



**FACULTAD INGENIERÍA
PROGRAMA DE INGENIERÍA DE SISTEMAS Y COMPUTACIÓN
ESPECIALIZACIÓN EN AUDITORÍA DE SISTEMAS DE INFORMACIÓN
BOGOTÁ D.C.**

LICENCIA CREATIVE COMMONS: Atribución no comercial sin derivadas

AÑO DE ELABORACIÓN: 2019

TÍTULO: Auditoría para los procesos de pruebas y calidad del software del proyecto comisiones Callidus Accenture Colombia basada en la norma ISO 9001:2015.

AUTOR: Zubieta Vivas, Katherine Stella.

DIRECTOR/ASESOR:

López Sevillano, Alexandra María.

MODALIDAD: Trabajo de investigación.

PÁGINAS:	206	TABLAS:	37	CUADROS:	0	FIGURAS:	33	ANEXOS:	13
-----------------	------------	----------------	-----------	-----------------	----------	-----------------	-----------	----------------	-----------

CONTENIDO:

INTRODUCCIÓN

1. GENERALIDADES
2. MARCOS DE REFERENCIA
3. METODOLOGÍA
4. DESARROLLO DE LA PROPUESTA
5. PRODUCTOS A ENTREGAR
6. REFERENCIAS
7. ANEXOS

DESCRIPCIÓN:

Se presenta el desarrollo de la auditoria al sistema de información de los proceso de pruebas y calidad en el software de la fábrica de desarrollo Callidus Accenture



Colombia, con el objetivo de evaluar y generar el informe a la alta gerencia de las vulnerabilidades que posee su sistema actual, bajo las políticas de la compañía contrastados con la norma de calidad ISO 9001:2015 principalmente y uso de buenas prácticas de seguridad de la norma ISO 27002, lo anterior probando que esta norma genérica de calidad puede usarse para evaluar cualquier proceso de cualquier industria.

METODOLOGÍA:

En este trabajo se utilizó una metodología mixta (cualitativa - deductiva) para la recopilación, revisión y análisis de la información y/o datos. El método cualitativo tiene como objetivo la descripción de las cualidades de un fenómeno, para este caso el sistema del caso de estudio; la metodología deductiva es una estrategia de razonamiento empleada para deducir conclusiones lógicas a partir de una serie de premisas o principios, para este caso la aplicación de la norma ISO 9001:2015 principalmente para la recolección, medición, estructuración y presentación de la información, adicionalmente se hará uso de la norma 27002 para temas de evaluación de las buenas prácticas en el manejo de sistemas informáticos.

La metodología que se emplea para el desarrollo del trabajo de grado se compone de 3 etapas:

1. Inicio y planificación,
2. Ejecución y monitoreo y
3. Cierre.

Etapas I: Inicio y planificación:

En esta etapa se realiza la contextualización del sistema, reconocimiento de las partes involucradas que permitirán la extracción y suministro de información correspondiente a los procesos a evaluar, se presentará el marco de referencia a emplear es decir la norma ISO 9001:2015, además, se elaborarán las herramientas para extraer la información y documentar la evidencia a generar. Hitos involucrados: comprensión de las necesidades y expectativas de las partes interesadas, determinación del alcance y la gestión.

Etapas II: Ejecución y Monitoreo:

En esta etapa se aplicarán las herramientas para la captura y presentación de información que sea extraída de los responsables de los procesos, además con la confirmación visual de los resultados de la ejecución de los procesos se procede a

RESUMEN ANALÍTICO EN EDUCACIÓN - RAE -



UNIVERSIDAD CATÓLICA
de Colombia
Vigilada Mineducación

RIUCaC

registrar la evidencia. Hitos involucrados. mediciones, competencia de la organización, liderazgo, control de cambios, evaluación de desempeño y mejora.

Etapas III: Cierre:

En esta fase se generará y entregará el informe resultante de la auditoria a los procesos de pruebas y calidad en el software del proyecto Comisiones Callidus Accenture Colombia para los procesos abordados, esto acompañado de las evidencias, adicional a esto, se presentará la socialización del trabajo realizado para ser evaluado por los jurados asignados.

PALABRAS CLAVE: AUDITORIA, CALIDAD DEL SOFTWARE, CONTROL, ESTÁNDAR, EVIDENCIA, INFORME DE AUDITORÍA, ISO 9001:2015, ISO 27002, POLÍTICAS, PROCEDIMIENTOS, RIESGO, SOFTWARE, VULNERABILIDAD.

CONCLUSIONES:

Haber realizado la auditoria al área de pruebas y calidad del proyecto comisiones Callidus Accenture Colombia, basada en la norma ISO 9001:2015 permitió obtener información buscando abordar los hitos que precisa la norma, representar la información y generar la representación final del ciclo de la información y sus componentes de forma clara.

De acuerdo con el objetivo de caracterización de los procesos del área de pruebas y calidad en el software del proyecto se cumplió obteniendo un amplio nivel de detalle con la información recopilada de diversas fuentes, sin embargo, esto tomó tiempo ya que no se encuentra centralizada y actualizada en un único documento en la biblioteca de medios del proyecto. Se conoció por qué no todos los proyectos de la compañía son auditados.

Para el objetivo de diseño y construcción de herramientas para la recolección de información y evidencia de los procesos del área de pruebas y calidad en el software, se adaptaron y utilizaron formatos que se obtuvieron y modificaron en el transcurso de la especialización de auditoria de sistemas de información, esto se vio reflejado en las guías de auditoria a los procesos, identificación y valoración de activos de información y evaluación de riesgos principalmente. Además, se aprovecharon recursos con los que cuenta la compañía y que están a disposición para mantener la confidencialidad de los participantes como lo fue en el caso para realizar y aplicar la encuesta a la muestra de la población, de allí se tabularon y

RESUMEN ANALÍTICO EN EDUCACIÓN - RAE -



UNIVERSIDAD CATÓLICA
de Colombia
Vigilada Mineducación

RIUCaC

representaron algunas de las respuestas de los participantes, esta también permitió la interacción con los miembros del grupo en una autoevaluación en cuanto a las competencias de desempeño, las cuales son de interés para la alta gerencia, ya que no se contaba con esta información.

Por otra parte, como el proyecto no cuenta con la información centralizada en documentos, fue necesario recurrir a herramientas que permitieran capturar mayor nivel de detalle, para esto la entrevista estructurada cumplió con su deber, incluso, permitió conocer la visión del negocio a nivel global y forma de valoración empresarial del área, esto no fue sencillo, pues estructurar las preguntas para abordar temas específicos, puntuales y de valor conllevan tiempo, conocimiento y se deberán ir afinando con la práctica. Se evidenció que las actividades de los procesos se realizan basados en la experiencia y en algunos casos apoyados en algunos documentos no siempre actualizados.

Sobre el objetivo de determinar el nivel de riesgo existente en los procesos de pruebas y calidad fue de mayor complejidad por lo extenso de acuerdo con la cantidad de activos de información identificados. Dado que el proyecto no es responsable de mantener y proteger los dispositivos físicos (excepto el computador personal), el personal si interactúa con los servicios, sistemas y herramientas que son provistas por el cliente, por lo cual, la identificación de los riesgos se centró en la aplicación de buenas prácticas en la seguridad de la información por parte de los usuarios del área de pruebas y calidad, conforme a la Norma ISO 27002; lo que permitió identificar los riesgos, su valoración y representación en la matriz de calor, el esfuerzo en la identificación tanto de amenaza como vulnerabilidad para cada uno y la descripción o redacción del riesgo tomó su tiempo para cumplir con las partes indispensables en esta, como el qué principio de auditoría se afectaba, el por qué, el qué afectaba y lo que generaba.

El resultado final permitió visualizar que, si bien el riesgo está presente en cada activo, para este caso en se encuentran en su mayoría manejados ya que se ubican en cuadrantes de calor de probabilidad e impacto bajo y moderado, al fortalecer y reforzar las políticas de buenas prácticas en seguridad de la información pueden llegar a disminuir el nivel de riesgo en muchos de estos riesgos.

Se reconoce que con la participación y colaboración principalmente de los auditados y la gerencia del proyecto, se permitió generar un informe sobre el

**RESUMEN ANALÍTICO EN EDUCACIÓN
- RAE -**



UNIVERSIDAD CATÓLICA
de Colombia
Vigilada Mineducación

RIUCaC

resultado de la auditoría con marco de referencia la norma ISO 9001:2015, el cual ofrece una evaluación y recomendación a los procesos de pruebas y calidad en el software.

La generación de información documentada para el área se limita básicamente a las exigidas por el cliente en los formatos especificados para la realización de los procesos de gestión de los requerimientos, y la necesaria para la gestión de las pruebas, esto para control y seguimiento interno por iniciativa propia del responsable, los cuales no cuentan con una estructura formal que contenga control de versiones, revisores, fechas, tampoco realiza un riguroso proceso de marcha atrás en cada uno de los requerimientos para asegurar la calidad y funcionamiento llegado el caso de ser necesario la desinstalación de los productos desplegados en el ambiente.

Globalmente, se evidencia que existe y se ejecuta el ciclo PHVA, cumpliendo el enfoque de procesos como caracteriza la norma ISO 9001:2015, sin embargo, para querer aplicar a una certificación internacional como una norma ISO, es necesario generar documentos estructurados que se concentren en documentar cada uno de los procesos completos con gran detalle, además deberán especificar cada uno de los temas de la organización/proyecto y no se tenga que capturar esta información de múltiples fuentes como sucedió en este caso. Para un proyecto que no ha sido auditado y que, de querer aplicar a una certificación especializada, la evaluación frente a la norma ISO 9001:2015 es un excelente punto de partida que permitirá reconocer, planear y afinar detalles, acciones y documentos.

FUENTES:

Accenture. (2019). *Acerca de Accenture*. Recuperado el 6 de 3 de 2019, de Acerca de Accenture: <https://www.accenture.com/co-es/company>

Accenture. (22 de 01 de 2019). Biblioteca de Medios proyecto Comisiones Callidus Colombia. *Presentación Callidus Accenture Colombia 20190122*. Bogotá, Colombia. Recuperado el 15 de 03 de 2019

AGENCIA NACIONAL DE DEFENSA JURÍDICA DEL ESTADO. (30 de 6 de 2016). *GUÍA DE INVENTARIO DE ACTIVOS*,. Recuperado el 1 de 4 de 2019, de GUÍA DE INVENTARIO DE ACTIVOS,: https://www.defensajuridica.gov.co/servicios-al-ciudadano/ley_transparencia/Documents/guia_inventario_activos_clasificacion_publicacion_de_informacion_130916.pdf

**RESUMEN ANALÍTICO EN EDUCACIÓN
- RAE -**



UNIVERSIDAD CATÓLICA
de Colombia
Vigilada Mineducación

RIUCaC

AGENCIA NACIONAL INMOBILIARIA. (11 de 10 de 2016). *PROCEDIMIENTO PARA LA CLASIFICACIÓN Y PUBLICACIÓN DEL TIPO DE*. Recuperado el 1 de 4 de 2019, de PROCEDIMIENTO PARA LA CLASIFICACIÓN Y PUBLICACIÓN DEL TIPO DE ACTIVO (INFORMACIÓN):

<http://www.agenciavirgiliobarco.gov.co/Entidad/PlaneacionGestion/SistemaIntegradoGestion/GTIC-PR-01Clasificaci%C3%B3npublicaci%C3%B3ndeltipodeactivoinformaci%C3%B3n.pdf>

Alsina. (2016). *Alsina*. Recuperado el 2 de 3 de 2019, de Alsina: <https://www.alsina.com/alsina/empresa-certificada-iso-9001/>

Ashwin Srinivas, Bryan Kurey. (Abril de Abril de 2014). *Harvard Business Review*. (H. B. Review, Editor, H. B. Review, Productor, & Harvard Business Review) Recuperado el 18 de 02 de 2019, de Creating a Culture of Quality: <https://hbr.org/2014/04/creating-a-culture-of-quality>

BUREAU VERITAS COLOMBIA. (2016). *BUREAU VERITAS COLOMBIA*. Recuperado el 27 de 2 de 2019, de BUREAU VERITAS COLOMBIA: <https://www.bureauveritas.es/home/about-us/profile-logo>

CCTI. (11 de 3 de 2019). *¿Sabías qué? (CMMI)*. Recuperado el 19 de 4 de 2019, de ¿Sabías qué? (CMMI): <https://ccti.com.co/index.php/blog/197-sabias-que-cmmi>

COLCAFE. (2018). *COLCAFE*. Recuperado el 2 de 9 de 2018, de COLCAFE: <http://es.industriacolombianadecafe.com/es-ve/nuestracompa%C3%B1a/certificaciones.aspx>

CONCEPTDEFINICION.DE. (2011). *Definición de Proceso*. Recuperado el 8 de 9 de 2018, de Definición de Proceso: <https://conceptdefinicion.de/proceso/>

Destino Negocio. (2015). Recuperado el 18 de 2 de 2019, de Destino Negocio: <https://destinonegocio.com/co/emprendimiento-co/que-es-y-para-que-sirve-la-norma-iso-90012015/>

EmprendePyme.net. (2016). *La auditoría interna*. Recuperado el 8 de 9 de 2018, de La auditoría interna: <https://www.emprendepyme.net/auditoria-interna.html>

Escuela Europea de Excelencia. (18 de 7 de 2017). *Información documentada: ¿Qué cambió en cuanto a terminología?* Recuperado el 19 de 4 de 2019, de Información documentada: ¿Qué cambió en cuanto a terminología?: <https://www.nueva-iso-9001-2015.com/2017/07/informacion-documentada-cambio-terminologia/>

Fuentelsaz Gallego, C. (2006). *Elaboración y presentación de un proyecto de investigación y una tesina*. Barcelona: Edicions Universitat Barcelona.

Gómez Martínez, J. A. (2016). *Guía para la aplicación de ISO 9001:2015*. Bogotá: Alfaomega.

**RESUMEN ANALÍTICO EN EDUCACIÓN
- RAE -**



UNIVERSIDAD CATÓLICA
de Colombia
Vigilada Mineducación

RIUCaC

GRUPO ACMS CONSULTORES. (16 de 2 de 2019). *Grupo ACMS Consultores*. Recuperado el 19 de 4 de 2019, de Grupo ACMS Consultores: <https://www.grupoacms.com/norma-iso-33000>

ICONTEC. (19 de 8 de 2009). *Norma Técnica Colombiana NTC-ISO/IEC 27005 - Alcaldía de Envigado*. Recuperado el 18 de 4 de 2019, de Norma Técnica Colombiana NTC-ISO/IEC 27005 - Alcaldía de Envigado: <http://gmas2.envigado.gov.co/gmas/downloadFile.public?repositorioArchivo=000000001071&ruta=/documentacion/0000001359/0000000107>

ICONTEC. (2016). *INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN*. Recuperado el 27 de 02 de 2019, de INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN: <http://www.icontec.org/NC/QS/Paginas/Rec.aspx>

Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC). (23 de 9 de 2015). *NORMA TÉCNICA COLOMBIANA NTC-ISO 9001 2015-09-23 SISTEMAS DE GESTIÓN DE LA CALIDAD*. Recuperado el 8 de 3 de 2019, de [http://www.minvivienda.gov.co/Documents/Sobre%20el%20Ministerio/Sistemas-de-Gestion/NTC ISO 9001 2015.pdf](http://www.minvivienda.gov.co/Documents/Sobre%20el%20Ministerio/Sistemas-de-Gestion/NTC%20ISO%209001%202015.pdf)

International Organization for Standardization. (23 de 9 de 2015). *ISO 9001:2015 Quality management systems -- Requirements*. (I. O. Standardization, Ed.) Recuperado el 9 de 3 de 2019, de ISO 9001:2015 Quality management systems -- Requirements: <https://www.iso.org/standard/62085.html>

International Organization for Standardization. (6 de 3 de 2019). *International Organization for Standardization*. Obtenido de ISO 9000 family - Quality management: <https://www.iso.org/iso-9001-quality-management.html>

International Organization for Standardization ISO/IEC. (08 de 2018). *ISO/IEC 30141:2018*. Recuperado el 11 de 3 de 2019, de ISO/IEC 30141:2018: <https://www.iso.org/standard/65695.html>

Interoil Colombia Exploration and Production. (2010). *Interoil Colombia Exploration and Production*. Recuperado el 27 de 2 de 2019, de InterOil Colombia Exploration and Production: <http://www.interoil.com.co/comp.php>

ISO. (2013). *International Organization for Standardization*. Recuperado el 8 de 9 de 2018, de ISO/IEC 27002:2013: <https://www.iso.org/standard/54533.html>

ISO. (2015). *International Organization for Standardization*. Recuperado el 8 de 9 de 2018, de ISO 9000 family - Quality management: <https://www.iso.org/iso-9001-quality-management.html>

ISO. (2015). *ISO 9000:2015(es) Sistemas de gestión de la calidad — Fundamentos y vocabulario*. Recuperado el 8 de 9 de 2018, de ISO 9000:2015(es) Sistemas de gestión de la calidad — Fundamentos y vocabulario: <https://www.iso.org/obp/ui/#iso:std:iso:9000:ed-4:v1:es:term:3.6.2>

**RESUMEN ANALÍTICO EN EDUCACIÓN
- RAE -**



UNIVERSIDAD CATÓLICA
de Colombia
Vigilada Mineducación

RIUCaC

ISO. (08 de 09 de 2018). *ISO Survey 2017*. Ginebra: ISO. Recuperado el 08 de 09 de 2018, de ISO Survey 2017: <https://www.iso.org/the-iso-survey.html>

ISO 33000 ESPAÑA. (16 de 02 de 2019). *ISO 33000*. Recuperado el 19 de 4 de 2019, de ISO 33000: <http://www.iso33000.es/index.php/familia-iso-33000>

ISO TOOLS. (20 de 05 de 2015). *Los requisitos para implementar y certificar la norma ISO 9001*. Recuperado el 13 de 09 de 2018, de Los requisitos para implementar y certificar la norma ISO 9001: <https://www.isotools.com.co/requisitos-para-implementar-y-certificar-norma-iso-9001/>

J. Pérez Porto, A. G. (2012). *DEFINICION DE*, 2. Recuperado el 8 de 9 de 2018, de DEFINICION DE: <https://definicion.de/producto/>

MINTIC. (17 de 2 de 2019). *MINTIC*. Recuperado el 16 de 09 de 2018, de Plan Estratégico Sectorial 2019-2022 Borrador: https://www.mintic.gov.co/portal/604/articles-82084_plan_estrategico_sector_tic_20192022.pdf

Ojeda, M. (6 de 4 de 2018). *ISO, COBIT e ITIL, ¿cuál de estas normas y estándares internacionales te conviene más para potenciar tu empresa?* Recuperado el 11 de 3 de 2019, de ISO, COBIT e ITIL, ¿cuál de estas normas y estándares internacionales te conviene más para potenciar tu empresa?: <https://www.gb-advisors.com/es/normas-y-estandares-internacionales/>

Pérez Porto, J. (2017). Recuperado el 19 de 9 de 2018, de <https://definicion.de/encuesta/>

Postobón. (2018). *Postobón*. Recuperado el 2 de 9 de 2018, de Postobón: <https://www.postobon.com>

Riesco, S. (9 de 11 de 2018). *¿Cuáles son las normas ISO más importantes?* Recuperado el 11 de 3 de 2019, de ¿Cuáles son las normas ISO más importantes?: https://www.formazion.com/noticias_formacion/cuales-son-las-normas-iso-mas-importantes-org-5273.html

Significados.com. (24 de 1 de 2018). *Significados.com*. Recuperado el 2 de 1 de 2019, de Significados.com: <https://www.significados.com/sistema-de-informacion/>

Speth, C. (2016). *El análisis DAFO: Los secretos para fortalecer su negocio*. Plurilingua Publishing.

TATA TECHNOLOGIES. (31 de 6 de 2017). *TATA TECHNOLOGIES*. Recuperado el 2 de 9 de 2018, de TATA TECHNOLOGIES: <https://www.tatatechnologies.com/mx/about-us/certifications/>

Velneo. (16 de 1 de 2019). *El desarrollo de software de gestión en Colombia en 2019*. Recuperado el 19 de 4 de 2019, de El desarrollo de software de gestión en Colombia en 2019: <https://velneo.es/el-desarrollo-de-software-de-gestion-en-colombia-en-2019/>

**RESUMEN ANALÍTICO EN EDUCACIÓN
- RAE -**



UNIVERSIDAD CATÓLICA
de Colombia
Vigilada Mineducación

RIUCaC

Venemedia Comunicaciones C.A.. (6 de 3 de 2019). *Definición de Accenture*. Recuperado el 8 de 3 de 2019, de Definición de Accenture:

<https://conceptodefinicion.de/accenture/>

VINCA LLC. (8 de 9 de 2018). *Qué es ISO*. Recuperado el 8 de 3 de 2019, de Qué es ISO: <http://www.normas9000.com/content/que-es-iso.aspx>

LISTA DE ANEXOS:

Anexo 1. Cronograma

Anexo 2. Presupuesto

Anexo 3. Acta inicio de auditoría

Anexo 4. Encuesta realizada a los integrantes del proyecto

Anexo 4.1 Resultados de la encuesta

Anexo 4.2. Datos estadísticos

Anexo 5. Entrevista estructurada

Anexo 5.1. Entrevista estructurada

Anexo 6. Evidencias procesos auditados

Anexo 7. Criterios para valoración de activos

Anexo 7.1. Anexo C NTC-ISO/IEC 27005 amenazas comunes

Anexo 7.2. Anexo D NTC-ISO/IEC 27005 vulnerabilidades

Anexo 8. Informe de auditoría.