

**UNIVERSIDAD PRIVADA ANTENOR
ORREGO**

FACULTAD DE INGENIERIA

Escuela Profesional de Ingeniería de Computación y Sistemas



**TESIS PARA OBTENER EL TITULO PROFESIOANL DE
INGENIERO DE COMPUTACION Y SISTEMAS**

**“MODELO DE AUDITORIA PARA EVALUAR LOS SISTEMAS
DE INFORMACION DEL GOBIERNO REGIONAL DE LA
LIBERTAD PARA EL AÑO 2018”**

**LÍNEA DE INVESTIGACIÓN: GESTIÓN DE PROYECTO
TECNOLÓGICOS**

Autor: Br. Luis Anthony Armas Saldaña

Asesor: Ing. Jaime Eduardo Díaz Sánchez

Trujillo - Perú

2020

Fecha de Sustentación: 09/11/20

“MODELO DE AUDITORIA PARA EVALUAR LOS SISTEMAS DE INFORMACION DEL GOBIERNO REGIONAL DE LA LIBERTAD PARA EL AÑO 2018”

Elaborado por:



Br. Luis Anthony Armas Saldaña

Aprobada por:



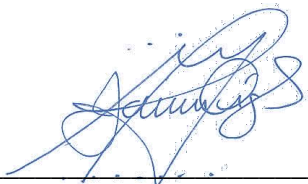
Ing. Edward Fernando Castillo Robles
Presidente
CIP: 192352



Ing. Karla Vanessa Meléndez Revilla
Secretario
CIP: 120097



Ing. José Antonio Calderon Sedano
Vocal
CIP: 139198



Ing. Jaime Eduardo Díaz Sánchez
Asesor
CIP: 73304

DEDICATORIA

El presente proyecto de investigación se la dedico a mis padres por haber dado su apoyo incondicional a lo largo de mi carrera profesional.

A mi hermana por siempre estar presente y dándome palabras de aliento para poder lograr mis metas.

AGRADECIMIENTO

Agradezco a Dios por su bendición y por darme buena salud, quien con su ayuda me ayudo a terminar esta etapa de mi vida de forma exitosa.

Mi profundo agradecimiento a todos los miembros de mi familia por confiar en mí y por darme palabras de aliento que me ayudaron a seguir adelante.

A mi hermana por estar siempre presente en mi vida quien me brindo sus buenos consejos y que me hizo sentir orgullo de lo que soy, dándome ese apoyo incondicional para lograr este objetivo propuesto.

A mi asesor el Ing. Jaime Díaz Sánchez, por haberme guiado con su experiencia y profesionalismo.

MODELO DE AUDITORIA PARA EVALUAR LOS SISTEMAS DE INFORMACION DEL GOBIERNO REGIONAL DE LA LIBERTAD PARA EL AÑO 2018.

RESUMEN

Por: Br Armas Saldaña Luis Anthony

Las empresas públicas y privadas consideran la información como uno de sus activos más valiosos, es por ello que siempre desean tener un control permanente de los datos para tener confiabilidad, seguridad, confidencialidad e integridad, esta presencia provoca la necesidad de auditoria de sistemas.

En el Gobierno Regional de La Libertad se identificó que el sistema de información presenta paralizaciones, lentitud y registros incompletos, los cuales dan un indicio que el sistema de información no es eficiente para los trabajadores de la institución.

Se propone un modelo para elaborar auditoria de sistemas que facilite a un grupo auditor la posibilidad de poder auditar el sistema de información del Gobierno Regional de la Libertad para así poder de detectar vulnerabilidades y amenazas en la información. El presente modelo de auditoria está elaborado bajo los criterios de la Contraloría General de la Republica ISO 27010 “Calidad de Producto de Software”, Normas de control interno(NCI) y las buenas prácticas de COBIT.

Palabra Clave: Auditoria de sistemas,ISO 25010 “Calidad de producto de software”, NCI (Normas de Control Interno), COBIT,modelo de auditoria.

ABSTRACT

Public and private companies consider information as one of their most valuable assets, which is why they always want to have permanent control of the data to have reliability, security, confidentiality and integrity, this presence causes the need for systems auditing.

In the Regional Government of La Libertad, it was identified that the information system presents stoppages, slowness and incomplete records, which indicate that the information system is not efficient for the institution's workers.

A development framework is proposed to elaborate systems audits that facilitate to an audit group with the possibility of being able to audit the information system of the Gobierno Regional de La Libertad in order to detect vulnerabilities and threats in the information. The present development framework is elaborated under the criteria of the General Comptroller of the Republic ISO 25000 “Software Product Quality”, Internal Control Standars and the good practices of COBIT.

Keywords: Systems audit, ISO 25010 "Software Product Quality", NCI (Internal Control Standards), COBIT, audit model.


PRESENTACIÓN

Señores Miembros del Jurado

Cumpliendo con los requerimientos estipulados en el reglamento de Grados y Títulos de la “Universidad Privada Antenor Orrego” para optar el grado de Ingeniero de Computación y Sistemas, ponemos a vuestra disposición la presente tesis titulada: **MODELO DE AUDITORIA PARA EVALUAR LOS SISTEMAS DE INFORMACION DEL GOBIERNO REGIONAL DE LA LIBERTAD PARA EL AÑO 2018.**

Gracias

Trujillo, 9 de Noviembre de 2020



Br. Armas Saldaña Luis Anthony

INDICE

I.	INTRODUCCION	10
1.1	Problema de investigación	10
a.	Planteamiento del problema	10
b.	Delimitación del problema	13
c.	Características y análisis del problema	13
d.	Formulación del problema	13
e.	Alcance.....	13
f.	Aportes	14
g.	Limitaciones	14
1.2	Objetivos	14
1.3	Justificación del estudio	15
II.	MARCO DE REFERENCIA	15
2.1	Antecedentes del estudio.....	15
2.2	Marco teórico	17
2.3	Marco conceptual	23
2.4	Sistema de hipótesis	23
III.	METODOLOGIA EMPLEADA.....	25
3.1	Tipo y nivel de investigación	25
3.2	Población y muestra de estudio.....	25
3.3	Diseño de investigación	25
3.4	Técnicas e instrumentos de investigación	25
3.5	Procedimientos y análisis de datos.....	26
IV.	PRESENTACION DE RESULTADOS.....	27
4.1	Descripción del SIGA	27
4.2	Modelado.....	28

4.2.1	Estudio de la ISO 25010, COBIT 2019 Y NCI.....	28
4.2.2	Formular modelo de auditoria.....	35
4.2.3	Valida modelo de auditoria.....	39
4.3	Planificación.....	40
4.3.1	Apertura auditoria.....	40
4.3.2	Definir muestra de auditoria.....	41
4.3.3	Planificar visitas, entrevistas y otros.....	41
4.3.4	Artefactos para la auditoria.....	42
4.4	Ejecución.....	47
4.4.1	Evaluar las interfaces de usuario, reportes y otros.....	47
4.4.2	Evaluar Base de datos.....	54
4.4.3	Evaluar la documentación.....	55
4.5	Informes.....	58
4.5.1	Elaborar informe de auditoria.....	58
4.5.2	Elaborar informe gerencial.....	71
4.5.3	Cierre de la auditoria.....	72
V.	DISCUSIÓN DE LOS RESULTADOS.....	73
VI.	CONCLUSIONES.....	76

INDICE DE TABLAS

Tabla 1:	Tabla de Variable Dependiente.....	24
Tabla 2:	Tabla de Variable Independiente.....	24
Tabla 3:	Tabla de Rango de Calificación de la eficiencia del SI.....	37
Tabla 4:	Tabla de No conformidades por artefactos.....	72
Tabla 5:	Tabla de Cantidad de Observaciones por normas y buenas practicas.....	72
Tabla 6:	Tabla de Normas y Buenas practicas.....	73
Tabla 7:	Tabla de Evaluación de la eficiencia.....	73

INDICE DE GRAFICOS

Figura 1:	Características de calidad de software.....	28
Figura 2:	Manual de generación de pedidos del SIGA.....	55
Figura 3:	Diagrama Ishikawa.....	70
Figura 4:	No conformidades por artefactos.....	72

Figura 5: Cantidad de normas y buenas practicas	73
Figura 6: Evaluación de la eficiencia	74

I. INTRODUCCION

1.1 Problema de investigación

a. Planteamiento del problema

Para algunas organizaciones el tema de auditoria de sistemas no es relativamente común o no tienen conocimiento del tema, esto frente a la competencia no les genera una buena ventaja competitiva.

Las empresas públicas y privadas consideran la información como uno de sus activos más valiosos, es por ello que siempre desean tener un control eficiente de los datos para asegurar disponibilidad, confidencialidad e integridad, esta presencia provoca la necesidad de auditoria de sistemas.

Los sistemas de información se han vuelto indispensables en las organizaciones por ende deben ser eficientes para lograr una buena toma decisiones y así lograr los objetivos estratégicos propuesto por cada empresa. Un eficiente sistema de información permite a la organización tener datos más seguros (disponibilidad, confidencialidad e integridad.

Realizar una auditoría de sistemas de información permite a las organizaciones resguardar y proteger la información es por ello que todos los sistemas de información deben ser eficientes.

Existen estándares internaciones que se aplican a todo tipo de empresas en el mundo y existen las buenas prácticas que permiten ser un marco de referencia para las diferentes TI, algunos de estos estándares y buenas prácticas son necesarias para poder realizar de manera adecuada una auditoria de sistemas, y así las organizaciones tengan un valor agregado. Algunos estándares y buenas prácticas que se utilizan ISO 25010, ISO 19011 y COBIT 5.

Según (Excentia, 2018) “La familia ISO 25000 proporciona una guía para el uso de la nueva serie de normas internacionales denominadas Sistemas y Requisitos de Calidad de Software y Evolución (SQuaRE). El objetivo de ISO 2500 es proporcionar una visión general de los contenidos de SQuaRE modelos de referencia y definiciones comunes, así como la relación entre los documentos.”

Según (Excentia, 2018) “La familia ISO 25000 proporciona una guía para el uso de la nueva serie de normas internacionales denominadas Sistemas y Requisitos de Calidad de Software y Evolución (SQuaRE). El objetivo de ISO 2500 es proporcionar una visión general de los contenidos de SQuaRE modelos de referencia y definiciones comunes, así como la relación entre los documentos.

Los requisitos de la ISO 25000 se centran además en dos procesos principales: Especificación de requisitos de calidad de software y evaluación de la calidad del software, soportada por el proceso de medición de calidad del software.”

Según (EEE, 2015) “La Norma ISO 19011 proporciona orientación sobre la gestión de un programa de auditoría, sobre la planificación y la realización de una auditoría del Sistema de Gestión, así como la competencia y la evaluación de un auditor y un equipo auditor. Ayuda a las organizaciones a mejorar el desempeño de los Sistemas de Gestión que se encuentren implementados en la organización. ”.

Según (Consulting, 2019) “El marco COBIT es aceptado internacionalmente como una buena práctica para el control de la información, TI y los riesgos que conllevan. COBIT se utiliza para implementar el gobierno de IT y mejorar los controles de IT. Contiene objetivos de control, directivas de aseguramiento, medidas de desempeño y resultados, factores críticos de éxito y modelos de madurez.”

En el Perú existen entes reguladores y documentos que sirven para la gestión de seguridad de la información el cual es importante aplicarlas dentro de las organizaciones. Algunos entes y documentos que utilizan como referencia es la Contraloría General de la República que “es el ente técnico rector del Sistema Nacional de Control, dotado de autonomía administrativa, funcional, económica y financiera, que tiene por misión dirigir y supervisar con eficiencia y eficacia el control gubernamental, orientando su accionar al fortalecimiento y transparencia de la gestión de las entidades” (Contraloria General de la Republica, 2019).

La auditoría de sistemas valida la integridad de la información y de los datos almacenados en las bases de datos de los sistemas de información y su procesamiento. Sin embargo, no existe un modelo de auditoria que permita ejecutar una auditoria de sistemas de información.

El que no exista un modelo de auditoria en las instituciones del estado para el desarrollo de la auditoria de sistemas retrasa en la buena toma de decisiones como ocurre en el Gobierno Regional de La Libertad.

El Gobierno Regional de La Libertad carece de un modelo para poder realizar auditoría a sus sistemas de información (SIGA, SISGEDO) por ende no se puede realizar un estudio a fondo para detectar las deficiencias de la misma

Los sistemas de información de Gobierno Regional de La Libertad no han sido auditados pudiendo no ser eficientes, generando errores (paralizaciones, lentitud, registros incompletos) dentro de la organización, que pueden perjudicar a lo largo del tiempo en las metas establecidas por la organización lo que conlleva a la insatisfacción de los usuarios internos y externos.

b. Delimitación del problema

El trabajo de investigación se llevará a cabo en el Gobierno Regional de La Libertad

c. Características y análisis del problema

Se identificaron los siguientes problemas:

- El sistema de información del Gobierno regional de La Libertad nunca ha sido auditado por ende no se ha evaluado el trabajo de la empresa y se desconoce si se utiliza todas las herramientas necesarias para obtener un resultado beneficioso para la organización.
- El Gobierno Regional de La Libertad carece de un modelo para realizar auditoria de sistemas el cual no le da un valor agregado a la organización.
- El sistema de información puede no ser eficiente ya que se cometen errores como paralizaciones, registros incompletos, lentitud en la gestión poniendo en riesgo la información y desperdiciando tiempo valioso dentro del Gobierno Regional de La Libertad.

d. Formulación del problema

¿Cómo evaluar la eficiencia del SIGA del Gobierno Regional de La Libertad?

e. Alcance

En el presente trabajo se implementará un modelo para la elaboración de auditoria para el sistema de información del gobierno regional de la libertad para el año 2018 donde la auditoria será practicada acorde el estándar ISO 19011 “Directrices para la auditoria de sistemas de gestión” , La familia ISO 25000 , la normatividad legal vigente y las buenas prácticas (COBIT)

f. Aportes

Proporcionar un modelo para la auditoria de sistemas de información y base de datos.

Integrar en un modelo de auditoria los conceptos y buenas prácticas de los estándares ISO 19011, La Familia ISO 25000 ,Normas de Control Interno y COBIT 5.0.

Formular herramientas aplicables a auditorias de entidades gubernamentales.

g. Limitaciones

El tiempo para realizar el modelo de auditoria es relativamente escaso.

El personal del Gobierno Regional de La Libertad desea que la información obtenida sea netamente estudiantil y confidencial.

Poco conocimiento del personal acerca del modelo de auditoria de sistemas que se quiere implementar.

Errores humanos que siempre están presentes en el trabajo de investigación.

1.2 Objetivos

Diseñar un modelo para ejecutar auditoria de sistemas para evaluar la eficiencia del SIGA en el Gobierno Regional de La Libertad

El objetivo general tiene los siguientes objetivos específicos:

- Diseñar un modelo para auditar la eficiencia de un sistema de información.
- Formular indicadores de eficiencia de un sistema de información
- Evaluar la eficiencia del SIGA del Gobierno Regional de La Libertad.

1.3 Justificación del estudio

La implementación de un modelo para la auditoría de sistemas es importante porque sería una herramienta de consulta para un grupo auditor que realice una auditoría al sistema de información del Gobierno Regional de La Libertad, aportando hacer una auditoría de una manera más eficiente y eficaz.

Con el modelo de auditoría implementado se podrá identificar y evaluar los riesgos dentro de la base de datos del Gobierno Regional de La Libertad optimizando el tiempo de la auditoría.

No ha existido ningún inconveniente en el Gobierno Regional de La Libertad ya que se ha tenido un acceso total al sistema de información con el permiso de los administradores que contribuyeron conmigo desinteresadamente, para así poder realizar el presente trabajo sin ningún percance y complicaciones.

II. MARCO DE REFERENCIA

2.1 Antecedentes del estudio

Se realizaron búsquedas correspondientes en el repositorio de la UPAO y no se encontró proyectos de investigación o tesis relacionadas al tema.

(Avelar Galdamez, Rosa Palacios, & Minero Cuchilla, 2019) en su trabajo de investigación indica que “Las tecnologías van avanzando cada vez más y se han involucrado en cualquier área comercial, de manera que los procesos se han automatizado y el manejo de información dentro de una Asociación Cooperativa es extensa. Con esto crece el riesgo para ellas, de ser vulnerables sobre todo aquellas que no poseen un sistema de evaluación o prevención que mitigue dicho riesgo.

Así mismo, la auditoría ha evolucionado a través del tiempo, adaptándose a los avances económicos, sociales, tecnológicos, entre otros, de esta manera nace la Auditoría de Sistemas; este tipo de auditoría es una auditoría especial cuyo objetivo es salvaguardar la información y minimizar los riesgos a un nivel aceptable”

Sin embargo para (Alejo, 2017) en su trabajo “Modelos De Auditoria Para El Mejoramiento Del Sistema De Control Interno De Instituciones Financieras En Colombia Basado En Lineamientos De La Ley Sarbanes Oxley Seccion 404” indica que “ La auditoría es un proceso sistemático que tiene por objeto recopilar información primordial para las organizaciones, posteriormente se examina dicha información y se evalúa el estado actual de las mismas, este estado se evidencia a través de la emisión de un juicio por parte de auditores asignados para tal fin.

Por lo anterior se considera la auditoria como una disciplina que proporciona los mecanismos esenciales para la valoración de una organización, esto es, a través de controles y técnicas que permiten identificar mitigar o eliminar riesgos. Adicionalmente dicha disciplina proporciona las mejores prácticas a implementar en las organizaciones con el fin de estimar la confiabilidad e integridad de la información”

Para (Pro, 2016) en su trabajo de investigación “Auditoría De Sistemas De Información En Un Entorno Informático” indica que” La Informática está inmersa en la gestión integral de la empresa, recalando que la informática no gestiona propiamente la empresa, ayuda a la toma de decisiones, pero no decide por sí misma. Por ende, debido a su importancia en el funcionamiento de la compañía, existe la Auditoría Informática, que no es otra cosa que un examen crítico que se realiza con el fin de evaluar la eficacia y eficiencia de una sección, un organismo, una entidad, entre otras.”

Para (Ramos, 2015) en su tesis de titulación “Propuesta De Un Plan De Auditoria Informática Para El "Sistema De Información En Salud" Y El "Aplicativo Para El Registro De Formatos SIS" En Los Establecimientos De Salud De La Unidad Ejecutora 400 En La Región Piura En El Año 2015” indica que “La propuesta de auditoria informática a los sistemas es de vital importancia para que cuando se presente algún tipo de inconveniente o supervisión se tenga una ayuda para saber cómo actuar frente a alguna amenaza que puede poner en riesgo la información, o en general para que se evalúe los sistemas de información desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información.”

“A la fecha la auditoria interna dentro de la sociedad y las organizaciones tanto nacionales como internacionales es de suma importancia porque incide favorablemente en garantizar la eficacia a y calidad de los procesos, además que permite el crecimiento, reconocimiento y una gran cantidad de beneficios permanentes para las empresas y también para el trabajador.” (Veliz, 2017)

2.2 Marco teórico

2.2.1 Auditoria

“Es el examen sistemático e independiente para determinar si las actividades y sus correspondientes resultados cumplen las disposiciones previstas y si dichas disposiciones se aplican eficazmente y son adecuadas para lograr los objetivos”. (Couto, 2019).

Auditoría de sistemas

“La auditoría de sistemas supone la revisión y evaluación de los controles y sistemas de informática, así como su utilización, eficiencia y seguridad en la empresa, la cual procesa la información. Gracias a la auditoría de sistemas como alternativa de control, seguimiento y revisión, el proceso informático y las tecnologías se emplean de manera más eficiente y segura, garantizando una adecuada toma de decisiones.” (Nuño, 2017)

2.2.2 Sistema de información

(Raymundo, 2018) manifiesta que “Un sistema de información en una compañía, es una serie de componentes que se interrelacionan con el objetivo de recopilar, procesar, almacenar y transmitir información como soporte a los niveles directivos dentro de la organización, auxiliando en la toma de decisiones, el control, el análisis y la coordinación”

(Leandro, 2018) Indica que “La información está constituida por un grupo de datos ya supervisados y ordenados, que sirven para construir un mensaje basado en un cierto fenómeno o ente. La información permite resolver problemas y tomar decisiones. Deben tener las siguientes características:

- Exactitud: La información ha de ser precisa y libre de errores.

- **Completitud:** La información debe contener todos aquellos hechos que pudieran ser importantes.
- **Economicidad:** El costo en que se debe incurrir para obtener la información debería ser menor que el beneficio proporcionado por ésta a la organización.
- **Confianza:** Para dar crédito a la información obtenida, se ha de garantizar tanto la calidad de los datos utilizados, como la de las fuentes de información.
- **Relevancia:** La información ha de ser útil para la toma de decisiones. En este sentido, conviene evitar todos aquellos hechos que sean superfluos o que no aporten ningún valor.
- **Nivel de detalle:** La información debe presentar el nivel de detalle indicado a la decisión a que se destina. Se debe proporcionar con la presentación y el formato adecuados para que resulte sencilla y fácil de manejar.
- **Verificabilidad:** La información ha de poder ser contrastada y comprobada en todo momento.”

Tipos

Según (Tranformacion digital , 2017) indica que “existen 6 principales tipos de sistema de información que son:

Sistemas de procesamiento de transacciones

Es un sistema computarizado que realiza y registra las transacciones rutinarias diarias necesarias para el funcionamiento de la empresa. Se encuentran en el nivel más bajo de la jerarquía organizacional y soportan las actividades cotidianas del negocio.

Sistemas de control de procesos de negocio

Son los que monitorizan y controlan los procesos industriales o físicos, como puede ser la refinación de petróleo, generación de energía o los sistemas de producción de acero en una planta siderúrgica.

Sistema de colaboración empresarial

Son uno de los tipos de sistemas de información más utilizados. Ayudan a los directivos de una empresa a controlar el flujo de información en sus organizaciones.

Se trata de uno de los tipos de sistemas de información que no son específicos de un nivel concreto en la organización, sino que proporcionan un soporte importante para una amplia gama de usuarios. Estos sistemas de información están diseñados para soportar tareas de oficina como sistemas multimedia, correos electrónicos, videoconferencias y transferencias de archivos.

Sistema de información de gestión

Son un tipo de sistemas de información que recopilan y procesan información de diferentes fuentes para ayudar en la toma de decisiones en lo referente a la gestión de la organización. Los sistemas de información de gestión proporcionan información en forma de informes y estadísticas.

Sistema de apoyo a la toma de decisiones

Es un sistema basado en ordenadores destinado a ser utilizado por un gerente particular o por un grupo de gerentes a cualquier nivel organizacional para tomar una decisión en el proceso de resolver una problemática semiestructurada. Los sistemas de apoyo a la toma de decisiones son un tipo de sistema computarizado de información organizacional que ayuda al gerente en la toma de decisiones cuando necesita modelar, formular, calcular, comparar, seleccionar la mejor opción o predecir los escenarios.

Sistema de información ejecutiva

Son los que proporcionan un acceso rápido a la información interna y externa, presentada a menudo en formato gráfico, pero con la capacidad de presentar datos básicos más detallados si es necesario. Los sistemas información ejecutiva proporcionan información crítica de una amplia variedad de fuentes internas y externas en formatos fáciles de usar para ejecutivos y gerentes.

Un sistema de información ejecutiva proporciona a los altos directivos un sistema para ayudar a tomar decisiones estratégicas.”

Calidad de sistemas de información

“La calidad del software se puede considerar como el grado en el que el software posee una combinación claramente definida y deseable de atributos de calidad. Este estándar, pues trata de definir la calidad del software para un sistema mediante una lista de atributos de calidad de software requerido por el propio sistema .” (Piattini, Garcia, & Pino, 2018)

“Establece que la calidad en los sistemas de información se debe considerar como una responsabilidad que tiene que ser compartida por todos los usuarios internos de la organización. Cabe agregar, que los sistemas de información pueden desempeñar un importante labor en los programa de calidad, ya que están estrechamente vinculados con el trabajo diario de todas las áreas de una organización. Los sistemas de información son complejos y la solución a problemas de calidad también. Es relevante mencionar que la introducción del sistema de información tiene que ser un poderoso impacto en la conducta organizacional.” (Antúnez, 2015)

“El modelo de calidad representa la piedra angular en torno a la cual se establece el sistema para la evaluación de la calidad del

producto. En este modelo se determinan las características de calidad que se van a tener en cuenta a la hora de evaluar las propiedades de un producto software determinado.

La calidad del producto software se puede interpretar como el grado en que dicho producto satisface los requisitos de sus usuarios aportando de esta manera un valor. Son precisamente estos requisitos (funcionalidad, rendimiento, seguridad, mantenibilidad, etc.) los que se encuentran representados en el modelo de calidad, el cual categoriza la calidad del producto en características y subcaracterísticas.

El modelo de calidad del producto definido por la ISO/IEC 25010 se encuentra compuesto por las ocho características de calidad que son:

- Adecuación funcional.
- Eficiencia de desempeño.
- Compatibilidad.
- Usabilidad.
- Fiabilidad.
- Seguridad.
- Mantenibilidad.
- Portabilidad.” (ISO 25000, 2018)

2.2.3 Eficiencia

“La eficiencia significa un nivel de rendimiento de un proceso el cual utiliza la menor cantidad de entradas o insumos para crear la mayor cantidad de productos o resultados. La eficiencia se relaciona con el uso de todos los insumos en la producción de cualquier producto, incluyendo el tiempo personal y la energía. La eficiencia es un concepto medible que puede determinarse determinando la relación entre el rendimiento útil y el total. Minimiza el desperdicio de recursos tales como materiales físicos, energía y tiempo, mientras que consigue con éxito la salida deseada.” (Valdes, 2018)

Eficiencia en los sistemas de información

“La efectividad busca una alta productividad, un aumento de la misma y una consecuente mejora de los servicios. La eficiencia, se relaciona con la manera de cumplir el objetivo. Con la búsqueda de mayor eficiencia se busca hacer más por menos, bajar costos, reducir las labores rutinarias y repetitivas. (Arroyo, 2015)

Un sistema de información eficiente es cuando:

- Permite un ahorro de costos
- Permite una reducción de labores manuales
- Permite una reducción de espacio físico.”

La ISO 25010 , COBIT 5 y Normas de Control Interno permiten la evaluación de la eficiencia de los Sistemas de Información

2.3 Marco conceptual

Auditoria de sistemas: Es la revisión y evaluación de los controles y sistemas de informática, así como su utilización, eficiencia y seguridad en la empresa, la cual procesa la información.

Compleitud: Es cuando todos los datos están completos sin espacios en blanco.

Eficiencia: Es la utilización de todos los medios disponibles de manera racional para llegar a una meta.

Errores: Es una falla en los sistemas de información que puede reportar cierres inesperados o produciendo cosas no previstas.

Integridad: Es que la información no pueda ser modificada o borrada ante intentos maliciosos salvo que tenga los permisos necesarios.

Paralizaciones: Es cuando un software se detiene de toda operación que estaba realizando

Sistema de información: Es un conjunto de elementos que interactúan entre sí con un fin común para satisfacer las necesidades en una organización

SIGA: Sistema integrado de gestión administrativa.

2.4 Sistema de hipótesis

2.4.1 General

Modelo de auditoria de sistemas permite evaluar la eficiencia del SIGA en el Gobierno Regional de La Libertad.

2.4.2 Variables

VARIABLE DEPENDIENTE (VD), X=Evaluación de la eficiencia del SIGA

VARIABLE INDEPENDIENTE (VI), Y= Modelo de auditoria de sistemas.

2.4.3 Operacionalización de las variables

Tabla 1: Variable Dependiente

Variable dependiente: Evaluación de la eficiencia en el sistema de información			
Dimensiones	Indicadores	Unidad de medida	Instrumento de Investigación
Nivel de errores	% de errores	$\frac{\text{Nro de registros erróneos}}{\text{Total de registros}}$	Hoja de captura de datos
Nivel de paralizaciones	Tiempo promedio de paralizaciones	$\frac{\sum_i (\text{Tiempo de paralización})_i}{\text{Horas laborales } n}$	Hoja de captura de datos
Nivel de completitud	Integridad de datos	$\frac{\text{Nro de registros completos}}{\text{Total de registros}}$	Hoja de captura de datos

Tabla 2: Variable Independiente

Variable independiente: Modelo de auditoria de sistemas			
Dimensiones	Indicadores	Unidad de medida	Instrumento de Investigación
Artefactos de auditoria	Documentos	Numero de documentos	Hoja de captura de datos
Registros de auditoria	Archivadores	Numero de archivadores	Hoja de capturas de datos
Procedimientos	Procedimientos	Número de procedimientos	Hoja de captura de datos

III. METODOLOGIA EMPLEADA

3.1 Tipo y nivel de investigación

El nivel de investigación es Correlacional

3.2 Población y muestra de estudio

Los sistemas de información del Gobierno Regional de La Libertad Sistema de información del área de la Sub Gerencia de logística y servicios generales.

3.3 Diseño de investigación

Experimental

3.4 Técnicas e instrumentos de investigación

Técnica	Forma de aplicación	Forma de obtención
Observación	Personal o por medios electrónicos	Observación directa
Análisis de documentos	Personal o por medios electrónicos	Información de la web
Entrevista	Personal o por medios electrónicos	Abiertas

3.5 Procedimientos y análisis de datos

3.5.1 Procedimientos

Fase	Actividades	Entregable
Modelado	<ul style="list-style-type: none">• Estudiar de la ISO, COBIT y NCI• Formular modelo de auditoria• Validar modelo de auditoria	Modelo de Auditoría
Planificación	<ul style="list-style-type: none">• Aperturar la auditoria• Definir muestra de la auditoria• Planificar las visitas, entrevista y otros.• Elaborar CheckList	Plan y programa de la auditoria
Ejecución	<ul style="list-style-type: none">• Evaluar las interfaces de usuario, reportes y otros• Evaluar la Base de Datos• Evaluar la documentación.	Documentos de aspectos de importancia Documentos de comunicación de hallazgos
Informes	<ul style="list-style-type: none">• Elaborar informe de auditoría.• Elaborar informe gerencial• Cierre de la Auditoria	Informe de Auditoria

3.5.2 Análisis de datos

Para este análisis se utilizarán tablas y gráficos y pruebas estadísticas correspondientes

IV. PRESENTACION DE RESULTADOS

El modelo de auditoria propuesto consta de 4 etapas, las cuales cuentan con actividades que serán desarrolladas en la siguiente investigación.

4.1 Descripción del SIGA

El sistema integrado de gestión administrativa (SIGA) está desarrollado para brindar transparencia en la gestión y administración del Gobierno Regional de la Libertad.

Así mismo el sistema integrado de gestión administrativa(SIGA) ayuda al ordenamiento y simplificación de los procesos administrativos de la gestión del Gobierno Regional de La Libertad.

Requerimientos:

Requerimiento de Microprocesador

Optimo: Procesador Intel Pentium IV

Mínimo: Procesador Intel Pentium I

Requerimiento de Memoria RAM

Optimo: 256 Mb

Mínimo: 128 Mb

4.2 Modelado.

4.2.1 Estudio de la ISO 25010, COBIT 2019 Y NCI

A. ISO 25010

La ISO 25010 propone un conjunto de criterios para evaluar la calidad de producto de software. Este modelo nos permite identificar qué características se necesita a la hora de diagnosticar un software.

Para evaluar el grado de satisfacción de un producto software es necesario saber en que medida satisface el producto software a los requisitos de sus usuarios.

La ISO 25010 está dividida en 8 características de calidad del producto software:



Figura 1: Características de calidad de software

Fuente: (ISO25000, 2019)

Se analizan las características y subcaracterísticas que se utilizaran de acuerdo a la eficiencia del sistema de información. En base a los conceptos del subtítulo 2.2.3

A. Adecuación Funcional

Atributo	Evaluación
Compleitud Funcional	Se selecciona, porque cubre todas las necesidades de los usuarios a través de grupo de funcionalidades.
Corrección Funcional	Se selecciona, porque permite proporcionar resultados correctos y precisos.
Pertinencia Funcional	Se selecciona, porque proporciona un grupo de funciones específicas para las necesidades de usuarios específicos.

B. Eficiencia de desempeño

Atributo	Evaluación
Comportamiento Temporal	Se selecciona, porque permite verificar los tiempos de respuesta, procesamientos y rendimiento de un sistema.
Utilización de Recursos	Se selecciona, porque permite verificar las cantidades y recursos que se utilizan del software.
Capacidad	Se selecciona, porque permite verificar el límite de un parámetro de un sistema.

C. Compatibilidad

Atributo	Evaluación
Coexistencia	No se selecciona, porque no se necesita coexistir con otro sistema independiente para compartir recursos.
Interoperabilidad	No se selecciona, porque no se necesita dos o mas sistemas para compartir información

D. Usabilidad

Atributo	Evaluación
Inteligibilidad	No se selecciona, porque permite al usuario entender si el software va acorde a sus necesidades.
Aprendizaje	No se selecciona, porque permite al usuario aprender su aplicación.
Operabilidad	No se selecciona, porque permite al usuario manejarlo con facilidad.
Protección frente a errores de usuarios	Si se selecciona porque permite a los usuarios evitar errores.
Estética	No se selecciona, porque permite agrandar y satisfacer al usuario a través de una interfaz
Accesibilidad	No se selecciona, porque permite que el sistema sea utilizado por usuarios con discapacidades.

E. Fiabilidad

Atributo	Evaluación
Madurez	Si se selecciona, porque permite satisfacer las necesidades de fiabilidad.
Disponibilidad	Si se selecciona, porque permite que un sistema este operativo cuando se desee.
Tolerancia a fallos	Si se selecciona, porque permite que un sistema se ejecute en presencia de fallos.
Capacidad de recuperación	No se selecciona, porque permite recuperar datos afectados en caso el sistema tenga una interrupción o fallo.

F. Seguridad

Atributo	Evaluación
Confidencialidad	No se selecciona, porque permite la protección contra el acceso de datos e información
Integridad	Si se selecciona, porque permite prevenir el acceso o modificaciones sin autorización.
No Repudio	No se selecciona, porque permite evidenciar las acciones o eventos, de manera que no puedan ser repudiados.
Autenticidad	No se selecciona, porque permite demostrar la identidad de un usuario.
Responsabilidad	No se selecciona, porque permite rastrear de forma eficaz de los actos de una entidad.

G. Mantenibilidad

Atributo	Evaluación
Modularidad	No se selecciona, porque permite hacer un cambio en sin que tenga impacto mínimo en lo demás.
Reusabilidad	No se selecciona, porque permite que una característica pueda ser utilizada por más de un sistema.
Analizabilidad	No se selecciona, porque permite verificar los efectos de algún cambio sobre el resto del sistema.
Capacidad de ser modificado	No se selecciona, porque permite al sistema ser modificado sin afectar negativamente el desempeño.
Capacidad de ser probado	No se selecciona, porque permite establecer medios de prueba para verificar si se cumplen los requisitos establecidos.

H. Portabilidad

Atributo	Evaluación
Adaptabilidad	Si se selecciona, porque permite ser adaptado efectivamente en otros entornos de software y hardware.
Facilidad de instalación	Se selecciona, porque permite que el software sea instalado de forma exitosa.
Capacidad de ser reemplazado	Se selecciona, porque permite ser utilizado por otro software que tiene el mismo propósito o entorno.

B. COBIT

DSS06 Gestionar Controles de Proceso de Negocio

Atributo	Evaluación
DSS06.01 Alinear las actividades de control embebidas en los procesos de negocio con los objetivos corporativos	No se selecciona, porque permite que los procesos de negocio se puedan monitorear lo que permite verificar los riesgos corporativos.
DSS06.02 Controlar el procesamiento de la información	Se selecciona, porque permite que el procesamiento de la información sea completa, precisa y segura a través de las actividades de proceso de negocio
DSS06.03 Gestionar roles, responsabilidades privilegios de acceso y niveles de autorización	Se selecciona, porque permite asignar los roles de acceso , privilegios y niveles de autoridad para así poder apoyar los objetivos del proceso de negocio
DSS06.04 Gestionar errores y excepciones	Se selecciona, porque permite la precisión y garantía de la información a través de la gestión errores y excepciones las cuales facilitan la corrección de información
DSS06.05 Asegurar la trazabilidad de los eventos y responsabilidades y de información.	No se selecciona, porque asegura que la información puede ser rastreada hasta los usuarios responsables , proporcionando información de confianza
DSS06.06 Asegurar los activos de la información	No se selecciona, porque permite asegurar los activos de la información que es accedida por los usuarios mediante métodos ya establecidos.

C. Normas de Control Interno (NCI)

La función de las normas de control interno es fortalecer y mejorar la gestión pública, protegiendo el patrimonio público y así poder lograr los objetivos y metas institucionales.

NORMA GENERAL PARA EL COMPONENTE DE INFORMACIÓN Y COMUNICACIÓN

Se entiende por el componente de información y comunicación, los métodos, procesos, canales, medios y acciones que, con enfoque sistémico y regular, aseguren el flujo de información en todas las direcciones con calidad y oportunidad. Esto permite cumplir con las responsabilidades individuales y grupales.

Funciones y características de la información

La información es resultado de las actividades operativas, financieras y de control provenientes del interior o exterior de la entidad. Debe transmitir una situación existente en un determinado momento reuniendo las características de confiabilidad, oportunidad y utilidad con la finalidad que el usuario disponga de elementos esenciales en la ejecución de sus tareas operativas o de gestión.

Información y responsabilidad

La información debe permitir a los funcionarios y servidores públicos cumplir con sus obligaciones y responsabilidades. Los datos pertinentes deben ser captados, identificados, seleccionados, registrados, estructurados en información y comunicados en tiempo y forma oportuna.

Calidad y suficiencia de la información

El titular o funcionario designado debe asegurar la confiabilidad, calidad, suficiencia, pertinencia y oportunidad de la información que se genere y comunique. Para ello se debe diseñar, evaluar e implementar mecanismos necesarios que aseguren las características con las que debe contar toda información útil como parte del sistema de control interno.

Sistemas de información

Los sistemas de información diseñados e implementados por la entidad constituyen un instrumento para el establecimiento de las estrategias organizacionales y, por ende, para el logro de los objetivos y las metas. Por ello deberá ajustarse a las características, necesidades y naturaleza de la entidad. De este modo, el sistema de información provee la información como insumo para la toma de decisiones, facilitando y garantizando la transparencia en la rendición de cuentas.

4.2.2 Formular modelo de auditoria

De acuerdo al análisis realizado se utilizarán las siguientes características y subcaracterísticas de la ISO 25010.

1. Adecuación Funcional	1.1 Completitud funcional
	1.2 Corrección funcional
	1.3 Pertenencia Funcional
2. Eficiencia de desempeño	2.1 Comportamiento temporal
	2.2 Utilización de recursos
	2.3 Capacidad
3. Usabilidad	3.1 Protección frente errores de usuarios
4. Fiabilidad	4.1 Madurez
	4.2 Disponibilidad
	4.3 Tolerancia a fallos
5. Seguridad	5.1 Integridad
6. Portabilidad	6.1 Adaptabilidad
	6.2 Facilidad de instalación
	6.3 Capacidad de ser reemplazado

De igual manera de COBIT 5.

1. DSS06.02	1.1. Controlar el procesamiento de la información
2. DSS06.03	2.1. Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización
3. DSS06.04	3.1. Gestionar errores y excepciones

Finalmente, de las Normas de Control Interno se utilizarán:

Norma General para el componente de información y comunicación	1.1. Funciones y características de la información
	1.2. Información y responsabilidad
	1.3. Calidad y suficiencia de la información
	1.4. Sistemas de información

Siendo el modelo de auditoria propuesto

		ISO 25010	COBIT
Norma General para el componen ente de información y comunicación	Funciones y características de la información		1.1: Permite que la información sea confiable para que el usuario realice sus labores.
	Información y responsabilidad	1.3 Permite que los usuarios específicos realicen sus tareas de acuerdo a sus funciones correspondientes. 3.1 Permite que el usuario registre la información de manera correcta.	1.1 Permite que el usuario obtenga la información que les corresponde. 2.1. Permite que el usuario tenga restricciones y privilegios al acceder a la información
	Calidad y suficiente de la información	1.1 Permite que el usuario asegure que la información sea confiable y de calidad. 1.2 Permite que la información proporcionada sea correcta y precisa 5.1. Permite prevenir que la información sea alterada.	1.1 Permite que la información procesada sea completa, precisas y segura. 2.1 Permite que la información sea registrada de acuerdo a los niveles y privilegios. 3.1. Permite asegurar la garantía de la información frente a los errores .
	Sistemas de información	2.1 Permite verificar el procesamiento, rendimiento y tiempos de respuestas del sistema de información. 2.2 Permite diagnosticar los recursos que utiliza el sistema de información. 2.3 Permite corroborar el límite de los parámetros del sistema de información 4.1 Permite que el sistema de información este operativo durante un tiempo estimado. 4.2 Permite que el sistema de información siempre esté disponible.	

	<p>4.3 Permite que el sistema de información continúe ejecutándose frente a la presencia de fallos.</p> <p>5.1 Permite al sistema de información evitar el acceso y modificaciones sin tener los privilegios correspondientes.</p> <p>6.1 Permite que el sistema de información se ejecute en cual entonces de hardware y software.</p> <p>6.2 Permite que el sistema de información puede instalarse de forma sencilla y correcta.</p> <p>6.3. Permite que el sistema de información utilizado pueda ser reemplazo por otro sistema de información con las mismas características.</p>	
--	---	--

La evaluación de los resultados al finalizar el modelo propuesto se realizará en base a la tabla siguiente:

Tabla N° 3:Rango de Calificación de la eficiencia del SI		
Rangos	Calificación	Descripción
Mayor al 95%	Muy buena	El Sistema de información funciona en excelentes condiciones
Entre el 85 y 95%, inclusive	Buena	El Sistema de información funciona en buenas condiciones
Entre 75 y 85%, inclusive	Regular	El Sistema de información funciona en regulares condiciones
Entre 50 y 75%, inclusive	Mala	El Sistema de información funciona en pésimas condiciones
Menor al 50%, inclusive	Muy mala	El Sistema de información funciona en muy pésimas condiciones

4.2.3 Valida modelo de auditoria

Para validar el modelo se elaboró la siguiente encuesta:

N	Pregunta	TD	D	N	A	TD	Suma	Porcentaje
1	Muestra coherencia con los objetivos de la auditoria							
2	Permite evaluar la eficiencia del SI							
3	Permite evaluar la responsabilidad de los usuarios							
4	Permite evaluar el rendimiento del SI							
5	Permite evaluar la calidad de la información							
6	Permite evaluar que el SI sea tolerante a fallos							
7	Permite evaluar la calidad del SI							
8	Permite evaluar los errores de los usuarios							
9	Permite evaluar el rendimiento del SI							
10	Permite evaluar los recursos que utiliza el SI							

La encuesta fue aplicada a 05(CINCO) especialista de auditoria de sistemas de información, obteniendo los siguientes resultados:

N	Pregunta	TD	D	N	A	TD	Suma	Porcent aje
1	Muestra coherencia con los objetivos de la auditoria	0	0	1	3	1	20	8.00%
2	Permite evaluar la eficiencia del SI	0	0	0	4	1	21	8.40%
3	Permite evaluar la responsabilidad de los usuarios	0	0	0	4	1	21	8.40%
4	Permite evaluar el rendimiento del SI	0	0	1	3	1	20	8.00%
5	Permite evaluar la calidad de la información	0	0	0	4	1	21	8.40%
6	Permite evaluar que el SI sea tolerante a fallos	0	0	1	1	3	20	8.00%
7	Permite evaluar la calidad del SI	0	0	0	4	1	21	8.40%
8	Permite evaluar los errores de los usuarios	0	0	1	3	1	21	8.40%
9	Permite evaluar el rendimiento del SI	0	0	1	3	1	21	8.40%
10	Permite evaluar los recursos que utiliza el SI	0	0	0	4	1	20	8.00%
							206	82.40%

El resultado de aceptación o aprobación es del 82.4% por lo que el modelo ha sido validado.

4.3 Planificación.

4.3.1 Apertura auditoria

Se realizó una reunión en el Gobierno Regional de La Libertad el día 03 de febrero de 2020 con el encargado del Área de La Sub Gerencia de Tecnología de información y con el Jefe de Desarrollo de Software indicando el inicio de la auditoria del Sistema Integrado de Gestión Administrativa (SIGA), BD_GRELL (Base de datos) y entre otros documentos.

Los acuerdos son los siguientes:

- Brindar un ambiente de trabajo con la seguridad correspondiente para el auditor.
- El sistema de información a auditar es el Sistema Integrado de Gestión Administrativa y su base de datos y la documentación correspondiente.
- Se aprueba el plan de visitas, entrevistas y reuniones con los responsables del Sistema Integrado de Gestión Administrativa (SIGA) y su base de datos y la documentación correspondiente.
- Otorgar las facilidades de acceso a los documentos, instalaciones, Sistema Integrado de Gestión Administrativa y su base de datos, que fueran necesarios para la ejecución de la auditoria.
- El *objetivo* de la auditoria es evaluar la eficiencia del Sistema Integrado de Gestión Administrativa.

- La información recopilada o adquirida dentro del Gobierno Regional de La Libertad será de uso netamente académico sin otros fines.
- Los *objetivos específicos* de la auditoría son:
 - Garantizar información de calidad.
 - Prevenir y evitar riesgos asociados al SIGA.
 - Asegurar el continuo rendimiento del SIGA.

Sin otro particular se dio finalizada la reunión.

4.3.2 Definir muestra de auditoría

Se evaluará la eficiencia del Sistema Integrado de Gestión Administrativa (SIGA) su base de datos y la documentación correspondiente del Gobierno Regional de La Libertad.

4.3.3 Planificar visitas, entrevistas y otros

La auditoría tendrá un plazo de 20 días laborales iniciando el 03/02/2020 y culminando el 28/02/2020 como se muestra en el siguiente cronograma de actividades:

▣ Auditoría del SIGA	20 días	lun 3/02/20	vie 28/02/20
▣ Planificación	4 días	lun 3/02/20	jue 6/02/20
Apertura de la auditoría	1 día	lun 3/02/20	lun 3/02/20
Elaborar CheckList	2 días	mié 5/02/20	jue 6/02/20
▣ Ejecución	11 días	vie 7/02/20	vie 21/02/20
Inicio de auditoría	1 día	vie 7/02/20	vie 7/02/20
Ejecutar Check List	2 días	lun 10/02/20	mar 11/02/20
Evaluar Interfaz de usuario	3 días	mar 11/02/20	jue 13/02/20
Evaluar Base de Datos	2 días	mié 12/02/20	jue 13/02/20
Evaluar documentación	3 días	jue 13/02/20	lun 17/02/20
▣ Informe	5 días	lun 24/02/20	vie 28/02/20
Elaborar Informe de auditoría	4 días	lun 24/02/20	jue 27/02/20
Elaborar Informe Gerencial	1 día	vie 28/02/20	vie 28/02/20

4.3.4 Artefactos para la auditoría

4.3.4.1 CheckList para evaluar la confiabilidad de la información (Objetivo 1.1 de COBIT)

Nro.	Pregunta	SI	NO	NA	OBSERVACIONES
1.	¿La información del SIGA es confiable para que el usuario realice sus labores?				
2.	¿Toda la información del SIGA es útil para los usuarios?				
3.	¿Existe información redundante en el SIGA?				
4.	¿El SIGA transmite la información de manera confiable a los usuarios?				
5.	¿El SIGA garantiza la seguridad de la información hasta que el usuario la solicite?				
6.	¿Existe un usuario que tiene acceso a 2 o más cuentas?				
7.	¿Cada usuario tiene una cuenta personal ?				
8.	¿Existe un documento el cual informe cuales son las labores de los usuarios?				

4.3.4.2 Entrevista respecto a las facilidades para el cumplimiento de sus tareas (Controles 1.3 y 3.1 de la ISO 25010 y Objetivo 1.1, 2.1, de COBIT)

- 1.- ¿El usuario realiza únicamente sus labores que le corresponden dentro del SIGA?
- 2.- ¿El usuario puede registrar información incompleta del SIGA?
- 3.- ¿El usuario tiene restricciones para acceder a la información del SIGA?
- 4.- ¿Se impide el acceso a cierto tipo de información del SIGA al usuario?
- 5.- ¿Los usuarios tienen acceso a todos los módulos del SIGA?

- 6.- ¿Los usuarios tienen acceso solo a los módulos que le corresponde?
7. ¿Los usuarios pueden registrar información en módulos que no le corresponde?
8. ¿Existe un reporte de todas las modificaciones de los usuarios en el día/semana/mes?

4.3.4.3 CheckList para evaluar la calidad y suficiente de la información (Control 1.1, 1.2 ,5.1 de la ISO 25010)

Nro.	Pregunta	SI	NO	NA	OBSERVACIONES
1.	¿La información obtenida del SIGA por el usuario es de calidad?				
2.	¿Los reportes de la información del SIGA cumplen las expectativas de los usuarios?				
3.	¿Se puede modificar o alterar la información del SIGA obtenida por el usuario?				
4.	¿Se puede eliminar la información obtenida por el usuario?				
5.	¿Los usuarios pueden acceder a información que no le concierne?				
6.	¿La información obtenida del SIGA es precisa?				
7.	¿Existen restricciones para que un usuario pueda eliminar la información?				
8.	¿Existen restricciones para que un usuario pueda modificar la información?				
9.	¿La información del SIGA es integra?				

4.3.4.4 Entrevista para evaluar la calidad de la información. (Objetivo 1.1,2.1,3.1 de COBIT)

1. ¿La información obtenida del SIGA por el usuario es siempre completa?
2. ¿La información del SIGA es registrada de acuerdo a los niveles y privilegios de los usuarios?
3. ¿El SIGA garantiza la información frente a errores?
4. ¿Los reportes de información del SIGA es precisa?

5. ¿La información dentro del SIGA siempre está disponible?
6. ¿La información obtenida por el usuario tiene la garantía de que no haya alterada?
7. ¿Existe un usuario con todos los niveles de acceso?
8. ¿Existe coherencia en los reportes de la información obtenida en el SIGA?

4.3.4.5 Entrevista para evaluar la eficiencia del SIGA (Control 2.1,2.2,2.3,5.1 de la ISO 25010)

1. ¿El tiempo de respuesta a alguna operación del SIGA están dentro de los parámetros permitidos?
2. ¿Los recursos utilizados del SIGA están dentro de los parámetros permitidos?
3. ¿El SIGA tiene la capacidad para que el usuario evite errores?
4. ¿El SIGA está operativo durante un tiempo estimado?
5. ¿El SIGA siempre está disponible para su acceso?
6. ¿Existe un límite para la cantidad de recursos que utiliza un usuario?
7. ¿El SIGA envía un mensaje de error cuando no se completó una operación?
8. ¿El SIGA se mantiene operativo mientras se le hace algún mantenimiento?
9. ¿El SIGA permite el acceso no autorizado a algún usuario?
10. ¿El SIGA tiene la capacidad de evitar el acceso y modificación a la información?
11. ¿El SIGA tiene un reporte de errores que han sucedido durante la labor diaria?
12. ¿El SIGA tiene un login para poder ingresar al sistema?
13. ¿En caso de un registro o alguna modificación accidental se puede recuperar el registro modificado?

14. ¿Cuándo hay una sobrecarga de información el SIGA deja de funcionar?
15. ¿El SIGA permite el acceso a múltiples usuarios?
16. ¿El SIGA es fácil de usar?

4.3.4.6 Evaluación de la disponibilidad del SIGA (Control 4.1, 4.2 ,4.3 de la ISO 25010)

1. Verificar que el SIGA esté disponible las 24 horas
2. Verificar paralizaciones dentro del SIGA
3. Verificar que el SIGA se mantenga ejecutándose frente a presencia de fallos
4. Verificar que el SIGA esté disponible durante un tiempo estimado
5. Verificar que el SIGA este disponible dentro del horario laboral

4.3.4.7 CheckList para evaluar la portabilidad del SIGA (Control 6.1 ,6.2 ,6.3 de la ISO 25010)

Nro.	Pregunta	SI	NO	NA	OBSERVACIONES
1	¿El SIGA puede ejecutarse en cualquier tipo PC´s?				
2	¿El SIGA puede ejecutarse en diferentes S.O?				
3	¿La instalación del SIGA es de manera fácil o sencilla?				
4	¿El SIGA puede ser reemplazado fácilmente por otro tipo de sistema de información?				
5	¿Existe un manual de instalación del SIGA?				
6	¿EL SIGA tiene algún requerimiento especial para su instalación?				

4.3.4.8 Evaluación de la Base de datos

Nro.	Pregunta	SI	NO	NA	OBSERVACIONES
1.	¿Están documentados las prácticas y procedimientos relativos a la Base de datos?				
2.	¿Está documentado la Configuración del Gestor de Base de Datos?				
3.	¿Se tiene conocimiento sobre la política de seguridad de la base de datos?				
4.	¿Está documentado la configuración del log de base de datos?				
5.	¿Se aplican políticas de seguridad al log de base de datos?				
6.	¿Tiene acceso al archivo log de la Base de Datos?				
7.	¿Tiene acceso como usuario al log base de datos?				
8.	¿Puede modificar o eliminar algún registro del archivo log?				
9.	¿Las operaciones que se realizan son registradas correctamente en el archivo log?				
10.	¿Existe algún procedimiento interno de tolerancia a fallos?				
11.	¿Los usuarios tienen conocimiento del plan de contingencia en caso de desastre?				
12.	¿Todas las personas tienen acceso total a la configuración del servidor?				
13.	¿Los usuarios solo tienen acceso a sus funciones correspondientes?				
14.	¿Se ha establecido en el sistema algún procedimiento de tolerancia a fallos de servidor?				
15.	¿Se tiene algún registro o log sobre las actividades realizadas?				
16.	¿Posee la base de datos un diseño físico y lógico?				
17.	¿Se cuenta con niveles de seguridad para el acceso a la Base de Datos?				
18.	¿Se registran en el sistema procedimientos de modificaciones y actualizaciones de la BD?				
19.	¿Existen controles programados para evitar el acceso no autorizado a la BD?				
20.	¿Existe un plan de contingencia para el sistema de BD?				
21.	¿Se realiza copias de seguridad (diariamente, semanalmente, mensualmente, etc.)?				
22.	¿Se renuevan las claves de los usuarios de la Base de Datos?				
23.	¿Existe algún usuario que tenga asignado el acceso total del servidor?				
24.	¿Se establecieron personas autorizadas por medio de permisos, que puedan modificar las BD?				

4.4 Ejecución.

4.4.1 Evaluar las interfaces de usuario, reportes y otros

4.4.1.1 CheckList para evaluar la confiabilidad de la información (Objetivo 1.1 de COBIT)

Nro.	Pregunta	SI	NO	NA	OBSERVACIONES
1.	¿La información del SIGA es confiable para que el usuario realice sus labores?	X			
2.	¿Toda la información del SIGA es útil para los usuarios?	X			
3.	¿Existe información redundante en el SIGA?		X		
4.	¿El SIGA transmite la información de manera confiable a los usuarios?	X			
5.	¿El SIGA garantiza la seguridad de la información hasta que el usuario la solicite?		X		
6.	¿Existe un usuario que tiene acceso a 2 o más cuentas?		X		
7.	¿Cada usuario tiene una cuenta personal?	X			
8.	¿Existe un documento el cual informe cuales son las labores de los usuarios?		X		

Comentario:

Se puede verificar que no existe información redundante y que si es confiable para los usuarios a excepción de no existe un documento de las funciones que deben realizar los usuarios.

4.4.1.2 Entrevista respecto a las facilidades para el cumplimiento de sus tareas (Controles 1.3 y 3.1 de la ISO 25010 y Objetivo 1.1 y 2.1 de COBIT)

1. ¿El usuario realiza únicamente sus labores que le corresponden dentro del SIGA?

Según el jefe inmediato le indica las labores específicas que debe de realizar.

2. ¿El usuario puede registrar información incompleta del SIGA?

Actualmente no se pueden registrar campos vacíos.

3. ¿El usuario tiene restricciones para acceder a la información del SIGA?

No tiene ninguna restricción, solo necesita su usuario y contraseña

4. ¿Se impide el acceso a cierto tipo de información del SIGA al usuario?

Una vez que ingresa con sus credenciales ya tiene el acceso a todos los módulos del SIGA.

5. ¿Los usuarios tienen acceso a todos los módulos del SIGA?

Si

6. ¿Los usuarios tienen acceso solo a los módulos que le corresponde?

El usuario que ingresa al SIGA tiene acceso a todos los módulos.

7. ¿Los usuarios pueden registrar información en módulos que no le corresponde?

Por el motivo de que los usuarios tienen acceso a todos los módulos es posible que registre data en módulos que no le corresponde.

8. ¿Existe un reporte de todas las modificaciones de los usuarios en el día/semana/mes?

No extraemos reporte de las modificaciones que hacen los usuarios.

Comentario:

Se puede verificar que el SIGA cuenta con un Login y una vez dentro todos los usuarios tienen acceso a todos los módulos sin restricciones y no existen un reporte de la modificación que hacen los usuarios. Actualmente no se registran campos vacíos de información.

4.4.1.3 CheckList para evaluar la calidad y suficiente de la información. (Control 1.1, 1.2 ,5.1 de la ISO 25010)

Nro.	Pregunta	SI	NO	NA	OBSERVACIONES
1.	¿La información obtenida del SIGA por el usuario es de calidad?	X			
2.	¿Los reportes de la información del SIGA cumplen las expectativas de los usuarios?	X			
3.	¿Se puede modificar o alterar la información del SIGA obtenida por el usuario?	X			
4.	¿Se puede eliminar la información obtenida por el usuario?	X			
5.	¿Los usuarios pueden acceder a información que no le concierne?	X			
6.	¿La información obtenida del SIGA es precisa?	X			
7.	¿Existen restricciones para que un usuario pueda eliminar la información?	X			
8.	¿Existen restricciones para que un usuario pueda modificar la información?	X			
9.	¿La información del SIGA es íntegra?	X			

Comentario:

Se puede verificar que todos los usuarios tienen acceso a toda la información del SIGA y puede alterar información (Modificar o eliminar) en módulos que no le corresponden.

4.4.1.4 Entrevista para evaluar la calidad de la información. (Objetivo 1.1, 2.1 y 3.1 de COBIT)

1. ¿La información obtenida del SIGA por el usuario es siempre completa?
Los reportes de información mayormente siempre son completos debido a que en años anteriores la información no se registraba completamente.
2. ¿La información del SIGA es registrada de acuerdo a los niveles y privilegios de los usuarios?

Por el momento los usuarios no tienen asignados el tipo de privilegio que le corresponde.

3. ¿El SIGA garantiza la información frente a errores?
Si, a excepción cuando hay cortes de energía.
4. ¿Los reportes de información del SIGA es precisa?
Si, los reportes consultados por los usuarios son precisos.
5. ¿La información dentro del SIGA siempre está disponible?
El SIGA está disponible las 24 horas del día.
6. ¿La información obtenida por el usuario tiene la garantía de que no haya alterada?
No se ha tenido ningún inconveniente con la información.
7. ¿Existe un usuario con todos los niveles de acceso?
El usuario Administrador tiene un control total del SIGA.
8. ¿Existe coherencia en los reportes de la información obtenida en el SIGA?
Si, en caso el usuario desee agregar algún campo adicional, se le implementa.

Comentario:

Se puede verificar que la información está disponible las 24 horas del día a excepción cuando hay cortes de energía, los reportes y registros de información no son completos y pueden ser alteradas. Los reportes de información son específicos y coherentes, pero no existen privilegios o niveles al acceder a la información

4.4.1.5 Entrevista para evaluar la eficiencia del SIGA (Control 2.1, 2.2, 2.3 y 5.1 de la ISO 25010)

1. ¿El tiempo de respuesta a alguna operación del SIGA están dentro de los parámetros permitidos?
2. No se ha medido el tiempo de respuesta de las operaciones dentro del SIGA.
3. ¿Los recursos utilizados del SIGA están dentro de los parámetros permitidos?
4. No se ha medido los recursos que utiliza el SIGA.
5. ¿El SIGA tiene la capacidad para que el usuario evite errores?
6. El SIGA tiene alertas en caso de que falten campos o le falte alguna operación por completar.
7. ¿El SIGA está operativo durante un tiempo estimado?
8. Está disponible las 24 horas
9. ¿El SIGA siempre está disponible para su acceso?
10. Siempre está disponible para los usuarios.
11. ¿Existe un límite para la cantidad de recursos que utiliza un usuario?
12. No se ha establecido límites en la utilización de recursos.
13. ¿El SIGA envía un mensaje de error cuando no se completó una operación?
14. Si, se muestra un mensaje de alerta indicando la operación faltante.
15. ¿El SIGA se mantiene operativo mientras se le hace algún mantenimiento?
16. No, se paraliza las actividades dentro del GRL
17. ¿El SIGA permite el acceso no autorizado a algún usuario?
18. El SIGA tiene implementado un inicio de sesión para su acceso.
19. ¿El SIGA tiene la capacidad de evitar el acceso y modificación a la información?
20. La información está disponible para todos los usuarios, en caso de las modificaciones, se muestra una alerta al usuario si está seguro de modificar la información.

21. ¿El SIGA tiene un reporte de errores que han sucedido durante la labor diaria?
22. No se ha implementado un reporte de errores dentro SIGA.
23. ¿El SIGA tiene un Login para poder ingresar al sistema?
24. Si, cuenta con un inicio de sesión.
25. ¿En caso de un registro o alguna modificación accidental se puede recuperar el registro modificado?
26. No, se tendría que verificar los documentos en físico para volver a modificarlos.
27. ¿Cuándo hay una sobrecarga de información el SIGA deja de funcionar?
28. No ha sucedido alguna sobrecarga de energía, pero si hubo corte de energía anteriormente.
29. ¿El SIGA permite el acceso a múltiples usuarios?
30. El SIGA es multiusuario
31. ¿El SIGA es fácil de usar?
32. Se capacita a los a usuarios el SIGA para que sea más fácil su uso

Comentario:

Se pudo verificar que el SIGA cuenta con un control de acceso (Login) y está disponible las 24 horas del día y es multiusuario, no se ha medido valores en tiempo de respuesta y los recursos que utiliza el SIGA, no se ha asignado un límite de recursos que puede ser utilizado por un usuario. En caso hay un mantenimiento las labores se suspenden momentáneamente y no existe un informe de errores del SIGA. Existen alertas cuando el usuario desea registrar información incompleta y se capacita a los usuarios para utilizar SIGA.

4.4.1.6 Evaluación de la disponibilidad del SIGA (Control 4.1, 4.2 y 4.3 de la ISO 25010)

1. Verificar que el SIGA esté disponible las 24 horas
Se pudo verificar que el SIGA está disponible las 24 horas del día.

2. Verificar paralizaciones dentro del SIGA
Se observaron paralizaciones en los registros y en los reportes de la información.
3. Verificar que el SIGA se mantenga ejecutándose frente a presencia de fallos
Se observó que a pesar de las paralizaciones o lentitud el SIGA se ejecutaba normalmente.
4. Verificar que el SIGA esté disponible durante un tiempo estimado
El SIGA estuvo disponible dentro del tiempo establecido.
5. Verificar que el SIGA este disponible dentro del horario laboral
El SIGA estuvo disponible dentro del horario laboral.
6. Verificar Registro completos
Se observó que no todos los registros estuvieron completos.

Comentario:

Se pudo verificar que todos los registros no están completos y que a pesar de existir lentitud y paralizaciones al consultar reportes de información el SIGA sigue ejecutándose dentro del horario laboral con normalidad.

**4.4.1.7 CheckList para evaluar la portabilidad del SIGA
(Control 6.1, 6.2 y 6.3 de la ISO 25010)**

Nro	Pregunta	SI	NO	NA	OBSERVACIONES
1	¿El SIGA puede ejecutarse en cualquier tipo PC´s?	X			
2	¿El SIGA puede ejecutarse en diferentes SO?	X			
3	¿La instalación del SIGA es de manera fácil o sencilla?	X			
4	¿El SIGA puede ser reemplazado fácilmente por otro tipo de sistema de información?		X		
5	¿Existe un manual de instalación del SIGA?		X		
6	¿EL SIGA tiene algún requerimiento especial para su instalación?		X		

Comentario:

Se pudo verificar que el SIGA no cuenta con un manual de instalación y puede ejecutarse e instalarse en todo tipo de PC's y sistemas operativos. No tiene un requerimiento especial para su instalación.

4.4.2 Evaluar Base de datos

Nro.	Pregunta	SI	NO	NA	OBSERVACIONES
1.	¿Están documentados las prácticas y procedimientos relativos a la Base de datos?	X			
2.	¿Está documentado la Configuración del Gestor de Base de Datos?	X			
3.	¿Se tiene conocimiento sobre la política de seguridad de la base de datos?		X		
4.	¿Está documentado la configuración del log de base de datos?		X		
5.	¿Se aplican políticas de seguridad al log de base de datos?		X		
6.	¿Tiene acceso al archivo log de la Base de Datos?	X			
7.	¿Tiene acceso como usuario al log base de datos?	X			
8.	¿Puede modificar o eliminar algún registro del archivo log?	X			
9.	¿Las operaciones que se realizan son registradas correctamente en el archivo log?	X			
10.	¿Existe algún procedimiento interno de tolerancia a fallos?		X		
11.	¿Los usuarios tienen conocimiento del plan de contingencia en caso de desastre?		X		
12.	¿Todas las personas tienen acceso total a la configuración del servidor?		X		
13.	¿Los usuarios solo tienen acceso a sus funciones correspondientes?		X		
14.	¿Se ha establecido en el sistema algún procedimiento de tolerancia a fallos de servidor?		X		
15.	¿Se tiene algún registro o log sobre las actividades realizadas?		X		
16.	¿Posee la base de datos un diseño físico y lógico?	X			
17.	¿Se cuenta con niveles de seguridad para el acceso a la Base de Datos?	X			

Nro.	Pregunta	SI	NO	NA	OBSERVACIONES
18.	¿Se registran en el sistema procedimientos de modificaciones y actualizaciones de la BD?	X			
19.	¿Existen controles programados para evitar el acceso no autorizado a la BD?		X		
20.	¿Existe un plan de contingencia para el sistema de BD?		X		
21.	¿Se realiza copias de seguridad (diariamente, semanalmente, mensualmente, etc.)?	X			SEMANALMENTE
22.	¿Se renuevan las claves de los usuarios de la Base de Datos?	X			Cada 3 meses
23.	¿Existe algún usuario que tenga asignado el acceso total del servidor?	X			
24.	¿Se establecieron personas autorizadas por medio de permisos, que puedan modificar las BD?		X		

Comentario:

Se puede verificar que todas las operaciones que se realizan en la base de datos son registradas en los archivos log correctamente las cuales pueden ser limpiadas o eliminadas y existe documentación para los procedimientos de la base de datos. La base de datos cuenta con diseño físico y lógico en la documentación y no se ha establecido algún control de tolerancia a fallos.

Las backups se realizan semanalmente.

4.4.3 Evaluar la documentación

Se tomó conocimiento del Gobierno Regional de La Libertad cuenta con manuales digitales del Sistema Integrado de Gestión Administrativa (SIGA) y de su base de datos (BD_GRLL)

4.4.3.1 Manual de usuario SIGA

Se evaluó el manual de usuario del SIGA para los trabajadores del Gobierno Regional de La Libertad que contiene los siguientes 5 capítulos:

1. Ingreso al SIGA.
2. Generación de pedidos de compra/servicios.
3. Modificación de registros cargados.
4. Eliminación de registros cargados.
5. Consultas y reportes.

I. INGRESO AL SIGA

1. En la pantalla de su escritorio, se visualizará el icono del acceso directo al sistema SIGA

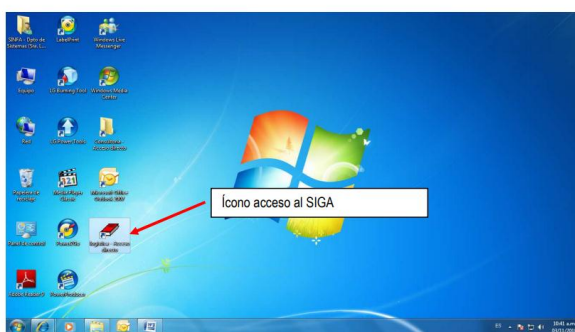


Figura N° 2: Manual para la generación de pedidos por centro de costo del SIGA
Fuente : (GRLL, 2016)

Comentario:

En el manual se verificó que información esta detallada para cada de las operaciones que deben de seguir los usuarios.

El manual no está actualizado ya que es del año 2016.

4.4.3.2 Manual BD_GRLL v2

Se evaluó el manual cuyo nombre es BD_GRLL V2, el cual instruye la nomenclatura de la base de datos del Gobierno Regional de La Libertad.

El manual muestra cómo están y como deberían ser creadas las:

- a. Base de datos.
- b. Tablas.
- c. Campos.
- d. Constrains.
- e. Indexes.
- f. Stored Procedures.

Comentario:

Se verificó que el manual cuenta con información detallada paso a paso de cómo realizar las operaciones dentro del gestor de base de datos siguiendo un formato detallado y específico.

El manual esta es del año 2015

4.5 Informes.

4.5.1 Elaborar informe de auditoria

4.5.1.1 Aspectos Positivos.

Al desarrollar la Auditoria en el Gobierno Regional de La Libertad se pudo evidenciar el uso de buenas prácticas para el buen funcionamiento del SIGA, que son las siguientes:

Datos e Información

1. La información que se encuentra almacenada en el Sistema Integrado de Gestión Administrativa (SIGA) es confiable y no es redundante (Repetido) para los usuarios.
2. Los reportes de información del Sistema Integrado de Gestión Administrativa (SIGA) son precisos y coherentes cumpliendo las expectativas de los usuarios.
3. La Información del SIGA está disponible las 24 horas del día.
4. El jefe inmediato brinda una capacitación para realizar las labores específicas dentro del Gobierno Regional de La Libertad, evitando errores laborales humanos al registrar o alterar información.

SIGA

5. El Sistema Integrado de Gestión Administrativa (SIGA) está disponible las 24 horas del día, cuenta con un control de acceso (LOGIN) para poder ingresar y cada usuario cuenta con una sola cuenta.
6. El SIGA envía alertas o mensajes indicándole al usuario que una transacción no está completa.

7. Se muestran al usuario mensajes o alertas al tratar de modificar o eliminar registros de información y soporta múltiples usuarios conectados simultáneamente.
8. Se cuenta con un manual de usuario el cual permite su fácil funcionamiento.

Base de Datos.

9. El Administrador de la Base de Datos es el único que tiene acceso a todas las acciones dentro del Gestor de base de datos (SQL Server).
10. Se estableció niveles de acceso para los usuarios de la base de datos y sus contraseñas se renuevan cada 3 meses.
11. La base de datos cuenta con un diseño físico y lógico
12. Todas las operaciones que se realizan dentro del Sistema integrado de Gestión Administrativo (SIGA) se encuentran registrados en los archivos Log de la Base de datos.
13. Los Backup (Copias de seguridad) se realizan semanalmente.

Manuales

14. Se tiene un manual para la aplicación del SIGA que es del año 2016 que aún sigue vigente, el formato esta de forma digital con información para realizar las labores diarias.

15. También existe un manual de la base de datos y su nomenclatura que es del año 2015 y aún sigue vigente, Cuenta con información detallada para realizar las diferentes operaciones dentro de la base de datos.

4.5.1.2 Aspectos Negativos.

A. Observación 1 “Los usuarios tienen acceso a módulos que no le corresponde, generando el riesgo de pérdida de confidencialidad de información de distintas áreas.”

Artefacto utilizado: CheckList y Observación.

a. Criterio

Norma de Control Interno, ISO25010 “Calidad de Productos de software” control 1.3 “Pertinencia Funcional” cuyo propósito es “Permite que los usuarios específicos realicen sus tareas de acuerdo a sus funciones correspondientes” y COBIT 2019 en el control 1.1 “Controlar el procesamiento de la información” cuyo propósito es “Permite que el usuario obtenga solo la información que le corresponde.” control 2.1 “Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización” cuyo propósito es “Permite que el usuario tenga restricciones y privilegios al acceder a la información”

b. Causas

Los hechos encontrados se debieron a:

- No se validaron restricciones a los usuarios.
- No se validó el SIGA cuando fue desarrollado.

c. Efectos

La información seguirá no siendo confidencial para los usuarios dentro del Gobierno Regional de La Libertad.

B. Observación 2 “Los reportes de información contiene información incompleta, generando el riesgo de pérdida de confiabilidad de la información”

Artefacto utilizado: Entrevista y Observación.

a. Criterio

Normas de Control Interno, COBIT 2019 en el control 1.1 “Controlar el procesamiento de la información” cuyo propósito es “Permite que la información procesada sea completa, precisa y segura.” y ISO 25010 “Calidad de Producto de software” control 1.1 “Complejidad Funcional” cuyo propósito es “Permite que el usuario asegure que la información sea confiable y de calidad”

b. Causas

Los hechos encontrados se debieron a:

- No se validaron los datos al guardar información dentro del SIGA.
- Escasa capacitación de los usuarios.
- No se validó el SIGA cuando fue desarrollado.

c. Efectos

Los reportes de información no serán confiables para los usuarios.

C. **Observación 3** “Los usuarios no cuentan con privilegios para acceder a la información, generando un posible robo de información de módulos que no lo corresponden”

Artefacto utilizado: Entrevista y Observación.

a. Criterio

Norma de Control Interno, COBIT 2019 en el control 1.1 “Controlar el procesamiento de la información” cuyo propósito es “Permite que la información procesada sea confiable, precisa y segura” y en la ISO 25010 “Calidad de Producto de Software” en el control 1.2 “Información y responsabilidad” cuyo propósito es “Permite que la información proporcionada sea correcta y segura”

b. Causas

Los hechos encontrados se debieron a:

- No se asignaron privilegios a los usuarios.
- No se cuenta con restricciones dentro del SIGA

c. Efectos

Posible robo de información de distintas áreas del Gobierno Regional de La Libertad.

D. **Observación 4** “La información puede alterarse por los usuarios de distintas áreas, generando pérdida de integridad de información y produciendo reportes dudosos”

Artefacto utilizado: Entrevista y Observación.

a. Criterio

Normas de Control Interno, COBIT 2019 en el control 2.1 “Gestionar Roles, responsabilidades,

privilegios de acceso y niveles de autorización” cuyo propósito es “Permite que el usuario tenga restricciones y privilegios al acceder a la información” y “Permite que la información sea registrada de acuerdo a los niveles y privilegios” y en la ISO 25010 “Calidad de Producto de Software” en el control 5.1 “Integridad” cuyo propósito es “Permite que la información sea alterada.”

b. Causas

Los hechos encontrados se debieron a:

Sin privilegios de acceso a la información de los usuarios.

Si restricciones asignadas a los usuarios.

No se validó el SIGA cuando fue desarrollado.

c. Efectos

Toda información seguirá siendo visible a todos los usuarios.

Posible alteración en módulos que no le corresponde a los usuarios.

E. **Observación 5** “La información no cuenta con un historial de modificaciones que han realizado los usuarios, generando pérdida de la confiabilidad y exactitud de la información.”

Artefacto utilizado: Entrevista y Observación.

a. Criterio

Normas de Control Interno, COBIT 2019 en el control 1.1 “Controlar el procesamiento de la información” cuyo propósito es “permite que la información sea confiable para que el usuario realice sus labores” y la ISO 25010 “Calidad de

Producto de software” en el control 1.1 “Permite que el usuario asegure la información sea confiable y de calidad”

b. Causas

Los hechos encontrados se debieron a:

No se implementó un historial de modificaciones de información de los usuarios.

c. Efectos

No se tiene conocimientos de la alteración de información de los usuarios dentro del SIGA.

Posible pérdida de confiabilidad de información.

F. **Observación 6** “Los tiempos de respuestas de cada operación no han sido calculados, generando tiempo muerto en las labores diarias.”

Artefacto utilizado: Entrevista y Observación.

a. Criterio

Normas de Control Interno, ISO 25010 “Calidad de Producto de Software” control 2.1 “Comportamiento Temporal” cuyo propósito es “Permite verificar el procesamiento, rendimiento y tiempos de respuesta de los Sistemas de Información”

b. Causas

Los hechos encontrados se debieron a:

- No se realizó un diagnóstico de los tiempos de respuesta de las operaciones dentro del SIGA.
- No se establecieron límites de tiempo en las operaciones.

c. Efectos

Tiempos muertos en las labores diarias y deficiencia en las operaciones que realizan los usuarios.

G. Observación 7 “Los recursos que utiliza el SIGA no han sido medidos, generando el riesgo de bajo rendimiento de las transacciones diarias.”

Artefacto utilizado: Entrevista y Observación.

a. Criterio

Normas de Control Interno, ISO 25010 “Calidad de Producto de Software” en el control 2.2 “Utilización de recursos” cuyo propósito es “Permite diagnosticar los recursos que utiliza el sistema de información”

b. Causas

Los hechos encontrados se debieron a:

- No se establecieron límites en los recursos que utiliza el SIGA.
- No se validó el SIGA en base a los recursos utilizados.

c. Efectos

Bajo rendimiento en las operaciones diarias de los usuarios.

Posible lentitud en las operaciones diarias.

H. Observación 8 “El mantenimiento que se realiza al SIGA paraliza las labores, generando un riesgo de pérdida de eficiencia de los usuarios en sus labores.”

Artefacto utilizado: Entrevista y Observación.

a. Criterio

Normas de Control Interno , ISO 25010 “Calidad de Producto de Software” en el control 4.2 “Disponibilidad” cuyo propósito es “Permite que el sistema de información siempre esté disponible”

b. Causas

Los hechos encontrados se debieron a:

No se previó futuros mantenimientos del SIGA.

No se establecieron condiciones de mantenimiento dentro del SIGA

c. Efectos

Baja eficiencia de los usuarios en sus labores diarias.

Tiempo muerto en las labores diarias.

I. **Observación 9** “El SIGA carece de un historial de reportes de errores, generando un riesgo de pérdida de eficiencia del SIGA”

Artefacto utilizado: Entrevista y Observación.

a. Criterio

Normas de Control Interno, ISO 25010 “Calidad de Producto de Software” en el control 4.3 “Tolerancia a fallos” cuyo propósito es “Permite que el sistema de información continúe ejecutándose frente a la presencia de fallos”

b. Causas

Los hechos encontrados se debieron a:

- No se implementó un historial de errores fallas de los usuarios dentro del SIGA

c. Efectos

No se tiene conocimiento de las fallas en las labores diarias de los usuarios dentro del SIGA.

Posible pérdida de la eficiencia del SIGA.

J. Observación 10 “La presencia de lentitud y paralizaciones al registrar y extraer reportes de información, generan riesgo de pérdida de la disponibilidad del SIGA”

Artefacto utilizado: Entrevista y Observación.

a. Criterio

Normas de Control Interno, ISO 25010 “Calidad de Producto de Software” control 4.2 “Disponibilidad” cuyo propósito es “Permite que el sistema de información siempre esté disponible” y control 4.3 “Tolerancia a fallos” cuyo propósito es “Permite que el Sistema de información continúe ejecutándose a la presencia de fallos”

b. Causas

Los hechos encontrados se debieron a:

- No se realizan mantenimientos constantes.
- No se establecieron límites en los recursos que utiliza el SIGA.

c. Efectos

Pérdida de parcial de la disponibilidad del SIGA y de la oportunidad de información de los usuarios.

Bajo rendimiento laboral de los usuarios.

K. Observación 11 “Documentación inexistente de la configuración de Log de la base de datos, generando riesgo de pérdida de registro de las transacciones que se realizan.”

Artefacto utilizado: CheckList y Observación.

a. Criterio

Normas de Control Interno, ISO 25010 “Calidad de Producto de Software” en el control 5.1 “Integridad” cuyo propósito es “Permite evitar el acceso y modificaciones sin tener los privilegios correspondientes.” y de COBIT 2019 en el control 1.1 “Controlar el procesamiento de la información” cuyo propósito es “Permite que la información sea confiable para que el usuario realice sus labores”

b. Causas

Los hechos encontrados se debieron a:

- No existen documentos para la configuración o mantenimientos de las transacciones de los usuarios.

c. Efectos

Perdida de la credibilidad de la Información

Posible pérdida del registro de transacciones de la BD.

L. **Observación 12** “Políticas de seguridad de la base de datos sin establecer, generando riesgo de pérdida y difusión de información”

Artefacto utilizado: CheckList y Observación.

a. Criterio

Normas de Control Interno, COBIT 2019 en el control 1.1 “Controlar el procesamiento de información” cuyo propósito es “Permite que la información procesada sea completa, precisa y segura” y del control 2.1 “Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización” cuyo propósito es

“Permite que el usuario tenga restricciones y privilegios al acceder a la información” y
“Permite que la información sea registrada de acuerdo a los niveles y privilegios”

b. Causas

Los hechos encontrados se debieron a:

- No se establecieron políticas de seguridad a la Base de datos.

c. Efectos

Posible pérdida o robo de la información.

Posible difusión de información confidencial.

M. Observación 13 “Mala asignación de privilegios a los usuarios de la base de datos, generando riesgo de pérdida de integridad y confidencialidad de la información.”

Artefacto utilizado: CheckList y Observación.

a. Criterio

Normas de Control Interno, COBIT 2019 control 2.1 “Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización” cuyo propósito es “Permite que el usuario tenga restricciones y privilegios a acceder a la información” y en la ISO 25010 “Calidad de Producto de Software” en el control 5.1 “Integridad” cuyo propósito es “Permite que la información sea alterada”

b. Causas

Los hechos encontrados se debieron a:

No se asignaron correctamente privilegios y restricciones a los usuarios.

No se capacito al personal.

c. Efectos

La información no es confidencial.

Posible pérdida de la integridad de la información.

N. **Observación 14** “Plan de contingencia inexistente de la base de datos, generando pérdida del restablecimiento del correcto funcionamiento de la base de datos”

Artefacto utilizado: CheckList y Observación.

a. Criterio

Normas de Control Interno, COBIT 2019 en el control 3.1 “Gestionar errores y excepciones” cuyo propósito es “Permite asegurar la garantía de la información frente a errores.”

b. Causas

Los hechos encontrados se debieron a:

- No se estableció un plan de contingencia a la Base de datos.
- Falta de capacitación.

c. Efectos

Pérdida total o parcial de la información.

4.5.2 Elaborar informe gerencial

Se realizó un diagrama de Ishikawa (Causa/Efecto)

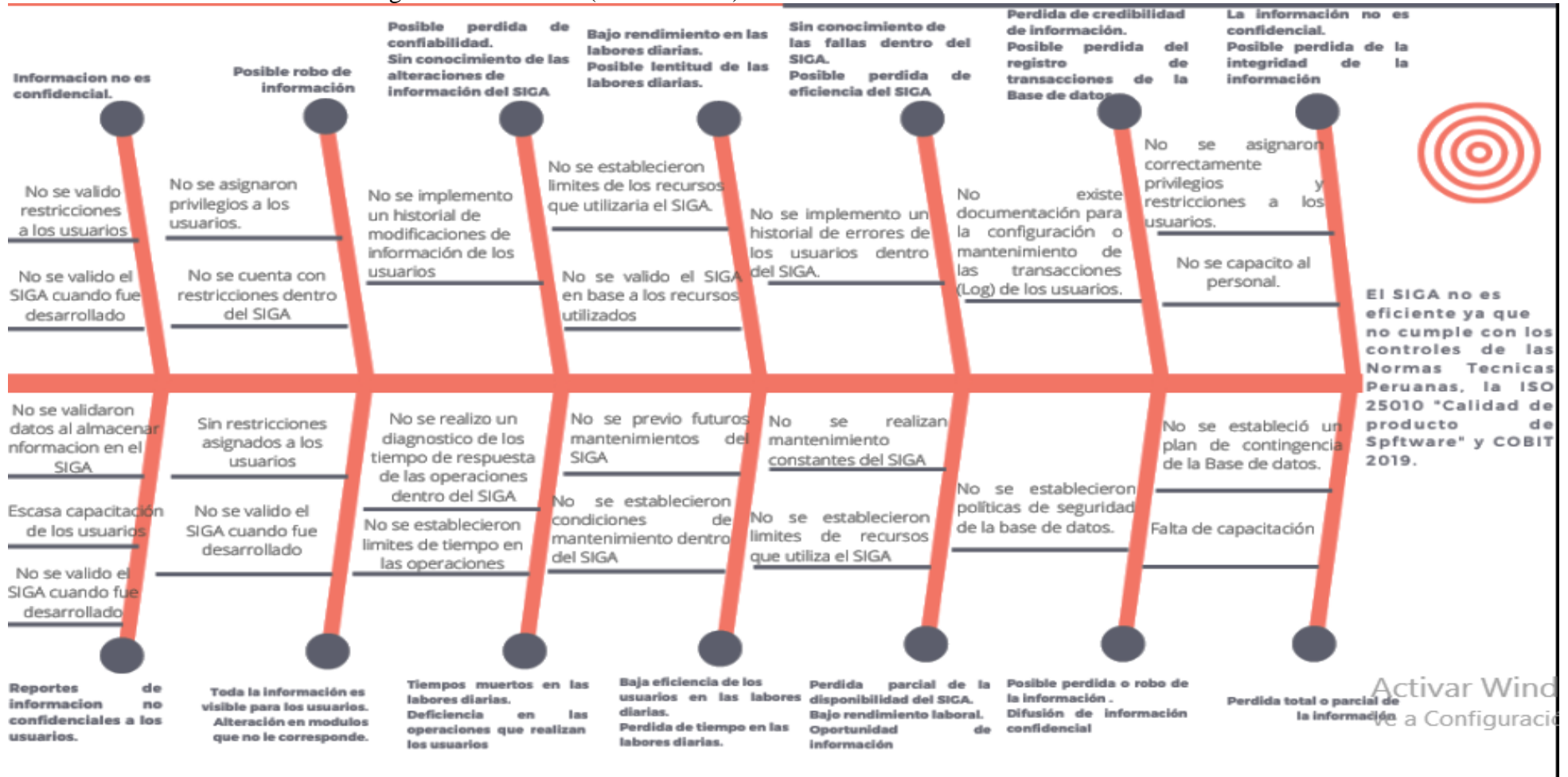


Figura N°3: Diagrama Ishikawa
Fuente: Propia(Hecho en canvas.com) [Visitar](#)

4.5.3 Cierre de la auditoria

Se dio por finalizada la auditoria del Sistema Integrado de Gestión Administrativa (SIGA) agradeciendo por su compromiso, buen ambiente de trabajo y colaboración de los trabajadores dentro del Gobierno Regional de La Libertad para llevar a cabo una eficiente auditoria en el cual se utilizaron: (NCI) Normas de control interno , ISO 25010 “Calidad de Producto de software” y COBIT 2019.

Se brindó lo siguiente:

- Hallazgos Positivos
- Hallazgos Negativos(Observaciones)
- Recomendaciones
- Conclusiones

Se fijó la fecha de entrega del informe de auditoría y aceptando los resultados brindados mediante la auditoria se dio por finalizada la auditoria de Sistema Integrado de Gestión Administrativa.

V. DISCUSIÓN DE LOS RESULTADOS

Del capítulo anterior, las observaciones (no conformidades) por artefacto de auditoría son los siguientes:

Tabla N°4: No conformidades por artefacto

Artefacto	No conformidades	Porcentaje
Entrevista	7	50%
Checklist	4	29%
Pruebas	3	21%
Total:	14	100%



Figura N°4: No conformidades por artefacto

Respecto a las normas y buenas prácticas, los resultados son:

Tabla 5: Cantidad de Observaciones por normas y buenas practicas

Observación	NCI	ISO 25010	COBIT
Observación 1	SI	SI	SI
Observación 2	SI	SI	SI
Observación 3	SI	SI	SI
Observación 4	SI	SI	SI
Observación 5	SI	SI	SI
Observación 6	SI	SI	NO
Observación 7	SI	SI	NO
Observación 8	SI	SI	NO
Observación 9	SI	SI	NO
Observación 10	SI	SI	NO
Observación 11	SI	SI	SI
Observación 12	SI	NO	SI
Observación 13	SI	SI	SI
Observación 14	SI	NO	SI
Total	14	12	9

Respecto al cuadro anterior se analiza que :

Tabla 6: Cantidad de normas y buenas practicas

CONTROL	CANTIDAD	PORCENTAJE(%)
NCI	14	40%
ISO 25010	12	34%
COBIT	9	26%
TOTAL	35	100

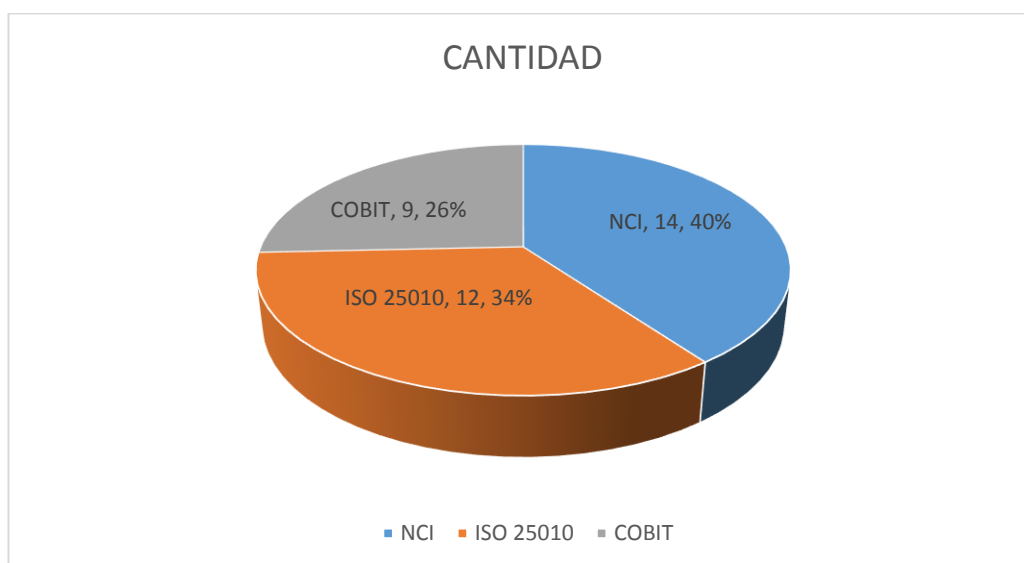


Figura N°5: Cantidad de normas y buenas practicas

Respecto a la eficiencia, los resultados son:

Conformidades=Aspectos Positivos(Página 57)

No Conformidades= Aspectos Negativos(Página 59)

Tabla N°7: Evaluación de la eficiencia

Artefacto	Conformidades	No conformidades
Entrevista	4	7
Checklist	7	4
Pruebas	4	3
Total	15	14
Total(%)	52%	48%

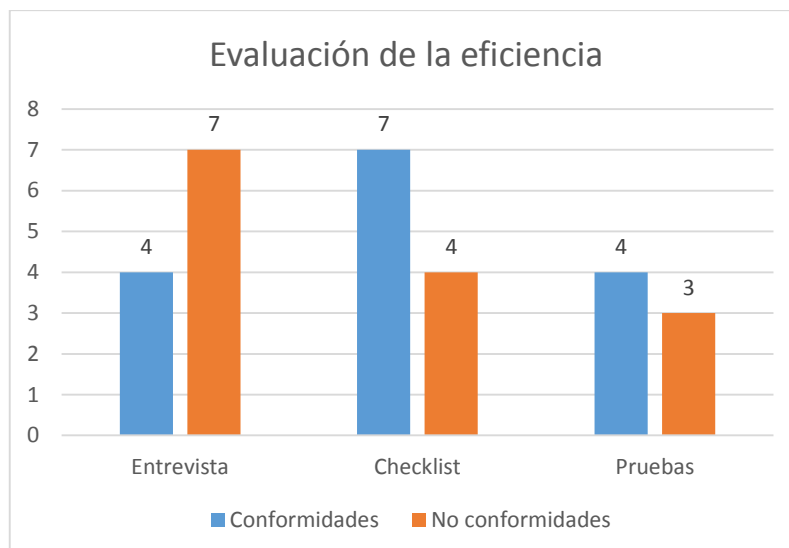


Figura N°6: Evaluación de la Eficiencia

En base a lo anterior, el nivel de aprobación de la eficiencia del SIGA es del 52% y según la Tabla N° 3 (Página 37), la calificación obtenida es MALA.

Para mejorar la calificación del SIGA se recomienda lo siguiente:

- a. Restringir acceso a módulos que no le corresponde a los usuarios
- b. Validar los campos para el registro de la información.
- c. Asignar privilegios de acceso a los usuarios.
- d. Implementar un historial de modificaciones de los usuarios.
- e. Asignar los tiempos de respuesta moderados para cada operación dentro del SIGA.
- f. Establecer límites en los recursos que utiliza el SIGA
- g. Elaborar políticas de seguridad y plan de contingencia de la base de datos .

VI. CONCLUSIONES.

1. El diseño del modelo para auditar permite una fácil evaluación de la eficiencia del sistema de información.
2. Al diseñar el modelo de auditoría para evaluar la eficiencia del Sistema Integrado de Gestión Administrativa (SIGA), de manera fácil se identificaron TRES (03) indicadores de eficiencia: % de errores, Tiempo promedio de paralizaciones, integridad de datos.
3. Al aplicar el modelo de auditoría la eficiencia del Sistema Integrado de Gestión Administrativa (SIGA) dentro del Gobierno Regional de La Libertad, obtuvo una calificación del 52%. Esto significa que el SIGA no está siendo usado de manera correcta por los usuarios.

VII. RECOMENDACIONES

Informatizar el proceso de auditoría para evaluar la eficiencia del Sistema Integrado De Gestión Administrativa (SIGA).

Realizar una auditoria anualmente para mantener y/o aumentar la eficiencia del Sistema Integrado de Gestión Administrativa (SIGA) y la Base de Datos del Gobierno Regional de La Libertad.

Impartir conocimientos a los trabajadores sobre la auditoria de sistemas para futuras auditorias.

VIII. REFERENCIAS BIBLIOGRAFICAS

- Admin. (02 de Septiembre de 2016). *GESTION CALIDAD Consulting*. Obtenido de <http://gestion-calidad.com/seguridad-informacion>
- Alejo, D. (2017). *MODELOS DE AUDITORIA PARA EL MEJORAMIENTO DEL SISTEMA DE CONTROL INTERNO DE INSTITUCIONES FINANCIERAS EN COLOMBIA BASADO EN LINEAMIENTOS DE LA LEY SARBANES OXLEY SECCION 404*. Colombia.
- Antúnez, Y. (2015). *Garantia de calidad de software*. Bogota.
- Arroyo, S. O. (20 de Julio de 2015). *Gestiopolis*. Obtenido de Web profit ltda: <https://www.gestiopolis.com/sistemas-de-informacion-y-organizacion/>
- Avelar Galdamez, J., Rosa Palacios, K., & Minero Cuchilla, K. (2019). *PROPUESTA DE LINEAMIENTOS PARA EJECUTAR UNA AUDITORÍA DE SISTEMAS CON IMPLEMENTACIÓN COBIT 5, PARA LAS COOPERATIVAS DE AHORRO Y CRÉDITO DEL DEPARTAMENTO DE SAN VICENTE*. El Salvador.
- Consulting, C. I. (2019). *Cloudcorp IT Consulting*. Obtenido de Cloudcorp IT Consulting: <https://www.cloudcorp.com.ec/estandares-de-si>
- Contraloria General de la Republica. (23 de Enero de 2019). *El Peruano*. Obtenido de El Peruano: <https://busquedas.elperuano.pe/normaslegales/aprueban-la-estructura-organica-y-el-reglamento-de-organizac-resolucion-n-030-2019-cg-1734670-1/>
- Couto, L. L. (2019). *Auditoria del sistema APPCC*. ESPAÑA: Ediciones Díaz de Santos.
- EEE. (2 de Noviembre de 2015). *Escuela Europea de Excelencia*. Obtenido de ESCUELA EUROPEA DE EXCELENCIA: <https://www.escuelaeuropeaexcelencia.com/2015/11/norma-iso-19011-principios-de-auditoria/>
- Excentia. (18 de Abril de 2018). *ISO 25000 La calidad del producto software*. Obtenido de ISO 25000: La calidad del producto software: <https://www.excentia.es/iso-25000>
- GRL. (2016).
- ISO 25000. (11 de Enero de 2018). *ISO 25000*. Obtenido de ISO 25000 calidad de producto de software: <http://iso25000.com/index.php/normas-iso-25000/iso-25010?id=10&limit=3>
- ISO25000. (2019). <https://iso25000.com/index.php/normas-iso-25000/iso-25010?limit=3&limitstart=0>.

- Leandro, P. (2018). *Fundación Universitaria Konrad Lorenz*. Obtenido de Gestion de la informacion:
<https://webcache.googleusercontent.com/search?q=cache:YpGb6hiFp0gJ:https://virtual.konradlorenz.edu.co/mod/resource/view.php%3Fid%3D316729+&cd=2&hl=es&ct=clnk&gl=pe>
- Nuño, P. (25 de Abril de 2017). *Auditoría de sistemas*. Obtenido de <https://www.emprendepyme.net/auditoria-de-sistemas.html>
- Piattini, M., Garcia, F., & Pino, F. (2018). *Calidad de Sistemas de Información. 4ª edición ampliada y actualizada*. España: RA-MA editorial.
- Pro, D. (2016). *AUDITORÍA DE SISTEMAS DE INFORMACIÓN EN UN ENTORNO INFORMATICO*. Cordoba.
- Ramos, C. (2015). *PROPUESTA DE UN PLAN DE AUDITORIA INFORMATICA PARA EL "SISTEMA DE INFORMACION EN SALUD" Y EL "APLICATIVO PARA EL REGISTRO DE FORMATOS SIS" EN LOS ESTABLECIMIENTOS DE SALUD DE LA UNIDAD EJECUTORA 400 EN LA REGION PIURA EN EL AÑO 2015* . Piura.
- Raymundo, C. (10 de Septiembre de 2018). *STUDOCU*. Obtenido de Universidad Juárez del Estado de Durango: <https://www.studocu.com/es-mx/document/universidad-juarez-del-estado-de-durango/administracion/resumenes/admin-septiembre/6298581/view>
- Tranformacion digital . (19 de Julio de 2017). *KYOCERA*. Obtenido de KYOCERA: <https://smarterworkspaces.kyocera.es/blog/los-6-principales-tipos-sistemas-informacion/>
- Valdes, F. P. (21 de Julio de 2018). *debateplural*. Obtenido de Triple Tecnologia: <http://debateplural.com/2018/07/21/eficiencia-y-eficacia-que-es-mejor-para-una-organizacion-2/>
- Veliz, K. (2017). *Auditoria interna y su incidencia en los procesos contables en las*. Lima.