información en esta comunicación, y ni DTTL, ni sus firmas miembro, Entidades Relacionadas, empleados o agentes será responsable de cualquier pérdida o daño alguno que surja directa o indirectamente en relación con cualquier persona que confíe en esta comunicación. DTTL y cada una de sus firmas miembro y sus Entidades Relacionadas, son entidades legalmente separadas e independientes.