Importancia de la Integridad de Datos en la Industria Farmacéutica

Maria Isabel Montoya Correa

Monografía presentada para optar al título de Especialista en Gestión y Aseguramiento de la Calidad en Laboratorios Clínico y de Ensayo

Asesora
Nathalia Andrea Gómez Grimaldos, Doctor (PhD) en Biotecnología

Universidad de Antioquia
Escuela de Microbiología
Especialización en Gestión y Aseguramiento de la Calidad de Laboratorios Clínico y de Ensayo
Medellín, Antioquia, Colombia
2024

Cita	(Montoya Correa, 2024)
Referencia **Estilo APA 7 (2020)**	Montoya Correa, M. (2024). *Importancia de la Integridad de Datos en la Industria Farmacéutica* [Trabajo de grado especialización]. Universidad de Antioquia, Medellín, Colombia.

Especialización en Gestión y Aseguramiento de la Calidad en Laboratorios Clínico y de Ensayo, Cohorte I.

APROBADO:

Nathalia A. Gómez G

Tabla de contenido

Resumen

Una de las principales problemáticas a las que se enfrentan actualmente los laboratorios farmacéuticos y que impacta directamente a la gestión y aseguramiento de la calidad, es la integridad de datos. Si bien este tema no es nada nuevo, ha tomado gran importancia y relevancia debido a las implicaciones normativas y de acreditación que implican, además de los riesgos e impactos que pueden surgir para la salud de los pacientes y la calidad de los productos.

Hablar de la integridad de datos, implica también abordar problemáticas como la seguridad de la información, la farmacovigilancia, la confidencialidad y tratamiento de los datos personales y los ciberataques, ya que la mayoría de organizaciones se encuentran expuestas a estas y pueden verse afectadas en algún momento por el uso inadecuado de la información.

El presente trabajo tiene como objetivo identificar las principales problemáticas que se presentan en la industria farmacéutica con respecto al manejo y seguridad de la información, las regulaciones, guías y requisitos y el estado actual de las organizaciones farmacéuticas frente a esto.

Según la revisión bibliográfica realizada, se concluyó que las principales problemáticas de la integridad de datos en las organizaciones, las relacionadas con la falta de mecanismos de control adecuados para el manejo de la información, la implementación de normas y establecimiento de planes y controles que contribuyan a minimizar los riesgos de posibles ciberataques y manipulación indebida de la información.

Se recomienda trabajar en el mejoramiento de los sistemas de gestión y evaluación de los riesgos informáticos a los que está expuesta la organización y la manera en que estos impactan su modelo de negocios.

Palabras claves: Integridad de datos, seguridad de la información, farmacovigilacia, ciberseguridad, industria farmacéutica.

Introducción

Uno de los principales objetivos de un sistema de gestión y aseguramiento de calidad de un laboratorio farmacéutico es generar resultados (información), a partir de la producción de datos que son obtenidos por la aplicación de procedimientos y técnicas analíticas adecuadas con el fin de asegurar que un medicamento es apto y confiable para su uso. El control y aseguramiento de calidad del laboratorio, son parte indispensable para cumplir con este objetivo, la falta de alguno de estos componentes compromete la validez de los resultados analíticos.

Uno de los temas más crítico en cuanto al aseguramiento de la calidad y al que actualmente los laboratorios farmacéuticos presentan especial atención es la integridad de datos, no solo porque a nivel normativo es exigido y es la principal causa de los hallazgos que se presentan durante las inspecciones de buenas prácticas de manufactura y buenas prácticas de laboratorio, teniendo fuertes implicaciones en temas de acreditación, porque representa un gran riesgo para la seguridad, en la calidad de los medicamentos y en la salud del paciente.

Según la FDA, la integridad de datos se refiere, no solo a la integridad, sino también a la coherencia y precisión de los datos. Los datos completos, consistentes y precisos deben ser atribuibles, legibles, registrados al mismo tiempo, originales o en copia fiel y precisos (ALCOA).

La integridad de los datos es fundamental durante todo el ciclo de vida de los datos, incluyendo la creación, modificación, procesamiento, mantenimiento, archivo, recuperación, transmisión y disposición de los datos una vez que finaliza el periodo de retención de los registros. El diseño y los controles del sistema deben permitir la fácil detección de errores, omisiones y resultados anómalos a lo largo del ciclo de vida de los datos[1].

Garantizar la integridad de los datos requiere sistemas de gestión de riesgo de calidad adecuados, incluida la adhesión a principios científicos sólidos y buenas prácticas de documentación[2].

Si bien el tema de integridad de datos es amplio y se puede abordar desde diferentes perspectivas, la finalidad de este texto es dar una visión general sobre la importancia de este en los laboratorios de análisis en la industria farmacéutica.

Los laboratorios de análisis en la industria farmacéutica, son responsables de generar una gran cantidad de datos, tanto físicos (papel), como digitales. Datos que hacen parte de toda la cadena de registros que aseguran la trazabilidad de un análisis desde que una muestra es ingresada al laboratorio hasta obtener el resultado final de la misma muestra.

Mantener estos registros de manera oportuna no es una tarea fácil, ya que los laboratorios de análisis en Colombia aún no cuentan con muchos procesos sistematizados, que adicional a otras características como la dinámica rutinaria de un laboratorio con ingreso de gran cantidad de muestras, laboratorios con variedad de análisis, con gran rotación del personal, con múltiples equipos que generan datos y con un proceso de registro generalmente manual, donde es común que se presenten circunstancias que puedan generar errores y pérdida de la información, que conlleva a repeticiones, desviaciones e invalidez de los resultados generados por el laboratorio. Razón por la cual, es justo en este punto del proceso, donde los sistemas de gestión y aseguramiento de la calidad, tienen un gran impacto y responsabilidad, a la hora de implementar estrategias que permitan mejorar los procesos del laboratorio y garantizar que la información sea confiable.

Como se mencionó anteriormente, el concepto de integridad de datos está compuesto por unos principios básicos, que implementados correctamente pueden mejorar estas problemáticas, de forma que el sistema documental y de calidad sea sólido, minimizando errores, retrasos y hallazgos en inspecciones internas y externas.

El anexo 5 de la guía de Orientación sobre buenas prácticas de gestión de datos y registros de la OMS, menciona los principios y estrategias que se deben implementar a nivel organizacional para fortalecer el sistema de gestión de calidad en cuanto al tema de integridad de datos.

A continuación, se mencionan algunas de las cuales a nivel de laboratorio son de implementación básica y necesaria.

En cuanto al recurso humano:

- El personal debe estar capacitado en políticas de integridad de datos y aceptar cumplirlas. Se debe asegurar que el personal esté capacitado para comprender y distinguir entre una conducta apropiada e inapropiada, incluida la falsificación deliberada, y debe ser consciente de las posibles consecuencias.

- El personal debe seguir buenas prácticas documentales tanto para los registros en papel como para los registros electrónicos a fin de garantizar la integridad de los datos. Estos principios requieren que la documentación tenga las características de ser atribuible, legible, registrada al mismo tiempo, original y precisa (ALCOA).

- Asignación de recursos humanos y técnicos adecuados para que la carga de trabajo, las horas de trabajo y las presiones sobre los responsables de la generación de datos y el mantenimiento de registros no aumenten los errores.

- Asegurarse de que el personal sea consciente de la importancia de su función para garantizar la integridad de los datos y la relación de estas actividades con la calidad del producto y la seguridad del paciente.

- Establecer y mantener un ambiente de trabajo que minimice el riesgo de registros no conformes, así como los registros y datos erróneos. Un elemento esencial de la cultura de calidad es la comunicación transparente y abierta de desviaciones, errores, omisiones y resultados aberrantes en todos los niveles de la organización.

En cuanto a metodología, equipos y sistemas:

- Las metodologías y los sistemas de mantenimiento de registros, ya sean en papel o digitales, deben diseñarse de manera que fomenten el cumplimiento de los principios de integridad de los datos.

- Restringir la capacidad de cambiar cualquier dato de fecha y hora, en equipos utilizados para registrar eventos cronometrados, ejemplo, relojes de sistema en sistemas electrónicos e instrumentación de procesos.

- Restringir los derechos de acceso de los usuarios a los sistemas automatizados para evitar modificaciones de datos.

- Asegurarse de que la captura de datos automatizada o las impresoras están conectadas y conectadas a equipos, como balanzas, para garantizar el registro independiente y oportuno de los datos.

Estos son solo algunos casos de todos los implicados en el aseguramiento de la integridad de datos en un laboratorio de análisis. Cabe resaltar que cada organización debe establecer, implementar y mantener un sistema de gestión de calidad adecuado y acorde a sus requerimientos, a las directrices y normativas vigentes.

Este sistema de gestión de calidad es quien debe establecer las políticas de integridad de datos que requiera el laboratorio y estas a su vez deben estar documentadas, actualizadas y divulgadas a todo el personal.

1 Planteamiento del problema

El concepto de integridad de datos surge como una necesidad de tener bajo control toda la información generada en el laboratorio, ya sean registros, datos analíticos, formatos, datos electrónicos o escritos, esto con el fin de que toda esta información esté protegida y sea real, que no haya ninguna adulteración, modificación accidental o intencional[3].

Para un laboratorio farmacéutico, la integridad de datos es un tema esencial, que se enfoca en asegurar la validez y confiabilidad de los resultados obtenidos en las pruebas y/o análisis realizados[4].

En los últimos años este tema se ha vuelto muy relevante para los laboratorios en Colombia, debido a las malas prácticas detectadas por los diferentes entes reguladores durante las auditorías realizadas a organizaciones del sector, es importante resaltar que hay un largo camino por recorrer con respecto a este tema y los laboratorios se enfrentan a grandes retos con el fin de desarrollar sistemas de calidad sólidos de tal forma que toda la información generada a partir de sus procesos productivos se encuentre disponible y segura[5].

Entre los principales desafíos a los que se deben enfrentar los laboratorios para mantener la seguridad de los datos se encuentran:

- La manipulación indebida, mal intencionada o no autorizada de los datos, esto puede llevar a reportar resultados erróneos, y que para el caso de un laboratorio productor y comercializador de medicamentos podría desencadenar en sacar al mercado un producto de mala calidad y que en última instancia supondría para la organización pérdida de la confiabilidad y pérdida de clientes.

- La trazabilidad de la información aparte de ser uno de los pilares más importantes para los laboratorios, es otro de los puntos que debe tener especial atención, ya que de esto depende que sea posible identificar si a lo largo del tiempo los datos han sido modificados o manipulados de alguna forma, además la trazabilidad es la que permite asegurar la confiabilidad de la información.

- Los laboratorios deben cumplir con muchas normativas y regulaciones que permiten su funcionamiento, así mismo la integridad de datos es uno de los requisitos fundamentales para asegurar frente a cualquier ente regulador, la validez de los resultados emitidos. A su vez el incumplimiento con estas normativas puede tener consecuencias legales y afectar el buen nombre del laboratorio.

La falta de las medidas de seguridad adecuadas para la información generada en el laboratorio o cualquier organización, puede exponer los datos a accesos no autorizados o manipulaciones malintencionadas que pueden comprometer su integridad y confidencialidad[5].

Es por esto, que es de suma importancia implementar medidas eficaces, que incluyan controles de calidad estrictos, sistemas de gestión sólidos y realizar procesos de auditorías constantes, que apunten a la disminución de los riesgos latentes a los que está expuesta, la información y así mitigar los posibles problemas derivados de estos y que pueden tener impactos negativos en la credibilidad del buen nombre del laboratorio, así como en la salud de pacientes y consumidores finales, para el caso de la industria farmacéutica y los laboratorios clínicos.

Si bien este es un tema muy conocido actualmente en el ámbito o contexto farmacéutico debido a las regulaciones a las que están sujetas organizaciones, aún no ha sido muy explorado en relación a la ciberseguridad o seguridad de la información, con el fin de proteger directamente a consumidores y pacientes.

Uno de los temas de gran relevancia para abordar la seguridad de la información en la producción de medicamentos es la farmacovigilancia.

La farmacovigilancia y la seguridad de la información son aspectos críticos en el ámbito de la salud y la industria farmacéutica, desempeñan un papel crucial en la detección, evaluación, comprensión y prevención de los efectos adversos de los medicamentos, es la encargada de identificar, evaluar y prevenir los efectos secundarios relacionados con el consumo de medicamentos, e identificar los factores de riesgo asociados a estos efectos[6]. Su importancia radica en diversos aspectos:

Detección de Efectos Adversos: Permite detectar los efectos adversos de los medicamentos tanto durante su fase de investigación y desarrollo como después de su comercialización. Esto es esencial para asegurar la seguridad de los pacientes.

Protección de la salud pública: La farmacovigilancia juega un papel fundamental en la protección de la salud pública al identificar y prevenir los efectos adversos de los medicamentos. La detección temprana de reacciones adversas permite tomar medidas rápidas para minimizar el riesgo para los pacientes y la comunidad en general.

Información para la Toma de Decisiones: La información que se obtiene a través de la farmacovigilancia es fundamental para tomar decisiones informadas sobre la seguridad y eficacia de los medicamentos, además contribuye a garantizar que los medicamentos se utilicen de manera segura y efectiva por parte de los pacientes.

Vigilancia a lo largo del Ciclo de Vida del Medicamento: La farmacovigilancia se aplica en todas las etapas del ciclo de vida del medicamento, desde su investigación y desarrollo hasta su

comercialización y uso posterior. Esto asegura una vigilancia continua y una evaluación constante de la seguridad de los medicamentos.

Cumplimiento normativo: La farmacovigilancia es un requisito regulatorio en muchos países para las empresas farmacéuticas. Garantizar la seguridad de la información relacionada con la farmacovigilancia es esencial para cumplir con las normativas de protección de datos y privacidad, así como con los requisitos de informes establecidos por las autoridades reguladoras.

Protección de datos sensibles: La información recopilada en el contexto de la farmacovigilancia puede incluir datos personales y médicos sensibles de los pacientes. Es fundamental proteger esta información contra accesos no autorizados, pérdidas o manipulaciones para garantizar la privacidad y confidencialidad de los individuos involucrados[7].

El sector farmacéutico presenta también deficiencias significativas en lo que refiere a la trazabilidad de la información, esto impacta altamente en la falsificación de medicamentos y la manipulación de la información, debido a dos factores como, información de los datos se encuentra incompleta, no hay controles suficientes en cuanto a la manipulación indebida de los datos[8].

Actualmente las organizaciones de todos los sectores sufren constantes ciberataques. Estos ataques no se deben solo a la seguridad informática de los sistemas que implementan las empresas, sino también en gran medida a la falta de capacitación a los empleados que son los principales focos de ataque, por el uso del correo electrónico, la forma de manejar la información dentro y fuera de las instituciones, la seguridad de los dispositivos utilizados, cuentas, contraseñas y usuarios compartidos con otros compañeros y cualquier otro factor que pueda poner en riesgo o vulnerabilidad el sistema. El uso de documentación física y/o manual, también es un factor que facilita ataques o manipulación indebida de la información.

Por lo anterior es imprescindible para las organizaciones farmacéuticas, buscar soluciones que faciliten el almacenamiento y seguimiento de la información durante toda la cadena de suministro del producto desde la obtención de las materias primas hasta cumplir con el ciclo logístico de la distribución de los productos al consumidor final.

Estas soluciones deben plantearse mediante un enfoque basado en la identificación de los riesgos a los que se ve expuesta la organización.

Según la Guía para la Implementación de Seguridad de la Información en una MIPYME, del Ministerio de Tecnologías de la Información y la Comunicación en Colombia, existen diferentes modalidades de ataque registradas en todo tipo de organización, entre los de mayor índice se encuentran:

Email Spoofing Financiero: Técnica de ingeniería social donde se crea un mensaje aparentemente verídico autorizando determinada acción en la nómina o contable.

Clasificación indebida de la información financiera: El atacante puede vulnerar el sistema informático, y debido a la ausencia de una clasificación de los datos el ciberdelincuente puede generar la capacidad para acceder al operador de las transacciones; en este sentido intentará acceder al ambiente informático y robar datos dentro del contexto transaccional.

Mensaje engañoso "Hoax" y Spam: Son aquellos que generalmente puede llegar a la bandeja de entrada desde una dirección electrónica desconocida; el mensaje fraudulento siempre indicará la acción inmediata para realizar una actividad, por otro lado, el "Spam" pretende enviar al usuario a publicidad engañosa o muchas veces re-direccionarlo a sitios web con contenido malicioso o dañino.

Robo de Información: Es la apropiación indebida de información confidencial por parte del ciberdelincuente.

Vishing: Actividad delincuencial de ingeniería social que se produce mediante una llamada telefónica a algún miembro de la empresa haciéndose pasar por un proveedor para tener acceso algún elemento confidencial o generar alguna actividad de pago frente alguna deuda.

Pishing: Suplantación de sitios web de manera fraudulenta para capturar datos financieros, privados, personales o confidenciales, para el apoderamiento de bases de datos financieras de la empresa.

Robo de identidad: Es una actividad delictiva asociada a la suplantación de clientes financieros de la empresa, empleando tarjetas de crédito o cupos de endeudamiento que permiten por parte de la empresa brindar fuga de información y hacer ataques de ingeniería social.

Malware Financiero: Programas diseñados con el fin de apoderarse de información confidencial y privada de la empresa u organización para que un tercero pueda realizar modificaciones en los sistemas informáticos y así generar fraudes de mayor cuantía[9].

Esta guía entonces ofrece información muy valiosa, sobre los tipos de amenazas y ataques a los que se ven enfrentadas las organizaciones y a su vez presenta unas directrices de cómo implementar herramientas o acciones útiles que permitan a las mismas organizaciones protegerse de ciberataques que conllevan a pérdidas económicas y de información crítica.

También hay que hablar de los deberes de la industria con la información de los clientes, salvaguardar la información y la confidencialidad, protección de datos personales, riesgos y sanciones que se pueden tener por no cuidar bien esa información[10].

Por otro lado, también se debe abordar la importancia que tiene el tratamiento y la protección de datos personales dentro de todo el tema de la integridad de datos, ya que las organizaciones tienen el deber de salvaguardar toda la información que reciben de clientes,

usuarios, proveedores y empleados y a su vez, el no cumplimiento de esta protección puede implicar sanciones y o riesgos para las empresas, frente a las regulaciones existentes.

Los datos personales, son un tipo de información que ha ido tomando gran relevancia e importancia de una manera progresiva en el ámbito social y económico[11].

Existen 3 principio básicos para que el tratamiento de los datos personales cuente con legalidad en todos los escenarios,

- Principio de información: mediante el cual la persona o entidad que suministra los datos tiene derecho de conocer qué manejo les dará a estos quien los esté requiriendo.

- Principio de finalidad del tratamiento: el uso de los datos obtenidos debe tener un propósito legal y claro.

- Principio de minimización de datos: este principio busca que los datos solicitados sean exclusivamente los requeridos para el fin previsto[12].

Con respecto al tratamiento de datos, organismos internacionales mencionan la importancia de contar con principios que complementen las normas existentes con el fin de tener una mejor garantía en dicha protección. La Asamblea General de las Naciones Unidas estableció por medio de una resolución algunos principios sobre tratamiento de datos personales, por otro lado, la Organización para la Cooperación y Desarrollo Económico (OCDE), ofreció algunas recomendaciones que mencionan también principios a tener en cuenta con el fin de salvaguardar la seguridad de los datos personales[12].

En Colombia la legislación sobre la protección de datos personales es una mezcla del artículo 15 de la Constitución de 1991 con más de setenta normas promulgadas desde 1951.

Entre las regulaciones principales se encuentran:

La Ley 1266 de 2008, reúne la mayoría de aspectos propios de la regulación de datos personales, como son, los principios que incluyen el tratamiento de esa información; las obligaciones de los operadores y sus administradores; los derechos de los titulares de los datos; las pautas de circulación nacional de la información personal; las reglas sobre la transferencia internacional de datos y las autoridades de control[11].

Y la Ley 1581 de 2012 donde se regula el salvaguardar los datos desde su recolección hasta su transmisión, exigiendo así que el tratamiento de la información recibida cumpla con los parámetros necesarios para garantizar la protección integral de los mismos[12].

Para el caso de los laboratorios, la norma ISO 17025 en el apartado 4 sobre requisitos generales, menciona los deberes que tiene el laboratorio en cuanto a la imparcialidad y la confidencialidad de los datos[13].

2 Justificación

La seguridad de la información en los laboratorios farmacéuticos es de suma importancia debido a la naturaleza sensible y crítica de los datos que se manejan en estos entornos. En la era digital, donde la mayoría de la documentación se encuentra en formato electrónico, la necesidad de proteger estos datos se vuelve aún más crucial. La seguridad de la información se fundamenta en la protección de la confidencialidad, integridad y disponibilidad de los datos frente a diversas amenazas, tanto internas como externas[14].

La confidencialidad asegura que solo las personas autorizadas puedan acceder a la información relevante, evitando así la divulgación no autorizada. Por su parte, la integridad garantiza que los datos no sean alterados, manteniendo su precisión y fiabilidad. Finalmente, la disponibilidad asegura que la información esté accesible cuando sea necesario, evitando interrupciones no deseadas en los servicios y operaciones[15].

La importancia de la seguridad de la información en los laboratorios farmacéuticos se refleja en las severas consecuencias que pueden derivarse de las violaciones de seguridad. Estas pueden incluir la pérdida de clientes, multas regulatorias y daños a la reputación de la organización[16]. En un entorno empresarial cada vez más regulado, el cumplimiento de estándares y regulaciones de seguridad es fundamental para evitar sanciones legales y financieras.

Además, la seguridad de la información fomenta la innovación y el desarrollo tecnológico al proteger la propiedad intelectual y los activos digitales de una organización[17]. Esto promueve un entorno de negocio seguro y confiable, estimulando la inversión y el crecimiento económico.

En el ámbito de la salud, la seguridad de la información en los laboratorios farmacéuticos es vital para cumplir con las regulaciones y estándares de la industria. También contribuye a mantener la confianza de los clientes y consumidores al garantizar la integridad y reproducibilidad de los resultados[18].

En resumen, asegurar la información en los laboratorios farmacéuticos es fundamental para preservar la privacidad de los pacientes, mantener la integridad de los datos y salvaguardar los activos de la organización. Además, contribuye a cumplir con las regulaciones de la industria, promueve la confianza del cliente y estimula la innovación y el crecimiento económico.

3 Objetivos

3.1 Objetivo general

Analizar la importancia de la integridad de datos y la seguridad de la información en la industria farmacéutica.

3.2 Objetivos específicos

- Presentar las principales problemáticas que se presentan en la industria farmacéutica con respecto a la generación, manejo y seguridad de la información.

- Identificar las principales regulaciones, guías y requisitos a nivel mundial y nacional para la implementación de un sistema de integridad de la información y manejo de datos en la industria farmacéutica.

- Evaluar el estado actual de las organizaciones de tipo farmacéutico frente a la implementación de estrategias y controles para el aseguramiento y gestión de la información.

4 Marco teórico

Los conceptos fundamentales de la integridad de datos se vienen implementando desde la aparición de los primeros sistemas de almacenamiento de la información, como documentos en papel y las primeras bases de datos electrónicas. La integridad de datos o seguridad de la información surgen de la necesidad de asegurar que dicha información que era almacenada fuera precisa y confiable.

En 1970, se introducen las primeras técnicas de control de la integridad en sistemas de gestión. Con el advenimiento de las bases de datos relacionales, surgió uno de los principales enfoques sobre la integridad de datos, Edgar F Codd, conocido por ser el creador modelo relacional de las bases de datos, en su trabajo "*A Relational Model of Data for Large Shared Data Banks*" (1970), sentó las bases teóricas para la gestión de datos, en este trabajo abordo principalmente el tema del manejo y categorización de los bancos de datos, enfocándose en la protección de los usuarios y los datos almacenados, cuando el sistema sufre alguna modificación o fallo[19].

Para la década de los 90, con el crecimiento del internet y los sistemas de almacenamiento, la integridad de datos se convirtió en un tema aún más relevante en las organizaciones a nivel mundial dándole un enfoque de seguridad y prevención de la corrupción de datos. Se comenzaron a desarrollar técnicas avanzadas para mejorar y corregir las inconsistencias presentadas en las bases de datos y sistemas tradicionales que se venían implementando, esto con el fin de que las bases de datos fueran consistentes, y se pudieran corregir errores en los programas, que generarán datos inconsistentes por fallas de software o hardware, principalmente porque ya se comenzaban a implementar sistemas multiusuario, donde ejecutan diferentes operaciones al mismo tiempo.

Es por esto que para esta década se comenzaron a implementar mecanismos de control de concurrencia que garantizaran que los datos mantuvieran su coherencia a pesar de accesos simultáneos de diferentes usuarios[20].

Ya para el siglo XXI se intensifica la preocupación por la integridad de datos, el surgimiento de tecnologías como el almacenamiento en la nube y el análisis de big data han planteado nuevos desafíos en términos de garantizar la integridad de los datos en entornos altamente dinámicos y escalables.

Al mismo tiempo aparecen las regulaciones como el GDPR (Reglamento General de Protección de Datos) de la Unión Europea, lo que convierte la integridad de datos en un tema central[21].

Es posible darnos cuenta, que la integridad de datos y la seguridad de la información se han convertido en un tema de alta criticidad para las organizaciones de todo tipo a nivel mundial, cada vez las regulaciones se vuelven más estrictas y proteger la información tanto de clientes, pacientes

y consumidores, como de la organización, es pilar fundamental en todos los sistemas de información.

A grandes rasgos esta ha sido la evolución de la integridad de datos y como ha sido abordada a nivel mundial frente a los diferentes sistemas de información.

Sin embargo, para este trabajo el tema principal que nos compete es la integridad de datos en la industria farmacéutica. La industria farmacéutica, desde sus inicios, ha estado sujeta a todo tipo de regulaciones para garantizar la calidad, seguridad y eficacia de sus productos y/o procesos. En la actualidad, la integridad de datos se ha convertido en un aspecto crucial dentro de las regulaciones vigentes.

Durante las décadas de 1960 y 1970, se establecieron las primeras regulaciones de BPM en varios países, incluidos Estados Unidos y países europeos. Estas regulaciones incluían requisitos específicos para garantizar la integridad de datos en los registros de fabricación, como la documentación completa y precisa de los procedimientos de fabricación, las pruebas de calidad y los resultados analíticos.

Para estas mismas fechas se desarrollaron las primeras regulaciones de BPL para abordar preocupaciones sobre la calidad y la fiabilidad de los datos generados en estudios preclínicos y análisis de laboratorio. Estas regulaciones establecen requisitos específicos para la documentación adecuada de procedimientos de laboratorio, el mantenimiento de registros precisos y la validación de métodos analíticos.

Estas regulaciones marcaron un hito importante en el desarrollo de estándares de calidad y seguridad en la industria farmacéutica, y sentaron las bases para futuras regulaciones centradas en la integridad de datos[22].

Con el auge de las nuevas tecnologías, la informática se convirtió en una herramienta indispensable en la industria farmacéutica, lo que llevó al desarrollo y la implementación generalizada de sistemas computarizados para una amplia gama de aplicaciones, incluidos los sistemas de gestión de la calidad (QMS), sistemas diseñados para gestionar y controlar los procesos de calidad en una organización farmacéutica que abarcan una amplia gama de funciones, como la gestión de documentos, la gestión de cambios, el control de registros, las investigaciones de desviaciones y la gestión de riesgos y los sistemas de gestión de laboratorio (LIMS), diseñados para gestionar y automatizar los procesos de laboratorio, incluida la gestión de muestras, la planificación de ensayos, la recolección y análisis de datos, y la generación de informes y que son fundamentales para mejorar la eficiencia, la precisión y la integridad de los datos en entornos de laboratorio. Sin embargo, esta adopción de tecnologías informáticas también presentó nuevos desafíos relacionados con la integridad de datos[23].

Con la implementación de sistemas QMS y LIMS en la década de 1980, surgió la necesidad de garantizar la integridad de los datos generados y gestionados por estos sistemas. Esto incluye asegurar la precisión, confiabilidad, rastreabilidad y seguridad de los datos almacenados en el sistema, así como garantizar que los procesos de gestión de la calidad sean consistentes y cumplan con los requisitos regulatorios. Garantizar también la trazabilidad de las muestras y los resultados, mantener registros precisos y proteger la integridad de los datos frente a la adulteración o la pérdida[23].

Para los años 1990 a 2000, la FDA y la Agencia Europea de Medicamentos (EMA) emitieron varias directrices y regulaciones específicas relacionadas con la integridad de datos en la industria farmacéutica. Estas regulaciones se centraron en garantizar la calidad, fiabilidad y seguridad de los datos generados durante todas las etapas del ciclo de vida de los productos farmacéuticos.

La FDA emitió la Guía de Validación de Sistemas Computarizados en 1983, actualizándose posteriormente en 2003 para reflejar los avances tecnológicos y las mejores prácticas emergentes. Esta guía proporciona directrices detalladas sobre la validación de sistemas informáticos utilizados en actividades reguladas por la FDA, como la fabricación, el control de calidad y la gestión de registros[24].

La guía de la FDA aborda varios aspectos clave de la validación de sistemas computarizados, incluidos:

- Requisitos de documentación.
- Verificación del software.
- Gestión de cambios.
- Seguridad de datos y acceso autorizado.
- Mantenimiento del sistema.

La EMA a su vez, también emitió varias directrices relacionadas con la integridad de datos en el contexto de las Buenas Prácticas de Manufactura (BPM). Estas directrices establecen los estándares y requisitos que deben cumplir los fabricantes de productos farmacéuticos para garantizar la calidad y la integridad de los datos generados durante la fabricación, el envasado y el etiquetado de productos farmacéuticos[25].

Algunos temas abordados por las directrices de BPM de la EMA incluyen:

- Gestión de registros.
- Validación de sistemas informáticos.
- Protección contra la adulteración de datos.
- Cumplimiento de los requisitos regulatorios.

En la actualidad, la atención hacia la seguridad de los datos en toda la cadena de suministro farmacéutica ha aumentado significativamente debido a varios factores, como la globalización de la industria farmacéutica, el aumento de la complejidad de los productos y la aparición de nuevas amenazas cibernéticas. Garantizar la integridad y seguridad de los datos en todas las etapas de la cadena de suministro es crucial para proteger la calidad y la eficacia de los productos farmacéuticos, así como para cumplir con los requisitos regulatorios

En cuanto a la cadena de suministro global, la seguridad de los datos se ha convertido en un área de enfoque crítico. Esto implica garantizar la integridad y seguridad de los datos en todas las etapas de la cadena de suministro, desde la fabricación hasta la distribución, a través de la implementación de estándares y prácticas robustas de gestión de datos y seguridad cibernética.

La seguridad de los datos en la fabricación farmacéutica implica garantizar la integridad de los datos generados durante los procesos de fabricación, envasado y etiquetado de productos. Esto incluye la implementación de controles de acceso, medidas de seguridad física y lógica, así como la validación de sistemas informáticos y la gestión adecuada de los registros electrónicos[26].

La seguridad de los datos en la distribución farmacéutica se refiere a garantizar la integridad de los datos relacionados con el almacenamiento, transporte y entrega de productos a lo largo de la cadena de suministro. Esto implica la implementación de medidas de seguridad física, seguimiento y rastreo de productos, así como la validación de sistemas de gestión de inventario y logística[27].

5 Metodología

Este trabajo aborda el tema de la integridad de datos, haciendo una revisión de la situación actual de las organizaciones, especialmente aquellas de tipo farmacéutico.

Se realizó una investigación cualitativa, teórica, documental y descriptiva haciendo un recorrido histórico sobre la integridad y seguridad de la información y abordando diferentes problemáticas y las estrategias propuestas a nivel normativo e implementadas con el fin de amortiguar los impactos que generan dichas problemáticas.

El método utilizado fue la revisión documental, partiendo de la búsqueda en bases como Science Direct, google scholar, DOAJ, PubMed e ICONTEC. La combinación de búsqueda estuvo compuesta por los términos "*Information security", "Information laboratory security", "Farmacovigilancia", "Seguridad de la información", "ciberseguridad", "Integridad de datos", "Data integrity", "Industria farmacéutica", "Laboratorios farmacéuticos*".

Se seleccionaron aquellos textos considerados pertinentes para el desarrollo de la temática y que aportaran argumentos sólidos. No se tuvo como criterio de aceptación el año de publicación; sin embargo, se aplicaron como criterios de inclusión artículos de investigación sobre el tema de interés, normativas vigentes y algunas páginas web.

6 Resultados

Asegurar la integridad de la información es una de las tareas más complejas de cualquier organización y al mismo tiempo, es uno de los aspectos más vulnerables, puesto que es común que, con el afán de implementar procesos automatizados para agilizar y optimizar la recolección de datos, muchas veces no se establecen los parámetros o controles necesarios para verificar que la información es almacenada correctamente y que esta es precisa y confiable[28].

El campo de la integridad de datos, se convierte en el centro de atención, debido a que se encuentra en constante riesgo de presentar problemas de confusión, comunicación o desconocimiento por parte de aquellos involucrados directamente en el proceso de manejar, generar y almacenar información[28].

En la actualidad, la información se ha convertido en un activo muy valioso en todas las industrias y es necesario protegerla, sin embargo, en muchos casos es difícil saber cómo hacerlo, debido a que son muchos los factores que la ponen en riesgo.

Entre las principales problemáticas se incluyen, la manipulación no autorizada de los datos, violaciones de privacidad, robo de información confidencial y ataques cibernéticos[9].

Los ataques informáticos consisten en la modificación intencional de los datos, sin autorización alguna, en algún momento de su ciclo de vida, el cual comprende las siguientes etapas[28]:

- Introducción, creación o adquisición de datos.
- Procesamiento o derivación de datos.
- Almacenamiento, replicación y distribución de datos.
- Archivado y recuperación de datos.
- Realización de copias de respaldo y restablecimiento de datos.
- Borrado, eliminación y destrucción de datos.

Para la industria farmacéutica, la implementación de sistemas de integridad de datos nace debido a diversas violaciones de la información, que fueron observadas por la FDA durante las inspecciones realizadas a laboratorios y organizaciones fabricantes de medicamentos y por la necesidad de tener el control de todos los registros, ya sean electrónicos, en papel o híbridos, generados en ellos. El concepto de integridad de datos, se conoce como la certeza de que los datos registrados son exactos, completos, intactos y mantenidos dentro de su contexto original (ALCOA), incluyendo la relación con otros datos registrados. Asegurar la integridad, significa proteger los datos originales de modificaciones accidentales o intencionales, falsificaciones y eliminaciones[29].

Por tal motivo, en marzo de 1997, la FDA emitió las regulaciones sobre registros electrónicos, las cuales aplican a todas aquellas áreas que se acogen a la FDA y que tienen como

objetivo permitir el uso más amplio posible de la tecnología electrónica, compatible con la responsabilidad que tiene la FDA de proteger la salud pública[30].

El aseguramiento de la información cumple entonces un papel primordial dentro de las buenas prácticas de manufactura de medicamentos, y todos sus atributos deben mantenerse durante el ciclo de vida de los datos, desde su creación hasta el final de su período de retención[31].

En este sentido, es importante que las organizaciones cuenten con sistemas de documentales robustos, donde se establezcan, controlen, monitoreen y registren todas las actividades que de una u otra forma impactan sobre la calidad del producto. El sistema documental debe mantener la trazabilidad para demostrar que el proceso cumple con la aplicación de buenas prácticas y que además cuenta con los controles necesarios para garantizar la integridad y disponibilidad de la información que dicho proceso genera[31].

Por otro lado, el proceso de elaboración de productos farmacéuticos se debe ejecutar siguiendo normas que rigen dicha fabricación y que permiten asegurar la calidad, seguridad y eficacia del producto final[29].

Al mismo tiempo, quienes fabrican medicamentos, deben implementar y mantener sistemas de gestión de calidad acordes a los requisitos vigentes de normas como las ISO, igualmente como parte integral del sistema se deben incluir los requisitos de la regulación sobre BPM de productos farmacéuticos. Dentro de los referentes internacionales más importantes se encuentran la Food and Drug Administration (FDA) que es la agencia reguladora de Estados Unidos, la Agencia Europea de Medicamentos (EMA) para los países de la Unión Europea y por supuesto, la Organización Mundial de la Salud (OMS)[32].

Estos organismos, sus reglamentaciones y directrices establecen los estándares y requisitos que se deben cumplir para garantizar la protección e integridad de los datos en la industria farmacéutica.

Tanto la parte 11 del título 21 del CFR, como el anexo 11 de GMP de la Unión Europea y la OMS mencionan los diferentes controles que pueden utilizarse en el momento de crear y almacenar datos electrónicos.

La parte 11 (FDA) establece principios donde se considera que los registros, firmas electrónicas y firmas manuscritas son confiables y equivalentes a los registros en papel, mientras que el anexo 11 y os informes técnicos de la OMS aborda los principios del uso de sistemas computarizados para cumplir con los requisitos de las BPM y los procesos de validación[32].

La *Guía PIC's sobre Integridad de Datos* proporciona una orientación para la inspección e interpretación de los requisitos de GMP en la práctica documental y en la integridad de datos para la buena gestión[33].

A su vez, el reporte Técnico N° 84 de la *PDA: requisitos de integridad de datos en las operaciones de fabricación y embalaje*, detalla los parámetros para definir un análisis de riesgo basado en el riesgo humano y sus posibles fallas para garantizar la integridad de datos en un laboratorio[34].

Otra regulación importante de mencionar con respectos este tema es la ISO/IEC 27001 la cual establece los requisitos para implementar y mejorar un sistema de gestión de seguridad informática, con el objetivo de proteger la información y teniendo en cuenta los diferentes incidentes que puedan presentarse[18].

Para el caso de Colombia, la Resolución 3619:2013 del Ministerio de Salud y Protección Social, en el numeral 4 (Registros) menciona la información que deben contener los registros físicos, el mantenimiento y almacenamiento de los mismos. Igualmente incluye los atributos (ALCOA) para los datos generados en los laboratorios y organizaciones farmacéuticas[35].

En el numeral 5 (Equipos procesadores de datos) de esta misma Resolución, se habla de la integridad en los registros electrónicos y la validación de sistemas computarizados.[35]

Como se ha mencionado anteriormente, con la llegada de la era digital y la implementación de nuevas tecnologías en la industria farmacéutica, la integridad de datos, está asociada al cumplimiento de los requisitos del ALCOA, recientemente llamado ALCOA+; es decir que los datos deben ser Atribuibles, Legibles, Contemporáneos, Originales y Precisos.[32]

Para proteger su información, las organizaciones implementan diferentes estrategias y herramientas que deben estar ligadas al sistema de gestión y encaminadas al cumplimiento de las Buenas Prácticas Documentales y de las normativas internacionales.

La alta Gerencia tiene la responsabilidad de apoyar los temas relativos a la seguridad interna de la organización:

- Definir roles y responsabilidades
- Crear una política de seguridad de la información que dicte las directrices para resguardar los activos de la información.
- Capacitar constantemente a los empleados sobre la política de la información de la organización y sensibilizarlos sobre las amenazas informáticas a las que se encuentran expuestos[9].

Entre muchas otras estrategias para la protección de datos, se encuentran:

- Implementar nombres de usuarios y contraseñas únicas para cada persona.
- Definir niveles de acceso de los sistemas informáticos
- Proteger registros para evitar modificaciones o eliminación
- Respaldar los datos mediante audit trail, para registrar actividades, mantenimiento y uso del sistema.

- Contar con backup que permita exportar datos con cierta frecuencia.
- Validación de software y hojas de cálculo.

A nivel de Colombia, una de las estrategias que han implementado diferentes organizaciones como una forma de proteger su información y contrarrestar los riesgos latentes, es la implementación y certificación en la norma ISO 27001[18].

De igual forma, las organizaciones farmacéuticas y los laboratorios, al obtener certificaciones tipo BPM y BPL, están cumpliendo con los requisitos exigidos por las normas y a su vez preservar la integridad de los datos.

7 Discusión y Conclusiones

Según lo consultado en esta investigación, se puede concluir que las principales problemáticas de la integridad de datos en las organizaciones, son aquellas relacionadas con la ausencia de mecanismos de control adecuados para el manejo de la información.

La alta dirección es responsable de implementar una política de manejo de la información, acorde con sus necesidades y que les permita una mayor confiabilidad y satisfacción a sus clientes.

Para las organizaciones farmacéuticas es importante la implementación de normas, al tiempo que se establecen planes y controles que contribuyan a minimizar los riesgos de posibles ciberataques y manipulación indebida de la información.

Colombia se encuentra en el proceso de adopción de estándares internacionales para garantizar una adecuada protección de la información, sin embargo, aún queda un largo camino por recorrer para que los fabricantes de medicamentos tengan la total certeza de que su información se encuentra segura y de que sus sistemas no serán vulnerados de ninguna forma. Aun así, es importante resaltar los esfuerzos realizados respecto al tema y la cantidad de herramientas y trabajos aplicados actualmente para el fortalecimiento de estos sistemas.

8 Recomendaciones

Se recomienda implementar normas como la ISO 27001, puesto que permite a las empresas implementar controles que brindan seguridad y confianza en la prestación de sus servicios.

Se debe trabajar en mejorar los sistemas de gestión, hacerlos más robustos e inviolentables y evaluar desde cada organización los riesgos informáticos a los que está expuesta y la manera en que estos impactan su modelo de negocios.

Es necesario analizar con mayor detenimiento la situación actual de las farmacéuticas en Colombia y los trabajos que se están desarrollando en este campo.

Referencias

1. OMS, (2016). Guidance on good data and record management practices, anexx 5.

2. FFDA, (2018). Data Integrity and Compliance With Drug CGMP Questions and Answers Guidance for Industry.

3. Naeem, T. (25 de Marzo 2024). ¿ Qué es la integridad de datos en una base de datos?¿ Por qué lo necesitas?. Astera. Integridad de datos en una base de datos: ¿por qué es importante? Astera

4. PARF, R. (2010). Buenas Prácticas de la OMS para laboratorios de control de calidad de productos farmacéuticos. *Red Panamericana de Armonización de la Reglamentación Farmacéutica. Obtenido de http://www. paho. org/hq/dmdocuments/2011/Espanol-control-calidadlaboratorios-farmaceuticos. pdf*.

5. Costa, E. M., & Barea, M. M. (2003). La industria farmacéutica y la farmacovigilancia. *Offarm: farmacia y sociedad*, *22*(6), 134-138.

6. Escobar de Cornejo, A. M. (2023). *Procedimiento Estándar de Operación referente de farmacovigilancia: funciones, responsabilidades y actividades en una farmacia de primera categoría* (Doctoral dissertation, Universidad de El Salvador).

7. World Health Organization. (2002). The importance of pharmacovigilance.

8. Tian, H., & Li, Y. (2021, June). Pharmaceutical anti-counterfeiting traceability system based on block chain double chain. In *2021 International Conference on Computer Engineering and Application (ICCEA)* (pp. 45-49). IEEE.

9. MINTIC. (06 de Noviembre 2016). *Guía para la Implementación de Seguridad de la Información en una MIPYME*. articles-5482_Guia_Seguridad_informacion_Mypimes.pdf (mintic.gov.co)

10. Argüelles, K. (Abril 14,2022). *PROTECCIÓN DE DATOS PERSONALES EN COLOMBIA: RIESGOS Y SANCIONES*. Diálogos Punitivos. Protección de datos personales en Colombia: riesgos y sanciones - Diálogos Punitivos (dialogospunitivos.com)
11. Remolina-Angarita, N. (2010). *¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo?*, 16 *International Law, Revista Colombiana de Derecho Internacional*, 489-524.
12. Ayala Fandiño, J. E., Ariza Herrera, J., & González De La Zerda, L. E. (2020). La protección de datos en la era digital: Colombia-España.

13. ICONTEC. (2017). Requisitos Generales para la Cpmpetencia de los Laboratorios de Ensayo y Calibración. ISO/IEC 17025:2017.

14. Whitman, M. E., & Mattord, H. J. (2016). Threats to information protection-industry and academic perspectives: an annotated bibliography. *Journal of Cybersecurity Education, Research and Practice*, *2016*(2), 4.
15. Excellence, I. (2018). Los tres pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad. *Recuperado de https://www. pmg-ssi. com/2018/02/confidencialidad-integridad-y-disponibilidad*.

16. Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: towards socio-organizational perspectives. *Information systems journal*, *11*(2), 127-153.

17. Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of information systems*, *18*, 106-125.

18. Alvarez Isaza, Z. M. (2016). *ISO/IEC 2700: 2013-sistemas de gestión de seguridad de la información* (Bachelor's thesis, Universidad Piloto de Colombia).

19. Codd, E. F. (1970). A relational model of data for large shared data banks. *Communications of the ACM*, *13*(6), 377-387.

20. Bernstein, P. A., Hadzilacos, V., & Goodman, N. (1987). *Concurrency control and recovery in database systems* (Vol. 370). Reading: Addison-wesley.

21. Abadi, D. J., Madden, S. R., & Hachem, N. (2008, June). Column-stores vs. row-stores: how different are they really?. In *Proceedings of the 2008 ACM SIGMOD international conference on Management of data* (pp. 967-980).

22. Organisation for Economic Co-operation and Development. OECD Principles of good laboratory practice. The application of the GLP principles to field studies. Paris: OECD; 1998. (OECD Series on principles of good laboratory practice and compliance monitoring, no. 6, ENV/MC/CHEM(92)50).

23. Vloeberghs, D., & Bellens, J. (1996). Implementing the ISO 9000 standards in Belgium. *Quality progress*, *29*(6), 43.

24. FDA. (Mayo, 2007). *Guidance for Industry Computerized Systems Used in Clinical Investigations.*

25. Gouveia, B. G., Rijo, P., Gonçalo, T. S., & Reis, C. P. (2015). Good manufacturing practices for medicinal products for human use. *Journal of Pharmacy and Bioallied Sciences*, *7*(2), 87-96.

26. Charoo, N. A., Khan, M. A., & Rahman, Z. (2023). Data integrity issues in pharmaceutical industry: Common observations, challenges and mitigations strategies. *International Journal of Pharmaceutics*, *631*, 122503.

27. Pharma source. Pharma Supply Chain: A comprehensive guide to the pharmaceutical supply chain**. Pharma Supply Chain: A comprehensive guide to the pharmaceutical supply chain - PharmaSource**

28. Gallardo-Bernal, I. (2015). Ataques Informáticos Basados en la Integridad de la Información. *Revista Salud y Administración*, *2*(5), 43-50.

29. Lombardic, M. P. N. P. (2019). *Implementación del Sistema de Integridad de Datos, para Datos Electrónicos, en el Laboratorio Farmacéutico Synthon Chile* (Doctoral dissertation, Pontificia Universidad Catolica de Chile (Chile)).

30. . "Part 11, Electronic Records; Electronic Signatures – Scope and Application" (Parte 11, registros electrónicos; firmas electrónicas; alcance y aplicación) https://www.fda.gov/regulatory-information/search-fda-guidance-documents/part-11-electronic-records-electronic-signatures-scope-and-application.

31. Villagrán Muñoz, R. (2020). Integridad de datos y su cumplimiento en equipos productivos.

32. Corbillón, L. M., Texidor, R. F., & Seino, D. G. (2019). Los sistemas computarizados: la industria farmacéutica y sus regulaciones. *Revista Cubana de Ingeniería*, *10*(3), 27-33.

33. PIC/S. (2018). *GOOD PRACTICES FOR DATA MANAGEMENT AND INTEGRITY IN REGULATED GMP/GDP ENVIRONMENTS. https://picscheme.org/users_uploads/news_news_documents/PI_041_1_Draft_3_Guidance_on_Data_Integrity.pdf*

34. PDA. (2020). *Technical Report No. 84 (TR 84) Integrating Data Integrity Requirements into Manufacturing & Packaging Operations. https://www.pda.org/bookstore/product-detail/5801-tr-84-data-integrity*

35. Ministerio de Salud y Protección Social. (2013). *Manual de Buenas Prácticas de Laboratorio de Control de Calidad de Productos Farmacéuticos*. Resolución 3619:201. https://www.minsalud.gov.co/Normatividad_Nuevo/Resoluci%C3%B3n%203619%20de%202013.pdf