

LA IMPORTANCIA DEL GOBIERNO DE LA INFORMACIÓN Y LA CALIDAD DE LOS  
DATOS PARA LA TOMA DE DECISIONES Y EL ESTABLECIMIENTO DE CONTROLES  
EN UNA ORGANIZACIÓN.



JULIANA ALEJANDRA GAMEZ LARA

CÓDIGO: 2501144

UNIVERSIDAD MILITAR NUEVA GRANADA

FACULTAD DE CIENCIAS ECONÓMICAS

DIRECCIÓN DE POSGRADOS

ESPECIALIZACIÓN DE CONTROL INTERNO

BOGOTÁ

2020

## **RESUMEN**

El presente ensayo tiene como finalidad exponer la importancia de la calidad de los datos y el gobierno de la información en las organizaciones. Comienza por plantear diferentes preguntas que deberían ser priorizadas y respondidas de forma sincera, esto con el objetivo de realizar una autoevaluación y conocer el estado en el que se encuentra.

También, se comparten algunos casos de la vida real, a modo de ejemplo con el propósito de mostrar las consecuencias del mal manejo de la información y la baja calidad de los datos en algunas áreas de la organización (Hospital XYZ). Además, se detallan los atributos que debe tener la calidad de los datos y el gobierno de la información para funcionar como un sistema de información maduro.

Finalmente se propone una metodología enmarcada en los modelos de mejora continua seis sigma (DMAIC) y ciclo de Deming (PHVA) para la implementación de un sistema de gestión de la seguridad de la información (ISO/IEC 27001:2013) y se argumenta como este sistema logra garantizar cierto nivel de confianza al sistema de control interno, en cuanto a la toma de decisiones y el establecimiento de controles por parte de la primera y segunda línea de defensa.

## **PALABRAS CLAVE**

Información, calidad, datos, gobierno, sistema, metodología, riesgo, autoevaluación, mejora.

## **ABSTRACT**

The purpose of this essay is to present the importance of data quality and information governance in organizations. It begins by posing different questions that should be prioritized

and answered honestly, with the aim of conducting a self-assessment and knowing the current conditions.

As we go deeper into the subject, some real-life cases are shared with the purpose of showing the consequences of mishandling information, and the low quality of data in some areas of the organization (XYZ Hospital). In addition, the attributes that data quality and information governance must have to function as a mature information system are detailed.

Finally, a methodology framed in the six sigma (DMAIC) and Deming cycle (PHVA) continuous improvement models is proposed for the implementation of an information security management system (ISO / IEC 27001: 2013) that manages to guarantee a certain level of confidence in the internal control system, in terms of decision-making and the establishment of controls by the first and second lines of defense.

## **KEYWORDS**

Information, quality, data, governance, system, methodology, risk, self-assessment, improvement.

## INTRODUCCION

*“Si miras cualquier tipo de organización moderna y piensas ‘¿Cuál es el instrumento de poder más potente?’, verás que es la información”. Ricardo Semler*

En la actualidad existen varias metodologías implementadas por las organizaciones, con el fin de mitigar riesgos y tomar decisiones que permitan el cumplimiento de los objetivos estratégicos de las mismas. Una de las metodologías más importantes es la calidad de datos y el gobierno de información, debido a que se puede visualizar la organización de una forma transversal y completa. Adicionalmente, el análisis continuo de los resultados posibilita el establecimiento de controles preventivos y eficaces que facilitan la sinergia entre las diferentes áreas de la organización.

La normatividad colombiana vigente, se limita únicamente a establecer marcos referentes a la seguridad de la información. Debido a este bajo nivel de exigencia, muchas organizaciones dejan de lado la calidad de los datos y el gobierno de la información como eje fundamental de sostenibilidad y mejora continua.

Por lo tanto, la alta dirección de las organizaciones debe definir y gestionar estrategias que conlleven a buenas prácticas basadas en marcos normativos internacionales. Dichas estrategias deben involucrar a cada uno de los stakeholders, con el fin de generar una cultura organizacional en el mediano y largo plazo. Contando con el compromiso de los stakeholders como premisa de efectividad, se expone a continuación la propuesta de una metodología de mejora continua aplicable a todo tipo de organización.

**TABLA DE CONTENIDO**

RESUMEN .....	II
PALABRAS CLAVE .....	II
ABSTRACT.....	II
KEYWORDS .....	III
INTRODUCCIÓN .....	IV
PREGUNTA PROBLEMA .....	3
OBJETIVO GÉNERAL.....	4
OBJETIVOS ESPECÍFICOS .....	4
MARCO TEÓRICO.....	4
DESARROLLO DEL TEMA.....	5
CONCLUSIONES .....	21
BIBLIOGRAFÍA .....	21

## **LISTA DE ILUSTRACIONES**

Ilustración 1: Atributos de la calidad de los datos .....	11
Ilustración 2: Atributos del gobierno de información.....	12
Ilustración 3: Metodología Seis Sigma (DMAIC) para implementar y mejorar continuamente la calidad de los datos y el gobierno de la información.....	15

## **LISTA DE TABLAS**

Tabla 1: Propuesta de autoevaluación calidad de datos y gobierno de información. ....	14
Tabla 2: Propuesta metodología combinada ciclo Deming (PHVA) y seis sigma (DMAIC). ....	17

## **PREGUNTA PROBLEMA**

¿Cuál es la importancia del gobierno de la información y la calidad de los datos para la toma de decisiones y el establecimiento de controles en una organización?

## **JUSTIFICACIÓN**

En la actualidad las organizaciones tienen como reto ejercer gobierno sobre la información y estabilizar los datos de acuerdo con los requisitos de calidad, esto con el fin de que funcionen como recursos e insumos para tener en cuenta a la hora de tomar decisiones de forma adecuada y oportuna en las diferentes áreas y sistemas de la organización, tales como:

A) El área financiera con respecto a inversiones, ejercicios de análisis de rentabilidad y análisis de costos.

B) El área comercial para llevar a cabo un enfoque de fuerza de venta y el establecimiento de precios de venta (BI)

C) El área de riesgos con el fin de mapear y dimensionar los riesgos más críticos y su debida gestión en una organización.

D) El área operativa con respecto a la supervisión de activos fijos, temas de obsolescencia de equipos y mantenimientos preventivos y correctivos

E) Fortalecer el Sistema de Control interno de una organización, de tal forma que permita tomar decisiones y establecer controles de forma preventiva con información idónea y correctamente documentada.

También, se propone una metodología de autoevaluación, definición, medición, análisis, mejora y control dentro del ciclo PHVA y el (DMAIC) de seis sigma para la implementación de un

sistema de gestión de la seguridad de la información (ISO/IEC 27001:2013), el cual da cobertura a algunos de los atributos de la calidad de los datos y el gobierno de la información.

## **OBJETIVO GENERAL**

Dar a conocer la importancia de los activos informacionales de una organización para la toma de decisiones, el establecimiento de controles preventivos y proponer metodologías de implementación que involucren la mejora continua.

## **OBJETIVOS ESPECÍFICOS**

a) Detallar la importancia y los atributos del gobierno de la información y la calidad de los datos.

d) Compartir prácticas que se puedan implementar en una organización respecto a la realización de una autoevaluación del estado de la organización, modelos de mejora continua seis sigma (DMAIC) y ciclo Deming (PHVA) junto con la exposición de retos y dificultades para establecer la calidad de los datos y el gobierno de la información.

## **MARCO TEÓRICO**

El desarrollo de este ensayo se fundamentó en la recolección y análisis de diferentes fuentes como, metodologías que tienen como propósito la mejora continua, autores enfocados en temas de calidad de los datos y gobierno de la información, documentos públicos en los que se establecen lineamientos del plan de calidad y los componentes de la información en Colombia, normas internacionales que no son certificables, pero pueden ser adoptadas como buena práctica en una organización, artículos y manuales para la estabilización de un gobierno de información. Desde el punto de vista empírico, se toman en

cuenta experiencias de vida analizadas desde el rol de control interno en las que se exponen las consecuencias de una mala gestión de la información.

## **DESARROLLO DEL TEMA**

El gran reto de las organizaciones en la actualidad es, el gobierno de la información y la calidad de los datos. La forma adecuada para abordar este reto es entender y priorizar las siguientes preguntas: ¿Por qué se necesita la calidad en los datos? ¿Para qué sirve la calidad de los datos? ¿Cuándo los necesito? ¿Cómo se logra la calidad de los datos y el gobierno de la información? ¿Quién es el encargado de lograr la calidad de los datos y el gobierno de la información? ¿A quién le benefician? ¿Qué áreas involucra la construcción de la información? ¿Qué características deben tener los datos y el gobierno de la información? Estas, permiten que las organizaciones en primer lugar realicen una autoevaluación sobre el estado de madurez del gobierno de la información y de sus datos. También, posibilita dimensionar que es lo que realmente está haciendo con sus datos, sus fortalezas, debilidades, amenazas y oportunidades, saber si son fiables y útiles o si por lo contrario tiene activos informacionales inútiles y/o mal gestionados. En segundo lugar, luego de haber realizado la autoevaluación podrá actuar y crear un plan de mejora respecto al estado en el que se encuentra, involucrando a la alta dirección en la estrategia de planeación e implementación. Esto, con el objetivo de establecer un gobierno de información sólido en el cual la cabeza de la organización despliegue la importancia y la vitalidad de dichas estrategias. Así, se logrará una nueva cultura organizacional y se normalizará la adecuada y oportuna gestión de los datos por parte de cada uno de los stakeholders. Y en tercer lugar se podrá realizar seguimiento al cumplimiento de la

estrategia implementada y estar permanentemente en un proceso de mejora continua.

Para dar respuesta al ¿por qué se necesita la calidad en los datos? Las organizaciones deben conocerse muy bien debido a que esta necesidad se puede derivar de un cumplimiento normativo, un cumplimiento de estándares de un ente acreditador o porque simplemente la calidad de datos es una estrategia y buena práctica de la organización.

En respuesta al ¿Para qué sirve la calidad de los datos? se plantea una visión general respecto a las necesidades de algunas áreas y sistemas de una organización como lo son:

a) El área financiera: En esta área es primordial tener una información idónea, fiable, objetiva, oportuna, consistente y auditable. De tal forma que esta funcione como insumo de entrada a la hora de tomar decisiones, realizar inversiones, realizar análisis de rentabilidad, análisis de costos, establecer precios, implementar indicadores y presentar documentos financieros de acuerdo con la normatividad vigente.

Un ejemplo claro de las consecuencias de no tener un gobierno de esta información es el caso del hospital XYZ ubicado en la ciudad Bogotá, Colombia, el cual contrató a la empresa consultora ABC con el objetivo de saber cuáles eran los servicios más rentables dentro de su portafolio. Como resultado de la consultoría, la empresa ABC concluyó que solo 3 de los 25 servicios que se encontraban en el portafolio eran rentables (trasplantes, pediatría y patologías cardiovasculares).

Al conocer estos resultados, la Alta Dirección del hospital XYZ quedó consternada, por lo que decidió corroborar esta información con una consultoría solicitada al área de Control Interno. En respuesta a esta solicitud, el Auditor Interno inició su análisis con el apoyo del área de costos y contabilidad solicitando los ingresos y los costos registrados a cada uno de los CeCos

(Centro de costos) del hospital XYZ, al verificar esta información se evidenció que había centros de costos que tenían registrados ingresos superiores a \$500.000.0000 por mes y no tenían ni un solo peso asignado en costos. Esta fue la primera alerta que le hizo pensar al Auditor Interno que algo en el resultado de la consultoría de la empresa ABC estaba mal, puesto que no es posible que un CeCo solo tenga ingresos sin requerir costos o gastos. Al seguir verificando, se observó que algunos ingresos y costos estaban siendo asignados a CeCos que no tenían nada que ver con el servicio al que se debió haber cargado. Es por estos imprevistos que el área de Control Interno del hospital XYZ concluyó y presentó como resultado 3 aspectos de gran importancia. En primer lugar, la empresa consultora ABC muy posiblemente había cometido errores en el análisis de rentabilidad y el resultado no era fiable. En segundo lugar, la información de ingresos y costos no estaba siendo asignada adecuadamente a los CeCos de cada servicio y en tercer lugar era imposible hacer un análisis de rentabilidad por servicio, debido a que los datos no eran consistentes.

Al visualizar la inconsistencia en la información financiera, desde la Alta Dirección se derivaron grandes preocupaciones y preguntas claves, una de ellas fue si los datos de ingresos y costos estaban en dicho desorden, ¿Cómo está el resto de la información financiera con la cual se toman decisiones relevantes en la organización como lo es el establecimiento de tarifas o realizar inversiones?

b) El área comercial: En esta área es de vital importancia tener datos de calidad y tener un gobierno de la información, debido a que en la actualidad existe una herramienta llamada BI (business intelligence) inteligencia de negocios en español, la cual requiere como insumo de entrada, datos fiables y consistentes de las tendencias del mercado y las necesidades de los consumidores. Lo anterior con el fin de realizar un análisis de la situación actual del negocio

frente a lo que requiere el mercado y así obtener una visión prospectiva y generar estrategias que se encuentren alineadas con los objetivos de la organización y permitan optimizar los procesos, centralizar los esfuerzos, tener mayor asertividad a la hora de atraer y retener clientes, conocer las necesidades de los clientes, fortalecer la marca, proyectar tendencias y tener un histórico del comportamiento de venta.

Una analogía que permite explicar adecuadamente el gobierno de la información implementando estrategias de inteligencia de negocios es la siguiente: imagine que está presenciando una competencia de arquería (tiro con flechas), y en la competencia solo se encuentran dos participantes; el participante número 1 es un novato con una habilidad innata y empírica de puntería, que a su vez desconoce la técnica y todas las variables que se deben tener en cuenta a la hora de disparar con un arco, es decir un competidor que solo confía en su sentido. Por el otro lado se tiene al participante número 2, quien es un competidor que posee una gran puntería, una técnica para disparar las flechas del arco y además hace parte de un equipo multidisciplinario que le aconseja sobre qué arco y flechas debe usar, con qué fuerza debe disparar, analiza a qué velocidad puede proyectarse la flecha según corrientes de viento. Ambos competidores deben darle al blanco, y el que le dé al centro del blanco, es el ganador. Al disparar, se observó que el participante número 1 corrió con suerte y logró darle en el blanco, pero no precisamente en el centro, sino más bien casi saliéndose del blanco. Con el participante número 2, se observó que antes de ejecutar su tiro, se dejó orientar por su equipo multidisciplinario, esto con el fin de realizar el ejercicio de la forma más acertada y teniendo en cuenta las variables y los datos que eran importantes y relevantes para su ejecución. Lo cual dio como resultado un tiro al centro del blanco.

Por lo cual se concluye que, el que tiene la información y la gestiona adecuadamente es el que tiene más probabilidad de ganar. Así mismo pasa en el mundo comercial de las empresas, si no se cuenta con competencias y datos aptos para ganar mercado, muy posiblemente no se obtendrán los resultados deseados.

c) En el área de riesgos funcionan como insumo de entrada al proceso de identificación, caracterización, valoración de riesgos y evaluación de controles, permitiendo así mapear las áreas y los riesgos críticos de la organización. Al concluir este ejercicio, el área de riesgos suministrará las herramientas a los dueños de los procesos y a la Alta dirección para que tomen decisiones al respecto y puedan gestionar adecuada y oportunamente los riesgos que mayor impacto tienen sobre la organización.

d) En el área operativa, el gobierno de la información se debe establecer en procesos como, por ejemplo: la supervisión de los activos fijos, los temas de obsolescencia de maquinaria y equipos y los mantenimientos preventivos y correctivos.

Un ejemplo claro de las consecuencias de no tener un gobierno de esta información es otro caso del hospital XYZ en el cual se manejaba un control de obsolescencia de maquinaria y equipos en un archivo de Excel que solo se actualizaba cuando era requerido, y no incluía la totalidad de los activos. Lo anterior demostró que era un control manual débil y brindaba información inconsistente e inoportuna. Un día de operación normal en el hospital XYZ se dañaron 2 de 3 angiografos, estos equipos se caracterizaban por mantener un flujo alto y constante de pacientes, el caos, la contingencia y el reproceso fue tan terrible, que la situación llegó a oídos del Director de Operaciones, quien rápidamente actuó solicitando reporte al responsable de obsolescencia de equipos biomédicos, a lo cual respondió que efectivamente el

equipo llevaba dos años de obsolescencia y no se habían percatado de la situación por no tener la información actualizada y no entender la importancia de la gestión de los datos.

e) En el sistema de control es esencial la calidad de los datos y el gobierno de la información, dado que con esta información los dueños de procesos y la Alta Dirección pueden tomar medidas preventivas, detectivas o correctivas frente a la posible materialización de riesgos que amenacen el cumplimiento de los objetivos o comprometan los recursos financieros, operativos, tecnológicos o de talento humano de la organización y posteriormente le permitirá implementar controles y estrategias que mitiguen el impacto y la causa del riesgo, dichos controles deben encontrarse documentados, implementados y socializados con todos los stakeholders que hagan parte del proceso. Además, esto permitirá garantizar o brindar cierto nivel de seguridad a la hora de tomar decisiones de alto impacto en una organización.

Para dar respuesta a la pregunta ¿Cuándo los necesito? cualquier persona diría que cuando sean requeridos, pero no es así de simple dado que estos requerimientos vienen acompañados con la respuesta a ¿Qué características debe tener los datos con calidad? es decir que los datos deben cumplir con los siguientes atributos según lo contemplado en la norma ISO/IEC 25012, metodología adoptada por el DNP (Departamento Nacional de Planeación) para establecer los lineamientos para el plan de calidad y los componentes de la información del año 2019.

*Ilustración 1: Atributos de la calidad de los datos*



*Fuente: Imagen modificada, clasificación de características definidas en ISO/IEC 25012.*

**Exactitud:** este atributo tiene relación con la precisión que se tenga en los datos.

**Compleitud:** este atributo se refiere a que los datos cuenten con todas las variables que debe contar para brindar una información integra.

**Consistencia:** este atributo se refiere a la coherencia de los datos respecto a la realidad.

**Credibilidad:** este atributo se relaciona con la fiabilidad y validez de los datos.

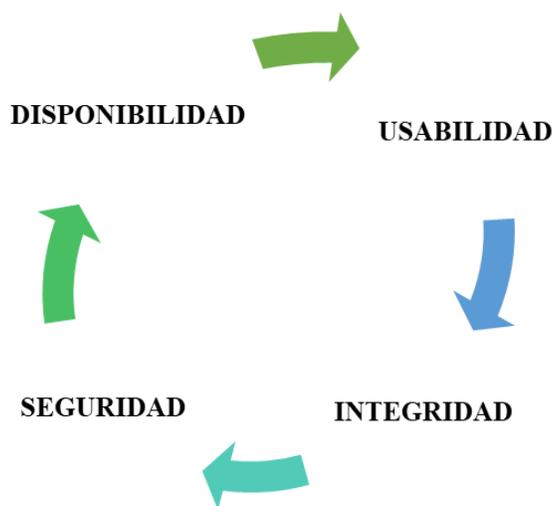
**Actualidad:** este atributo tiene que ver con que los datos se encuentren vigentes de acuerdo con requerimiento o simplemente al día.

Un ejemplo claro del incumplimiento de estos atributos es otro caso que ocurrió en el hospital XYZ cuando el Director General decidió citar a todos los directores administrativos uno a uno, con el objetivo de realizar un seguimiento relacionado con la gestión y la presentación de indicadores, referentes al primer semestre del año 2020. Esta actividad terminó sorprendiéndolo

con 3 datos diferentes del saldo de cartera a junio 2020 ya que la Dirección Financiera dio un valor, la Dirección Comercial encargada del proceso de recaudo dijo un valor diferente al de la Dirección Financiera y la Dirección de Tecnologías dio otro valor diferente al de las 2 direcciones anteriores. Como resultado de este ejercicio de seguimiento, el Director General concluyó que no existía ni gobierno de la información ni calidad de los datos, ya que se observaban tres fuentes diferentes de un dato único y este era totalmente diferente en las tres fuentes. Por lo cual es supremamente complejo tomar decisiones frente a este rubro tan crítico como la Cartera en el hospital XYZ.

En cuanto al gobierno de la información se plantean los siguientes atributos los cuales deben ser garantizados por la Alta Dirección, estableciendo objetivos estratégicos que conlleven a una gestión integral entre los stakeholders.

*Ilustración 2: Atributos del gobierno de información*



*Fuente: Elaboración propia*

**Disponibilidad:** este atributo del gobierno de la información relaciona los marcos que tiene la organización en cuanto a la ubicación y la accesibilidad de los datos.

**Usabilidad:** este atributo consta de los marcos que debe establecer la Alta Dirección referente a la facilidad de uso que tienen los datos y el para qué son necesarios o requeridos en la organización.

**Integridad:** este atributo se refiere al marco que debe establecer una organización respecto a la totalidad, el estado físico y lógico de la información.

**Seguridad:** este atributo se relaciona con que la organización debe establecer estrategias que garanticen la confianza de saber que la información se encuentra protegida y posee cierta restricción de acceso.

Teniendo en cuenta estos 4 atributos, el gobierno de la información tiene como propósito el cumplimiento de las siguientes metas:

a) Establecer, aprobar y desplegar a los stakeholders de la organización los objetivos, las estrategias, marcos normativos internos y externos referentes al sistema de información.

b) Supervisar el cumplimiento de requerimientos normativos o buenas prácticas dentro de la organización.

c) Conocer y apoyar los proyectos de inversión que tienen como fin mejorar la calidad de los datos y optimizar el sistema de información.

d) Comprender y sensibilizar a los stakeholders respecto a la importancia de la calidad de los datos, la seguridad, la usabilidad, la disponibilidad y la integridad de la información.

En cuanto al ejercicio de autoevaluación de madurez de los datos y el gobierno de la información, se puede evaluar cada uno de los activos informacionales de la organización asignando un valor numérico a cada uno de los 9 atributos expuestos, esto con el fin de

conocer las debilidades y las fortalezas que se tienen en los datos y el gobierno e implementar planes de mejora objetivos. A continuación, se muestra un ejemplo:

tabla 1: Propuesta de autoevaluación calidad de datos y gobierno de información.

AUTOEVALUACIÓN INFORMACIÓN DIRECCIÓN FINANCIERA HOSPITAL XYZ							VALORACIÓN DEL TOTAL	
PROCESO: GESTIÓN DE CARTERA (HOSPITAL XYZ)								
ATRIBUTOS	CALIFICACIÓN							
	1	2	3	4	5			
CALIDAD DE DATOS	Exactitud	1					1 A 5	INACEPTABLE
	Compleitud		2				6 A 10	DEFICIENTE
	Consistencia	1					11 A 15	ACEPTABLE
	Credibilidad	1					16 A 20	ADECUADO
	Actualidad		2				21 A 25	ÓPTIMO
<b>TOTAL</b>		<b>7</b>						
		<b>DEFICIENTE</b>						
GOBIERNO DE INFORMACIÓN	Seguridad		2					
	Usabilidad				4			
	Integridad	1						
	Disponibilidad			3				
<b>TOTAL</b>		<b>10</b>						
		<b>DEFICIENTE</b>						

Fuente: Elaboración propia.

De acuerdo con los resultados del ejercicio, se puede evidenciar que el hospital XYZ tiene deficiencias en la calidad de los datos y el gobierno de la información en el proceso de gestión de Cartera, por lo tanto, el dueño del proceso debe establecer una oportunidad de mejora que garantice la adecuada y oportuna gestión de la información correspondiente a su proceso, teniendo en cuenta sus necesidades, fortalezas, debilidades, oportunidades y amenazas.

En respuesta a ¿Cómo se logra la calidad de los datos y el gobierno de la información? ¿Quién los construye? ¿A quién le benefician? ¿Qué áreas involucra la construcción de la información? se propone implementar el método Seis Sigma como buena práctica para estabilizar esta estrategia, normalizar la cultura organizacional y permanecer en una mejora continua.

El método Seis Sigma tiene una herramienta llamada DMAIC por sus siglas en inglés (Define, Measure, Analyze, Improve, Control). Alaya Anis Ben (2018).

*Ilustración 3: Metodología Seis Sigma (DMAIC) para implementar y mejorar continuamente la calidad de los datos y el gobierno de la información*



*Fuente: Elaboración propia.*

En referencia al proceso (D) de definición se deben establecer los objetivos y las estrategias de la organización, los procedimientos de recolección, solicitud, generación, comunicación, custodia de la información, junto con la asignación de roles a cada una de las áreas y los colaboradores involucrados en los procesos relacionadas con calidad de datos y gobierno de la información, esto con el fin de convertirlo en un foco institucional y fomentar la cultura de mejora continua frente a este tema.

En relación con el proceso (M) de medición, se deben establecer métodos de evaluación para los atributos anteriormente mencionados referentes a calidad de datos (exactitud, completitud, consistencia, credibilidad y actualidad) y gobierno de la información (disponibilidad, usabilidad, integridad y seguridad). Además, de involucrar otras variables como

tiempos, cantidad y tipo de solicitud. Medición que debería llevarse a cabo por medio acuerdos de nivel de servicio e indicadores cualitativos y cuantitativos.

Con respecto al proceso (A) de análisis, se debe realizar este proceso con el fin de tener herramientas para poder tomar decisiones, teniendo en cuenta elementos de prospección como lo son los objetivos, las estrategias, los procedimientos documentados y los datos de medición.

Lo ideal sería que cada uno de los colaboradores desde su posición en la organización logre realizar este ejercicio de forma automática, ya que el análisis debe ser realizado de forma horizontal y vertical en una organización, en los casos en los que el resultado del análisis no sea favorable, se tendrá que comunicar a las partes involucradas.

En referencia al proceso (I) de mejora – Improve, este debe ser teneido en cuenta para corregir los errores de forma progresiva y transversal, además de enfocar los procesos y los involucrados al logro de los objetivos.

Con respecto al proceso (C) de control se debe tener una visión holística de todo lo descrito anteriormente, a fin de impulsar una cultura de autocontrol en cada uno de los colaboradores, junto con la realización de evaluaciones (auditorías) que permitan visualizar las fallas en la implementación o ausencia de controles, en cada uno de los procesos de la organización, los riesgos materializados o que posiblemente puedan materializarse, lo cual posibilitará fortalecer el sistema de control, establecer estrategias de aseguramiento y direccionar la priorización en la toma de decisiones en una organización.

Adicional a estos 5 procesos también se propone aplicar el ciclo de Deming (PHVA), en el cual lo que se encuentre en los procesos (D, M, A, I, C) se tomará como insumo a la hora de realizar la planeación (P). Posteriormente, se procede al hacer (H), de tal manera que se logre

ejecutar lo que se planeó. Luego, se debe realizar la verificación (V), con el objetivo de generar aseguramiento respecto a lo planeado y a lo ejecutado. Finalmente, se debe actuar (A) con planes de mejora o actividades correctivas que posibiliten resarcir algunas fallas y orientarse específicamente en el logro y el cumplimiento de los objetivos que fueron planteados inicialmente.

A continuación, se presenta un ejemplo de la implementación del método con el hospital XYZ.

*Tabla 2: Propuesta metodología combinada ciclo Deming (PHVA) y seis sigma (DMAIC).*

<b>OBJETIVO</b>
Establecer un sistema de gestión de la seguridad de la información basado en los estándares y requisitos de la (ISO/IEC 27001:2013) en el cual se garantice la usabilidad, integridad, disponibilidad y seguridad de la información del hospital XYZ.
<b>ESTRATEGIAS</b>
1. Implementar procesos que permitan dar cumplimiento a los requisitos de la (ISO/IEC 27001:2013), dirigidos y gestionados por parte del área de TI. 2. Mapear los riesgos que se encuentran directamente ligados a los temas referentes a la usabilidad, integridad, disponibilidad y seguridad de la información.
<b>ATRIBUTO DE GOBIERNO DE LA INFORMACIÓN QUE SERA IMPLEMENTADO</b>
Seguridad
<b>(P) PLANEAR</b>
<b>(D) DEFINIR</b>
1. Conocer la infraestructura que tiene el hospital XYZ, en cuanto a seguridad de la información, junto con una verificación de su estado en la operación (perfiles, niveles de atribución y accesos). 2. Mapear los terceros y aliados estratégicos que deben garantizar la seguridad de la información del hospital XYZ. 3. Definir las necesidades y/o requerimientos a los cuales el hospital XYZ debe presentar cumplimientos referentes a la seguridad de la información, por ejemplo:  - Las historias clínicas de los pacientes, según el artículo 34 de la ley 23 de 1981 de Colombia “La historia clínica es el registro obligatorio de las condiciones de salud del paciente. Es un documento

privado sometido a reserva que únicamente puede ser conocido por terceros previa autorización del paciente o en los casos previstos por la Ley”.

- Conservación de información contable, según el artículo 60 del decreto 410 de 1971, las organizaciones deben garantizar la integración de la información contable por un periodo de 10 años.

- Los estudios de investigación.

- La información administrativa.

- Los documentos que legalmente son confidenciales.

4. Identificar las áreas involucradas en el establecimiento de la seguridad de la información.
5. Identificar y conocer los flujos de información.
6. Identificar y definir las fuentes y proveedores de la información (tipo de información y medio por el cual ingresa la información).
7. Establecer, documentar, socializar y sensibilizar procedimientos de custodia de la información junto con la asignación de roles para su adecuado funcionamiento.
8. Identificar, caracterizar y evaluar los riesgos.
9. Establecer controles que sean dirigidos a las causas de los riesgos y ayuden a mitigar su impacto.
10. Establecer un programa de gobierno de la información en el cual se garantice los atributos de la calidad de los datos según la ISO/IEC 25012 (exactitud, completitud, consistencia, credibilidad, actualidad).
11. Establecer el alcance del sistema de gestión de la seguridad de la información.
12. Definir etapas de madurez del sistema

#### **(M) MEDIR**

Establecer métodos de evaluación, como, por ejemplo:

- Indicadores referentes a los roles y accesos del sistema (cantidad de usuarios con roles asignados en el sistema / cantidad de usuarios en el sistema) %.
- Indicador de fugas de información (eventos materializados de fugas de información)
- Alerta de acceso al sistema de información desde ordenadores (IP) diferentes a los que le pertenecen al hospital XYZ.
- Cubrimiento del sistema de seguridad de la información en los activos organizacionales según (ISO/IEC 27001:2013) (activos informacionales cubiertos por el sistema de seguridad de la información / total activos informacionales) %.

#### **(A) ANÁLISIS**

Establecer los momentos en los que se deben realizar los análisis, que información se tomará en cuenta para el análisis, quienes deben ser los responsables y que áreas se encuentran involucradas para realizar este ejercicio de establecer un sistema de gestión de la seguridad de la información.

#### **(I) IMPROVE – MEJORA**

Establecer la metodología de mejora (análisis de causa, acciones, responsables), en caso de que no sea requerida la mejora a causa de un error, un incumplimiento o una no conformidad, siempre se debe mantener la cultura de mejora continua y siempre buscar formas de mejorar el sistema de gestión de la seguridad de la información.

#### **(C) CONTROL**

Establecer en el sistema de control interno, los controles de primera y segunda línea de defensa referentes con el sistema de gestión de la seguridad de la información, detallando los responsables y las actividades de control.

<b>(H) HACER</b>
<b>Hacer lo que fue establecido en (D) Definido (C) controles</b>
Aprobación y GO desde la Alta dirección, documentación, socialización, sensibilización y ejecución de lo que fue establecido en la etapa de planeación (proceso D y proceso C).
<b>(V) VERIFICAR</b>
<b>Hacer lo que fue planeado en el proceso (M) Medición</b>
Realizar la medición en cada uno de los indicadores e ítems que fueron definidos en la planeación.
<b>Hacer lo que fue planeado en el proceso (A) Análisis</b>
Tomar como insumo de entrada para el proceso de análisis, los resultados de los indicadores que se expusieron anteriormente Vs el lineamiento del objetivo y las estrategias, ejemplo: Resultado del indicador de Cubrimiento del sistema de seguridad de la información en los activos organizacionales según (ISO/IEC 27001:2013) (activos informacionales cubiertos por el sistema de seguridad de la información / total activos informacionales) % Vs el objetivo de la organización (Establecer un sistema de gestión de la seguridad de la información basado en los estándares y requisitos de la (ISO/IEC 27001:2013) en el cual se garantice la usabilidad, integridad, disponibilidad y seguridad de la información del hospital XYZ). De acuerdo con este ejercicio prospectivo, se deben establecer planes de mejora o acciones correctivas.
<b>(A) ACTUAR</b>
<b>Hacer lo que fue planeado en el proceso (I)</b>
Poner en funcionamiento los planes de mejora o acciones correctivas que hayan sido concretados de acuerdo con los resultados del análisis de causa y la aprobación por parte de los responsables y las áreas involucradas.

*Fuente: Elaboración propia.*

Las dificultades o los retos para implementar esta propuesta son:

- a) Tener demasiados datos dispersos en la organización, hasta el punto de perder la trazabilidad o el flujo de la información.
- b) Priorizar los procesos o la información en la cual se va a implementar el sistema de gestión de la seguridad de la información.
- c) Establecer una cultura organizacional en la cual la cabeza de la organización sea consciente de la importancia y de igual forma se encuentre de acuerdo con desplegar marcos o políticas que orienten la conducta de los colaboradores en la organización.

d) Capacitar a los colaboradores respecto al saber hacer y el uso de los sistemas de información

e) Diseñar y establecer una arquitectura de TI que se alinee con el sistema de información y los objetivos de la organización.

Una de las oportunidades para que el hospital XYZ pudiera establecer un sistema de información seguro, fue la pandemia del COVID 19, esto debido a que la información de contagio de colaboradores y pacientes debía cumplir con cada uno de los atributos expuestos durante este ensayo. Hecho por el cual la alta dirección procedió inmediatamente a realizar el montaje de matrices de riesgos, tableros de mando, y seguridad en cuanto al acceso restringido de estos datos. La alta dirección al evidenciar los beneficios de este ejercicio decidieron replicarlo con los procesos más críticos del hospital XYZ.

Por último, la metodología expuesta anteriormente para una adecuada gestión de la información puede considerarse como un control preventivo, siempre y cuando sea integro y realizado por personal idóneo.

## **CONCLUSIÓN**

La calidad de los datos y el gobierno de la información debe cumplir con 9 atributos (exactitud, completitud, consistencia, credibilidad, actualidad, disponibilidad, usabilidad, integridad y seguridad) los cuales permitirán garantizar un nivel alto de confianza a la hora de tomar decisiones. También, conllevará al establecimiento de controles preventivos para mitigar riesgos financieros, operativos, legales y de fraude que comprometan los recursos de una organización y el cumplimiento de los objetivos

Para implementar un sistema de gestión de la seguridad de la información, se requiere de realizar una autoevaluación al sistema de información, fundamentándose en la valoración de los 9 atributos expuestos en el informe, concluidos los resultados y el análisis de la autoevaluación se propone la aplicación de una metodología en la que se definen los requerimientos, las necesidades, los responsables, las actividades que se realizaran, el conocimiento del flujo de la información en cada uno de los procesos, las áreas involucradas y una arquitectura tecnológica adecuada a los estándares de la ISO/IEC 27001, posteriormente se realiza el procesos de verificación y medición por medio de indicadores y finalmente se establecen e implementan planes mejora o acciones correctivas respecto al análisis de los resultados de medición y lo conforme con la planeación de los objetivos y las estrategias.

## **REFERENCIAS BIBLIOGRAFICAS**

- Alaya Anis ben, (2018). El método seis sigma, traducción al español por Serra Marina Martin 50minutos.es.
- Almagro Luis, Equipo técnico OEA, Equipo técnico AWS (2019). Clasificación de datos, White paper series edición 6, Estados Unidos.
- Caro Angelica, Fuentes Alejandra, Soto M. Antonieta, (2012). Desarrollando sistemas de información centrados en la calidad de datos, Ingeniare, Revista Chilena, Chile.
- Colina Vargas, A. M. (2019). El gobierno de datos: Un referente entre el gobierno de TI y la inteligencia de negocios. Ecociencia, 6(1), 3-13.  
<http://revistas.ecotec.edu.ec/index.php/ecociencia/article/view/186/152>
- Departamento Nacional de Planeación, (2019). Lineamiento plan de calidad componentes de información, Colombia.
- Garcés Zuluaga José Jaime, (2016). Caracterización de modelos de madurez en gobierno de datos, Universidad Pontificia Bolivariana facultad de ingeniería en tecnologías de información y Comunicación maestría en tecnologías de información y comunicación, Medellín.
- Ingeniería de software - Requisitos de calidad y evaluación de productos de software (SQuaRE) - Modelo de calidad de datos, (2008). ISO/IEC 25012, ISO / IEC JTC 1 / SC 7 Ingeniería de software y sistemas, Europa.
- Organización Internacional de Normalización (ISO), Comisión Electrotécnica Internacional (IEC), (2017). Norma ISO/IEC 27001 Tecnología de la información Técnicas de seguridad Sistemas de Gestión de la Seguridad de la Información Requisitos (ISO/IEC 27001:2013 incluyendo Cor 1:2014 y Cor 2:2015). CENELEC (Comité Europeo de Normalización Electrotécnica). Europa.