Revista de Investigación Talentos Volumen VI. (2), Julio – Diciembre 2019
ISSN Impreso: 1390-8197 ISSN Digital: 2631-2476

AUDITORÍA DE SEGURIDAD INFORMÁTICA A LA DIRECCION DISTRITAL 02D03 CHIMBO-SAN MIGUEL-EDUCACIÓN, APLICANDO COBIT 5.

COMPUTER SECURITY AUDIT FOR DISTRICT ADDRESS 02D03 CHIMBO SAN MIGUEL EDUCATION, APPLYING COBIT 5.

Angel Palacios Bayas [(1)], **Víctor Bósquez Barcenes** [(2)], **José Palacios Bayas** [(3)], **Luis Alfredo Camacho**[(4)]

[1]*Universidad Tecnológica Israel, Quito-Ecuador, apalacios.net@gmail.com*

[2]*Universidad Estatal de Bolívar, Guaranda-Ecuador victorbarcenes@gmail.com,*

[3]*Universidad Tecnológica Indoamérica. Ambato-Ecuador miguelpalacios17@hotmail.com:*

[4]*Universidad Técnica Estatal de Quevedo, Vía el Empalme KM 7. Campus La MaríaQuevedo, Los Rios, Ecuador.*

Resumen: *Los riesgos informáticos históricamente se han encontrado presentes cotidianamente y en auge, tanto en instituciones públicas como privadas, independientes del tamaño y la función a la que se dedican. Estos riesgos han sido consecuencia del inapropiado uso de normas, políticas, estándares, o incumplimiento de las mismas; de tal manera se ha realizado una auditoría de seguridad informática, a la unidad distrital de tecnologías de la información y comunicaciones (TIC's) de la Dirección Distrital 02d03 Chimbo-San Miguel-Educación, del periodo enero 2016-octubre 2017, en base a la metodología (ABR) Auditoría Basada en Riesgos, que se desarrolla en tres fases: Planeación, ejecución y comunicación de resultados, la misma que se fundamenta con el marco de referencia COBIT 5.0.*

Con el propósito de ejecutar la auditoría de seguridad informática, se construyó una matriz de riesgos, la cual permitió determinar los procesos más críticos de la unidad distrital TIC's, y dirigir la evaluación hacia ellos.

Recibido: 3 de julio de 2019
Aceptado: 23 de septiembre de 2019
Publicado como artículo científico en Revista de Investigación Talentos VI (2), 1-11

Posteriormente se elaboró el programa de auditoría, describiendo los instrumentos de evaluación y pruebas de controles; una vez realizada la investigación de campo, se ordenaron y analizaron los datos, considerando el marco de referencia COBIT 5.0. Los resultados de los análisis y hallazgos se plasmaron en un informe borrador que fue leído a la máxima autoridad del distrito educativo, en la cual se recogieron sugerencias y se elaboró el respectivo informe final.

Palabras Claves: *Auditoría Informática, Seguridad Informática, COBIT 5, Gestión de Riesgos Informáticos, Dirección Distrital 02d03 Chimbo-San Miguel-Educación.*

Abstract: *Historically, computer risks have been present on a daily and booming basis, both in public and private institutions, the size and function to which it is dedicated. These risks have been the consequence of the inappropriate use of norms, policies, standards, or non-compliance with them; In this way, a computer security audit was carried out on the district unit of information and communication technologies (TIC's) of the District Office 02d03 Chimbo-San Miguel-Educación, from January 2016 to October 2017, based on the methodology (ABR) Risk Based Audit, which is developed in three phases: Planning, execution and communication of results, which is based on the reference framework COBIT 5.0.*

With the purpose of executing the computer security audit, a risk matrix was constructed, which allowed determining the most critical processes of the ICT district unit, and directing the evaluation towards them. Subsequently, the audit program was elaborated, describing the evaluation instruments and control tests; once the field research was carried out, the data was ordered and analyzed, considering the reference frame COBIT 5.0. The results of the analyzes and findings were reflected in a draft report that was read to the highest authority of the educational district, in which suggestions were collected and the respective final report was prepared.

Keyworks: *Computer Audit, Information Security, COBIT 5.0, Risk Management, District Address 02d03 Chimbo - San Miguel-Education.*

I. INTRODUCCIÓN

A diario se observa en diferentes medios de comunicación varios tipos de ataques informáticos, como: fraudes, robo de información sensible, suplantación de identidad, daños en los softwares, interrupción en las comunicaciones (redes); incrementación de la piratería informática, entre otros. Lo cual ocasiona grandes pérdidas que pueden ser materiales, económicas, o de reputación (imagen institucional).

Esto es consecuencia que los ciberdelincuentes cada día son más sofisticados con la utilización de herramientas digitales y más audaces en el empleo de estrategias para engañar a las víctimas y robar información; mientras los usuarios de las redes e internet cada día incrementan más y demuestran un nivel elevado de ingenuidad con el uso adecuado de las Tecnologías de la Información y Comunicaciones, consecuencia de la falta de conocimiento básico de seguridad informática, o en razón que los usuarios menores de edad no son supervisados por los adultos; de tal manera se ha realizado una Auditoría Informática en la Dirección Distrital 02d03 Chimbo-San Miguel-Educación del periodo enero 2016-octubre 2017, con el propósito de identificar riesgos informáticos y mitigarlos oportunamente.

Existen varios trabajos de auditoría de sistemas que han ayudado en el desarrollo del presente trabajo investigativo, entre los cuales se puede mencionar: a nivel de postgrado se ha realizado los trabajos titulados: "Auditoría de Sistemas basada en riesgos a los procesos del Sistema Nacional de Nivelación y Admisión de la Secretaría de Educación Superior, Ciencia, Tecnología e Innovación, Aplicando COBIT 4.1 y COSO ERM", realizado por (Vaca Benalcázar & Casanova, 2014); donde se ha evaluado el riesgo, contemplando el marco de referencia COBIT 4.1; en el repositorio digital de la Universidad Regional Autónoma de los Andes (UNIANDES), consta el trabajo titulado: "Auditoría informática y la calidad del servicio de las tecnologías de la información en el distrito de educación 06D04 Colta – Guamote", realizado por: (Pulgar Haro, 2018), donde se concluye que el marco de referencia COBIT, ayuda a entender los sistemas de Tecnologías de la Información (TI), permite decidir el nivel de seguridad y aplicar controles a fin de proteger los activos (información, hardware, software…) de la entidad auditada, basándose en un modelo de desarrollo de gobernación de TI. Se ha sustentado la investigación con diferentes definiciones:

Auditoría.- Según la Autora: (Moreno, 2009) define: "La Auditoría es un proceso sistemático para obtener y evaluar de manera objetiva las evidencias relacionadas con informes sobre actividades económicas y otros acontecimientos, cuyo fin es determinar el grado de correspondencia del contenido informativo con las evidencias que le dieron origen, así como establecer si dichos informes se han elaborado observando los principios establecidos para el caso"

Seguridad Informática. - (Roa, 2013) Define "…La seguridad informática intenta proteger el almacenamiento, procesamiento y transmisión de información digital…"; mientras (Escrivá Gascó, Romero Serrano, & Ramada, 2013, pág. 7) expresa que "…La seguridad informática, por su parte, es una rama de la seguridad de la información que trata de proteger la información que utiliza una infraestructura informática y de

telecomunicaciones para ser almacenada o transmitida…".

Gestión de Riesgos. La gestión de riesgos es considerada como un método, que a través de una secuencia de actividades permite analizar las amenazas, valorar el impacto que pueden ocasionar si se materializan las amenazas; también se enfoca en clasificar el riesgo en Inherente y Riesgo Residual, con el propósito de implementar controles de seguridad que permitan mitigar, o eliminar el riesgo. (Erb, 2008)

COBIT 5.0.- (ISACA , 2012) define cómo: "Objetivos de control para Tecnología de la Información y Tecnologías relacionas, permite a las Organizaciones a construir un marco efectivo de Gobierno y Administración, basado en cinco principios y una serie holística de siete habilitadores, que optimizan la inversión en tecnología e información; así como su uso en beneficio de las partes interesadas, es el marco de referencia aceptado internacionalmente, como una buena práctica, para el control de la información y los riesgos asociados."

¿Los resultados de la auditoría de seguridad informática, permitirán a la máxima autoridad de la Dirección Distrital 02d03 Chimbo-San Miguel-Educación, tomar decisiones acertadas y oportunas en relación a la protección de los activos más importantes del distrito educativo?

II. MATERIALES Y MÉTODOS

La investigación es de carácter mixto (cualitativo y cuantitativo), la primera variable en razón que a través de la observación directa y visitas de campo se describieron los hechos que permitieron diagnosticar la problemática y orientar a la solución; mientras la segunda variable se utilizó en la valoración de riesgo. El diseño es de carácter no experimental.

El diseño de la auditoría de seguridad informática se ha caracterizado en hechos producidos naturalmente en la Dirección Distrital 02d03 Chimbo-San Miguel-Educación, los cuales se han analizado en base al marco de referencia COBIT 5.0

Los involucrados en la Auditoría de Seguridad Informática fueron:

Tabla 1.
PARTICIPANTES DE LA AUDITORÍA DE SEGURIDAD INFORMÁTICA

Descripción	Cantidad
Equipo Auditor	3
Director Distrital	1
Líderes departamentales	10
Analistas Distritales	51
TOTAL	65

Fuente: Los Autores.

Los instrumentos empleados en la Auditoría de Seguridad Informática han sido desarrollados por los autores en hojas de cálculo y procesadores de texto, siguiendo un formato sugerido por el supervisor de auditoría, entre los

cuales constan la matriz de riesgos, pruebas de cumplimento, plan, programa de auditoría y papeles de trabajo.

Metodologia. -La auditoría de seguridad informática fue realizada en base a la Metodología de Auditoría basada en riesgos (ABR) estándar de Auditoría de Sistemas, que consta de tres fases: Planificar, Ejecutar y Comunicar resultados.

1. **Planificar**

En esta fase, se ha establecido las relaciones entre auditores y representante de Dirección Distrital 02d03 Chimbo, San Miguel-Educación, con el propósito de determinar el alcance y los objetivos de la auditoría, para lo cual se realizó:

1. Estudio preliminar de la entidad auditada, con el propósito de comprender el entorno a auditar: Personas, procesos, tecnología, controles internos, estrategias, entre otros.
2. Análisis preparatorio del control interno, análisis de riesgos y materialidad.
3. Elaboración de programas de auditoría de los procesos objetos de evaluación.

A continuación, se detalla el plan de revisión de la unidad distrital de tecnologías de la información y comunicaciones, que comprende: Origen de la Auditoría, Marco de referencia, Alcance y Desarrollo.

1.1 Origen de la Auditoría. -Revisión de los procesos de la Unidad Distrital de Tecnologías de la Información y Comunicaciones, control interno, hardware, software, seguridades de la Dirección Distrital 02d03 Chimbo-San Miguel-Educación, que se considera la base perimetral indispensable del Distrito Educativo, para la realización y cumplimiento de las operaciones cotidianas.

1.2 Marco de Referencia. - Para la realización de la auditoría de seguridad informática a la Unidad Distrital de Tecnologías de la Información y Comunicaciones de la Dirección Distrital 02d03 Chimbo-San Miguel-Educación, se adoptó el marco de referencia COBIT 5.0, motivo que, a través de los objetivos de control de Tecnologías de la Información, permitió construir un marco efectivo de Gobierno de TI y administración.

1.3 Alcance. - El alcance de la auditoría a la seguridad informática, se delimitó a la Unidad Distrital de Tecnologías de la Información y Comunicaciones, de la Dirección Distrital 02d03 Chimbo, San Miguel-Educación, del periodo enero 2016-octubre 2017.

1.4 Desarrollo. - Se describen los pasos, métodos, técnicas, herramientas utilizadas durante la auditoría de seguridad informática.

2. Ejecutar

En esta fase, se reunió la información documental, evidencias, que permitieron a los auditores fundamentar los comentarios y sugerencias en relación al manejo y administración de seguridad de la Unidad de Tecnologías de la Información y Comunicaciones de la Dirección Distrital 02d03 Chimbo, San Miguel-Educación. Para ello se empleó diversas técnicas cómo: Entrevistas a la máxima autoridad del distrito educativo, encuestas a Líderes y Analistas Distritales, análisis documental, análisis de normas y estándares.

La información reunida, y analizada en base al criterio profesional por parte del equipo de auditores, fue: ordenada, clasificada y resguardada, con el propósito de justificar las recomendaciones en el informe de auditoría.

3. Comunicar Resultados

El equipo de auditoría consolidó los Papeles de Trabajo, con el propósito de analizar los hallazgos más relevantes, y redactar un informe borrador contenedor de conclusiones y recomendaciones necesarias, para el mejoramiento de la seguridad informática de la Unidad Distrital de Tecnologías de la Información y Comunicaciones. El informe fue entregado y socializado a la máxima autoridad del Distrito Educativo, para su evaluación y análisis.

El informe presentado por el equipo de auditoría contiene los siguientes aspectos:

- Periodo que comprende la auditoría de seguridad informática:
- Equipo auditor, que ha intervenido en la evaluación.
- Los objetivos de la auditoría.
- El marco de referencia utilizado, COBIT 5.0
- El alcance de la auditoría
- Los procedimientos de auditoría realizados
- La opinión de la auditoría
- Los resultados de la auditoría, basado en:

Condición: ¿Qué se encontró?

Criterio: COBIT e ISO 27000

Causa: ¿Qué origino el riesgo?

Efecto: ¿Qué puede llegar a suceder si llegará a materializarse el riesgo?

Recomendación: Descripción de controles, que ayudan a mitigar el riesgo.

III. RESULTADOS Y DISCUSIÓN

1. Resultados de la matriz de Riesgos Informáticos

Una vez aplicado los diferentes instrumentos de recolección de datos y herramientas de validación diseñados en la fase de planificación, se construyó la matriz de riesgos informáticos,

donde se calculó el riesgo inherente y riesgo residual, en base a los umbrales de riesgo, considerando las perspectivas de: Probabilidad e Impacto.

Probabilidad: Posible (3), Probable (2) y Remota (1).

Impacto: Alto (3), Moderado (2) y Bajo (1) (Muñoz Vega, y otros, 2015)

Tabla 2.
RESULTADOS DE PROCESOS TIC EN BASE A LA MATRIZ DE RIESGOS.

No	PROCESO	RIESGO INHERE	RIESGO RESIDUA
1	Contratación o adquisición de bienes y servicios tecnológicos	6	4.67
2	Creación de cuentas de usuarios y perfiles	6	4.67
3	Instalación de enlaces de internet y telefonía distrital.	6	3
4	Soporte Técnico Distrital	6.75	3.75

Fuente: Los Autores

2. Resultados de la Gestión de Riesgos

A continuación, se muestran los resultados del nivel de riesgo de los procesos auditados, de la Unidad Distrital de Tecnologías de la Información y Comunicaciones de la Dirección Distrital 02d03 Chimbo-San Miguel-Educación, donde se refleja la realidad de la gestión de los Procesos tanto técnicos, como documentales, del periodo de auditoría comprendido: enero 2016-octubre 2017; en el cual el resultado del nivel de riesgo es: Alto y Moderado, en conformidad con los umbrales de riesgo; por lo tanto a través del informe de auditoría se ha sugerido a la máxima autoridad del Distrito Educativo, adoptar las recomendaciones inmediatamente con el propósito de reducir el nivel de riesgo.

Tabla 3.

RESULTADOS DE LOS PROCESOS TIC, EN BASE A LA GESTIÓN DE RIESGOS.

Procesos de la Unidad de Tecnologías de la Información y Comunicaciones.	**Nivel de Riesgo**					
	Riesgo .Alto	**67-100%**	**Riesgo Modera**	**34-66%**	**Riesgo Bajo**	**1-33%**
Contratación o Adquisición de Bienes y Servicios Tecnológicos.			X	55,75%		
Creación de Cuentas de Usuarios y Perfiles para sistemas de información.			X	50,75%		
Instalación de Enlaces de Internet Datos y Telefonía Distrital.	X	68%				
Soporte Técnico (Distrital)			X	61,75%		

Fuente: Los Autores

-Los resultados de la auditoría informática, demuestran que el proceso de Contratación o Adquisición de Bienes y Servicios Tecnológicos de la Unidad de Tecnologías de la Información y Comunicaciones de la Dirección Distrital 02d03 Chimbo-San Miguel-Educación se ubica en un nivel de riesgo moderado, consecuencia que no se ha dado cumplimiento al Manual de Gestión Administrativa Distrital.

-El proceso de Creación de Cuentas de Usuarios y Perfiles para sistemas de información, se ubica en una escala de riesgo moderado con una ponderación del 50.75%, en base a los resultados de la ejecución del programa de auditoría del proceso, donde la principal problemática ha sido la proporción de datos incompletos por parte de los usuarios solicitantes y la falta de documentos que respalden la creación, habilitación de cuentas.

-El resultado del proceso de Instalación de Enlaces de Internet Datos y Telefonía Distrital, se ubica en un nivel de riesgo Alto, razón que durante la ejecución de la auditoría se evidenció que a nivel interno del Distrito Educativo la infraestructura tecnológica no cumple con las normas y estándares de cableado estructurado y conductores de energía eléctrica.

-El proceso de Soporte Técnico Distrital, se ubica en un nivel de riesgo moderado, con una ponderación 61.75% de la gestión de riesgos informáticos; motivo que los procedimientos de mantenimiento preventivo no han sido adecuados, y falta capacitación a los usuarios en temas de seguridad informática y solución de problemas.

3. Resultados de las Pruebas de Cumplimiento

Se realizó el análisis documental del periodo de auditoría enero 2016-octubre 2017, de los procesos de la Unidad Distrital Tecnologías de la Información y Comunicaciones vs los Criterios de COBIT 5, el cual ha sido elaborado en base a varias hojas de cálculo, donde se ha marcado el cumplimiento de cada criterio, según la información levantada de los procesos evaluados.

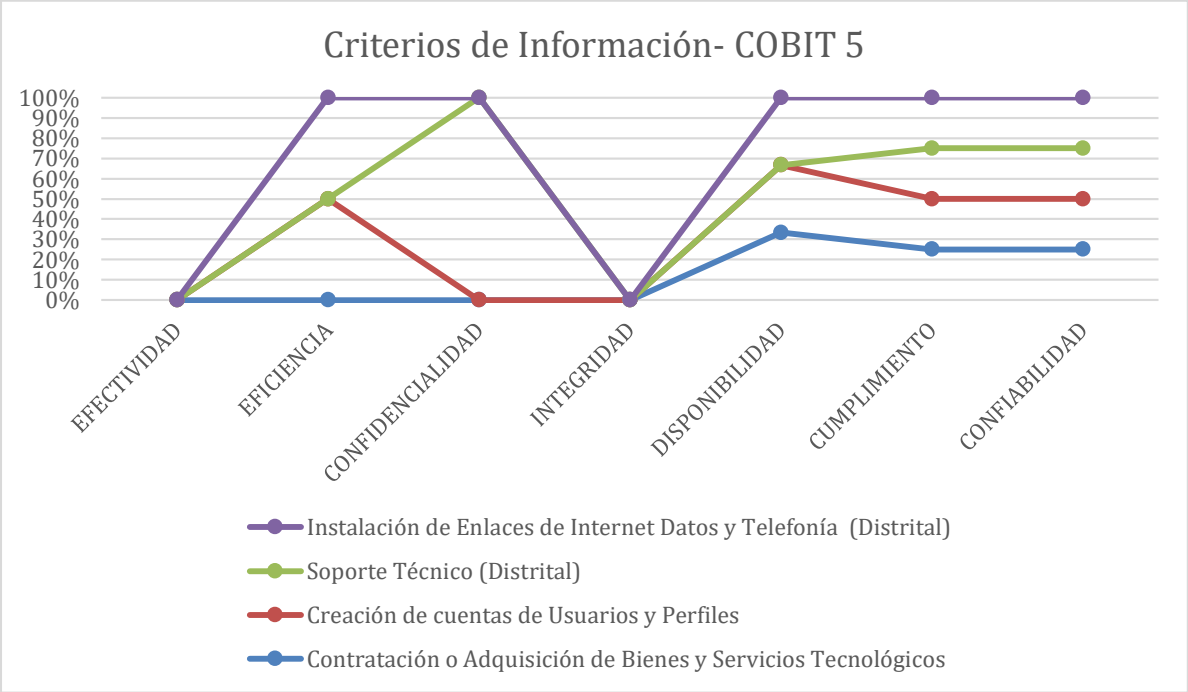

Fig 1 .*Evaluación documental de los procesos Tics con los criterios de Información COBIT 5*
Fuente: Los Autores

Se analizaron 171 documentos proporcionados por la Unidad de Tecnologías de la Información y Comunicaciones del periodo de la Auditoria enero 2016-octubre 2017.

-En la Ilustración 1, se puede observar que todos los procesos de la Unidad Distrital de Tecnologías de la Información y Comunicaciones vs los dominios de COBIT 5.0 no cumplen con la variable integridad, debido

que el acceso a la información carece de políticas de seguridad.

4. Resultados de las Pruebas Sustantivas

Se realizaron varias comprobaciones diseñadas por los autores y pruebas selectivas, en base un muestreo con el propósito de obtener evidencia y fundamentar las recomendaciones.

Tabla 4.
RESULTADOS DE LAS PRUEBAS SUSTANTIVAS

No	PROCESO	PROCEDIMIENTO DE AUDITORIA	HALLAZGOS
1	Contratación o adquisición de bienes y servicios tecnológicos	Solicitud de información, análisis documental y constatación in situ	1
2	Creación de cuentas de usuarios y perfiles	Revisión documental, entrevista, encuesta.	3
3	Instalación de enlaces de internet y telefonía distrital.	Revisión Técnica, análisis documental	6
4	Soporte Técnico Distrital	Revisión Técnica, análisis documental y entrevista.	5

Fuente: Los Autores

No se detallan los hallazgos en el presente artículo en razón de acuerdos de confidencialidad entre equipo auditor y entidad auditada. Sin embargo, se dio a conocer formalmente a la Dirección Distrital 02d03 Chimbo-San Miguel-Educación los principales hallazgos con las respectivas recomendaciones en el informe de auditoría.

IV. CONCLUSIONES

- No se cuenta con información completa, ni ordenada, lo cual fue un limitante para el desarrollo de la auditoría de seguridad informática.
- Los Procesos de la Unidad Distrital de Tecnologías de la Información y Comunicaciones, de la Dirección Distrital 02d03, se encuentran en un nivel de riesgo Alto y Moderado, de tal manera se requiere la adopción de acciones recomendadas en el informe de auditoría, con el propósito de precautelar los activos de la entidad auditada.
- COBIT 5. Es un marco de referencia integrado que ayudó significativamente en la realización de la auditoría de seguridad informática.

V. AGRADECIMIENTO

- A la Dirección Distrital 02d03 Chimbo-San Miguel-Educación, por haber permitido la realización de la auditoría de seguridad informática, y facilitado la información.
- Al Lcdo. Carlos Aroca Benítez, Analista Distrital TIC, quien ha sido un pilar fundamental en la Dirección Distrital 02d03 Chimbo-San Miguel-Educación, durante el desarrollo de la auditoría de seguridad informática.

- Al Ing. Christian Vaca, quién ha sido el supervisor de la auditoría de seguridad informática y con su amplia experiencia permitió culminar de manera exitosa la misma.

VI. BIBLIOGRAFÍA

Erb, M. (2008). *Gestión de Riesgo en la Seguridad Informática.* From https://protejete.wordpress.com/gdr_principal/gestion_riesgo_si/

Escrivá Gascó, G., Romero Serrano, M., & Ramada, D. J. (2013). *Seguridad Informática.* MACMILLAN Iberia, S.A.

ISACA . (2012). Cobit 5.

Lascano Laica, W. M. (2016, 08). Auditoría Informática, para mejorar la gestión de las Tecnologías de la Información, en el Minsiterio del Trabajo regional Ambato. Ambato, Tungurahua, Ecuador.

Moreno, E. (2009). *Auditoría.* El Cid Editor .

Muñoz Vega, C., Gil Aldea, T., Bachiller Méndez, I., Fernández Porto, M., Hernández Videla, L. A., Llorente, B. C., . . . Werner Alcón, C. (2015, 06). Caso Práctico de Apepito al Riesgo. España.

Pulgar Haro, G. (2018, Junio). Auditoría informática y la calidad del servicio de las tecnologías de la información en el distrito de educación 06D04 Colta - Guamote. Riobamba, Chimborazo, Ecuador.

Roa, J. (2013, 01 01). *Seguridad informática.* España, España, España: Mc Graw Hill.

Vaca Benalcázar , C. P., & Casanova, E. (2014, 05). Auditoría de Sistemas basada en riesgos a los procesos del Sistema Nacional de Nivelación y Admisión de la Secretaría de Educación Superior, Ciencia, Tecnología e Innovación, Aplicando COBIT 4.1 y COSO ERM. Quito, Pichincha, Ecuador.