UNIVERSIDAD TECNOLÓGICA ISRAEL

TRABAJO DE TITULACIÓN EN OPCIÓN AL GRADO DE:

INGENIERO EN SISTEMAS INFORMÁTICOS

TEMA: AUDITORÍA A LA SEGURIDAD INFORMÁTICA EN LA DIRECCIÓN DISTRITAL 02D03 CHIMBO-SAN MIGUEL-EDUCACIÓN DURANTE EL PERIODO ENERO 2016 - OCTUBRE 2017, UTILIZANDO LA NORMA INTERNACIONAL COBIT 5.

AUTOR: ANGEL RAMIRO PALACIOS BAYAS

TUTOR: ING. CHRISTIAN PATRICIO VACA BENALCÁZAR. MG. CPA

QUITO - ECUADOR

AÑO: 2018

DECLARACIÓN DE AUTORÍA

El documento de tesis con título: “AUDITORÍA A LA SEGURIDAD INFORMÁTICA EN LA DIRECCIÓN DISTRITAL 02D03 CHIMBO-SAN MIGUEL-EDUCACIÓN DURANTE EL PERIODO ENERO 2016 - OCTUBRE 2017, UTILIZANDO LA NORMA INTERNACIONAL COBIT 5”, ha sido desarrollado por el señor ANGEL RAMIRO PALACIOS BAYAS con C.C. No. 0201780038 persona que posee los derechos de autoría y responsabilidad, restringiéndose la copia o utilización de la información de esta tesis sin previa autorización.

ANGEL RAMIRO PALACIOS BAYAS

UNIVERSIDAD TECNOLÓGICA ISRAEL

CERTIFICACIÓN DEL TUTOR

En mi calidad de Tutor del Trabajo de Titulación certifico:

Que el trabajo de titulación **"AUDITORÍA A LA SEGURIDAD INFORMÁTICA EN LA DIRECCIÓN DISTRITAL 02D03 CHIMBO-SAN MIGUEL-EDUCACIÓN DURANTE EL PERIODO ENERO 2016 - OCTUBRE 2017, UTILIZANDO LA NORMA INTERNACIONAL COBIT 5.",** presentado por: Angel Ramiro Palacios Bayas, estudiante de la Carrera Ingeniería en Sistemas Informáticos, reúne los requisitos y méritos suficientes para ser sometido a la evaluación del Tribunal de Grado, que se designe, para su correspondiente estudio y calificación.

Quito D. M. Septiembre del 2018

TUTOR:

Ing. Christian Patricio Vaca Benalcázar. Mg. CPA

DEDICATORIA

Con mucho cariño dedico el presente trabajo de titulación a mi querida Madre: Tránsito (+) que desde el cielo guía y protege a toda la familia.

A mí querido Padre: Miguel, quien ha dedicado su vida al arduo trabajo de labrar la tierra y ha logrado sobresalir con su familia.

Angel Ramiro Palacios

AGRADECIMIENTO

A la Virgencita del Huayco “Mamá Naty”; por concederme: la salud, la protección en todo momento.

A mi hermano Miguel, quién ha sido el apoyo principal, durante el desarrollo de la carrera.

A mi querida esposa Nataly, quién me apoyado de una u otra manera.

A todos los Conductores Profesionales; quienes llevan sobre sí una responsabilidad enorme de transportarnos con seguridad hacia nuestro destino; y se desvelan por cumplir con su trabajo.

A las Autoridades de la EEB “Federico González Suárez” y UE “Diez de Agosto”, quienes me concedieron el permiso para la asistencia a clases.

Angel Ramiro Palacios

ÍNDICE GENERAL

DEDICATORIA.....iii
AGRADECIMIENTO.....iv
INDICE GENERAL.....v
INDICE DE FIGURAS.....viii
INDICE DE TABLAS.....ix
RESUMEN.....x
ABSTRACT.....xii
INTRODUCCION 1
ANTECEDENTES 1
PLANTEAMIENTO DEL PROBLEMA.....2
FORMULACION DEL PROBLEMA.....2
OBJETIVOS.....3
OBJETIVO GENERAL 3
OBJETIVOS ESPECÍFICOS: 3
ALCANCE.....3
DESCRIPCIÓN DE LOS CAPÍTULOS 4
CAPÍTULO 1 6
FUNDAMENTACIÓN TEÓRICA 6
1.1 ESTADO DEL ARTE 6
1.2 AUDITORÍA. 7
1.2.1 Historia de la Auditoría 7
1.2.2 Tipos de Auditoría 8
1.3 AUDITORÍA INFORMÁTICA 8
1.3.1 Características de una Auditoría en Informática 8
1.3.2 Campos de la Auditoría Informática 9
1.4 SEGURIDAD INFORMÁTICA 9
1.4.1 Etapas de la SI (Seguridad-Informática) 9
1.5 SEGURIDAD DE LA INFORMACIÓN 10
1.6 NORMAS PARA AUDITORÍA DE SI (SISTEMAS-INFORMACIÓN) 10
1.7 ESTÁNDARES DE AUDITORÍA 11
1.8 GUÍAS DE AUDITORÍA 13
1.9 COBIT 13

1.9.1 Cronología de COBIT 13
1.9.2 Principios de COBIT 5 14
1.9.3 Familia de Productos de COBIT 5 14
1.10 CONTROL INTERNO PARA TECNOLOGIAS DE LA INFORMACIÓN 14
1.10.1 COSO..... 14
1.10.2 GTAG.....15
1.10.3 NORMAS GUBERNAMENTALES 16
1.11 MANUAL DE GESTIÓN ADMINISTRATIVA DISTRITAL (SGC) 16
1.12 GESTIÓN DE RIESGOS 16
1.12.1 DEFINICIONES: EVENTO, RIESGO, RIESGO TECNOLÓGICO 17
1.12.2 DETERMINACIÓN DE LOS UMBRALES DE EVALUACIÓN DE RIESGOS 17
1.12.3 Clasificación de Riesgos 18
1.12.4 Respuestas a los Riesgos 19
1.12.5 METODOLOGÍAS PARA EL ANÁLISIS DE RIESGOS – TI 19
1.13 MODELO DE MADUREZ ISO 15504 19
CAPÍTULO 2 21
MARCO METODOLÓGICO 21
2 CARACTERIZACIÓN DEL SECTOR OBJETO DE ESTUDIO DEL PROBLEMA DE INVESTIGACIÓN .. 21
2.1 MISIÓN DE LA UNIDAD DISTRITAL DE TIC's 22
2.2 ENFOQUE METODOLÓGICO DE LA INVESTIGACIÓN 22
2.3 TIPOS DE INVESTIGACIÓN 22
2.3.1 Bibliográfica 22
2.3.2 Descriptiva 22
2.3.3 De Campo 23
2.4 POBLACIÓN Y MUESTRA 23
2.5 TÉCNICAS DE RECOLECCION DE DATOS 23
2.5.1 La Entrevista 23
2.5.2 La Encuesta 24
2.6 PROPUESTA DEL INVESTIGADOR 31
CAPÍTULO 3 32
PROPUESTA 32
3 TEMA 32
3.1.1 INTRODUCCIÓN 32
3.1.2 DESCRIPCIÓN DE LA PROPUESTA 32
3.2 ETAPA DE PLANEACIÓN DE LA AUDITORIA A LA SEGURIDAD INFORMATICA 33
3.2.1 OBJETIVOS 33

3.2.2 ALCANCE 33
3.2.3 ESTUDIO PRELIMINAR 34
3.2.4 EVALUACIÓN DE RIESGOS 34
3.2.5 PROGRAMA DE AUDITORÍA 36
3.2.6 CRONOGRAMA DE AUDITORÍA 40
3.3 ETAPA DE EJECUCION DE LA AUDITORIA A LA SEGURIDAD INFORMATICA 41
3.3.1 REVISIÓN Y EVALUACIÓN DE CONTROLES 41
3.3.2 PRUEBAS DE CUMPLIMIENTO 42
3.3.3 RESULTADOS DE LAS PRUEBAS DE CUMPLIMIENTO 47
3.3.4 PRUEBAS SUSTANTIVAS 48
3.3.5 Prueba Sustantiva – Proceso: Contratación o Adquisición de Bienes y Servicios Tecnológicos 48
3.3.6 Prueba Sustantiva – Proceso: Creación de Cuentas de Usuario y perfiles, para sistemas de Información. 48
3.3.7 Prueba Sustantiva – Proceso: Soporte Técnico 49
3.3.8 Prueba Sustantiva - Proceso: Soporte Técnico – Backups 50
3.3.9 Prueba Sustantiva - Proceso: Instalación de Enlaces de Internet, Datos y Telefonía 52
3.3.10 MAPEO OBJETIVOS DE PROCESOS TIC's, VS DOMINIOS Y PROCESOS COBIT 5 53
3.3.11 ANALISIS DEL MAPEO DE LOS OBJETIVOS TIC's-VS-DOMINIOS DE COBIT 5 55
3.3.12 ANÁLISIS PROCESOS TICS, CON LOS DOMINIOS DE COBIT 5 55
3.3.13 NIVEL DE MADUREZ DE LOS PROCESOS DE TICS-02D03 56
3.4 ETAPA DE COMUNICACIÓN DE RESULTADOS 57
3.4.1 INFORME DE AUDITORÍA A LA SEGURIDAD INFORMÁTICA 57
ÍNDICE DEL INFORME DE AUDITORIA A LA SEGURIDAD INFORMATICA 58
4 CONCLUSIONES Y RECOMENDACIONES 75
5 REFERENCIAS BIBLIOGRÁFICAS 77

ÍNDICE DE FIGURAS

Figura 1 .-Tipos de Auditorías 8
Figura 2.-Etapas de la Seguridad Informática 9
Figura 3.-Cronología de COBIT 13
Figura 4 .- Familia de COBIT 5 14
Figura 5.- Fases de una Gestión de Riesgo. 16
Figura 6 .-Valoración de la Probabilidad 18
Figura 7 .-Valoración del Impacto 18
Figura 8 .-Dirección-Distrital-02D03-Chimbo-San Miguel-Educación 21
Figura 9.-Pregunta Nro. 1-Encuesta a Servidores Públicos del Distrito Educativo 02d03. 26
Figura 10.-Pregunta Nro. 2-Encuesta a Servidores Públicos del Distrito Educativo 02d03 26
Figura 11.-Pregunta Nro. 3 Encuesta a Servidores Públicos del Distrito Educativo 02d03. 27
Figura 12.-Pregunta Nro. 4-Encuesta a Servidores Públicos del Distrito Educativo 02d03. 27
Figura 13.-Pregunta Nro. 5-Encuesta a Servidores Públicos del Distrito Educativo 02d03. 28
Figura 14.-Pregunta Nro. 1-Encuesta a usuarios del Distrito Educativo 02d03. 29
Figura 15.-Pregunta Nro. 2-Encuesta a usuarios del Distrito Educativo 02d03. 29
Figura 16.-Pregunta Nro. 3-Encuesta a usuarios del Distrito Educativo 02d03. 30
Figura 17.-Pregunta Nro. 4-Encuesta a usuarios del Distrito Educativo 02d03. 30
Figura 18.-Pregunta Nro. 5-Encuesta a usuarios del Distrito Educativo 02d03. 31
Figura 19.-Propuesta del Investigador 31
Figura 20 .-Mapa de Procesos 34
Figura 21.-Cronograma de la Auditoría 40
Figura 22.-Evaluación documental de los procesos Tics con los criterios de Información COBIT 5 47
Figura 23.-Arquitectura de Backups 51
Figura 24.-Análisis Mapeo-Objetivos procesos Tics, Vs. Dominios de COBIT 5 55

ÍNDICE DE TABLAS

Tabla 1. Normas Internacionales de Auditoría que deben considerarse en una Auditoría de Sistemas. 10
Tabla 2. Estándares de Auditoría 11
Tabla 3. Guías de Auditoría para TI 15
Tabla 4. Gestión de Riesgos 17
Tabla 5. Clasificación de Riesgos 18
Tabla 6 . Respuestas al Riesgos 19
Tabla 7. Niveles de Madurez-ISO 15004 20
Tabla 8. Descripción de la fórmula del cálculo de la muestra 23
Tabla 9.- Analistas y jefes de los departamentos del Distrito Educativo 24
Tabla 10. Muestra de usuarios del Distrito Educativo 02D03. 24
Tabla 11. Procesos de la Unidad Distrital TIC'S 33
Tabla 12. Promedio de riesgos más críticos 36
Tabla 13. Programa de Auditoría 38
Tabla 14. Matriz de Control 41
Tabla 15. Cuestionario de control – Contratación o Adquisición de Bienes y Servicios Tecnológicos 43
Tabla 16. Cuestionario de control – Creación de Cuentas de usuarios y perfiles, para sistemas de información 44
Tabla 17. Cuestionario de control - Soporte Técnico 45
Tabla 18. Cuestionario de control - Instalación de Enlaces de Internet, Datos y Telefonía 46
Tabla 19. Revisión Documental-Procesos TICS 47
Tabla 20. Activos faltantes en el Inventario de la Unidad Distrital Administrativa 48
Tabla 21. Inventario de Software 49
Tabla 22. *Tabulación de peticiones de Soporte Técnico* 51
Tabla 23. Mapeo Procesos Tics vs Objetivos COBIT 5 54
Tabla 24. Nivel de madurez - Procesos Tics-02d03, según ISO 15504 56
Tabla 25. Resultados de Procesos TICS-02d03 Evaluados 60
Tabla 26. Servidores Públicos relacionados con la Auditoría a la Seguridad Informática. 61
Tabla 27. Efectos del Incumplimiento del Manual de Gestión Administrativa Distrital. 64
Tabla 28. Efectos del Inventario de la Unidad de Tecnologías de la Información y Comunicaciones desactualizado. 65
Tabla 29. Falta de integridad en los datos 66
Tabla 30. Efectos de la Falta de Capacitación y Evaluación a los Usuarios, sobre el uso de cuentas y políticas de contraseñas. 67
Tabla 31. Efectos de la Falta de Seguimiento al Cumplimiento de los Procesos del Manual de Gestión Administrativa Distrital. 68
Tabla 32. Efectos de no utilizar Software Libre; ni de disponer de las licencias de Software Propietario. 69
Tabla 33. Efectos de la falta de Políticas de Continuidad de las Operaciones Tecnológicas. 71
Tabla 34. Efectos de la falta de Administración de la Red LAN 72
Tabla 35. Efectos de la falta de implementación de estándares en la Red LAN 73
Tabla 36. Efectos de la carencia de estándares en la Red LAN 74

RESUMEN

En la actualidad todas las instituciones independientemente del tamaño y del tipo de actividad a la que se dediquen requieren de la tecnología, tanto a nivel de infraestructura, como servicios, de tal manera que la Dirección Distrital 02d03-Chimbo-San Miguel-Educación tiene implementado procesos de gestión de calidad para todas las unidades conforme a la estructura organizacional, por lo tanto la investigación se enfoca en auditar la Unidad de Tecnologías de la Información y Comunicaciones, motivo que es la base fundamental de la operatividad tecnológica y de servicios del Distrito Educativo.

Con el avance tecnológico también han aparecido nuevos métodos de ataques informáticos, que, si no son detectados y controlados a tiempo, pueden llegar a ocasionar grandes pérdidas económicas o de reputación en las organizaciones, empresas… Por lo que se ha visto la necesidad de realizar una Auditoría a la Seguridad Informática en la Unidad Distrital de TIC's, razón que el Distrito Educativo 02d03 cuenta con varios activos que deben ser protegidos en su totalidad y desde la implantación de esta dependencia educativa, no se ha realizado ningún tipo de Auditoría Informática.

La investigación se realizó en base al marco de referencia COBIT.5, que a través de sus Dominios y procesos habilitadores ayuda a las organizaciones en auditorías y en la gestión de TI, generando valor en las partes interesadas, gestionando riesgos, optimizando recursos, así como también aportando en el cumplimiento de leyes, normativas y reglamentos.

El trabajo investigativo se realizó en función de la metodología de auditoría de sistemas: planeación, ejecución y comunicación de resultados, por lo que se partió de un estudio preliminar del Distrito Educativo 02d03, con el propósito de conocer y comprender el entorno a auditar, posterior se diseñó varias herramientas como encuestas, matrices de riesgos, matrices de control, las cuales ayudaron en la recolección de datos y evaluación de controles internos.

La matriz de riesgos se realizó en base a la metodología de análisis y gestión de riesgos MARGETIT, motivo que se relaciona con el uso de las Tecnologías de la Información (TI), permite también minimizar riesgos a través de la aplicación de controles de seguridad; y la información generada es muy valiosa.

Finalmente se revisaron y priorizaron los hallazgos, por medio de la consolidación de los diferentes papeles de trabajo, y se procedió a elaborar el borrador del informe de Auditoría a la Seguridad Informática, luego se socializo con el señor Director Distrital de Educación, donde se recogieron algunas recomendaciones y se plasmó el informe final.

De esta manera se contribuyó significativamente al Distrito Educativo 02d03, proporcionando información sobre la adecuada gestión de riesgos informáticos, con el propósito de precautelar los activos más importantes y aportar en el cumplimiento de los objetivos institucionales.

PALABRAS CLAVES

Auditoría Informática, Seguridad Informática, Gestión de Riesgos, COBIT, Control Interno.

ABSTRACT

Currently all institutions regardless of the size and type of activity to which they dedicate require technology, both at the infrastructure level, as services, so that the District Directorate 02d03-Chimbo-San Miguel-Education has implemented quality management processes for all units according to the organizational structure, therefore the research focuses on auditing the Information and Communications Technologies Unit, reason that is the fundamental basis of the technological operation and services of the Educational District

With the technological advance, new methods of computer attacks have also appeared, which, if not detected and controlled in time, can cause great economic losses or reputational losses in organizations, companies ... Because of what has been seen the need to carry out an Information Security Audit in the ICT District Unit, reason that Educational District 02d03 has several assets that must be protected in their entirety and since the implementation of this educational unit, no type of Computer Audit has been carried out.

The research was carried out based on the reference framework COBIT.5, which, through its Domains and enabling processes, assists organizations in auditing and in IT management, generating value in stakeholders, managing risks, optimizing resources, as well as as well as contributing in compliance with laws, regulations and regulations.

The research work was carried out based on the systems audit methodology: planning, execution and communication of results, so it was based on a preliminary study of Educational District 02d03, with the purpose of knowing and understanding the environment to be audited, later Several tools were designed, such as surveys, risk matrices, control matrices, which helped in the collection of data and evaluation of internal controls.

The risk matrix was based on the MARGETIT risk analysis and management methodology, which is related to the use of Information Technology (IT), it also allows minimizing risks through the application of security controls; and the information generated is very valuable.

Finally, the findings were reviewed and prioritized, through the consolidation of the different work papers, and the draft of the Informatics Security Audit report was drafted, then socialized with the District Director of Education, where they were collected. some recommendations and the final report was.

In this way, significant contribution was made to Education District 02d03, providing information on the adequate management of computer risks, with the purpose of protecting the most important assets and contributing to the fulfillment of institutional objectives.

KEYWORDS

Computer Audit, Computer Security, Risk Management, COBIT, Internal Control.

INTRODUCCIÓN

La Dirección Distrital 02D03 Chimbo-San Miguel-Educación, se ha creado el 25 de enero del 2012 a través del Acuerdo Ministerial 157-12; se encuentra ubicada en la Provincia Bolívar, cantón San Miguel, el referido distrito educativo ofrece varios servicios educativos cómo: Planificar, organizar, gestionar y evaluar las actividades académico, administrativas, que permitan apoyar al análisis, estudio y solución de problemas que afecten a la comunidad educativa y a sociedad en general.

El Distrito Educativo 02d03 es producto del proceso de desconcentración de la Ex Dirección Provincial de Educación Hispana e Intercultural Bilingüe de Bolívar, en conformidad con el proyecto de Nuevo-Modelo-de-Gestión-Educativa (NMGE), donde se ha propuesto la restructuración del Ministerio de Educación en toda la nacionalidad ecuatoriana.

Una de las grandes dificultades que se enfrenta en esta dependencia es no contar con información sobre la gestión de riesgos informáticos, debido a que la implantación de la Dirección Distrital 02d03 Chimbo-San Miguel-Educación se ha realizado en las instalaciones de del Ex Instituto Pedagógico Superior San Miguel, el cual lleva varios años de haberse construido para fines diferentes a los que se está usando actualmente, de tal manera que la instalación de la infraestructura tecnológica a nivel distrital se ha realizado progresivamente, sin contar emplear normas de instalación del cableado estructurado, políticas de seguridad, planes de contingencia, que permitan garantizar la operatividad y ofrecer servicios de calidad conforme a la normativa ISO 9001.

La Auditoría a la Seguridad Informática se desarrolló en base a varios procedimientos de auditoría en conformidad con los estándares y normas de auditorías de sistemas, realizando pruebas de cumplimiento y pruebas sustantivas, con la finalidad de gestionar oportunamente incidentes de seguridad informática que permitan adoptar los controles de seguridad más adecuados.

ANTECEDENTES

Desde la implantación de la Dirección Distrital 02D03 Chimbo-San Miguel-Educación, no se ha realizado ningún tipo de auditoría informática, que permita obtener información sobre

la gestión de riesgos informáticos, conocer el nivel de madurez de los procesos de la Unidad Distrital TIC's.

PLANTEAMIENTO DEL PROBLEMA

En base a varias visitas realizadas al Distrito Educativo 02d03, se ha observado varias dificultades relacionadas con la seguridad informática, las cuales se describe a continuación:

- Falta de Políticas de Seguridad Informática y Seguridad de la Información en la Unidad Distrital TIC's.
- Incumplimiento de los lineamientos del Manual de Gestión Administrativa Distrital.
- Uso de software sin contar la respectiva licencia del fabricante.
- Procedimientos de respaldos de información inadecuados.
- Falta de planes de contingencia.

La Auditoría a la Seguridad Informática permitirá fortalecer los niveles de Seguridad Informática, por medio de una adecuada gestión de riesgos informáticos, a través de la aplicación de políticas y controles de seguridad, con el propósito de proteger los activos más importantes del Distrito Educativo 02d03.

FORMULACIÓN DEL PROBLEMA

¿Cómo verificar de qué manera incide la seguridad informática, en la operatividad de la Dirección Distrital 02d03 Chimbo-San Miguel-Educación?

JUSTIFICACIÓN

Actualmente se vienen presentando algunas dificultades relacionadas con la operatividad de la infraestructura tecnológica, el manejo de la información y la prestación de servicios educativos, por lo que se hace urgente identificar las causas que está originando la problemática, a través de una Auditoría a la Seguridad Informática, de tal manera que se puedan aplicar controles de mitigación oportunamente, antes de que se llegue a materializar algún tipo de amenaza, y ocasione pérdidas irrecuperables, razón que desde la implantación del Distrito Educativo 02d03, en el año 2014, no se ha practicado ningún tipo de Auditoría de Informática.

La Auditoría a la Seguridad Informática, está basada en el marco de referencia COBIT 5, que, a través de su normativa, ayuda a cualquier tipo de organización a crear valor óptimo a partir de las Tecnologías de la Información, también se enfoca en separar el Gobierno de TI, de la Administración y reducir los niveles de riesgos, a más de ofrecer racionalización los diferentes recursos.

La Unidad Distrital TIC's hoy en día se ha convertido en un aspecto clave de las organizaciones en base a la operatividad tecnológica y la prestación de servicios, de tal manera que, si ocurriera un incidente relacionado con las TIC's, inmediatamente resultarían afectados gran parte o todas las operaciones del Distrito Educativo 02d03 serían interrumpidas; por lo que se pretende identificar vulnerabilidades del entorno informático y someterlos a evaluación.

OBJETIVOS

OBJETIVO GENERAL

Realizar una Auditoría de Seguridad Informática, en la Dirección Distrital -02D03-Chimbo-San Miguel-Educación, considerando los indicadores de la normativa COBIT 5, durante el periodo enero 2016-octubre 2017, como apoyo a una correcta gestión de riesgos.

OBJETIVOS ESPECÍFICOS:

- Fundamentar teóricamente: Auditoría Informática, Seguridad Informática, Tipos, Estándares, Normas, y Metodologías.
- Aplicar técnicas de recolección de datos, con el fin de conocer y comprender los procesos del Distrito Educativo 02D03.
- Desarrollar la Auditoría de Seguridad Informática, en base a la metodología de Planificar, Ejecutar y Comunicar Resultados.

ALCANCE

La auditoría a la seguridad informática, consiste en una evaluación exhaustiva, objetiva de los controles internos y externos de la Unidad Distrital TIC's, tanto a nivel de hardware,

como se software, enfocándose en los riesgos más críticos que arroje la matriz de riesgos informáticos.

Los procesos de la Unidad Distrital TIC's objetos de evaluación son:

1. Contratación o Adquisición de Bienes o Servicios Tecnológicos
2. Creación de cuentas de usuarios y perfiles para sistemas de información.
3. Soporte Técnico (Distrital)
    a) Plan de Contingencia de la Unidad Distrital TIC's.
    b) Respaldos de la Información.
    c) Licenciamiento de Software
4. Instalación de Enlaces de Internet Datos y Telefonía.
    a) Redes de Área Local
5. Cierre de cuentas de Sistemas que maneja el Distrito Educativo 02d03.
6. Habilitación de Servicios Tecnológicos restringidos.

En la Auditoría a la Seguridad Informática principalmente se encuentran involucrados todos los Servidores Públicos que conforman el Distrito Educativo y también quienes usan los servicios, de tal manera que se convertirán en la fuente de información, en el desarrollo del trabajo investigativo.

Los procesos de las categorías y subcategorías: "Coordinación Educativa, Desarrollo Profesional, Atención Ciudadana, Administración Escolar, Desarrollo Profesional, Denuncias"; Gestión de Talento Humano, Gestión de Infraestructura, Gestión Financiera, no están considerados en la Auditoría a la Seguridad Informática, motivo que la Unidad de TIC's es la base primordial para el normal funcionamiento de las demás Unidades.

Al concluir la investigación, se redactará un informe de Auditoría a la Seguridad Informática, donde se determine los principales hallazgos, con las respectivas causas, efectos y recomendaciones, basado en el marco de referencia COBIT 5 e ISO 27000, de tal manera de procura realizar una contribución significativa al Distrito Educativo, en la oportuna gestión de riesgos informáticos y la adecuada toma de decisiones.

DESCRIPCIÓN DE LOS CAPÍTULOS

El documento investigativo consta estructurado de la siguiente manera:

Introducción. En esta primera parte, se describe la problemática relacionada sobre la Seguridad Informática, se plantean los objetivos que orientan a la solución del problema, se sustenta la justificación de la realización de la Auditoría a la Seguridad Informática, y se delimita el alcance.

Capítulo 1. Está conformado por la recopilación del fundamento científico de las investigaciones realizadas por varios autores, conjuntamente con las opiniones del autor, en relación a: Auditoría, Auditoría Informática, Seguridad Informática, Seguridad de la Información, Normas de Auditorías de Sistemas nacionales e internacionales, Estándares de Auditoría de Sistemas de Información, COBIT, Control Interno, Normas Gubernamentales, Gestión de Riesgos Metodologías y Niveles de madurez de procesos.

Capítulo II. Corresponde al Marco Metodológico, la caracterización del sector, que es la descripción de la entidad a auditar, también consta los tipos de investigación empelados en la auditoría, la determinación de la población y muestra, las técnicas y herramientas de recolección de datos: entrevistas, encuestas, visitas in situ, observación directa, entre otras. Una vez obtenido los datos, se procedieron a tabular estadísticamente y a realizar el respectivo análisis, que permitió tener una visión global del problema a investigar y proponer la solución a la problemática.

Capítulo III. Consta en sí el desarrollo de la Auditoría a la Seguridad Informática considerando las fases de:

Planeación: Se inició con un estudio preliminar del Distrito Educativo, el diseño de herramientas de recolección y validación de datos, la identificación de riesgos, la elaboración del programa de Auditoría, conforme a los riesgos detectados en la Unidad Distrital TIC's.

Ejecución: Se aplicaron las diferentes herramientas diseñadas en la fase de Planeación, además se realizaron varias pruebas de cumplimiento y pruebas sustantivas.

Comunicación de resultados: Se consolidó los Papeles de Trabajo, se priorizaron los principales hallazgos y redactó el pre informe, se socializo en el Distrito Educativo, se recogieron recomendaciones y se elaboró el respectivo informe final, según las Normas Internacionales de Auditoría (NIA)

CAPÍTULO 1

FUNDAMENTACIÓN TEÓRICA

1.1 ESTADO DEL ARTE

"Se han desarrollado varias investigaciones preliminares relacionadas con el tema propuesto, una de las cuáles se encontró en Escuela Superior Politécnica del Ejército, titulada: Auditoría informática del sistema de información de la empresa Cocinas Internacionales utilizando COBIT Version.5; realizada por Ana Jiménez en el año 2016, donde se concluye que existen varios métodos de evaluación para una auditoría de seguridad de la información, una de ellas es la metodología de Auditoría Basada en Riesgos, la cual permite la identificación y selección de los procesos más críticos que forman parte del negocio." (Jiménez, 2016)

En la misma Universidad, a nivel de Postgrado, se descubrió la tesis titulada: "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", realizada por Edison Casanova y Christian Vaca, en el año 2014, donde da a conocer que mediante el modelo profesional COBIT, se ha podido evaluar y diagnosticar los procesos del SNNA, e identificar riesgos a través de la metodología Auditoría Basada en Riesgos. (Casanova Yandún & Vaca Benalcázar, 2014)

En el repositorio digital de la Universidad Tecnológica ISRAEL, se encontró la investigación Titulada "Auditoría Informática a la Empresa Ecua-Mails", realizada por: Adrián Patricio Pulgarín Álvarez, en el año 2016, donde se menciona que el Framework COBIT, es ampliamente extendido y proporciona una guía de excelentes prácticas, que se pueden aplicar en el control interno y supervisión de TI. (Pulgarín Alvarez, 2016)

También se investigó en el repositorio digital de la Universidad Regional Autónoma de los Andes, consta una investigación titulada: "Auditoría Informática basada en la norma ISO 27004, para el control del parque Tecnológico UNIANDES Puyo, realizada por Nelson Patricio Becerra Arévalo, en el año 2017, en la que se hace referencia a que la Auditoría Informática parte de la necesidad de contar con información que apoye a la toma de decisiones en relación a los controles de los procesos técnicos administrativos y mejorar la funcionalidad operativa sobre los equipos y recursos informáticos. (Becerra Arévalo, 2017)

1.2 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”

“Es la acumulación y evaluación de la evidencia basada en información para determinar y reportar sobre el grado de correspondencia entre la información y los criterios establecidos. La auditoría debe realizarla una persona independiente y competente” (Arens, Elder, & Beasley, 2007, pág. 5)

En base a las definiciones preliminares, se concluye que la Auditoría es una evaluación exhaustiva, objetiva, rigurosa, sobre una actividad, acontecimiento o proceso, basada en el cumplimiento de normas, estándares o reglamentos locales, nacionales e internacionales; a fin de encontrar grados de corresponsabilidad, en un determinado ámbito.

1.2.1 Historia de la Auditoría

El Autor: (Jimenez, 2009) describe: “Una especie de Auditoría se realizó en tiempos remotos, cuando los soberanos exigían el mantenimiento de las cuentas de su residencia por dos escribanos independientes”

La historia da a conocer que la auditoría se ha desarrollado en base al comercio, con la necesidad de hacer revisiones independientes de las cuentas. En el año de 1.862 la auditoría ha sido reconocida por primera vez como una profesión, enmarcada en la Ley Británica de Sociedades Anónimas, de aquel entonces. Se ha desarrollado en la nación de Inglaterra, posterior se ha introducido en Estados Unidos por el año de 1.900, con el propósito de detectar el fraude y errores.

Los fines actuales son: asegurar el cumplimiento de leyes, normas que regulan a las entidades con el objetivo de conocer los estados actuales de sus procesos, finanzas y ganancias de las empresas.

1.2.2 Tipos de Auditoría

Según los Autores (Arens, Elder, & Beasley, 2007), "En su libro de Auditoría, un enfoque integral, menciona tres tipos de auditorías"

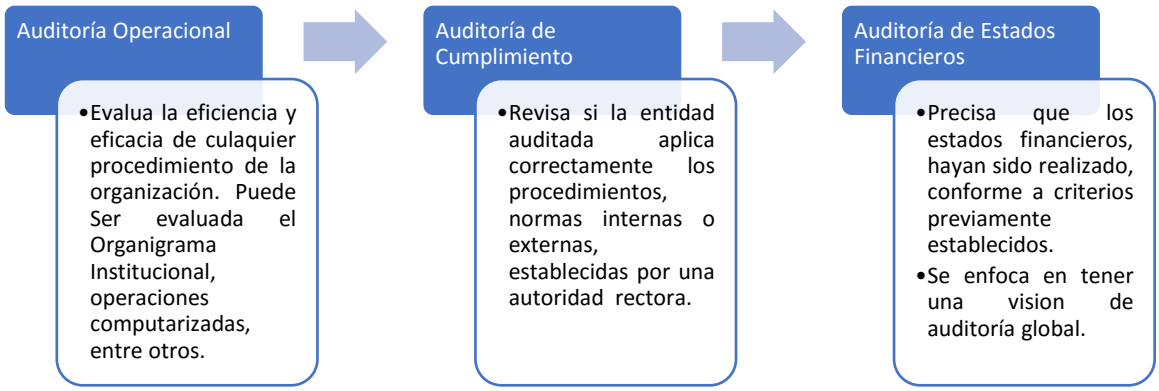


Figura 1 .-Tipos de Auditorías

Fuente: El Autor, a partir de (Arens, Elder, & Beasley, 2007)

Las auditorías pueden ser de dos tipos: interna o externa, la una cuando el auditor forma parte de la entidad auditada, mientras l otra cuando el auditor no tiene ninguna relación con la entidad auditada.

1.3 AUDITORÍA INFORMÁTICA

"Ron Weber en Auditing Conceptual Foundations and Practique, define que la Auditoría Informática es una función que ha sido desarrollada para asegurar la salvaguarda de los activos de los sistemas de computadoras… manteniendo la integridad de los datos y el cumplimiento de los objetivos de la organización en forma eficaz y eficiente; mientras que (Mair, 1991) Mair William manifiesta que Auditoría Informática es la verificación de los controles en las siguientes áreas de la organización:

1. Aplicaciones (programas de producción)
2. Desarrollo de sistemas
3. Instalación de centro de proceso" (Echenique, 2001, págs. 17,18)

1.3.1 Características de una Auditoría en Informática

Hace referencia a la protección del activo más importante de toda entidad (información); así como también los medios tecnológicos que se emplean en el procesamiento de datos, la protección del hardware, software, redes, comunicaciones, bases

de datos. De tal manera que pretende identificar vulnerabilidades y solventarlas a tiempo, por medio de la evaluación de los sistemas, procedimientos, datos, equipos de cómputo, con el propósito de identificar riesgo y aplicar controles adecuados para mitigar el riesgo.

1.3.2 Campos de la Auditoría Informática

"Se enfocan principalmente en: la evaluación administrativa del área de informática, evaluación de los sistemas y procedimientos, eficiencia que se tiene en el uso de la información, evaluación del proceso de datos… y de los equipos de cómputo como Software, Hardware, Redes, Bases de Datos, Comunicaciones, Seguridad y confidencialidad de la información." (Echenique, 2001, págs. 20,21)

1.4 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…".

La seguridad informática se clasifica en: Seguridad Física y Seguridad Lógica; la primera se asocia a la protección física del sistema, ante amenazas como inundaciones, incendios o robos; mientras la segunda se encarga de los mecanismos que protegen la parte lógica de un sistema informático como: datos, aplicaciones y Sistemas Operativos.

En conclusión, la auditoría informática, se encarga de proteger la información, los servicios y la infraestructura tecnológica que lo soporta.

1.4.1 Etapas de la SI (Seguridad-Informática)

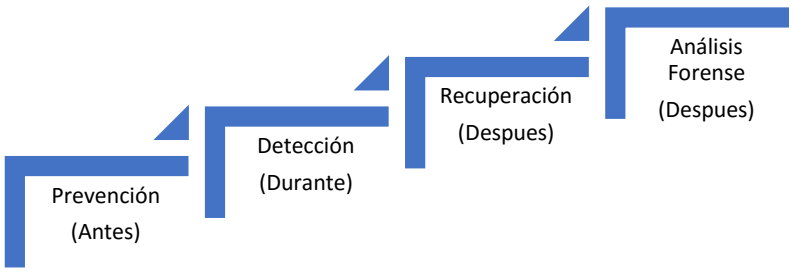


Figura 2.-Etapas de la Seguridad Informática

Fuente: El Autor

1.5 SEGURIDAD DE LA INFORMACIÓN

"Es el conjunto de medidas y procedimientos, tanto humanos como técnicos, que permiten proteger la integridad, confidencialidad y disponibilidad de la información.

- **Integridad:** certificado que tanto la información como sus métodos de proceso son exactos y completos.
- **Confidencialidad:** asegurando que únicamente pueden acceder a la información y modificarla los usuarios autorizados.
- **Disponibilidad:** permitiendo que la información esté disponible cuando los usuarios lo necesiten.

Este término, por lo tanto, es un concepto amplio que engloba medidas de seguridad que afectan… a cualquier tipo de información… soporte en el que se almacene, forma en que se transmita, etc." (Escrivá Gascó, Romero Serrano, & Ramada, 2013, pág. 7)

En base a las definiciones preliminares en relación a la Seguridad Informática se puede deducir que primero debe existir el objeto a proteger (información), luego a través de mecanismos, herramientas u otras técnicas de protección, permitan resguardar los activos más importantes de toda empresa. En conclusión, se puede decir que la Seguridad de la información, depende de la seguridad informática.

1.6 NORMAS PARA AUDITORÍA DE SI (SISTEMAS-INFORMACIÓN)

Entre las principales normas de auditoría de sistemas de información están: Las Normas Internacionales (NIA), los Estándares de ISACA, las Guías de ISACA, COBIT, entre otros.

Tabla 1. Normas Internacionales de Auditoría que deben considerarse en una Auditoría de Sistemas.

FASE	SECCIÓN	DESCRIPCIÓN

PLANIFICACIÓN	NIA 200 NIA 210 NIA 230 NIA 240 NIA 300 NIA 315 NIA 320 NIA 580 NIA 610	Hace referencia a los objetivos globales del profesional a auditar y el desarrollo de la auditoría, acorde con las respectivas normas. Se refiere al pacto de acuerdos del compromiso de la auditoría. Hace referencia sobre la documentación de auditoría Trata sobre la Responsabilidad del Auditor en una Auditoría de Estados Financieros, con respecto al Fraude. Se refiere a la planeación de la Auditoría Financiera Hace referencia sobe la Identificación y estimación de riesgos. Materialidad de la Planificación y Ejecución de la Auditoría. Representaciones de la Administración. Consideraciones del trabajo de una evaluación Interna.
EJECUCION	NIA 402 NIA 500 NIA 530 NIA 620	Consideraciones de la Auditoría que corresponda a una organización que utiliza servicios. Evidencia de la Auditoría debe ser: (Suficiente, Competente y Pertinente) Muestro de Auditoría Utilización de trabajos de un experto.
INFORME Y SEGUIMIENTO	NIA 260 NIA 265 NIA 700 NIA 705 NIA 706	Se refiere al proceso de comunicarse con los encargados del gobierno de la organización o empresa. Comunicación a la alta dirección de las diferencias que se den en el proceso de controles internos. Formación de la opinión y emisión del Informe de Auditoría sobre estados financieros. Se refiere a la modificación del dictamen en el Informe realizado por un auditor que no tenga ninguna relación con la entidad auditada. Párrafo sobre otros temas en el informe proporcionado por un auditor libre.

Fuente: El Autor

1.7 ESTÁNDARES DE AUDITORÍA

Tabla 2. Estándares de Auditoría

GRUPO	ESTATUTO	DESCRIPCIÓN

ESTÁNDARES GENERALES	1001	Indica el propósito, el compromiso, la autoridad del propósito de la auditoría.
	1002	Hace referencia sobre la independencia de la auditoría sobre el área auditada.
	1003	Hace referencia sobre la independencia profesional, se debe ser independiente y objetivo, en la actitud y en la apariencia.
	1004	Se refiere a la Expectativa razonable, en realizar la distribución en conformidad con los estándares de una auditoría.
	1005	Se refiere al adecuado cuidado profesional, se debe observar los estándares de auditoría, en la planificación, ejecución y comunicación de resultados.
	1006	Hace referencia la competencia, se deben poseer la capacidad y la competencia suficiente para realizar la asignación de la auditoría.
	1007	Hace referencia a las afirmaciones, mismas que deben ser posibles de ser: auditadas, deben ser completas, válidas y significantes.
	1008	Se refiere a los Criterios de evaluación del tema, estos deben presentar características de: objetividad, completitud, relevancia, entre otros.
ESTÁNDARES DE DESEMPEÑO	1201	Hace referencia a la Planeación de la distribución de una auditoría, mismas que se deben planificar y documentar en un Plan de Proyecto que aborden: Los Objetivos, el alcance, el cronograma y resultados esperados.
	1202	Se refiere a la valoración del riesgo en la planificación, debe ser adecuado y respaldado por una metodología, a fin de desarrollar el plan de auditoría de Sistemas de Información y priorizar la asignación de recursos.
	1203	Se refiere al desempeño y supervisión; se debe realizar en el trabajo en conformidad con el plan de auditoría de SI aprobado y dentro del cronograma acordado.
	1204	Se refiere a la Materialidad, donde hay que considerar las debilidades al momento de planificar la asignación, considerando a la vez la naturaleza, el tiempo y alcance.
	1205	Se refiere a la obtención de evidencia suficiente y apropiada. (Procedimientos realizados, documentos fuente, formato, información de corroboración, documentar el cumplimiento de leyes, regulaciones y políticas aplicables.
	1206	Se refiere al uso de trabajo de otros expertos, deben ser evaluados y aprobados la idoneidad, experiencia, recursos, independencia, procesos de control.
	1207	Hace referencia a que se debe comunicar de manera oportuna, cualquier acto ilegal o irregularidad material a la parte apropiada.

ESTÁNDARES DE REPORTE	1401	Hace referencia a los Reportes, mismos que deben informar los hallazgos al finalizar la asignación, incluye identificación de la empresa, destinatarios, restricciones, objetivos, alcance, hallazgos respaldados con evidencia suficiente, conclusión y recomendación de la auditoría, firma y fecha.
	1402	Se refiere a las actividades de seguimiento, mismas que deben ser observadas, a fin de concluir si la entidad auditada ha tomado las recomendaciones realizadas por el auditor.

Fuente: El Autor, a partir de (ISACA, 2013)

1.8 GUÍAS DE AUDITORÍA

Las guías de Auditoría apoyan a los estándares y se dividen en tres categorías:

1. **Guías generales Series 2000 (2001-2008)**.-Hacen referencia al estatuto de Auditoría, independencia de la Auditoría, independencia profesional, expectativa razonable, debido cuidado profesional, competencia, afirmaciones y criterios.
2. **Guías de rendimiento Series 2200 (2201-2208).-** Hace referencia a la planeación de la distribución, análisis de riesgo en la planificación, rendimiento y supervisión, materialidad, evidencia, trabajos de otros auditores, actos irregulares y muestreos.
3. **Guías de presentación de informes Series 2400 (2401-2402).-**Hacen referencia a los reportes y actividades de seguimiento.

1.9 COBIT

(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."

1.9.1 Cronología de COBIT

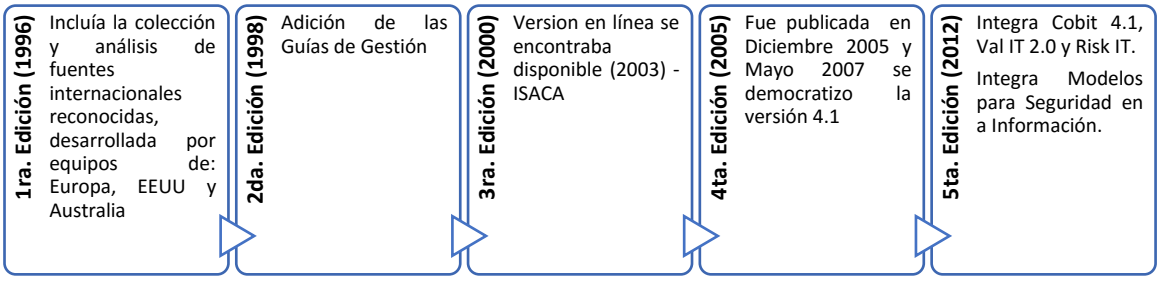


Figura 3.-Cronología de COBIT

Fuente: El Autor a partir de: (ITSI, 2016)

COBIT 5 propone 37 procesos, organizados en 5 Dominios: "Evaluar Dirigir y Monitorear, Alinear Planear y Organizar, Construir Adquirir e Implementar, Entregar Servir y Dar Soporte, Monitorear, Evaluar y Valorar" **(ISACA , 2012)**

1.9.2 Principios de COBIT 5

Existen cinco principios: el primero está relacionado con la satisfacción de las necesidades de las partes interesadas, se enfoca en la entrega de valor; el segundo principio trata sobre cubrir las organizaciones de extremo a extremo, donde cubre el Gobierno y la Administración; el tercer principio se enfoca en aplicar un solo marco de control integrado que abarca: COSO, ERM, e ISO 3100, como a los relacionados a TI: ISO 27000, ITIL, PMBOOK, CMMI; el cuarto principio hace referencia sobre un enfoque holístico de cultura, principios, políticas, marcos y recursos que pueden ser personas, infraestructura, aplicaciones. Finalmente existe el principio de separación del gobierno de la administración, donde el primero se encarga de asegurar el cumplimiento de objetivos organizacionales; mientras el segundo planifica, diseña, realiza y supervisa las actividades determinadas por el gobierno. (ISACA , 2012)

1.9.3 Familia de Productos de COBIT 5

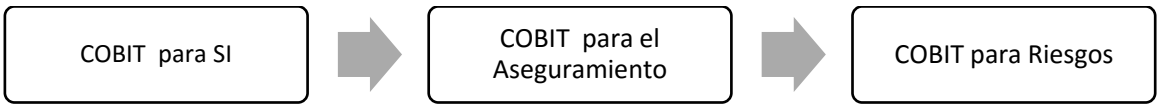


Figura 4 .- Familia de COBIT 5
Fuente: El Autor, a partir de: (ISACA , 2012)

1.10 CONTROL INTERNO PARA TECNOLOGIAS DE LA INFORMACIÓN

Entre los principales controles internos para auditoría de Sistemas están COSO, COBIT, GTAG.

1.10.1 COSO

Es un marco de control interno líder a nivel mundial por su desempeño, fue desarrollado por el Comité de organizaciones patrocinadoras de la Comisión Treadway, de EEUU, la primera versión ha sido en 1992 equivalente a Coso I, posterior COSO II en el año 2004 y la última versión es la COSO III del año 2013; se enfoca en adaptarse a cambios de los avances tecnológicos, ayuda en el cumplimiento de objetivos de las empresas, mitigación

de los riesgos hacia un nivel tolerable, apoya en las decisiones y al gobierno. (Galaz & Ruiz, 2015)

1.10.2 GTAG

Son guías de Auditoría de Tecnología Global, preparadas por el Instituto de Auditores Internos (IIA) están escritas en un lenguaje directo de negocio con el propósito de abordar de forma oportuna problemas relacionados con la gestión, el control y seguridad de las Tecnologías de la Información. La colección de GTAG se utiliza como un recurso disponible para los directores ejecutivos de auditoría sobre los distintos riesgos asociados a la tecnología y las prácticas recomendadas. (Instituto de Auditores Internos de España, 2014)

Tabla 3. Guías de Auditoría para TI

Ref.	GTAG
1	Controles de TI
2	Controles de administración de parches y cambios: cruciales para la cosecusión del éxito de las entidades.
3	Auditoría contínua: implicancias para el aseguramiento, la supervisión y la valoración de vulnerabilidades (riesgos)
4	Gestión de Auditoría de Tecnologías de la Información
5	Gestión y Auditoría de riesgos de privacidad
6	Gestión y Auditoría de puntos vulnerables de Tecnologías de la Información
7	Tercerización de Tecnologías de la Información
8	Auditar controles de Aplicaciones
9	Gestión de identidades y accesos
10	Administración de continuidad de negocio
11	Entregar el Plan de Auditoría de TI.
12	Evaluación de Proyectos TI.
13	Prevención y Detección de Fraude en un mundo automatizado.
14	Auditoría a la enterga de aplicaciones de usuarios
15	Gobierno de Seguridad de la Información
16	Tecnología de Análisis de Datos.

Fuente: El Autor, a partir de: (Instituto de Auditores Internos de España, 2014)

1.10.3 NORMAS GUBERNAMENTALES

En el Ecuador la Contraloría (CGE) ha establecido las Normas de Control Interno para evaluar entidades, organismos de carácter público y también de personal jurídico de derecho privado, que manejen recursos públicos: Se dispone de Normas generales (100), Ambiente de Control (200), Evaluación de Riesgos (300), Actividades de Control (400), Información-Comunicación (500), Seguimiento (600), las norma 410 (1-17) es relacionada con las TI (CONTRALORIA GENERAL DEL ESTADO, 2014)

1.11 MANUAL DE GESTIÓN ADMINISTRATIVA DISTRITAL (SGC)

Es un Manual, caracterizado por la certificación ISO-9001, de gestión de calidad que tiene implementado el Ministerio de Educación del Ecuador, con el cual se proporcionan servicios efectivos en cada Dirección Distrital a nivel nacional, a través de la estandarización de los procesos de atención ciudadana (AC); incrementando el regocijo del usuario, disminuyendo las quejas, los plazos de respuesta de servicios solicitados por usuarios de las instituciones educativas, logrando la satisfacción del usuario a través de un ciclo de mejora frecuente. (MINISTERIO DE EDUCACION DEL ECUADOR, 2015)

1.12 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.

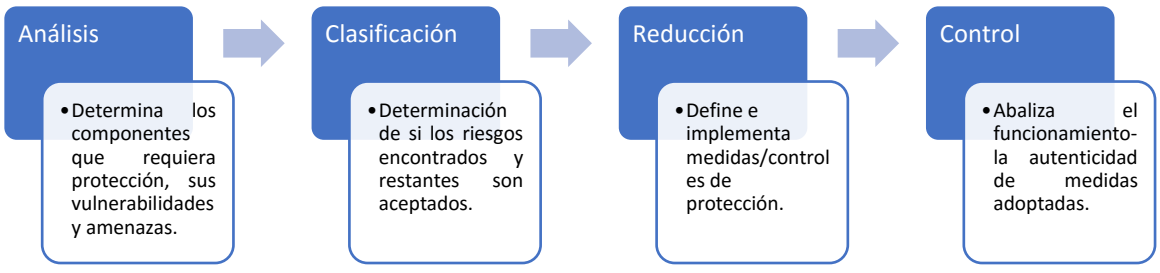


Figura 5.- Fases de una Gestión de Riesgo.

Fuente: El Autor, a partir de: (Erb, 2008)

La Gestión de Riesgos, se describe en la Tabla 4.

Tabla 4. Gestión de Riesgos

Nivel de Riesgo	Definición
Apetito al Riesgo	Nivel de riesgo aceptable para el cumplimiento de objetivos, establecidos por la autoridad rectora de las organizaciones.
Tolerancia al Riesgo.	Cantidad máxima de riesgo que está dispuesta a asumir la autoridad rectora de la organización con el propósito de cumplir los objetivos.
Capacidad de Riesgo	Cantidad y tipo de riesgo máximo que la organización es capaz de soportar con el propósito de cumplir los objetivos.

Fuente: El Autor, a partir de: (Casanova Yandún & Vaca Benalcázar, 2014)

1.12.1 DEFINICIONES: EVENTO, RIESGO, RIESGO TECNOLÓGICO

Evento. -Es un incidente o acontecimiento procedente de fuentes internas o externas, que afecta al alcance de objetivos; pueden generar un impacto en beneficio, o en contra, o a su vez de ambos tipos. (Price Waterhouse Coopers, 2005)

Riesgo. -Es la posibilidad de ocurrencia de un evento, y como consecuencia puede generar un impacto en relación al alcance de objetivos. Los riesgos también pueden incidir de manera positiva en el cumplimiento de objetivos.

Según el Estándar de Control Interno JB-2005-834 los riesgos, pueden provenir de diferentes factores: Personas, TI, Procesos, o Eventos Externos.

Riesgo Tecnológico. -ISACA define **"**El riesgo de negocio asociado al uso, propiedad, operación, participación, influencia y adopción de las Tecnologías de la Información (TI) en la organización"

1.12.2 DETERMINACIÓN DE LOS UMBRALES DE EVALUACIÓN DE RIESGOS

Son evaluados desde dos perspectivas: Probabilidad e Impacto, utilizando las técnicas de evaluación cualitativa o cuantitativa.

Probabilidad. - Se mide conforme a la Figura 6.

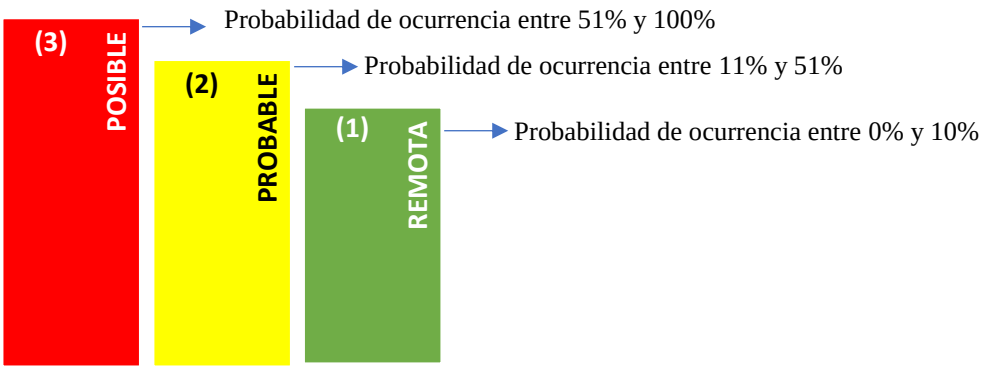


Figura 6 .-Valoración de la Probabilidad

Fuente: El Autor, a partir de: (Muñoz Vega, y otros, 2015)

Impacto. -Es calificado cuantitativamente en: Alto (3), Moderado (2) y Bajo (1), conforme se muestra a continuación.

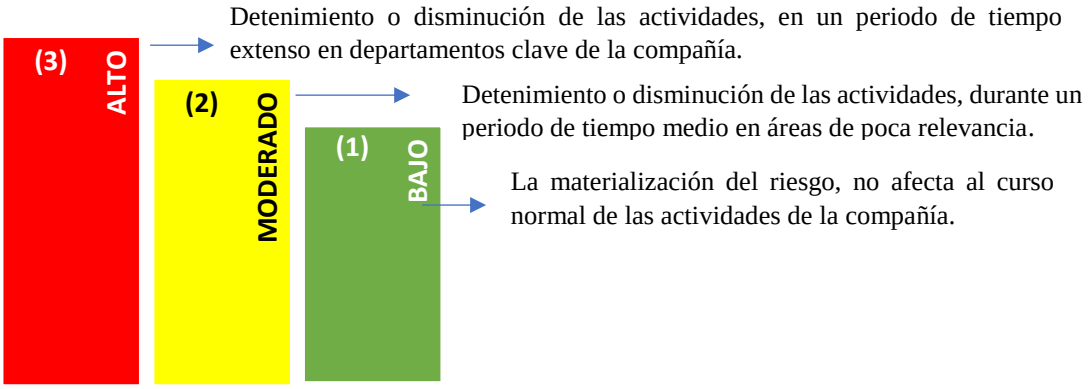


Figura 7 .-Valoración del Impacto

Fuente: El Autor, a partir de: (Muñoz Vega, y otros, 2015)

1.12.3 Clasificación de Riesgos

Tabla 5. Clasificación de Riesgos

CLASIFICACIÓN DE RIESGOS	
RIESGO	
Riesgo Inherente – RI	Es el riesgo propio de la naturaleza del giro del negocio que tiene la organización.
Riesgo de Control – RC	Es el peligro de que exista un error importante que no sea mitigado por los controles internos de la entidad.
Riesgo de Detección – RD	Es el peligro de concluir que no existan errores importantes cuando si los hay, producto de aplicar procedimientos inadecuados de auditoría.
Riesgo de Auditoría – RA	Corresponde a la suma (RI, RC y RD), permite establecer la capacidad de riesgo que puede aceptar en una evaluación.
Riesgo Residual – RR	Es el riesgo remanente, después de la acción realizada por la administración para modificar la probabilidad o impacto.

Fuente: El Autor, a partir de (Vaca, 2017)

1.12.4 Respuestas a los Riesgos

Tabla 6 . Respuestas al Riesgos

Categorías	Definición
Evitar los riesgos	Eliminar toda la posibilidad de que ocurran.
Reducir los riesgos	Por medio de la aplicación de controles.
Transferir los riesgos	Por medio de pólizas compartimos el riesgo.
Aceptar los Riesgos	Vivir con ellos bajo políticas y criterios que haya establecido la organización, para aceptarlos.

Fuente: El Autor, a partir de: (Casanova Yandún & Vaca Benalcázar, 2014)

1.12.5 METODOLOGÍAS PARA EL ANÁLISIS DE RIESGOS – TI

El objetivo de las Metodologías, es planificar la disminución de riesgos, detectar las debilidades existentes y ayudar con información estratégica en la toma de decisiones relacionadas con la seguridad informática.

OCTAVE. -EL objetivo de la metodología es facilitar la evaluación de riesgos en una organización, enfocándose a que la organización sea capaz de:

- Dirigir y gestionar sus evaluaciones de riesgo.
- Tomar decisiones, basándose en sus riesgos.
- Proteger los activos claves de la información.

MARGERIT 2.-El propósito es concienciar a los que están al frente de las organizaciones de que existen riesgos y que hay que gestionarlos, se conforma de cuatro fases: Planificación del Proyecto de Riesgos, Análisis de Riesgos, Gestión de Riesgos y Selección de Salvaguardas.

MEHARI. -El propósito de la metodología es analizar el riesgo y valorarlo, sigue todo un proceso de gestión de riesgo que puede ser comparado con las ISO/IEC 27003. (Calero, Flores, & Amador, 2016)

1.13 MODELO DE MADUREZ ISO 15504

"Es un modelo integrado con ISO 27000 de seguridad e ISO 20000 de servicios de tecnología de la información, permite evaluar los niveles de madurez de los procesos de Tecnologías de la Información hacia un ciclo de mejora, es un modelo CMMI, desarrollado por Carnegie-Mellon University" (Sistema de Gestión de Seguridad de la Información, 2018)

Tabla 7. Niveles de Madurez-ISO 15004

Valoración	Término	Descripción
0	Inmadura	No hay implementación de Procesos
1	Básica	Se alcanzan los objetivos de los Procesos
2	Gestionada	Gestión de procesos y productos
3	Establecida	Procesos-adoptados estándares
4	Predecible	Gestión cuantitativa
5	Optimizada	Mejora continua de los procesos

Fuente: El Autor, a partir de: **(Castiñeira, 2013)**

CAPÍTULO 2

MARCO METODOLÓGICO

2 CARACTERIZACIÓN DEL SECTOR OBJETO DE ESTUDIO DEL PROBLEMA DE INVESTIGACIÓN

La Dirección Distrital 02D03 Chimbo-San Miguel- Educación se encuentra ubicada en la Provincia Bolívar, cantón San Miguel, Avenida el Maestro, junto a la Unidad Educativa del Milenio “Angel Polibio Chaves”; es una entidad encargada de fomentar el desarrollo de la educación, el acervo cultural y garantizar el acceso democrático a la educación a la población de los Cantones Chimbo y San Miguel.

La instalación física es parte del Ex Instituto Tecnológico Superior San Miguel; cuenta con dos bloques de infraestructura, cada uno de 2 pisos; además dispone de espacios verdes, campos deportivos; servicio de guardianía privada.

Fue creada legalmente en base al Nuevo Modelo de Gestión Educativa y a través del Acuerdo Ministerial Nro. 0015-14 de fecha 03 de febrero del 2014, suscrito por Augusto Espinosa Ministro de Educación de aquel entonces.

Figura 8 .-Dirección-Distrital-02D03-Chimbo-San Miguel-Educación
Fuente: El Autor

El Distrito Educativo, con el propósito de realizar las diferentes actividades que impulsa, aplica procesos: Gobernantes y Adjetivos, acorde al Manual de Gestión Administrativa Distrital, basado en la Norma ISO 9001 del (SGC), el cual se detalla en el mapa de procesos en el capítulo de la propuesta.

2.1 MISIÓN DE LA UNIDAD DISTRITAL DE TIC's

"Aplicar e implementar las políticas, normas, procedimientos que efectivicen la gestión y administración de las TI, orientados al ahorro de recursos, sistematización y automatización de los procesos correspondientes al ámbito de su gestión." (MINISTERIO DE EDUCACION, 2012)

2.2 ENFOQUE METODOLÓGICO DE LA INVESTIGACIÓN

El enfoque metodológico que se utilizó en la investigación es cualitativa y cuantitativa, considerando la naturaleza del problema, los recursos humanos, materiales y el contexto distrital. Es cualitativo, debido a que se empleó entrevistas, guías de observación a fin de comprender la problemática; y es cuantitativo motivo que se recolectaron, procesaron y analizaron datos estadísticos.

2.3 TIPOS DE INVESTIGACIÓN

2.3.1 Bibliográfica

Se utilizó en la descripción del Marco Teórico, en base a la revisión de libros, tesis, artículos científicos a fin de comprender las diferentes opiniones de varios autores en relación a Auditoría, Auditoría Informática, Seguridad Informática, Estándares, Gestión de Riesgos, Marcos Normativos, COBIT, entre otros.

2.3.2 Descriptiva

También se lo conoce con el nombre de investigación exploratoria, la característica fundamental, es la de presentar una interpretación correcta de una situación o fenómeno, indicando sus rasgos más propios o distintos. Los tipos de estudios a realizar pueden ser: Encuestas, Casos Exploratorios, Casuales, Predictivos, entre otros.

2.3.3 De Campo

Consiste en un proceso disciplinado de recolectar, procesar y analizar datos obtenidos de fuentes primarias, a través de la aplicación de diferentes instrumentos de recogimiento de datos, con la finalidad de llegar a comprender el contexto distrital.

2.4 POBLACIÓN Y MUESTRA

La población está conformada por quienes conforman el Distrito Educativo 02d03, e inciden de manera directa o indirecta. A través de la siguiente fórmula se calculará la muestra, cuando se conoce el tamaño de la población.

$$Muestra = \frac{Población}{(Población - 1) * error^2 + 1}$$

Tabla 8. Descripción de la fórmula del cálculo de la muestra

Categoría	Abreviatura / Descripción
Muestra	M
Población	Número de sujetos objeto de estudio
Error máximo admitido	$0{,}05^2$

Fuente: El Autor

2.5 TÉCNICAS DE RECOLECCION DE DATOS

Entre las principales técnicas de recolección de datos que se aplicaron fueron: entrevista, encuesta, guías de observación, entre otros.

2.5.1 La Entrevista

Es una técnica de recolección de datos, basada en una guía de preguntas bien estructuradas objetivas y planificadas, con el objetivo de recabar información cualitativa; en Auditoría a la Seguridad Informática este instrumento se aplicó al señor director del Distrito Educativo 02d03 y Analista Distrital de la Unidad de TIC’s.

2.5.2 La Encuesta

Es una técnica que permite recoger datos, en base a la formulación de varias preguntas abiertas o cerradas a manera de cuestionarios, es utilizada principalmente cuando el tamaño de la población es grande.

Por tratarse de una población finita de 56 servidores públicos no se aplicó la fórmula para la obtención de la muestra.

Tabla 9.- Analistas y jefes de los departamentos del Distrito Educativo

Denominación	Nro.
Analistas Departamentales	51
Jefes Departamentales	10
TOTAL	**61**

Fuente: El Autor

Cálculo de la Muestra de las Encuestas a Usuarios del Distrito Educativo 02d03.

Para la obtención de la muestra se aplicó la fórmula especificada en el apartado de Población y Muestra.

$$M = \frac{701}{(701-1) * 0{,}05^2 + 1} \; M = \frac{701}{2{,}75}$$

M=255

Tabla 10. Muestra de usuarios del Distrito Educativo 02D03.

Denominación	Nro.
Autoridades de las Instituciones Educativas	92
Docentes	163
TOTAL	**255**

Fuente: El Autor

Análisis de las Entrevistas realizadas

- **Entrevista - Director Distrital -** Lcdo. David Galarza (Anexo 1)

El Señor director del Distrito Educativo 02d03, manifiesta que actualmente tiene implementado el Distrito Educativo 02d03 la WAN Educativa, misma que provee la conectividad a diferentes servicios que va hacia la CZ5 (Coordinación Zonal5) y directamente a planta central, de tal manera que el MINEDUC da seguimiento a los diferentes Distritos Educativos, a nivel nacional.

También da a conocer este tipo de infraestructura tecnológica ocasionalmente presenta indisponibilidad del servicio a veces a la semana o a veces en el mes se pierde la conectividad un día; menciona que los activos importantes del Distrito son: Los equipos informáticos razón que son las herramientas de trabajo del personal; y la información son los recursos con los que se trabaja, de tal manera que se respalda la información a través del modelo de gestión que tiene implementado el Ministerio de Educación (MINEDUC) y el Distrito Educativo 02d03.

Una de las medidas de seguridad menciona que por las noches dispone el servicio de guardianía y en el día cada servidor público es custodio de su bien; lo que falta fortalecer es la conectividad a varias unidades educativas que se encuentran en el sector rural y a los administradores Circuitales que están por lugares de difícil acceso; también menciona que las instalaciones son antiguas, que viene el Ex Instituto Superior Pedagógico San Miguel; finalmente menciona que no se ha realizado ningún tipo de auditoría informática y felicita la investigación que se está realizando porque permitirá aplicar los correctivos necesarios y evitar que no exista falencias a futuro.

- **Entrevista – Analista Distrital TIC's - Lcdo. Carlos Aroca. (**Anexo 2)

En base a la entrevista, se puede concluir que la mayor problemática son los requerimientos de soporte técnico y los eventos que se han detectado han sido contagio de virus informáticos, debido a que los usuarios no tienen una responsabilidad de seguridad informática al utilizar los equipos, también han existido daños en las partes físicas de algunos equipos informáticos, e incumplimiento del manual de procesos. En relación a la información se obtiene mensualmente respaldos de todas las oficinas en un disco duro externo.

Resultados de la Encuesta a Servidores Públicos y Usuarios del Distrito Educativo 02d03.

1) ¿Seleccione el nivel con el que usted se identifica en el tema Seguridad Informática?

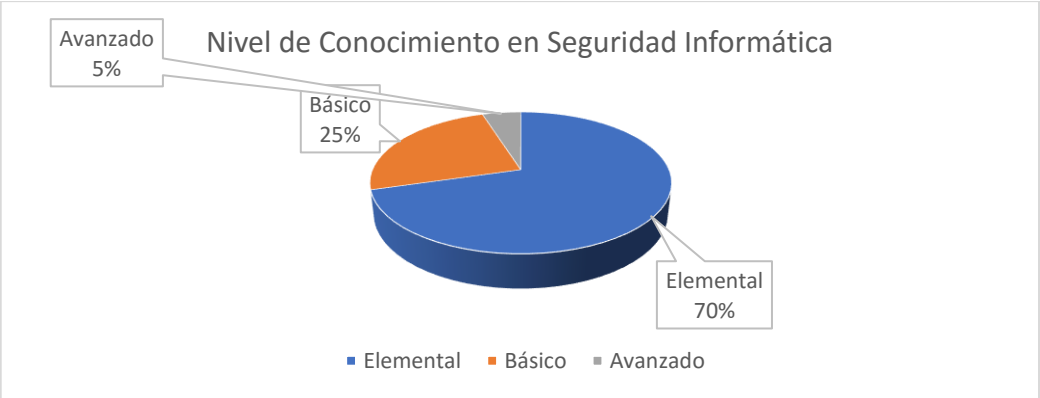


Figura 9.-Pregunta Nro. 1-Encuesta a Servidores Públicos del Distrito Educativo 02d03.
Fuente: El Autor

Análisis

La mayoría de encuestados concuerdan que cuentan con un nivel de conocimiento Elemental en temas de Seguridad Informática, lo cual es un riesgo debido al avance tecnológico y la cantidad de ataques informáticos que se producen cotidianamente, un porcentaje significativo del 25% tienen conocimiento básico de estos temas, y un 5% conocen seguridad informática en un nivel avanzado, lo cual facilitaría el fortalecimiento de la SI en el Distrito Educativo.

2) ¿El control de acceso a la estación de trabajo es…?

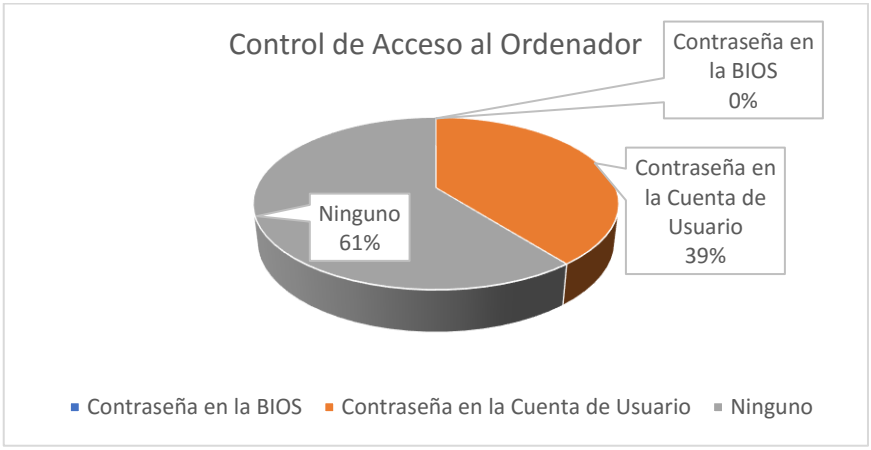


Figura 10.-Pregunta Nro. 2-Encuesta a Servidores Públicos del Distrito Educativo 02d03
Fuente: El Autor

Análisis

En un 61% de encuestados indican que las computadoras que usan en el trabajo no disponen de controles de acceso como contraseñas, de tal manera se genera riesgo en relación a la SI; mientras un 39% manifiestan que utilizan contraseñas en las cuentas de usuario.

3) ¿Con que frecuencia se ha presentado indisponibilidad de equipos o servicios Informáticos?

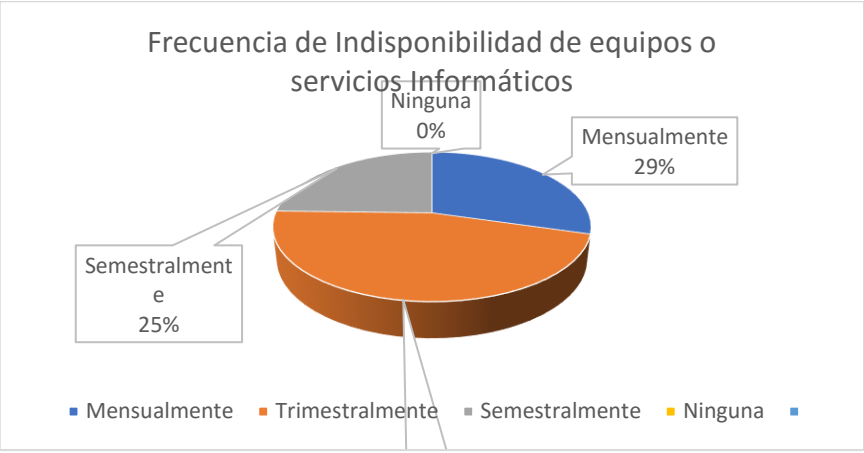


Figura 11.-Pregunta Nro. 3 Encuesta a Servidores Públicos del Distrito Educativo 02d03.
Fuente: El Autor

Análisis

Según los resultados de la encuesta en un 46% de encuestados revelan que trimestralmente, los equipos o servicios informáticos presentan algún tipo de indisponibilidad, por lo tanto, se debe aplicar controles de mitigación de inconvenientes, con el propósito de garantizar la continuidad de las operaciones tecnológicas y cumplir con el objetivo del Manual de gestión Administrativa Distrital de ofrecer servicios de calidad y eficientes; mientras un 25% responden que existe interrupciones de servicios semestralmente y un 29% opinan que es mensualmente.

4) ¿Dispone de Inventario Actualizado?

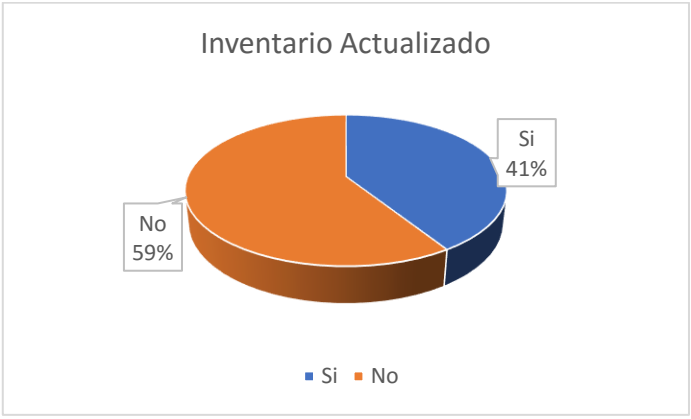


Figura 12.-Pregunta Nro. 4-Encuesta a Servidores Públicos del Distrito Educativo 02d03.
Fuente: El Autor

Análisis

En base a la encuesta el 59% de encuestados dan a conocer que no disponen del inventario actualizado de su oficina; de tal manera existe un alto riesgo de pérdida de los activos; mientras un 41% si mantienen actualizado los inventarios, lo cual es muy bueno para el Distrito Educativo 02d03.

5) ¿Considera que los equipos Informáticos deben ser remplazados por nuevos y de mejores características a fines de realizar un trabajo eficiente y confiable?

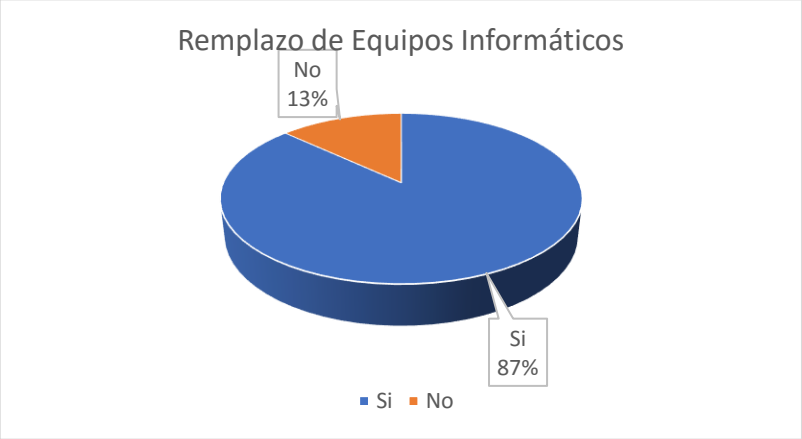


Figura 13.-Pregunta Nro. 5-Encuesta a Servidores Públicos del Distrito Educativo 02d03.
Fuente: El Autor

Análisis

La mayoría de encuestados desean que los equipos informáticos sean remplazados, a fin de realizar un trabajo eficiente y seguro; mientras un 13%, dan a conocer que se encuentran conformes

Resultados de la Encuesta a Usuarios del Distrito Educativo 02d03.

1) ¿Considera que los servicios ofrecidos por el Distrito Educativo 02d03, son eficientes?

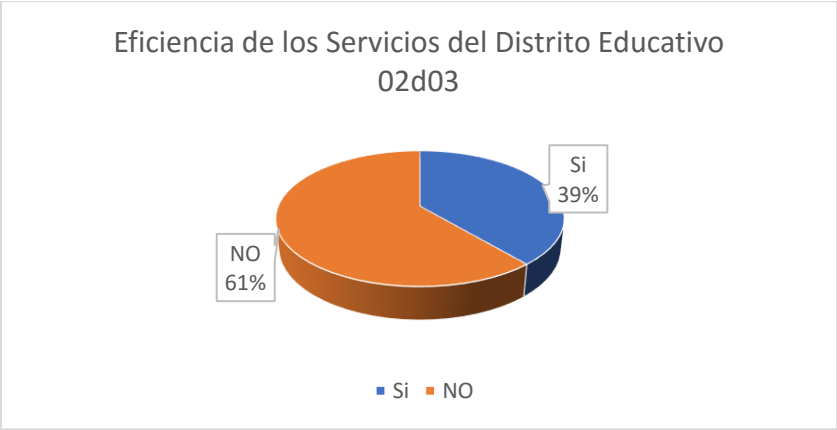


Figura 14.-Pregunta Nro. 1-Encuesta a usuarios del Distrito Educativo 02d03.

Fuente: El Autor

Análisis

Un 61% de encuestados están de acuerdo en que no son eficientes los servicios educativos ofrecidos por el Distrito Educativo 02d03, por lo tanto, se debería considerar realizar seguimientos a los procesos del Sistema de Gestión de Calidad (SGC), con el propósito de ofrecer mejores servicios a los usuarios internos o externos; mientras un significativo porcentaje del 39% de encuetados expresan que los servicios recibidos son eficientes.

2) ¿La comunicación entre Distrito Educativo e Instituciones Educativas es:

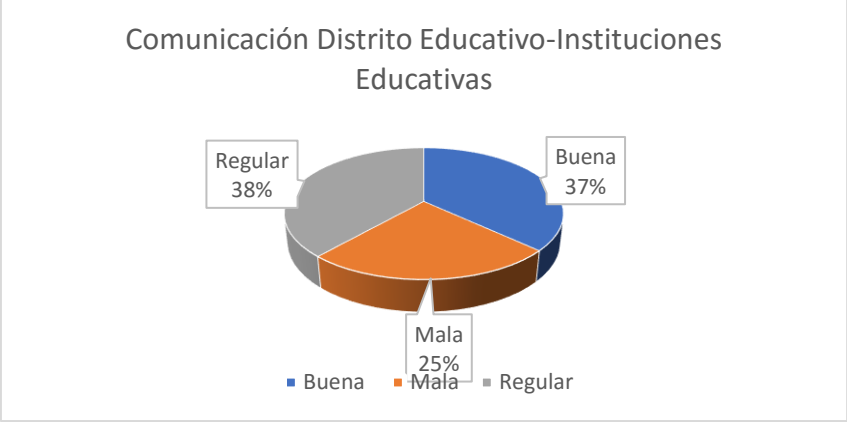


Figura 15.-Pregunta Nro. 2-Encuesta a usuarios del Distrito Educativo 02d03.

Fuente: El Autor

Análisis

Un 37% del personal encuestado califica como buena a la comunicación entre Distrito Educativo e Institución Educativa, mientras un 38% manifiesta que es Regular y un 25% califica de mala, lo cual hace un llamado a tomar acciones inmediatas de mejoras.

3) ¿La información es solicitada, a través de?

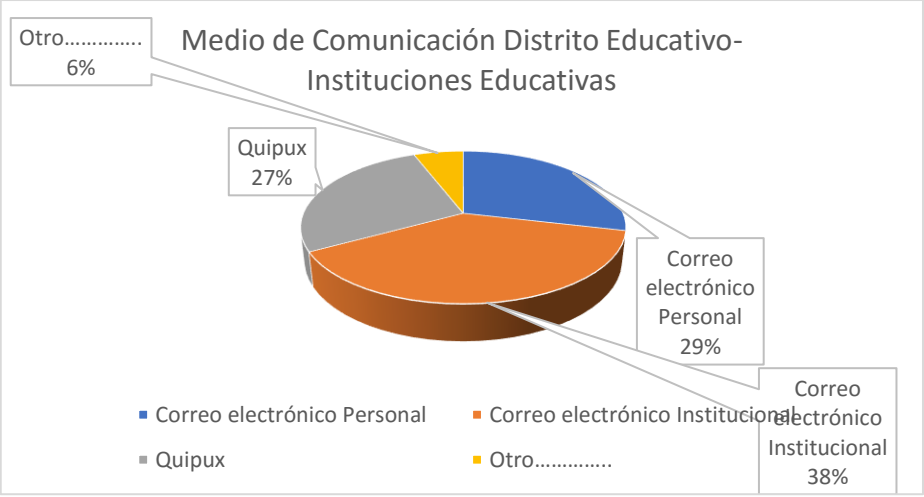


Figura 16.-Pregunta Nro. 3-Encuesta a usuarios del Distrito Educativo 02d03.
Fuente: El Autor

Análisis

En un porcentaje de 56% de encuestados revelan que la información es solicitada electrónicamente por el email institucional, mientras un 29% lo hace a través del correo electrónico personal, un 27% a través del Sistema de Gestión Documental Quipux y un 6% emplea otro medio como llamadas telefónicas, visitas in situ, entre otras…

4) ¿Cómo caracteriza los datos que proporciona al Distrito Educativo 02d03?

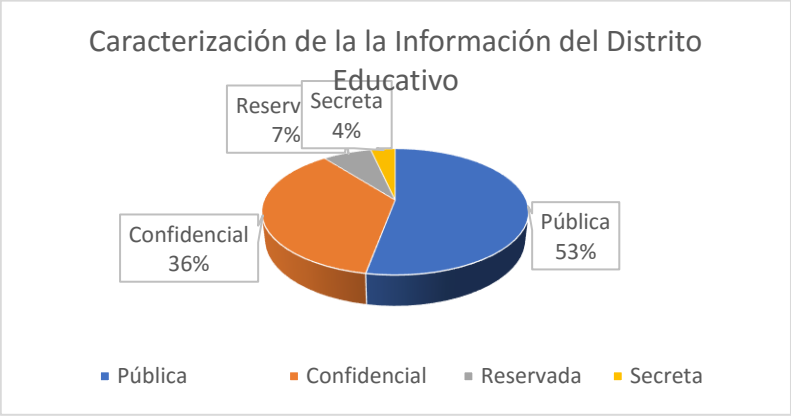


Figura 17.-Pregunta Nro. 4-Encuesta a usuarios del Distrito Educativo 02d03.
Fuente: El Autor

Análisis

Los encuestados indican que la información que se transmite entre Distrito Educativo e Instituciones Educativas en un 53% se catalogaría como información pública que no

afectaría si fuera revelada, un 36% manifiestan que es de carácter confidencial, afectaría a la honra de las personas si fuera descubierta, por ejemplo: Sumarios Administrativos, un 7% manifiestan que es de carácter reservado y un 4% de encuestados expresan que la información que maneja el Distrito es secreta.

5) ¿Está de acuerdo que se mejoren los servicios de la Unidad Distrital TIC's

Si ( ) No ( )

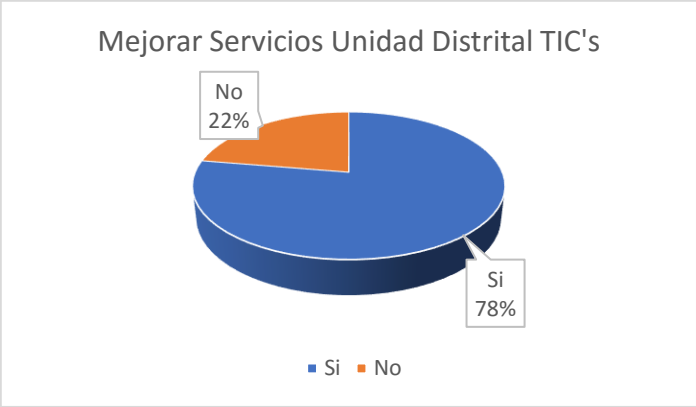


Figura 18.-Pregunta Nro. 5-Encuesta a usuarios del Distrito Educativo 02d03.

Fuente: El Autor

Análisis

La mayoría de encuestados consideran que, si hay que mejorar la infraestructura de la Unidad Distrital TIC's del Distrito Educativo 02d03, de tal manera se deben realizar gestiones inmediatas con el propósito de cumplir mejorar el indicador en referencia a la entrega de servicios de calidad a usuarios internos o externos; mientras una minoría están conformes con los servicios ofrecidos.

2.6 PROPUESTA DEL INVESTIGADOR

En base al procesamiento de datos, obtenidos a través los diferentes instrumentos de recolección de datos, el Distrito Educativo 02d03 ha propuesto la necesidad de realizar una Auditoría a la Seguridad Informática, a través del marco de referencia COBIT 5, y se desarrollará según las fases de la Auditoría de Sistemas, propuestas por las (NIA).

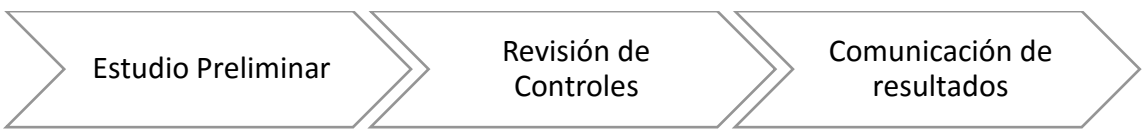


Figura 19.-Propuesta del Investigador

Fuente: El Autor

CAPÍTULO 3

PROPUESTA

3 TEMA

Auditoría a la Seguridad Informática, basada en el marco de referencia COBIT 5, durante el periodo enero 2016-octubre 2017, en la Dirección Distrital 02D03 Chimbo-San Miguel-Educación, como apoyo a una correcta gestión de riesgos.

3.1.1 INTRODUCCIÓN

A partir del año 2014 el Ministerio de Educación tiene implementado la Norma ISO9001 del Sistema de Gestión de Calidad, el cuál trabaja en base a 68 procesos en cada distrito educativo a nivel nacional, los cuáles se dividen en procesos: Gobernantes y Adjetivos, conforme se ilustra en el mapa de procesos en la fase de estudio preliminar de la propuesta.

El propósito del SGC es: disminuir las quejas, los plazos de entrega de los servicios solicitados por usuarios de las instituciones educativas, y lograr el regocijo de los usuarios a través de un ciclo de mejora frecuente.

La Unidad Distrital TIC's actualmente es considerada un punto estratégico para el cumplimiento de objetivos de las diferentes entidades, y más no solo un área de soporte; por lo tanto, es recomendable evaluar el área de informática, a fin de identificar falencias, aplicar controles que disminuyan los riesgos y conocer en qué aspectos mejorar, debido que es la base tecnológica de la operatividad del distrito educativo.

3.1.2 DESCRIPCIÓN DE LA PROPUESTA

La propuesta consiste en realizar una Auditoría a la Seguridad Informática en la Unidad Distrital TIC's, del Distrito Educativo 02d03, en base a la gestión adecuada de riesgos informáticos, enmarcados en lineamientos de COBIT 5, las NIA y los estándares de ISACA.

La auditoría se desarrolló, conforme a las etapas de las Auditoría de Sistemas, que se estructura en: Planeación, Evaluación de Controles, Pruebas Sustantivas y Comunicación de resultados.

3.2 ETAPA DE PLANEACIÓN DE LA AUDITORIA A LA SEGURIDAD INFORMATICA

En esta primera fase de la Auditoria a la Seguridad Informática se realizó varias visitas al Distrito Educativo 02d03, especialmente a la Unidad Distrital TIC's, con la finalidad de obtener un diagnóstico general, comprender la dinámica institucional, establecer objetivos, determinar el alcance, e identificar riesgos.

3.2.1 OBJETIVOS

GENERAL

- Realizar una Auditaría a la Seguridad Informática a la Unidad Distrital TIC's, del Distrito Educativo 02d03.

ESPECÍFICOS

- Levantar información in situ, sobre la Gestión de Riesgos Informáticos.
- Elaborar el programa auditoría a la seguridad informática.
- Realizar las respectivas pruebas de auditoría.
- Difundir los resultados a través del respectivo informe final.

3.2.2 ALCANCE

La Unidad Distrital TIC's ofrece varios servicios de soporte, según el SGC; a continuación, se detallan los procesos objetos de la auditoría a la seguridad informática.

Tabla 11. Procesos de la Unidad Distrital TIC'S

DISTRITO EDUCATIVO 02D03	
Unidad	**Proceso**
GESTION DE TICS	• Contratación, Adquisición- Bienes y Servicios TIC's • Creación de cuentas de usuarios-perfiles, para sistemas de información. • Soporte Técnico-Distrital • Instalación de enlaces de internet Datos y Telefonía (Distrital) • Cierre de cuentas de los Sistemas de Información. • Habilitación de Servicios Tecnológicos Restringidos

Fuente: El Autor

3.2.3 ESTUDIO PRELIMINAR

El Distrito Educativo 02d03, es considerado de tipo medio, motivo que no cuenta con más de 60 Servidores Públicos, la Estructura Organizacional, consta en el Anexo 3.

Posterior a su inicio de operaciones se ha implementado el SGC en base al mapa de procesos, según la norma ISO9001; el cual se muestra a continuación.

Figura 20 .-Mapa de Procesos
Fuente: El Autor a partir de: (COORPORACION 3D, 2014)

Entre las principales actividades que impulsa el distrito educativo es: Planificar, Organizar, Gestionar y Evaluar las actividades académico, administrativas, que permitan apoyar al análisis, estudio y solución de problemas que afecten a la comunidad educativa y a sociedad en general.

3.2.4 EVALUACIÓN DE RIESGOS

A fin de identificar los activos informáticos, se realizó una entrevista al Señor Director Distrital y Analista Distrital TIC’s, procedimientos que ayudaron a determinar los activos más importantes para el Distrito Educativo 02d03, también se realizaron visitas in situ, observaciones directas, entrevistas, encuestas, con el propósito de recolectar información, sobre Riesgos Informáticos. A continuación, se explica la conformación de la Matriz de Riesgos, en base a la información recolectada a través de varias entrevistas y visitas de observación.

En la Columna (1) constan las Referencias o Identificadores de los riesgos que se generan secuencialmente de manera automática, en la columna (2) se describe el Macro proceso (Seguridad Informática), en la columna (3) se describen los procesos tecnológicos, en la columna (4) se describen las diferentes actividades que realizan los procesos de la Unidad Distrital TIC's, en la columna (5) se especifica a qué tipo de proceso corresponden los procesos TIC's. Ejemplo: Proceso Estratégico, Operativo, de Soporte, en la columna (6) constan los procesos de Gobierno de TI, alineados con COBIT 5.

(1)	*(2)*	*(3)*	*(4)*	*(5)*	*(6)*
Ref.	Macroproceso	Subproceso	Actividad	Proceso ERM	Procesos IT COBIT

En la columna (7) consta el origen de riesgo que puede ser: (Humano, Tecnológico, Procesos, Externo) , en la columna (8) se describe las diferentes amenazas es de escritura libre, en la columna (9) consta la probabilidad de que ocurran o materialización del evento de riesgo, el método de calificación es cuantitativo (3=Posible, 2=Probable,1= Remota), en la columna (10) consta el Impacto que causaría si se materializara el evento de riesgo, la escala valorativa es cuantitativa según los umbrales de riesgo (3=Alto, 2= Moderado, 1=Bajo), en la columna (11) consta el Riesgo Inherente, calculado automáticamente del resultado de la multiplicación del Impacto * la Probabilidad, en la columna (12) se describen los controles que permiten mitigar las amenazas, por medio de las buenas prácticas, marcos de referencias o normativas.

(7)	*(8)*	*(9)*	*(10)*	*(11)*	*(12)*
Origen de Riesgo	Evento de Riesgo	Probabilidad	Impacto	Riesgo Inherente	Control

En la columna (13) consta el tipo de control (Preventivo, Detectivo, Correctivo), en la columna (14) se describe la frecuencia del control (Permanente, Periódico, Ocasional), en la columna (15) consta el grado de automatización del control (Automatizado, Semi automatizado, Manual), en la columna (16) consta la eficiencia del control (3=Efectivo,2= Poco Efectivo, 1=Deficiente), es calculado automáticamente, en la columna (17) consta el riesgo residual, es decir el nivel de riesgo luego de aplicar los controles, el cálculo es automático a través de la fórmula de suma del Riesgo Inherente – el Riesgo Residual.

Finalmente, en la columna (18) consta la respuesta que se dé al riesgo (Evitar, Reducir, Transferir, Aceptar) determinada por la Dirección.

(13)	*(14)*	*(15)*	*(16)*	*(17)*	*(18)*
Tipo	Frecuencia	Grado de Automatización	Eficiencia Control	Riesgo Residual	Respuesta al Riesgo

En el Anexo. 4, consta la Matriz completa de Riesgos Informáticos de la Unidad Distrital TIC's

A continuación, se describen los promedios de los riesgos más críticos.

Tabla 12. Promedio de riesgos más críticos

No.	PROCESO	RIESGO INHERENTE	RIESGO RESIDUAL
1	Contratación o Adquisición de Bienes y Servicios Tecnológicos	6	4,67
2	Creación de cuentas de usuarios y perfiles para sistemas de información	6	4,67
3	Instalación de enlaces de internet Datos y Telefonía	6	3
4	Soporte Técnico	6,75	3.75

Fuente: El Autor

La aplicación de controles disminuye notablemente el riesgo inherente.

3.2.5 PROGRAMA DE AUDITORÍA

A continuación, se muestra el Programa General de Auditoría, considerando las diferentes fases de toda Auditoría de Sistemas.

PROGRAMA DE AUDITORIA

Tema de Auditoria: Auditoría a la Seguridad Informática de la Dirección Distrital 02d03 Chimbo-San Miguel-Educación.

Objetivos de la Auditoria:

- ✓ Evaluar los procesos que gestionan las TIC's, con la finalidad de establecer el nivel adecuado de controles.
- ✓ Disponer de información que permita identificar el cumplimiento de requisitos legales relacionados al uso de información y la tecnología, con propósito de apoyar a la alta Dirección en una adecuada gestión de riesgos.
- ✓ Optimizar los recursos tecnológicos y plantear las prioridades de atención.

Alcance de la Auditoría

Se evaluarán los procesos de la Unidad Distrital TIC's, determinados como prioritarios por el Director Distrital 02d03, en base a la Matriz de riesgos tecnológicos.

Los procesos objetos de Auditoría son:

1. Contratación o Adquisición de Bienes y Servicios Tecnológicos.
2. Creación de cuentas de usuarios - perfiles.
3. Soporte Técnico (Distrital)
    a) Respaldos y Recuperación de Datos
    b) Continuidad del Negocio
    c) Licenciamiento de Software
4. Instalación de enlaces de internet Datos y Telefonía (Distrital)
    a) Redes de Área local

Planificación Previa:

Recursos:

- ✓ Humanos: (1 Auditor con conocimientos en Informática, 1 Supervisor - Experto en las Tics y Auditoria Informática)
- ✓ Técnicos: (Cámara fotográfica, Grabadora se Sonidos, Cuaderno de Notas, Laptop)
- ✓ Económicos: (Autofinanciamiento por el Autor)

- ✓ Fuentes de Información: (Director Distrital de Educación, Analista Distrital de la Unidad Distrital TIC's, Servidores Públicos del Distrito Educativo 02d03 y usuarios)
- ✓ Documentos de los procesos de la Unidad Distrital TIC's
- ✓ Instalaciones del Distrito Educativo - 02d03

Tabla 13. Programa de Auditoría

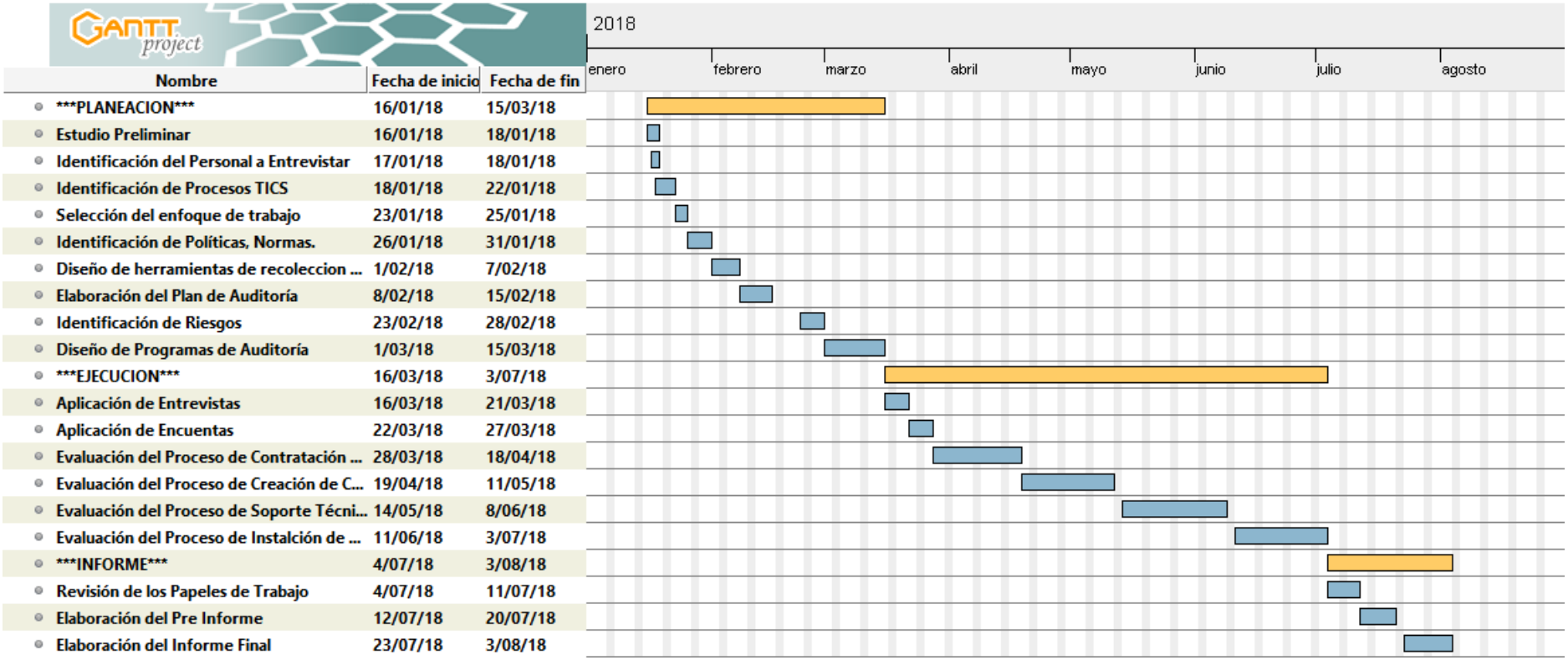
Fases de la Auditoría	**Área**	**Procedimientos de Auditoría**	**Realizado Por:** **Fecha:**	**Ref. PT.**
PLANIFICACION	Distrito Educativo - 02d03.	Gestión del Patrocinio de la Auditoría.	14-12-2017	ANEXO 5
		1.-Identificación del Personal a Entrevistar	Angel Palacios. 17-01-2018	ANEXO 6 PA_EN_001
		2.-Identificación de los Procesos de la Unidad Distrital TIC's.	Angel Palacios. 19-01-2018	ANEXO 7 PA_EN_002
		3.-Selección del Enfoque de trabajo (Metodología)	Angel Palacios. 23-01-2018	ANEXO 8 PA_EN_003
		4.-Identificación de las Normas, Políticas y Reglamentos.	Angel Palacios. 26-01-2018	ANEXO 9 PA_EN_004
		5.-Diseño de Herramientas de recolección y validación de Datos.	Angel Palacios. 01-02-2018	ANEXO 10 PA_EN_005
		6. Diseño del Plan de Auditoría.	Angel Palacios. 08-02-2018	ANEXO 11 PLA_A001
		8. Identificación de Riesgos	Angel Palacios. 23-02-2018	ANEXO 4
		9.Elaboración de Programas de Auditoría	Angel Palacios. 01-03-2018	ANEXO 12 PRG_A_001

EJECUCION	Distrito Educativo - 02d03.	1. Toma de Entrevista a Director Distrital	Angel Palacios. 16-03-2018	ANEXO 01 EJ_001
	Unidad Distrital TIC's	2. Toma de Entrevista a Analista Distrital TIC's	Angel Palacios. 20-03-2018	ANEXO 02 EJ_002
		4. Evaluación del Proceso de Contratación o Adquisición de Bienes y Servicios Tecnológicos.	Angel Palacios. 28-03-2018	ANEXO 13 PA_TICS_001
		5. Evaluación del Proceso de Creación de Cuentas de Usuarios y Perfiles.	Angel Palacios. 19-04-2018	ANEXO 14 PA_TICS_002
		6. Evaluación del Proceso de Soporte Técnico (Distrital)	Angel Palacios. 14-05-2018	ANEXO 15 PA_TICS_003
		7.Evaluación del Proceso de Instalación de enlaces de internet Datos y Telefonía (Distrital)	Angel Palacios. 11-06-218	ANEXO 16 PA_TICS_004
INFORME	Distrito Educativo - 02d03.	1.Revisión de Papeles de Trabajo	Angel Palacios. 04-07-2018	N/A
		2.Elaboración del pre Informe	Angel Palacios. 12-07-2018	N/A
		3.Elaboración del Informe Final (Comunicación de Resultados)	Angel Palacios. 23-07-2018	ANEXO 17

Fuente: El Autor

3.2.6 CRONOGRAMA DE AUDITORÍA

Se realizo en base a la metodología de Auditoría: Planeación, Ejecución e Informe, considerando los tiempos acordados entre Auditor y Distrito Educativo 02d03.



Nombre	Fecha de inicio	Fecha de fin
PLANEACION	16/01/18	15/03/18
Estudio Preliminar	16/01/18	18/01/18
Identificación del Personal a Entrevistar	17/01/18	18/01/18
Identificación de Procesos TICS	18/01/18	22/01/18
Selección del enfoque de trabajo	23/01/18	25/01/18
Identificación de Políticas, Normas.	26/01/18	31/01/18
Diseño de herramientas de recoleccion ...	1/02/18	7/02/18
Elaboración del Plan de Auditoría	8/02/18	15/02/18
Identificación de Riesgos	23/02/18	28/02/18
Diseño de Programas de Auditoría	1/03/18	15/03/18
EJECUCION	16/03/18	3/07/18
Aplicación de Entrevistas	16/03/18	21/03/18
Aplicación de Encuentas	22/03/18	27/03/18
Evaluación del Proceso de Contratación ...	28/03/18	18/04/18
Evaluación del Proceso de Creación de C...	19/04/18	11/05/18
Evaluación del Proceso de Soporte Técni...	14/05/18	8/06/18
Evaluación del Proceso de Instalción de ...	11/06/18	3/07/18
INFORME	4/07/18	3/08/18
Revisión de los Papeles de Trabajo	4/07/18	11/07/18
Elaboración del Pre Informe	12/07/18	20/07/18
Elaboración del Informe Final	23/07/18	3/08/18

Figura 21.-Cronograma de la Auditoría

Fuente: El Autor

3.3 ETAPA DE EJECUCION DE LA AUDITORIA A LA SEGURIDAD INFORMATICA

3.3.1 REVISIÓN Y EVALUACIÓN DE CONTROLES

Se diseñó matrices de control, con la finalidad de evaluar los procesos de la Unidad Distrital TIC's, la cual se estructuró conforme se muestra a continuación:

- *Columna (A)* Variables fundamentales de los Procesos Tics.
- *Columna (B)* Ponderación de la Probabilidad (1=Bajo; 5=Alto)
- *Columna (C)* Ponderación del Impacto (1=Bajo; 10=Alto)
- *Columna (D)* Total (Producto) de cada variable evaluada.

- **Tabla 14. Matriz de Control**

Filas	**Columnas**			
	A	**B**	**C**	**D**
1	**AUDITORÍA A LA SEGURIDAD INFORMÁTICA** **DIRECCION DISTRITAL 02D03 CHIMBO-SAN MIGUEL-EDUCACIÓN** **Proceso:…… Ref. P/T:**……			
		PROBALILIDAD (B)	**IMPACTO (C)**	**A*B**
2	**VARIABLES FUNDAMENTALES**	**Valor Referencia l (Bajo) - 5 (Alto)**	**Valor Referencial 1 (Bajo) - 10 (Alto)**	**TOTAL**
3	1.			
4	2.			
5	3.			
6	4.			
7	5.			
8	6.			
9	7.			
10	8.			
11	**PONDERACION TOTAL**			
12	**%**			
13	**Mínimo**	8	8	8
14	**Máximo**	40	80	400

Fuente: El Autor

El Mínimo equivalente a (8) corresponde a la suma de las variables fundamentales, asignando el valor más bajo (1) a cada variable y el valor de máximo (40) – (80) - (400) corresponde si se valorara con la máxima puntuación a cada una de las variables.

La ponderación Total es calculada a través de la suma de cada una de las variables - Columna (D); y porcentaje de riesgo es calculado por medio de la fórmula: = (D11*100) / D14.

D11=Resultado de la suma, 100=Consideración del 100% de eficacia y D14 corresponde al máximo valor.

No se detallan las variables fundamentales, motivo que se acordó utilizar con discreción la información de la auditoría a la seguridad informática, por lo que solamente se describe la estructura de la matriz de control empleada en la evaluación del riesgo, de los procesos de la Unidad Distrital TIC's; los resultados se describen en el Informe de la Auditoría a la Seguridad Informática.

3.3.2 PRUEBAS DE CUMPLIMIENTO

Se realizó un análisis documental de los Procesos de la Unidad Distrital TIC's, con el fin de verificar estrictamente si se está siguiendo los procedimientos del Manual de Gestión Administrativa Distrital (SGC). Se muestra en la Tabla 15. El Cuestionario de Control, empleado en las pruebas de Cumplimiento.

Tabla 15. Cuestionario de control – Contratación o Adquisición de Bienes y Servicios Tecnológicos

DIRECCION DISTRITAL 02D03 CHIMBO-SAN MIGUEL-EDUCACIÓN					
AUDITORÍA A LA SEGURIDAD INFORMÁTICA					
DOCUMENTO:	EVALUACION DE LA GESTION ADMINISTRATIVA		**Entrevistado y cargo:**	Lcdo. Carlos Aroca-Jefe de la Unidad de Tics	
PROCESO:	Contratación a Adquisición de Bienes y Servicios Tecnológicos.				
Fecha:	30/03/2018				
Auditor:	Angel Palacios				
No.	**PROCEDIMIENTOS DE VERIFICACIÓN**	**RESPUESTA SI-NO-n/a**	**OBSERVACION**		**REFERENCIA**
1	¿Existe documentos físicos o electrónicos de las Peticiones de Requerimientos?	NO	Las contrataciones ha sido realizada por el departamento Administrativo		ANEXO PA_EN_1.1.1
2	¿Se dispone de documentos de análisis de mercado?	NO	El análisis de mercado se ha realizado atraves de sitios de comercio electrónico.		
3	¿Se determinan las especificaciones técnicas, cuando se require un bién o servicio?	SI			
4	¿Se solicita la certificación presupuestaria?	SI	Las contrataciones no se han realizado, debido a la falta de certificación presupuestaria.		
5	¿Se ha verificado que los bienes cumplan con las especificaciones técnicas?	SI	Se ha verificado las especificaciones técnicas a traves de la observación directa de las adquisiciones que el Departamento Administrativo ha realizado.		
	RESPONSABLE TICS		**AUDITOR**		
NOMBRE	Lcdo. Carlos Aroca		Angel Palacios		
FIRMA					

Fuente: El Autor

Conclusiones:

- Se incumple el Manual de Gestión Administrativa Distrital.
- No se han realizado contrataciones o adquisiciones de bienes y servicios por la Unidad Distrital TIC's, debido a la falta de presupuesto.

Tabla 16. Cuestionario de control – Creación de Cuentas de usuarios y perfiles, para sistemas de información

DIRECCION DISTRITAL 02D03 CHIMBO-SAN MIGUEL-EDUCACIÓN					
AUDITORÍA A LA SEGURIDAD INFORMÁTICA					
DOCUMENTO:	EVALUACION DE LA GESTION ADMINISTRATIVA		**Entrevistado y cargo:**	Lcdo. Carlos Aroca-Jefe de la Unidad de Tics	
PROCESO:	Creación de Cuentas de Usuarios y Perfiles, para los Sistemas de Información.				
Fecha:	20/04/2018				
Auditor:	Angel Palacios				
No.	**PROCEDIMIENTOS DE VERIFICACIÓN**	**RESPUESTA SI-NO-n/a**	**OBSERVACION**		**REFERENCIA**
1	Solicitud de la creación de cuentas o perfiles.	SI	Cuando no se ha utilizado los formularios de creación de cuentas, se ha utilizado una matriz con similares campos.		ANEXO PA_TICS_002
2	¿En la creación de cuentas en Quipux, se han llenado los formularios?	SI	Existen formularios sin sellos de la Unidad de Talento Humano y sin firmas de responsabilidad.		
3	¿Cuándo han sido cuentas diferentes al Quipux; se ha adjuntado los requisitos pertinentes, como copia de nombramientos?	SI	Se ha adjuntado las copias de las Acciones de Personal		
4	¿Si la documentación ha sido entregada incompleta, se ha notificado al usuario, con la especificación de documentos faltantes?	NO			
5	¿Una vez creado el Quipux se ha dado respuesta al usuario, mediante Quipux?	SI			
	RESPONSABLE TICS		**AUDITOR**		
NOMBRE	Lcdo. Carlos Aroca		Angel Palacios		
FIRMA					

Fuente: El Autor

Conclusiones:

- Existen formularios sin firmas de responsabilidad, y sin sellos de la Unidad de Talento Humano Distrital.
- Se ha dado de alta a usuarios, sin contar con la respectiva documentación.

Tabla 17. Cuestionario de control - Soporte Técnico

DIRECCION DISTRITAL 02D03 CHIMBO-SAN MIGUEL-EDUCACIÓN					
AUDITORÍA A LA SEGURIDAD INFORMÁTICA					
DOCUMENTO:	EVALUACION DE LA GESTION ADMINISTRATIVA		**Entrevistado y cargo:**	Lcdo. Carlos Aroca-Jefe de la Unidad de Tics	
PROCESO:	Soporte Técnico				
Fecha:	15/05/2018				
Auditor:	Angel Palacios				
No.	**PROCEDIMIENTOS DE VERIFICACIÓN**	**RESPUESTA SI-NO-n/a**	**OBSERVACION**		**REFERENCIA**
1	¿Existe las peticiones electrónicas de requerimientos de Soporte Técnico, solicitadas por los usuarios?	NO	Los usuarios se acercan directamente a la unidad de TICS a solicitar el Soporte Técnico verbalmente, sin llenar el formulario.		ANEXO PA_TICS_003
2	¿Se dispone de formularios de resgistros de Soporte Técnico?	SI	Llena el Analista Distrital de TICS		
3	¿Existe determinación del tipo de requerimiento (Incidente o Petición de Servicios?	SI			
4	¿Existe registros de inspección y diagnóstico?	SI			
5	¿Existe documentación de las soluciones?	SI			
	RESPONSABLE TICS		**AUDITOR**		
NOMBRE	Lcdo. Carlos Aroca		Angel Palacios		
FIRMA					

Fuente: El Autor

Conclusiones

- Los usuarios incumplen el Manual de Gestión Administrativa Distrital, al solicitar verbalmente las peticiones de Soporte Técnico.
- La documentación consta en formato digital, en la red interna del Distrito Educativo.

Tabla 18. Cuestionario de control - Instalación de Enlaces de Internet, Datos y Telefonía

DIRECCION DISTRITAL 02D03 CHIMBO-SAN MIGUEL-EDUCACIÓN				
AUDITORÍA A LA SEGURIDAD INFORMÁTICA				
DOCUMENTO:	EVALUACION DE LA GESTION ADMINISTRATIVA		**Entrevistado y cargo:**	Lcdo. Carlos Aroca-Jefe de la Unidad de Tics
PROCESO:	Instalación de Enlaces de Internet, Datos y Telefonía			
Fecha:	12/06/2018			
Auditor:	Angel Palacios			

No.	PROCEDIMIENTOS DE VERIFICACIÓN	RESPUESTA SI-NO-n/a	OBSERVACION	REFERENCIA
1	¿Existe documentos sobre las peticiones de requerimientos del proceso?	NO		ANEXO PA_TICS_004
2	¿Existe documentación que conste dirección exacta de la Institución Educativa, Nombres y Números Telefónicos del Representante legal?	SI	Consta en el Acta de Entrega Recepción.	
3	¿Se ha revisado que los datos de los formularios, concuerden con el requerimiento solicitado por el usuario?	SI		
4	¿Los formularios se encuentran totalmente firmados?	NO	Se encontró formularios sin firma de Telconet	
5	¿Se ha realizado la verificación de la Instalación del Servicio?	SI		
6	¿Se ha remitido informes de la instalación del servicio a la Coordinación Zonal TICS?	NO		

	RESPONSABLE TICS	AUDITOR
NOMBRE	Lcdo. Carlos Aroca	Angel Palacios
FIRMA		

Fuente: El Autor

Conclusiones

- Se han realizado instalaciones de radios enlaces de internet durante el periodo de auditoría, pero no se dispone de la completitud de documentos del proceso.
- La instalación de radio enlaces se han realizado en zonas rurales, por lo que se desconoce su operatividad actual.

3.3.3 RESULTADOS DE LAS PRUEBAS DE CUMPLIMIENTO

Una vez realizado el análisis documental del periodo de auditoría enero 2016-octubre 2017, se determina que los documentos de los procesos de la Unidad Distrital TIC's, son incompletos en relación al SGC, se encuentran desorganizados, carecen de clasificación, y no cuentan con etiquetas.

A continuación, se puede observar un gráfico analítico de los Procesos TICS's, vs los Criterios de COBIT 5, el cual se elaboró en una hoja de cálculo, donde se fue marcando el cumplimiento de cada criterio, según la información levantada de los procesos evaluados.

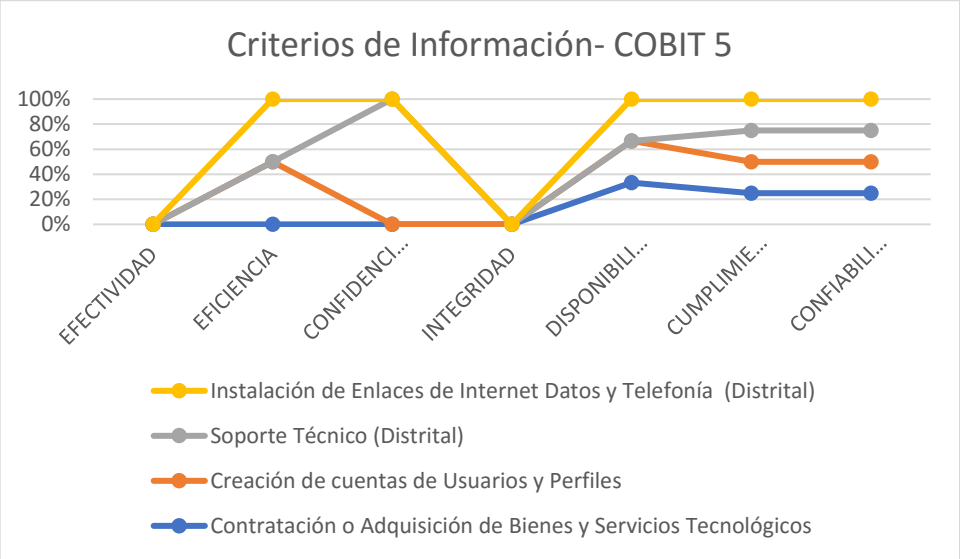


Figura 22.-Evaluación documental de los procesos Tics con los criterios de Información COBIT 5
Fuente: El Autor.

Se revisó un total de 171 documentos que proporcionó el Analista Distrital de TICS de los Procesos del SGC; el proceso de menor cumplimiento de Criterios de COBIT 5 es el de Contratación o Adquisición de Bienes y Servicios Tecnológicos.

En la Tabla 19, se puede observar el detalle de la documentación revisada y analizada.

Tabla 19. Revisión Documental-Procesos TICS

No.	PROCESO	CANTIDAD
1	Contratación o Adquisición de Bienes y Servicios Tecnológicos.	0
2	Creación de cuentas de usuario y perfiles, para sistemas de información.	97
3	Soporte Técnico	59
4	Instalación de Enlaces de Internet, Datos y Telefonía.	15
	TOTAL	**171**

Fuente: El Autor

3.3.4 PRUEBAS SUSTANTIVAS

3.3.5 Prueba Sustantiva – Proceso: Contratación o Adquisición de Bienes y Servicios Tecnológicos.

Procedimientos de Auditoría:

- Solicitud del inventario de la Unidad Distrital de TIC's a la Unidad Distrital Administrativa
- Constatación in situ del inventario tecnológico Distrital de fecha 14 de junio del 2017, entregado al Auditor.

Hallazgo

Se detectó varios activos tecnológicos faltantes en el Inventario de la Unidad Administrativa Distrital, el detalle de los mismos se muestra a continuación.

Tabla 20. Activos faltantes en el Inventario de la Unidad Distrital Administrativa

CANTIDAD	DESCRIPCIÓN DE ACTIVOS	UBICACIÓN
1	Router D-Link dir 510	
1	Switch D-Link de 8 puertos	Tics-02d03
1	Access Point	
1	Disco Duro WD-MYCLOUD	

Fuente: El Autor

Conclusión

No se dispone de inventario tecnológico actualizado en la Unidad Distrital de TIC's.

3.3.6 Prueba Sustantiva – Proceso: Creación de Cuentas de Usuario y perfiles, para sistemas de Información.

Procedimientos de Auditoría:

- Entrevista a los Servidores Públicos del Distrito Educativo - 02d03.
- Encuesta a los funcionarios del Distrito Educativo 02d03.
- Corroboración en la Unidad Distrital TIC's.

Las preguntas estaban enfocadas en conocer si se han cambiado las contraseñas de los sistemas que utilizan en el Distrito Educativo 02d03, a lo que la mayoría respondieron que no han sido cambiadas.

Hallazgo

Se contrasto las respuestas de la entrevista con el Analista Distrital TIC's el cuál confirmo la inexistencia una política de cambio de contraseñas, sin embargo, dio a conocer que esta práctica de seguridad dispone únicamente el correo institucional. www.correo.educación.gob.ec, en el cuál después de cada cierto periodo de tiempo caducan las claves, de tal manera que los usuarios tienen la obligación de modificar las claves.

Conclusiones

- Los resultados de la encuesta a los Servidores Públicos, en un 61% respondieron que las estaciones de trabajo no disponen de controles de acceso como contraseñas.
- En el Distrito Educativo 02d03, no se cuenta con políticas de uso, cambio de contraseñas, como control de seguridad.

3.3.7 Prueba Sustantiva – Proceso: Soporte Técnico

Procedimientos de Auditoría:

- Revisión técnica del software instalado en 38 estaciones de trabajo de las diferentes Unidades que conforman el Distrito Educativo - 02d03.
- Revisión documental del Plan de Contingencia de la Unidad Distrital TIC's.
- Entrevista al Analista Distrital TIC's, en relación a las licencias de software.

El resultado obtenido se describe a continuación.

Tabla 21. Inventario de Software

SISTEMA OPERATIVO				OFIMÁTICA			ANTIVIRUS						NAVEGADOR DE INTERNET	
Windows			Ubuntu	Office-versión		Libre Office	AVAST	AVG	AVIRA	MCAFEE	PANDA	Otro	Mozilla Firefox	Google Chrome
7	8	X		2010	2013									
35	2	1	36	33	3	2	17	9	3	1	1	2	34	4

Fuente: El Autor

Hallazgos

- Las estaciones de trabajo tienen instalado dos Sistemas Operativos (Windows y Ubuntu), pero durante el periodo de auditoría, no se ha observado a ningún funcionario trabajando en Ubuntu.
- 36 funcionarios hacen uso de las Aplicaciones de Microsoft Office; mientras 2 utilizan Libre Office.
- 5 computadoras no cuentan con ningún tipo de antivirus.

Conclusión

Los softwares instalados en las diferentes estaciones de trabajo del Distrito Educativo 02d03, no disponen de la respectiva licencia de software, consecuencia de la falta de presupuesto

3.3.8 Prueba Sustantiva - Proceso: Soporte Técnico – Backups

Procedimientos de Auditoría:

- Observación Directa
- Entrevista al Analista Distrital TIC's
- Revisión Documental

Hallazgos

- El respaldo de información se realiza cada que una computadora necesita mantenimiento en un disco duro My Cloud de 4TB conectada a la red interna del Distrito Educativo - 02d03.
- Todos los usuarios de la red interna, tienen acceso a la información del disco duro de respaldos, lo cual hace vulnerable a pérdidas, copias, eliminación o modificación de información no autorizada.
- En los registros de soporte técnico también se encontró que los respaldos se realizan en la unidad "D", de la propia computadora a dar mantenimiento correctivo, lo cual es un riesgo alto a pérdidas de información.
- Capacidad del correo institucional de capacidad limitada (40,96 MB), por lo que los usuarios solicitan peticiones de soporte técnico con el propósito de que se respalde la información de la bandeja de entrada y poder recibir emails nuevos.

- No se ha realizado mantenimientos preventivos programados, ni se realizan actualizaciones frecuentes de antivirus y eliminación de cookies, historial de los navegadores de internet.

En la Figura 23, se muestra el flujo de información del procedimiento de respaldos de la información que se realiza en el Distrito Educativo 02d03.

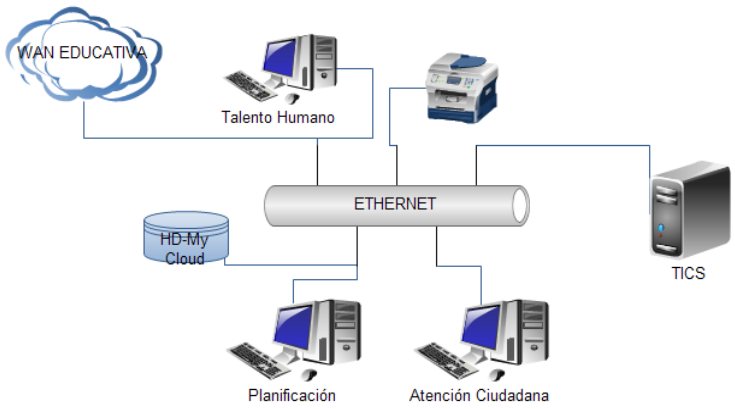


Figura 23.-Arquitectura de Backups
Fuente: El Autor

A continuación, en la Tabla 22, se muestra la tabulación de los requerimientos de soporte técnico, del periodo de auditoría.

Tabla 22. *Tabulación de peticiones de Soporte Técnico*

PRINCIPALES PROBLEMAS	Frecuencia. Periodo de auditoría: enero 2016-octubre 2017
Actualización de antivirus	1
Cambio de Tóner	16
Carga de tinta en impresoras	2
Reseteo de contador de impresiones	3
Configuración de Acceso a internet	1
Configuración de Outlook de escritorio	4
Creación de carpetas para almacenar la información del correo institucional.	4
Elaboración de Cable de red	1

Instalación de equipo informático y red	1
Instalación de punto eléctrico	1
Instalación de Switch	1
Instalación de módulo de memoria RAM	1
Liberar espacio en bandeja de correo institucional	1
Mantenimiento Preventivo	1
Predeterminar acceso al sitio web de gestión documental	1
Realización de respaldos en la Unidad "D"	4
Reinstalación de Office	1
Reinstalación del Sistema Operativo Windows 7 x64 e instalación de programas.	4
Remplazo de periféricos	4
Reseteo de clave de correo institucional	3
Respaldo de información de la bandeja de entrada del correo institucional, para recibir nuevos correos.	3
Eliminación de historial y cookies de navegadores de internet	1

Fuente: El Autor

Conclusión

- La mayor cantidad de peticiones de requerimientos de Soporte Técnico, han sido solicitados para cambios de tóner, lo cual hace un llamado a incentivar el uso de la información digital y apoyar a la política de cero papeles.

3.3.9 Prueba Sustantiva - Proceso: Instalación de Enlaces de Internet, Datos y Telefonía

Procedimientos de Auditoría:

- Revisión documental
- Revisión técnica de la configuración de red en 38 estaciones de trabajo.

Hallazgos

- No se evidencia administración de la Red LAN, usuarios cambian direcciones IP y generan conflicto en toda la red interna.
- La WAN Educativa es un limitante cuando se realizan video conferencias.
- No se dispone de controles de seguridad en red (Firewall), como medio de protección de restringir accesos no autorizados a la misma.
- No se monitorea el tráfico de la Red con ningún software.
- Existe una conexión de internet abierta que esta siendo sub utilizada.
- No se cuenta con diagramas de red que ayuden a detectar conflictos cuando, estos se generan.

Conclusiones

- La infraestructura de red está conformada por una topología tipo estrella, debido a que todos los equipos informáticos se conectan a través de un concentrador central.
- La clase de Red es Tipo "C" debido que está comprendida en direcciones IP de 192 a 223 bits, con la máscara de subred 255.255.255.0.
- El método de conexión a internet es a través de la WAN Educativa, la cual restringe el acceso a sitios web como redes sociales y limita a la descarga de programas.

3.3.10 MAPEO OBJETIVOS DE PROCESOS TIC's, VS DOMINIOS Y PROCESOS COBIT 5

Tabla 23. Mapeo Procesos Tics vs Objetivos COBIT 5

		MAPEO DE OBJETIVOS Y PROCESOS TICS VS DOMINIOS Y PROCESOS DE COBIT 5																																				
PROCESOS TICS-OBJETIVO	**ACTIVIDADES**	**Evaluar, Orientar y Supervisar**					**Alinear, Planificar y Organizar**													**Construir, Adquirir e Implementar**												**Entregar, dar Servicio y Soporte**						**Supervisar, Evaluar y Valorar**		
		EDM01	EDM02	EDM03	EDM04	EDM05	APO01	APO02	APO03	APO04	APO05	APO06	APO07	APO08	APO09	APO10	APO11	APO12	APO13	BAI01	BAI02	BAI03	BAI04	BAI05	BAI06	BAI07	BAI08	BAI09	BAI10	BAI11	BAI12	DSS01	DSS02	DSS03	DSS04	DSS05	DSS06	MEA01	MEA02	MEA03
PROCESO Contratación o Adquisición de Bienes y Servicios Tecnológicos. **OBJETIVO** Proveer oportunamente a la unidad requirente de bienes y servicios tecnológicos para la realización de un trabajo eficiente.	1. Adquisición de bienes tecnológicos				✓					✓																		✓												
PROCESO Creación de cuentas de usuarios y perfiles. **OBJETIVO** Normar la creación, desactivación y eliminación de cuentas de usuarios y perfiles para los sistemas de Información.	1. Emplea Políticas de creación y uso de contraseñas			✓		✓												✓	✓													✓								
PROCESO Soporte Técnico (Distrital). **OBJETIVO** Mantener en buen funcionamiento los equipos y sistemas informáticos y asistir de forma permanente y oportuna a los usuarios.	1. Asiste oportunamente y da solución a los problemas		✓																													✓	✓	✓	✓		✓			
PROCESO Instalación de enlaces de internet Datos y Telefonía (Distrital) **OBJETIVO** Habilitar oportunamente el acceso de los usuarios a enlaces de internet, datos y telefonía.	1. Dispone de Infraestructura tecnológica actual								✓	✓								✓	✓																✓				✓		

Fuente: El Autor

3.3.11 ANALISIS DEL MAPEO DE LOS OBJETIVOS TIC's-VS-DOMINIOS DE COBIT 5

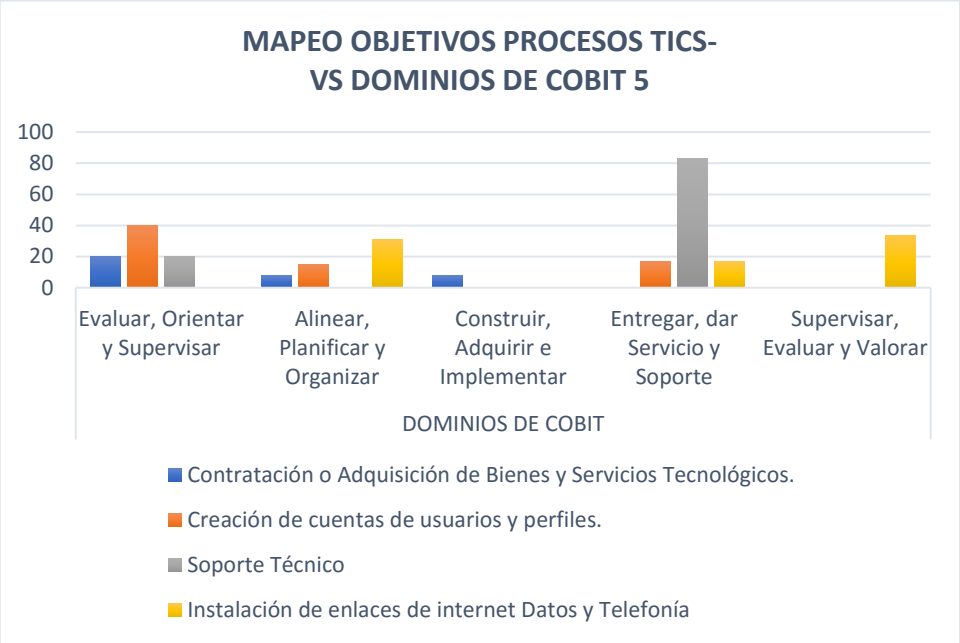


Figura 24.-Análisis Mapeo-Objetivos procesos Tics, Vs. Dominios de COBIT 5

Fuente: El Autor

3.3.12 ANÁLISIS PROCESOS TICS, CON LOS DOMINIOS DE COBIT 5

EVALUAR, ORIENTAR Y SUPERVISAR

Los procesos de TIC's no alcanzan al 50% del dominio de COBIT, esto da a conocer que las estrategias de la unidad, no están siendo efectivas con el alcance de los objetivos, debido a que no se está cumpliendo con el Manual de Gestión Administrativa Distrital.

ALINEAR, PLANIFICAR Y ORGANIZAR

El máximo valor alcanzado en el dominio de COBIT 5 es el 40%, esto indica que se debe mejorar el proceso, a fin de cumplir los objetivos.

CONSTRUIR, ADQUIRIR E IMPLEMENTAR

Es el indicador más bajo del dominio de COBIT 5 alcanza un 9%, esto es consecuencia de la falta de gestión de presupuesto para la Unidad Distrital TIC's.

ENTREGAR DAR SERVICIO Y SOPORTE

Es el Proceso más eficiente de la Unidad Distrital TIC's, supera el 80% del dominio de COBIT 5, resultado del cumplimiento del Manual de Gestión Administrativa Distrital.

SUPERVISAR, EVALUAR Y VALORAR

El indicador supera el 30% en relación a los dominios de COBIT 5, consecuencia que hace falta dar seguimiento al cumplimiento de los procesos, por parte del Gobierno de TI

3.3.13 NIVEL DE MADUREZ DE LOS PROCESOS DE TICS-02D03

Los Niveles de madurez, se determinaron en base a la normativa ISO15504, una vez realizada la fase de planeación y ejecución de la Auditoría, las cuales permitieron conocer los procesos y su nivel de gestión.

A continuación, se detallan los niveles de madurez de los procesos TIC's.

Tabla 24. Nivel de madurez - Procesos Tics-02d03, según ISO 15504

Procesos Tics-02d03	**Nivel de Madurez Iso-15504**					
	Inmadura (0)	Básica (1)	Gestionada (2)	Establecida (3)	Predecible (4)	Optimizada (5)
Contratación o Adquisición de Bienes y Servicios Tecnológicos.	X					
Creación de cuentas de usuarios y perfiles.		x				
Soporte Técnico			x			
Instalación de enlaces de internet Datos y Telefonía			x			

Fuente: El Autor

3.4 ETAPA DE COMUNICACIÓN DE RESULTADOS

3.4.1 INFORME DE AUDITORÍA A LA SEGURIDAD INFORMÁTICA

Para la elaboración del Informe se siguió la NIA 700

Informe de Auditoría

DIRECCION DISTRITAL 02D03 CHIMBO-SAN MIGUEL-EDUCACION

Auditoría número: ASI-001-2018

Auditoría a la Seguridad Informática, según el Marco de Referencia COBIT 5.

Periodo de Revisión: enero 2016-octubre 2017.

Distribución del Informe de Auditoría.

Dirigido a: Lcdo. David Galarza - Director Distrital

Lcdo. Carlos Aroca - Analista Distrital TIC’s

3.4.2 ÍNDICE DEL INFORME DE AUDITORIA A LA SEGURIDAD INFORMATICA

Portada

CAPITULO I

Introducción…… I

Antecedentes…… I

Objetivo…….. I

Alcance…….. II

Opinión de la Auditoría a la Seguridad Informática..…… II

Procedimientos de Auditoría…… II-III

Objetivos de la Unidad Distrital de TIC's…… III

Servidores Públicos, relacionados con la Auditoría ……. III

Conclusiones Generales de la Auditoría…… III-IV

Recomendaciones Importantes de la Auditoría…… IV

CAPITULO II

Resultados de la Auditoría……. V

1) **Título:** Incumplimiento del Manual de Gestión de Calidad…….. V-VI
2) **Título:** Inventario de la Unidad de Tecnologías de la Información y Comunicaciones desactualizado. VI-VII
3) **Título:** Carencia de Integridad en los Datos. VII-VIII
4) **Título:** Falta de capacitación y evaluación a los usuarios, sobre el uso de cuentas y políticas de contraseñas. VIII-IX
5) **Título:** Falta de seguimiento al cumplimiento de los procesos del Manual de Gestión Administrativa Distrital por la Dirección. IX-X
6) **Título:** No se utiliza software libre; ni se dispone de las licencias de software propietario. XI-XII
7) **Título:** Falta de Políticas de Continuidad de las Operaciones Tecnológicas…….. XII-XIII
8) **Título:** Falta de gerencia en la Red LAN…….. XIII-XIV
9) **Título:** Implementación de Estándares en la RED LAN……. XIV-XV
10) **Título:** Optimización de Recursos…… XVI

I

Informe de Auditoría a la Seguridad informática

AUDITORÍA A LA SEGURIDAD INFORMÁTICA EN LA DIRECCION DISTRITAL 02D03 CHIMBO-SAN MIGUEL-EDUCACION, DURANTE EL PERIODO ENERO 2016-OCTUBRE 2017, UTILIZANDO LA NORMA INTERNACIONAL COBIT 5.

Dirección Distrital 02d03 Chimbo-San Miguel-Educación

Fecha de Emisión: 18/08/2018

Auditor Responsable: Angel Palacios

Supervisor de Auditoría: Ing. Christian Vaca. Mg.

CAPITULO I

INTRODUCCION

ANTECEDENTES

La Auditoría a la Seguridad Informática se realizó, motivo que no se ha realizado ningún tipo de auditoría informática desde la implantación del Distrito Educativo 02d03, y no se cuenta con información sobre la gestión de riesgos de la unidad Distrital TIC's, además se ha venido presentando problemáticas con la prestación de servicios y uso de la infraestructura Tecnológica.

OBJETIVO

Expresar opiniones técnicas de los hallazgos encontrados en el desarrollo de la auditoría a la seguridad informática, con el propósito de ayudar al Distrito Educativo 02d03 en la adecuada gestión de riesgos y toma de decisiones.

ALCANCE

Se auditó la Unidad Distrital TIC's, priorizando los procesos categorizados: "Evitar", por la Dirección según la Matriz de riesgos.

- Contratación o Adquisición de Bienes y Servicios Tecnológicos
- Creación de Cuentas de Usuario y Perfiles para sistemas de información.
- Soporte Técnico (Distrital)
- Instalación de Enlaces de Internet, Datos y Telefonía.

OPINIÓN DE LA AUDITORÍA A LA SEGURIDAD INFORMÁTICA

La seguridad informática del Distrito Educativo 02d03, refleja la realidad de la gestión de los Procesos tanto técnicos, como documentales de la Unidad Distrital TIC's del periodo de auditoría enero 2016-octubre 2017, en el cual el resultado de riesgo es Alto y Moderado, en conformidad con los umbrales de riesgo; por lo tanto, se sugiere aplicar las recomendaciones del informe de auditoría, con el propósito de mitigar o reducir el riesgo.

Tabla 25. Resultados de Procesos TICS-02d03 Evaluados

Procesos de la Unidad de Tecnologías de la Información y Comunicaciones.	Nivel de Riesgo					
	Riesgo. Alto	**67-100%**	**Riesgo Moderado**	**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%		
Soporte Técnico (Distrital)			X	61,75%		
Instalación de Enlaces de Internet Datos y Telefonía Distrital.	X	68%				

Fuente: El Autor

PROCEDIMIENTOS DE AUDITORIA EMPLEADOS

- Estudio Preliminar del Distrito Educativo 02d03.
- Visitas In situ
- Guías de Observación

- Encuestas, Entrevistas
- Identificación y selección del enfoque de trabajo, Políticas, normas, marco de referencia.
- Recopilación de datos de la Unidad Distrital TIC's
- Revisión documental.
- Diseño de herramientas que permitan probar los controles internos.

Objetivos de la Unidad Distrital TIC's

- Proveer oportunamente a la unidad requirente de bienes y servicios tecnológicos para la realización de un trabajo eficiente.
- Normar la creación, desactivación y eliminación de cuentas de usuarios y perfiles para los sistemas de Información.
- Mantener en buen funcionamiento los equipos y sistemas informáticos y asistir de forma permanente y oportuna a los usuarios.
- Habilitar oportunamente el acceso de los usuarios a enlaces de internet, datos y telefonía.

SERVIDORES PÚBLICOS RELACIONADOS CON LA AUDITORÍA A LA SEGURIDAD INFORMÁTICA

Tabla 26. Servidores Públicos relacionados con la Auditoría a la Seguridad Informática.

Cargo	Nombres y Apellidos
Director Distrital-02d03	Lcdo. David Galarza
Analista Distrital TIC's	Lcdo. Carlos Aroca

Fuente: El Autor

CONCLUSIONES GENERALES DE LA AUDITORIA

- Se encontró documentación incompleta de los procesos TIC's, del periodo de auditoría enero 2016-octubre 2017, la cual carece de organización física, y no cuenta con políticas que restrinja el acceso a la información.
- Se contó con la predisposición y colaboración del Señor Director Distrital 02d03, del señor Analista de la Unidad Distrital TIC's, y demás Servidores Públicos del Distrito Educativo - 02d03.

- La matriz de riesgos informáticos, permitió priorizar los procesos que requieren mayor atención.
- La metodología de auditoría de sistemas, permitió realizar la auditoría a la seguridad informática etapa por etapa lo cual optimizo tiempo y dinero.

RECOMENDACIONES IMPORTANTES DE LA AUDITORIA

- Dar seguimiento al cumplimiento del Manual de Gestión Administrativa Distrital.
- Mejorar la cultura organizacional en relación al modo de trabajar (hacer conciencia de la existencia de riesgos y las consecuencias que puede ocasionar)
- La Dirección (Gobierno de TI) deberá gestionar presupuesto para que la Unidad Distrital TIC's, pueda realizar adquisiciones de hardware y software, con la finalidad de mejorar la infraestructura tecnológica y adquirir licencias de software.
- Elaborar Planes de Contingencia, que permitan enfrentar eventos adversos.

Durante el desarrollo de la Auditoría a la Seguridad Informática, se contó con el apoyo del Señor Director Distrital, Analista Distrital de la Unidad de TIC's, y demás Servidores Públicos del Distrito Educativo-02d03, de tal manera expreso mi profundo agradecimiento por la predisposición y colaboración durante la investigación.

A continuación, se detalla el informe de Auditoría a la Seguridad Informática, con los principales hallazgos, las casusas, los efectos y las recomendaciones, basadas en el marco de referencia COBIT 5.

Atentamente

Angel Ramiro Palacios Bayas

AUDITOR EXTERNO

CAPITULO II

RESULTADOS DE LA AUDITORIA A LA SEGURIDAD INFORMÁTICA

1. **Título:** INCUMPLIMIENTO DEL MANUAL DE GESTIÓN ADMINISTRATIVA DISTRITAL.

Proceso Tics: Contratación o Adquisición de Bienes y Servicios Tecnológicos.

Condición

Se identificó que se incumple el Manual de Gestión administrativa Distrital en el Proceso de Contratación o Adquisición de Bienes y Servicios Tecnológicos, por lo que dichos bienes han sido adquiridos por la Unidad Administrativa Distrital, durante el periodo de auditoría enero 2016-octubre 2017.

Criterio

El Manual de Gestión Administrativa Distrital, con código MINEDUC-GTICS-001, establece que la Contratación o Adquisición de Bienes y Servicios Tecnológicos, es un proceso de la Unidad Distrital TIC's.

COBIT 5, a través del dominio de: Monitorear-Evaluar y Valorar, por medio del proceso: (MEA02) hace referencia a la facilitación de la identificación de deficiencias de control interno y ofrece actividades de mejora, para conducir hacia el logro de los objetivos de las entidades.

Causas

- Falta de Cultura Organizacional en relación al cumplimiento de los Procedimientos del Manual de Gestión Administrativa Distrital.
- Falta de seguimiento al cumplimiento de los Procesos, por parte de la Dirección.

Efectos

Tabla 27. Efectos del Incumplimiento del Manual de Gestión Administrativa Distrital.

Nivel de Riesgo			Actividad	Proceso
Alto	Moderado	Bajo		
		X	Posible indisponibilidad de servicios tecnológicos debido a la falta de adquisiciones de hardware y software que permitan prevenir o solventar las interrupciones operacionales.	Contratación o Adquisición de Bienes y Servicios Tecnológicos.
X			Posible pérdida de la Certificación ISO 9001, consecuencia del incumplimiento del Manual de Gestión Administrativa Distrital.	

Fuente: El Autor

Recomendaciones:

- Socializar frecuentemente los Procesos de la Unidad Distrital TIC's en conformidad con el Sistema de Gestión Administrativa Distrital, a todos los Servidores Públicos del Distrito Educativo.
- La Dirección deberá dar seguimiento al cumplimiento de los Procesos TIC's.

2. **Título:** INVENTARIO DE LA UNIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES DESACTUALIZADO.

Proceso Tics: Contratación o Adquisición de Bienes y Servicios Tecnológicos.

Condición

No se dispone de inventario tecnológico actualizado, por lo tanto, no es posible mantener un control eficiente de los activos tecnológicos.

Criterio

ISO 27002 – 2013 a través del Dominio Gestión de Activos dispone que las empresas deben tener conocimiento preciso sobre todos los activos que dispone: Activos físicos, recursos de software, recursos de información, servicios; como parte importante de la correcta

administración de riesgos, deberán estar clasificados por su sensibilidad y criticidad de la información.

Causa

Inexistencia de controles Internos en relación a la protección de activos tecnológicos.

Efectos

Tabla 28. Efectos del Inventario de la Unidad de Tecnologías de la Información y Comunicaciones desactualizado.

Nivel de Riesgo			Actividad	Proceso
Alto	Moderado	Bajo		
	x		Dificultad de priorizar la protección de los activos para su tratamiento.	Contratación o Adquisición de Bienes y Servicios Tecnológicos.
x			Pérdida de activos tecnológicos.	

Fuente: El Autor

Recomendación

Aplicar la norma ISO 27002 – 2013 Gestión de Activos

3. **Título:** CARENCIA DE INTEGRIDAD EN LOS DATOS.

Proceso Tics: Creación de Cuentas de Usuarios y Perfiles, para los Sistemas de Información.

Condición

Se identificó 11 formularios de creación de cuentas de usuarios y perfiles sin las firmas de responsabilidad, y 17 formularios sin sellos de validación de la unidad de Talento Humano, de un total de 63 formularios.

Criterio

COBIT 5. A través del dominio de: Evaluar, Dirigir y Monitorear; y el proceso: (EDM03), da a conocer que el riesgo debe ser comunicado y debe ser gestionado.

Causa

Incumplimiento del flujo de información del Manual de Gestión Administrativa Distrital.

Efectos

Tabla 29. Falta de integridad en los datos

Nivel de Riesgo			Actividad	Proceso
Alto	Moderado	Bajo		
		x	Formularios sin firmas	Creación de Cuentas de Usuarios y Perfiles, para los Sistemas de Información.
		x	Formularios sin sellos	

Fuente: El Autor

Recomendación

Gestionar el riesgo en base al dominio de COBIT 5 Evaluar, Dirigir y Monitorear; y el proceso: (EDM03).

4. **Título:** FALTA DE CAPACITACIÓN Y EVALUACIÓN A LOS USUARIOS, SOBRE EL USO DE CUENTAS Y POLÍTICAS DE CONTRASEÑAS.

Proceso Tics: Creación de Cuentas de Usuarios y Perfiles, para los Sistemas de Información.

Condición

- Se detectó que los Servidores Públicos de la Unidad de Talento Humano y Atención Ciudadana al salir de la oficina a reuniones u otra actividad dejan abierto las Sesiones del Sistema de Gestión Documental Quipux, y los navegadores de Internet, recuerdan los nombres de usuarios y contraseñas.
- Para salir del Quipux hacen clic directamente en el botón de control cerrar.
- En la Unidad Administrativa Distrital la contraseña del Quipux del jefe se comparte, con el fin de realizar autorizaciones de Quipux, cuando el mismo no se encuentra presente.

Criterio

ISO 27002 – 2013 a través del Dominio de: Control de Accesos, propone que se debe determinar, documentar y hacer una revisión a las Políticas de Control de Accesos, en base a los requerimientos de las entidades.

Causas

- Falta de programas de capacitación en materia de Seguridad Informática.
- Los Servidores Públicos, aún no han sido víctimas de ataques informáticos

Efectos

Tabla 30. Efectos de la Falta de Capacitación y Evaluación a los Usuarios, sobre el uso de cuentas y políticas de contraseñas.

Nivel de Riesgo			Actividad	Proceso
Alto	Moderado	Bajo		
x			Sabotaje	Creación de Cuentas de Usuarios y Perfiles, para los Sistemas de Información.
	x		Infección de Virus Informáticos	

Fuente: El Autor

Recomendación

Elaborar Políticas de Control de Acceso a los ordenadores y sistemas del Distrito Educativo - 02d03, a nivel de hardware, software y acceso a redes informáticas.

5. **Título:** FALTA DE SEGUIMIENTO AL CUMPLIMIENTO DE LOS PROCESOS DEL SGC POR LA DIRECCION

Proceso Tics: Soporte Técnico

X

Condición

- Se detectó que se llevaba registros de los procesos TICS, solo hasta el mes de enero del año 2017, se indagó la causa y se concluyó que era consecuencia de la transición de Directores Distritales.

Criterio

COBIT 5, a través del dominio de: Monitorear, Evaluar y Valorar; por medio del proceso habilitador: (MEA01), hace referencia que se debe supervisar los procesos que se estén cumpliendo en conformidad con los objetivos establecidos, de tal manera que se debe remitir informes de forma sistemática y planificada.

Causas

- Falta de seguimiento al cumplimento del Manual de Gestión Administrativa Distrital, por parte de la Coordinación Zonal 5.
- Falta de Políticas Internas, en relación al incumplimiento del Manual de Gestión Administrativa Distrital.

Efectos

Tabla 31. Efectos de la falta de seguimiento al cumplimiento de los procesos del Manual de Gestión Administrativa Distrital.

Nivel de Riesgo			Actividad	Proceso
Alto	Moderado	Bajo		
X			Pérdida de la Certificación ISO 9001, por incumplimiento del Manual de Gestión Administrativa Distrital.	Soporte Técnico
	X		Demoras en dar respuestas a los usuarios.	
	X		Información desorganizada e incompleta	

Fuente: El Autor

Recomendaciones:

- Planificar capacitaciones trimestralmente, en relación al uso del Manual de Gestión Administrativa Distrital.
- Elaborar políticas internas, que sancione a los Servidores Públicos que incumplan el Manual de Gestión Administrativa Distrital.
- Evaluar mensualmente la utilización del Manual de Gestión Administrativa Distrital y remitir informes a la Coordinación Zonal 5.

6. **Título:** NO SE UTILIZA SOFTWARE LIBRE; NI SE DISPONE DE LAS LICENCIAS DE SOFTWARE PROPIETARIO.

Proceso Tics: Soporte Técnico

Condición

- Se detectó que se hace uso de Software sin licencia, tanto a nivel de Sistema Operativo, cómo también programas de oficina y antivirus.

Criterio

Decreto Ejecutivo 1014. Art. 1 Establecer como política pública para las entidades de la Administración Pública Central la utilización de software libre en sus sistemas y equipamientos informáticos.

Causas

- Desconocimiento de la existencia y uso del Software Libre, por parte de los usuarios.
- Los Servidores Públicos han sido formados desde hace años en Software Propietario y se les hace difícil cambiar de paradigma.

Efectos

Tabla 32. Efectos de no utilizar Software Libre; ni de disponer de las licencias de Software Propietario.

Nivel de Riesgo	Actividad	Proceso

Alto	Moderado	Bajo		
X			Peligro de ataques de malware y mayor vulnerabilidad a infección de virus informáticos.	Soporte Técnico
	X		Demandas por uso de software ilegal	
X			Pérdida de la Certificación ISO 9001	

Fuente: El Autor

Recomendaciones:

- Programar capacitaciones sobre el uso de Software Libre.
- Instalación de programas de Software Libre que sustituyan a los propietarios.
- Adquirir las respectivas licencias del software que se utiliza en el Distrito Educativo 02d03.

7. **Título:** FALTA DE POLÍTICAS DE CONTINUIDAD DE LAS OPERACIONES TECNOLÓGICAS

Proceso Tics: Soporte Técnico

Condición

Se identificó que el Distrito Educativo - 02d03, no dispone de planes de continencia; así como tampoco se cuenta con políticas de realización de respaldos de información, debido a que los Backups se centralizan en un solo disco duro conectado a la red interna, sin protección física, ni restricciones de acceso lógicos.

Criterio

COBIT 5, en el dominio Construir, Adquirir e Implementar, a través del proceso habilitador de: Administrar la Disponibilidad y Capacidad (BAI04), da a conocer que se debe equilibrar los requerimientos actuales y futuros de disponibilidad, basados en requerimientos del negocio, la evaluación de riesgos, a fin de planificar e implementar; con el propósito de cumplir con los requerimientos identificados.

Causas

- Falta de un Servidor de Archivos
- Falta de Innovación Tecnológica
- Falta de presupuesto.

Efectos

Tabla 33. Efectos de la falta de Políticas de Continuidad de las Operaciones Tecnológicas.

Nivel de Riesgo			Actividad	Proceso
Alto	Moderado	Bajo		
x			Indisponibilidad de los Servicios Tecnológicos	Soporte Técnico
x			Pérdida de información valiosa para el Distrito Educativo - 02d03	

Recomendaciones:

- Elaborar planes de Contingencia con la finalidad de enfrentar posibles eventos adversos en el Distrito Educativo - 02d03
- Realizar capacitaciones y simulacros del plan de Contingencia.
- Almacenar los respaldos de información en un lugar diferente al actual.

8. **Título:** FALTA DE GERENCIA EN LA RED LAN

Proceso Tics: Instalación de Enlaces de Internet, Datos y Telefonía.

Condición

- Se detectó que no existe administración de la Red LAN del Distrito Educativo - 02d03, por lo que no disponen de ningún firewall, no se monitorea el tráfico de la red y los usuarios cambian las direcciones IP, generando conflictos de duplicidad de direccionamiento IP.

Criterio

COBIT 5, a través del Dominio: Construir, Adquirir e Implementar Entregar, y el proceso: Administrar la Configuración (BAI10), hace referencia sobre verificar y auditar la información de la configuración, con el propósito de que el activo pueda gestionarse eficientemente y enfrentar a los incidentes de servicio.

ISO 27002:2013, a través del dominio Seguridad en los equipos, menciona que se debe proteger a los equipos contra las amenazas físicas y ambientales, con el propósito de reducir el riesgo de accesos no autorizados a la información y la protección contra pérdidas o robo.

Causas

- Falta de un responsable que se encargue de Administrar la Red LAN.
- Falta de inversión tecnológica en la Unidad Distrital TIC's.

Efectos

Tabla 34. Efectos de la falta de Administración de la Red LAN

Nivel de Riesgo			Actividad	Proceso
Alto	Moderado	Bajo		
x			Infiltraciones en la red LAN	Instalación de Enlaces de Internet, Datos y Telefonía.
	x		Propagación de códigos maliciosos, a través de la red	

Fuente: El Autor

Recomendaciones:

- Elaborar un plan de administración de la Red LAN del Distrito Educativo 02d03.
- Gestionar adquisiciones de hardware y software para la red.
- Realizar una reingeniería de la infraestructura de red.

9. Título: IMPLEMENTACIÓN DE ESTÁNDARES EN LA RED LAN

Proceso Tics: Instalación de Enlaces de Internet, Datos y Telefonía.

Condición

- Se identificó que el cableado estructurado, se ha realizado sin considerar ninguna norma durante el proceso de instalación, por lo que hay cables por diferentes lugares que se desconoce que función cumplen cada uno de ellos, porque no se encuentran etiquetados, también varias instalaciones eléctricas generan riesgo.

Criterio

ISO 27002:2013, a través del dominio Seguridad en los equipos y el proceso seguridad en el cableado propone que se debe proteger el cableado de energía y de telecomunicaciones que transporten datos o soporten servicios de información contra posibles intercepciones o daños.

Causas

- Cableado estructurado realizado en base a las necesidades y disponibilidad de materiales del Distrito Educativo 02d03.

Efectos

Tabla 35. Efectos de la falta de implementación de estándares en la Red LAN

Nivel de Riesgo			Actividad	Proceso
Alto	Moderado	Bajo		
X			Interrupciones del servicio	Instalación de Enlaces de Internet, Datos y Telefonía.
X			Puntos de energía eléctrica pueden ocasionar circuito eléctrico.	

Fuente: El Autor

Recomendación:

- Utilizar para el cableado estructurado el estándar TIA o la guía técnica ANIXTER.
- Contratar una póliza de seguro, para enfrentar eventos adversos.

10. Título: OPTIMIZACIÓN DE RECURSOS

Proceso Tics: Instalación de Enlaces de Internet, Datos y Telefonía.

Condición

- Se identificó que se dispone de una red de internet adicional sin restricciones de acceso, con el propósito de llevar a cabo las video conferencias, en el Distrito Educativo - 02d03.

Criterio

COBIT 5, en el Dominio: Evaluar, Dirigir y Monitorear, a través del proceso: Asegurar la Optimización de los Recursos (EDM04), se refiere a asegurar que las capacidades (Personas, Procesos y Tecnologías), presenten disponibilidad para soportar eficazmente los objetivos de la empresa aun coste óptimo.

Causas

- Falta de gestión de un puerto de Red de acceso libre, por medio de la WAN Educativa.
- Falta de seguimiento a cierre de servicios, al momento de remplazar por un nuevo.

Efectos

Tabla 36. Efectos de la carencia de estándares en la Red LAN

Nivel de Riesgo			Actividad	Proceso
Alto	Moderado	Bajo		
x			Costo adicional de la red de internet abierta	Instalación de Enlaces de Internet, Datos y Telefonía.
	x		Sub utilización de los recursos de Internet	

Fuente: El Autor

Recomendación:

- Gestionar la habilitación de un puerto de la WAN Educativa, con el propósito de realizar video conferencias.

4 CONCLUSIONES Y RECOMENDACIONES

- Se fundamentó teóricamente los diferentes conceptos de Auditoria a la Seguridad Informática, Tipos, Estándares, normas y metodologías.
- Las técnicas de recolección de datos, ayudaron a contextualizar el problema y orientaron a la solución.
- La Auditoría a la seguridad informática, se realizó conforme a las fases de: Planeación, Ejecución y Comunicación de Resultados.
- Los Procesos de TI Distrital 02d03, se encuentran en el nivel de riesgo Alto y Moderado, de tal manera que se requiere la adopción de acciones inmediatas recomendadas en el informe.
- Se diseñó el programa de auditoría, conforme a los riesgos detectados.
- Se realizaron pruebas de cumplimiento y pruebas sustantivas a los Procesos Tics-02d03.
- Los procesos de TI-02d03, se encuentran en un nivel de madurez gestionado.
- Se redactó el informe de auditoría, conforme a las normas establecidas y se comunicaron los resultados.

RECOMENDACIONES

- Se recomienda auditar los procesos relacionados con las Tecnologías de la Información y Comunicaciones de las demás Unidades.
- Dar seguimiento trimestralmente a las recomendaciones de Auditoría a la Seguridad Informática.
- Aplicar el marco de referencia COBIT 5 e ISO 27000, en futuras auditorías.
- La Dirección de seguimiento al cumplimiento de los Procesos conforme al Manual de Gestión Administrativa Distrital.
- Asignar personal en el Distrito Educativo 02d03, con funciones de auditoría, seguridad informática y administración de la Red.

5 REFERENCIAS BIBLIOGRÁFICAS

Arens, A., Elder, R., & Beasley, M. (2007). *Auditoría Un enfoque integral.* México: Pearson.

Becerra Arévalo, N. P. (2017). *Auditoría Informática, basada en la Norma ISO 27004, para el control del parque Técnológico UNIANDES Puyo.* Ambato: UNIANDES.

Calero, V., Flores, Q., & Amador, D. (06 de 2016). ADAPTACIÓN DE LA METODOLOGÍA MEHARI A LA FASE DE PLANEACION DE UN SGSI PARA UN PROCEDIMIENTO DE ESTUDIO PROPUESTO.

Caranqui, V. (2014). *AUDITORÍA INFORMÁTICA ORIENTADA A LA SEGURIDAD DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN EN LA EMPRESA "ENTERSYSTEMS LTDA." DE LA CIUDAD DE RIOBAMBA, PERIODO 2012.* Riobamba: ESCUELA SUPERIOR POLITÉCNICA DE CHIMBORAZO.

Casanova Yandún, E. G., & Vaca Benalcázar, C. P. (2014). *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: ESPE.

Castiñeira, V. (29 de 05 de 2013). Guía de implantación del estándar ISO/IEC 15504 en PYMES.

CONTRALORIA GENERAL DEL ESTADO. (16 de 12 de 2014). NORMAS DE CONTROL INTERNO DE LA CONTRALORIA GENERAL DEL ESTADO. Quito, Pichincha, Ecuador.

COORPORACION 3D. (13 de 02 de 2014). ISO 9001-2008 Inducción al Sistema de Gestión de Calidad. Quito, Pichincha, Ecuador.

Echenique, J. A. (2001). *AUDITORIA EN INFORMATICA.* México: Mc Graw Hill.

Erb, M. (2008). *Gestión de Riesgo en la Seguridad Informática.* Obtenido de 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.

Escrivá, R. R. (2013). *Seguridad Informática.* MACMILLAN Iberia, S.A.

Galaz, Y., & Ruiz, U. (2015). Marco de referencia COSO ERM.

Gallego, F. (2004). Cálculo del tamaño de la muestra. Barcelona, España.

Instituto de Auditores Internos de España. (03 de 2014). Cobertura del Riesgo Tecnológico: hacia una Auditoría Interna de TI Integrada. España.

ISACA . (2012). Cobit 5.

ISACA. (2013). Estándares Actuales.

ISOTools. (7 de 12 de 2016). *ISOTools Excellence Colombia*. Obtenido de https://www.isotools.com.co/como-integrar-los-marcos-normativos-coso-cobit-e-iso-27001/

ITSI. (2016). *COBIT*. Obtenido de http://cobitequipo03.blogspot.com/p/4.html

Jara, B. (2012). *AUDITORÍA INFORMÁTICA DE LA GESTIÓN DE TI PARA LA EMPRESA "ADVANCE CONSULTING" UTILIZANDO EL MODELO COBIT. .* Quito: PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR .

Jimenez, A. (2009). *Historia de la Auditoría.* El cid Editor Apuntes.

Jiménez, A. (28 de Junio de 2016). *Repositorio Institucional de la Universidad de las Fuerzas Armadas ESPE.* Obtenido de https://repositorio.espe.edu.ec/handle/21000/12111

Mair, W. (1991). Auditoría Administrativa.

MINISTERIO DE EDUCACION. (25 de 01 de 2012). Acuerdo 020-12. Quito, Pichincha, Ecuador.

Ministerio de Educación. (Seotiembre de 2013). *Ministerio de Educación.* Obtenido de https://educacion.gob.ec/wp-content/uploads/downloads/2013/10/Desglose_DirDist_SEP.pdf

MINISTERIO DE EDUCACION DEL ECUADOR. (20 de 07 de 2015). Manual de Calidad de Gestión Administrativa Distrital. Quito, Pichincha, 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. (06 de 2015). Caso Práctico de Apepito al Riesgo. España.

Palacios Bayas, A. R. (02 de 03 de 2018).

Pulgarín Alvarez, A. P. (2016). *Auditoría Informática a la Empresa Ecua-Mails.* Quito: Universidad Tecnológica ISRAEL.

Ramírez, L. (01 de 12 de 2015). Ecuador, Ecuador.

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

Rodríguez, A. (2015). Análsis y Gestión de Riesgos en un Sistema Informático.

Sistema de Gestión de Seguridad de la Información. (01 de 2018). *Blog especializado en Sistema de Gestión de Seguridad de la Información*. Obtenido de https://twitter.com/intent/tweet?text=La%20norma%20ISO%2FIEC%2015504%20%22Determinaci%C3%B3n%20de%20la%20Capacidad%20de%20Mejora%20del%20Proceso%20de%20Software%22&url=https%3A%2F%2Fwww.pmg-ssi.com%2F2018%2F01%2Festandar-internacional-iso-iec-15504%2F&ori

Vaca, C. P. (09 de 08 de 2017). FUNDAMENTOS - COBIT. Quito, Pichincha, Ecuador.

Young, & Ernst. (2011). Seguridad de la Información, en un mundo sin fronteras. *Perspectivas, sobre los riesgos de TI*, 4.

ANEXOS

ANEXOS

ANEXO 1

Entrevista a: Lcdo. David Galarza director de la Dirección Distrital 02d03 Chimbo-San Miguel-Educación

Objetivo: Conocer el contexto organizacional del Distrito Educativo - 02d03.

1) ¿Desde qué fecha se encuentra como Director Distrital?

   ……..
2) ¿Cómo puede describir la situación organizacional, cuando llego a formar parte del Distrito Educativo?

   …….
3) ¿Cuáles considera que son los activos más importantes de la Dirección distrital?

   ……..
4) ¿Podría mencionar en que debería mejorar el Distrito Educativo?

   …….
5) ¿Qué haría en caso de presentase un incidente de pérdida o divulgación de información sensible o confidencial?

   ……..
6) ¿Qué medidas de seguridad tiene el distrito?

   ……..
7) ¿Cómo es la comunicación con los líderes de los departamentos y analistas?

   ……..
8) ¿Qué piensa de la Auditoría Informática que se está realizando en el Distrito Educativo?

   ……..

ANEXO 2

Entrevista a: Lcdo. Carlos Aroca – Analista Distrital de la Unidad de Tecnología de la Información y Comunicaciones.

Objetivo. Comprender la problemática del Distrito Educativo, a nivel de Tics y sus factores.

1) ¿Cuáles han sido los principales problemas informáticos que usted ha tenido en su departamento?

   …….

2) ¿Cómo los ha solucionado?

   …….

3) ¿Qué controles de seguridad informática aplica desde su departamento hacia los demás?

   ……..

4) ¿Cuáles considera los activos más importantes de la Dirección Distrital de Educación?

   ……

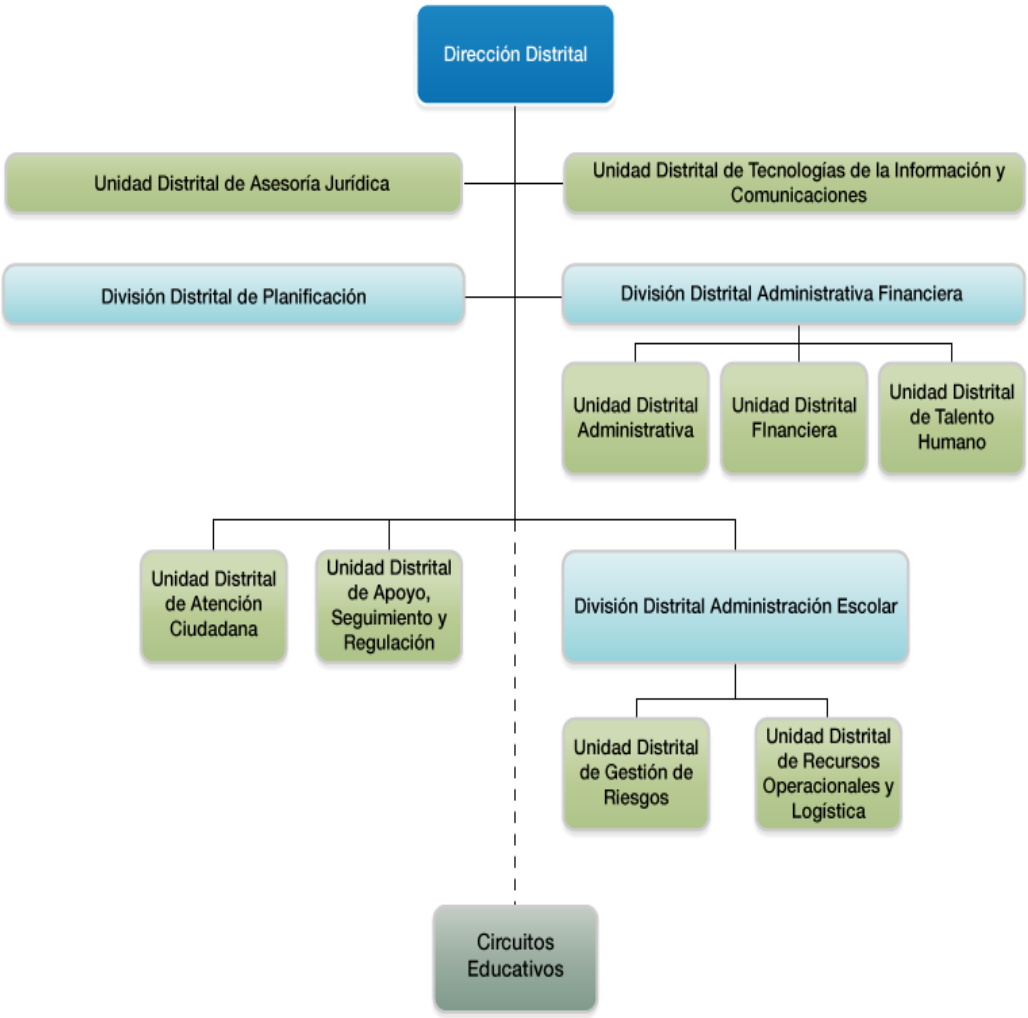
5) ¿Qué medios utiliza para proteger la información?

   ……..

Entrevista a Analista Distrital de Tecnologías de la Información y Comunicaciones del Distrito Educativo - 02d03.

ANEXO 3

Organigrama del Distrito Educativo 02d03



ANEXO 4

Matriz de Riesgos Informáticos

Ministerio de Educación del Ecuador

MATRIZ DE RIESGOS INFORMÁTICOS

UNIDAD DE TECNOLOGÍA DE LA INFORMACION Y COMUNICACIONES

DIRECCION DISTRITAL 02D03 CHIMBO-SAN MIGUEL-EDUCACIÓN

PROBABILIDAD		IMPACTO		TIPO DE CONTROL		FRECUENCIA DE OCURRENCIA		GRADO DE AUTOMATIZACIÓN		EFICIENCIA		RESPUESTA AL RIESGO
Ponderación	Descripción	Ponderación	Descripción	Ponderación	Descripción	Ponderación	Descripción	Ponderación	Descripción	Ponderación	Descripción	Evitar
3	Posible	3	Alto	3	Preventivo	3	Permament	3	Automatizado	3	Efectivo	Reducir
2	Probable	2	Moderado	2	Detectivo	2	Periódico	2	Semi Automatizado	2	Poco Efectivo	Transferir
1	Remota	1	Bajo	1	Correctivo	1	Ocasional	1	Manual	1	Ineficiente	Aceptar

								Riesgo Inherente			Controles					Riesgo Residual	
Ref.	Macroproceso	Subproceso / Activos	Factor de Riesgo (Actividad)	Proceso ERM	Procesos IT COBIT 5	Origen de Riesgo	Evento de Riesgo	Probabilidad	Impacto	Riesgo Inherente	Control	Tipo	Frecuencia	Grado de Automatización	Eficiencia Control	Riesgo Residual	Respuesta al Riesgo
R1	Seguridad Informática	Contratación o Adquisición de Bienes y Servicios Tecnológicos	Solicitud vía correo electrónico o Quipux	Proceso Estratégico	Alinear, Planificar y Organizar	Tecnológico	Indisponibilidad del correo electrónico	2	3	6	Manual de Sistema de Gestión Adminsitrativa Distrital	3	3	2	1,33	4,67	Evitar
R2	Seguridad Informática	Contratación o Adquisición de Bienes y Servicios Tecnológicos	Análisis de mercado en sitios web de E-comerce	Proceso Estratégico	Alinear, Planificar y Organizar	Externo	Fraude	2	3	6	BAI09 Gestionar los Activos	3	3	3	3,00	3,00	Reducir
R3	Seguridad Informática	Contratación o Adquisición de Bienes y Servicios Tecnológicos	No se realizan Inversiones en Ti	Proceso Estratégico	Alinear, Planificar y Organizar	Tecnológico	Interrupción de los servicios tecnológicos	2	3	6	BAI04 Gestionar la Disponibilidad y Capacidad	3	3	3	3,00	3,00	Reducir
R4	Seguridad Informática	Contratación o Adquisición de Bienes y Servicios Tecnológicos	No se dispone de Inventario Tecnológico Actualizado	Proceso Estratégico	Alinear, Planificar y Organizar	Humano	Robo/Pérdida de equipos informáticos	2	3	6	EDM04. Asegurar la optimización de los recursos	3	3	3	3,00	3,00	Reducir
R5	Seguridad Informática	Creación de cuentas de usuarios y perfiles	Documentación de creación de cuentas de usuario y perfiles	Proceso Operativo	Entregar, dar Servicio y Soporte	Humano	Toma de decisiones inadecuadas	3	3	9	APO01 Gestionar el Marco de	3	3	3	3,00	6,00	Reducir

Ref.	Macroproceso	Subproceso / Activos	Factor de Riesgo (Actividad)	Proceso ERM	Procesos IT COBIT 5	Origen de Riesgo	Evento de Riesgo	Probabilidad	Impacto	Riesgo Inherente	Control	Tipo	Frecuencia	Grado de Automatización	Eficiencia Control	Riesgo Residual	Respuesta al Riesgo
R6	Seguridad Informática	Creación de cuentas de usuarios y perfiles	Desactivación inoportuna de cuentas de usuario y perfiles	Proceso Operativo	Entregar, dar Servicio y Soporte	Externo	Fraude	2	3	6	Manual de Sistema de Gestión Adminsitrativa Distrital	3	3	2	1,33	4,67	Evitar
R7	Seguridad Informática	Creación de cuentas de usuarios y perfiles	Falta de Políticas de creación y uso de contraseñas	Proceso Operativo	Entregar, dar Servicio y Soporte	Externo	Vulnerabilidad a la confidencialidad	3	3	9	Cobit 5 y la Seguridad de la información	3	3	3	3,00	6,00	Reducir
R8	Seguridad Informática	Soporte Técnico	No se dispone de Documentación organizada de peticiones de Soporte Técnico	Proceso de Soporte	Entregar, dar Servicio y Soporte	Procesos	Bajar la puntuación de la certificación ISO9001 de Gestión de Calidad	2	3	6	DSS02 Gestionar las peticiones y los incidentes del servicio	3	3	3	3,00	3,00	Aceptar
R9	Seguridad Informática	Soporte Técnico	No existe informes de inspección y diagnóstico	Proceso de Soporte	Entregar, dar Servicio y Soporte	Procesos	Pérdida de eficiencia del cumplimiento del proceso	3	3	9	Manual de Sistema de Gestión Adminsitrativa Distrital	3	3	2	1,33	7,67	Aceptar

Ref.	Macroproceso	Subproceso / Activos	Factor de Riesgo (Actividad)	Proceso ERM	Procesos IT COBIT 5	Origen de Riesgo	Evento de Riesgo	Probabilidad	Impacto	Riesgo Inherente	Control	Tipo	Frecuencia	Grado de Automatización	Eficiencia Control	Riesgo Residual	Respuesta al Riesgo
R10	Seguridad Informática	Soporte Técnico	Falta de licenciamiento de Software en Sistemas Operativos, Ofimática y Seguridad	Proceso de Soporte	Entregar, dar Servicio y Soporte	Procesos	Pérdida de la certificación ISO 9001	2	3	6	Decreto 1014 Uso del software libre	3	3	3	3,00	3,00	Evitar
R11	Seguridad Informática	Soporte Técnico	Usuarios y Claves de sistema Quipux Autoguardadas en los navegadores de Internet	Proceso de Soporte	Entregar, dar Servicio y Soporte	Tecnológico	Acceso no autorizado a sistemas de información.	2	3	6	APO13 Gestionar la Seguridad	3	3	3	3,00	3,00	Evitar
R12	Seguridad Informática	Soporte Técnico	No se dispone de políticas de Continuidad de Negocio	Proceso de Soporte	Entregar, dar Servicio y Soporte	Tecnológico	Indisponibilidad de la Operatividad Tecnológica.	3	3	9	DS4.2 Estrategia de la continuidad de TI	3	3	3	3,00	6,00	Reducir
R13	Seguridad Informática	Soporte Técnico	Estaciones de trabajo sin antivirus	Proceso de Soporte	Entregar, dar Servicio y Soporte	Tecnológico	Infección de virus informáticos	3	3	9	Iso27002	3	3	3	3,00	6,00	Reducir

Ref.	Macroproceso	Subproceso / Activos	Factor de Riesgo (Actividad)	Proceso ERM	Procesos IT COBIT 5	Origen de Riesgo	Evento de Riesgo	Probabilidad	Impacto	Riesgo Inherente	Control	Tipo	Frecuencia	Grado de Automatización	Eficiencia Control	Riesgo Residual	Respuesta al Riesgo
R14	Seguridad Informática	Soporte Técnico	No se cuenta con controles de acceso lógico al computador	Proceso de Soporte	Entregar, dar Servicio y Soporte	Humano	Vulnerabilidad a pérdida/robo de la confidencialidad de la información.	2	3	6	Iso27002	3	3	3	3,00	3,00	Reducir
R15	Seguridad Informática	Soporte Técnico	No se gestiona de manera adecuada los respaldos de información.	Proceso de Soporte	Entregar, dar Servicio y Soporte	Tecnológico	Interrupción de los servicios tecnológicos	2	3	6	Iso27002	3	3	3	3,00	3,00	Evitar
R16	Seguridad Informática	Soporte Técnico	No se cuenta con registros de incidentes/soluciones	Proceso de Soporte	Entregar, dar Servicio y Soporte	Humano	Pérdida de eficiencia del cumplimiento del proceso	2	3	6	PO1.3 Evaluación de desempeño.	3	3	2	1,33	4,67	Aceptar
R17	Seguridad Informática	Soporte Técnico	Se ensamblan nuevas computadoras, con fuentes y case utilizados .	Proceso de Soporte	Entregar, dar Servicio y Soporte	Humano	Daños Irreversibles en las piezas nuevas	3	3	9	DSS04 Gestión de la continuidad	3	3	3	3,00	6,00	Evitar
R18	Seguridad Informática	Instalación de enlaces de internet Datos y Telefonía	No se cuenta con un registro o archivo completo de las peticiones del proceso.	Proceso Operativo	Alinear, Planificar y Organizar	Humano	Toma de decisiones poco adecuadas	2	3	6	BAI02 Gestionar la Identificación y la construcción de soluciones	3	2	2	0,89	5,11	Aceptar

Ref.	Macroproceso	Subproceso / Activos	Factor de Riesgo (Actividad)	Proceso ERM	Procesos IT COBIT 5	Origen de Riesgo	Evento de Riesgo	Probabilidad	Impacto	Riesgo Inherente	Control	Tipo	Frecuencia	Grado de Automatización	Eficiencia Control	Riesgo Residual	Respuesta al Riesgo
R19	Seguridad Informática	Instalación de enlaces de internet Datos y Telefonía	No se cuenta con un plan de seguridad informática	Proceso Operativo	Alinear, Planificar y Organizar	Tecnológico	Acceso no autorizado a la red informática	2	3	6	APO02. Gestionar la Seguridad	3	3	3	3,00	3,00	Reducir
R20	Seguridad Informática	Instalación de enlaces de internet Datos y Telefonía	No se cuenta con un archivo completo de los formularios del proceso	Proceso Operativo	Alinear, Planificar y Organizar	Humano	Toma de decisiones poco adecuadas	2	3	6	APO01.08 Mantener la conformidad con políticas y procedimientos	3	3	3	3,00	3,00	Aceptar
R21	Seguridad Informática	Instalación de enlaces de internet Datos y Telefonía	Solo se dispone de Actas de Entrega Recepción, más no se cuenta con Informes de la Instalación del Servicio.	Proceso Operativo	Alinear, Planificar y Organizar	Humano	Toma de decisiones poco adecuadas	2	3	6	Manual de Sistema de Gestión Adminsitrativa Distrital	3	3	2	1,33	4,67	Aceptar
R22	Seguridad Informática	Instalación de enlaces de internet Datos y Telefonía	Falta de seguridad física sobre los dispositivos de red	Proceso Operativo	Alinear, Planificar y Organizar	Externo	Robo de dispositivos de red	2	3	6	APO02. Gestionar la Seguridad	3	3	3	3,00	3,00	Evitar

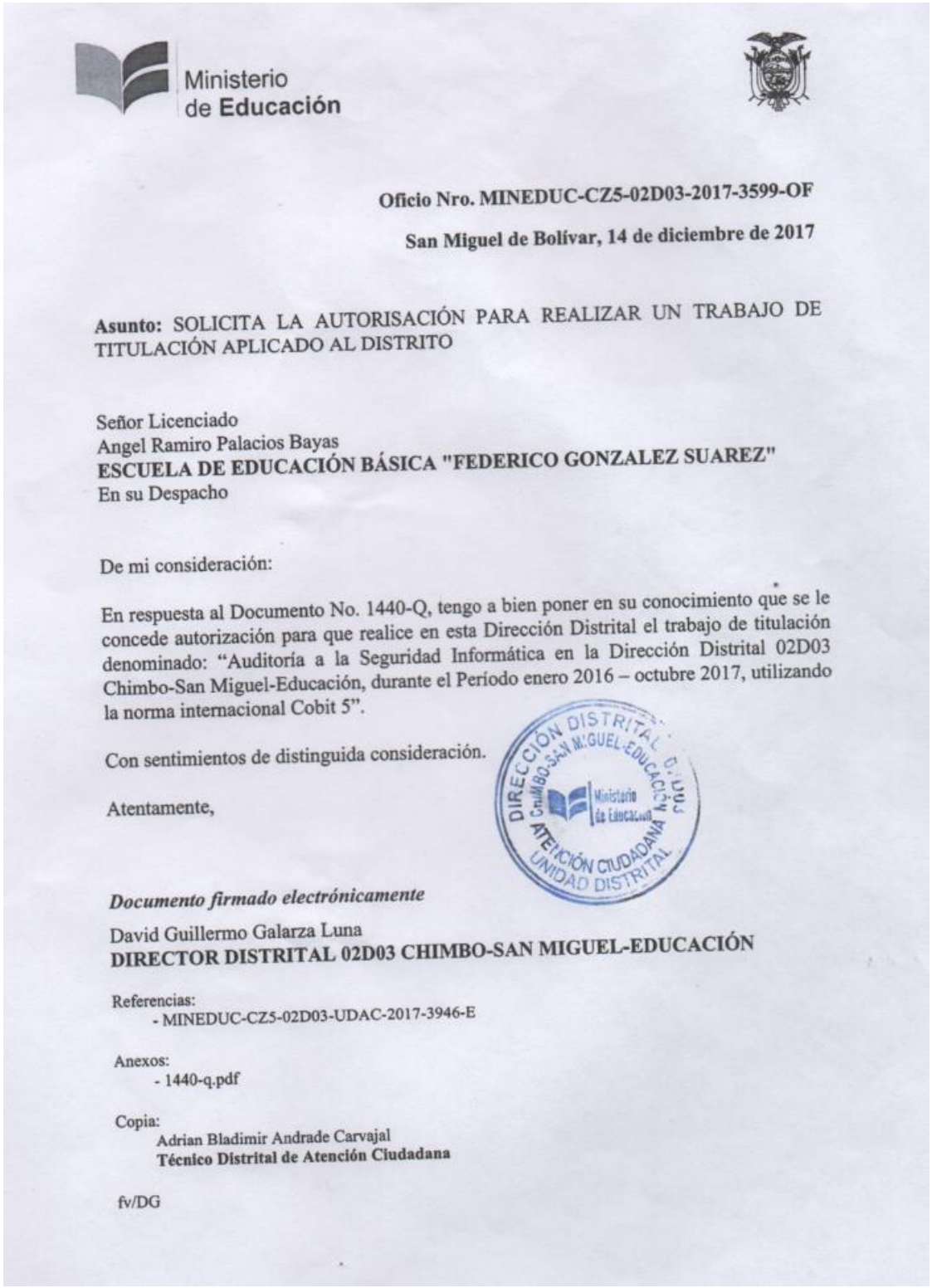
Ref.	Macroproceso	Subproceso / Activos	Factor de Riesgo (Actividad)	Proceso ERM	Procesos IT COBIT 5	Origen de Riesgo	Evento de Riesgo	Probabilidad	Impacto	Riesgo Inherente	Control	Tipo	Frecuencia	Grado de Automatización	Eficiencia Control	Riesgo Residual	Respuesta al Riesgo
R23	Seguridad Informática	Instalación de enlaces de internet Datos y Telefonía	Falta de seguridad lógica sobre los dispositivos de red (Firewall)	Proceso Operativo	Alinear, Planificar y Organizar	Externo	Sabotaje	2	3	6	APO02. Gestionar la Seguridad	3	3	3	3,00	3,00	Reducir
R24	Seguridad Informática	Instalación de enlaces de internet Datos y Telefonía	Falta de puertos de red, para crecimiento del parque informatico	Proceso Operativo	Alinear, Planificar y Organizar	Tecnológico	Indisponibilidad de la Operatividad Tecnológica.	3	3	9	APO03. Gestionar la Arquitectura Empresarial	3	3	2	1,33	7,67	Reducir
R25	Seguridad Informática	Instalación de enlaces de internet Datos y Telefonía	No se cuenta con planta se suministro de energía electrica	Proceso Operativo	Alinear, Planificar y Organizar	Tecnológico	Indisponibilidad de servicios Tecnológicos.	3	3	9	DS4.2 Estrategia de la continuidad de TI	3	3	3	3,00	6,00	Aceptar
R26	Seguridad Informática	Instalación de enlaces de internet Datos y Telefonía	No se cuenta con planos/diagramas de la infraestructura de Red	Proceso Operativo	Alinear, Planificar y Organizar	Procesos	Indisponibilidad de la Continuidad del servicio	2	3	6	Cobit 5 y la Seguridad de la información	3	3	3	3,00	3,00	Evitar
R27	Seguridad Informática	Cierre de cuentas de Sistemas de Información	No se cuenta con una estadística sobre las peticiones del proceso	Proceso de Soporte	Entregar, dar Servicio y Soporte	Procesos	Toma de decisiones inadecuadas	3	3	9	Manual de Sistema de Gestión Adminsitrativa Distrital	3	3	2	1,33	7,67	Aceptar

Ref.	Macroproceso	Subproceso / Activos	Factor de Riesgo (Actividad)	Proceso ERM	Procesos IT COBIT 5	Origen de Riesgo	Evento de Riesgo	Probabilidad	Impacto	Riesgo Inherente	Control	Tipo	Frecuencia	Grado de Automatización	Eficiencia Control	Riesgo Residual	Respuesta al Riesgo
R28	Seguridad Informática	Cierre de cuentas de Sistemas de Información	No se cuenta con la documentación del Proceso	Proceso de Soporte	Entregar, dar Servicio y Soporte	Humano	Toma de decisiones inadecuadas	3	3	9	Manual de Sistema de Gestión Adminsitrativa Distrital	3	3	2	1,33	7,67	Reducir
R29	Seguridad Informática	Habilitación de Servicios Tecnológicos Restringidos	Incumplimiento de las Políticas de uso de computador	Proceso Operativo	Entregar, dar Servicio y Soporte	Tecnológico	Infección de virus informáticos	3	3	9	Supervisar, Evaluar y Valorar el Sistema de Control Interno	3	3	2	1,33	7,67	Reducir
R30	Seguridad Informática	Habilitación de Servicios Tecnológicos Restringidos	No se cuenta con la documentación de los requerimientos de habilitación de servicios tecnológicos restringidos	Proceso Operativo	Entregar, dar Servicio y Soporte	Humano	Toma de decisiones inadecuadas	2	3	6	Manual de Sistema de Gestión Adminsitrativa Distrital	3	3	2	1,33	4,67	Reducir

Ref.	Macroproceso	Subproceso / Activos	Factor de Riesgo (Actividad)	Proceso ERM	Procesos IT COBIT 5	Origen de Riesgo	Evento de Riesgo	Probabilidad	Impacto	Riesgo Inherente	Control	Tipo	Frecuencia	Grado de Automatización	Eficiencia Control	Riesgo Residual	Respuesta al Riesgo
R31	Seguridad Informática	Habilitación de Servicios Tecnológicos Restringidos	No se dispone de los formularios del proceso	Proceso Operativo	Entregar, dar Servicio y Soporte	Humano	Toma de decisiones inadecuadas	2	3	6	Manual de Sistema de Gestión Adminsitrativa Distrital	3	3	2	1,33	4,67	Reducir
R32	Seguridad Informática	Habilitación de Servicios Tecnológicos Restringidos	No se dispone de las notificaciones al usuario del servicio habilitado.	Proceso Operativo	Entregar, dar Servicio y Soporte	Humano	Toma de decisiones inadecuadas	2	3	6	Manual de Sistema de Gestión Adminsitrativa Distrital	3	3	2	1,33	4,67	Reducir

ANEXO 5

Gestión del Patrocinio de la Auditoría a la Seguridad Informática



Ministerio de Educación

Oficio Nro. MINEDUC-CZ5-02D03-2017-3599-OF

San Miguel de Bolívar, 14 de diciembre de 2017

Asunto: SOLICITA LA AUTORISACIÓN PARA REALIZAR UN TRABAJO DE TITULACIÓN APLICADO AL DISTRITO

Señor Licenciado
Angel Ramiro Palacios Bayas
ESCUELA DE EDUCACIÓN BÁSICA "FEDERICO GONZALEZ SUAREZ"
En su Despacho

De mi consideración:

En respuesta al Documento No. 1440-Q, tengo a bien poner en su conocimiento que se le concede autorización para que realice en esta Dirección Distrital el trabajo de titulación denominado: "Auditoría a la Seguridad Informática en la Dirección Distrital 02D03 Chimbo-San Miguel-Educación, durante el Período enero 2016 – octubre 2017, utilizando la norma internacional Cobit 5".

Con sentimientos de distinguida consideración.

Atentamente,

DIRECCIÓN DISTRITAL 02D03 CHIMBO-SAN MIGUEL-EDUCACIÓN Ministerio de Educación ATENCIÓN CIUDADANA UNIDAD DISTRITAL

Documento firmado electrónicamente

David Guillermo Galarza Luna
DIRECTOR DISTRITAL 02D03 CHIMBO-SAN MIGUEL-EDUCACIÓN

Referencias:
- MINEDUC-CZ5-02D03-UDAC-2017-3946-E

Anexos:
- 1440-q.pdf

Copia:
Adrian Bladimir Andrade Carvajal
Técnico Distrital de Atención Ciudadana

fv/DG

ANEXO 6

Papel de Trabajo. - Selección del Personal a entrevistar

	PAPEL DE TRABAJO		
Tema de Auditoría:	Auditoría a la Seguridad Informática en la Dirección Distrital 02d03 Chimbo-San Miguel-Educación, durante el periodo enero 2016 - octubre 2017; utilizando el marco de referencia Cobit 5.	**Referencia:**	PA_EN_001
Entidad Auditada:	DIRECCION DISTRITAL 02D03 CHIMBO-SAN MIGUEL-EDUCACION	**Elaborado por:** Angel Palacios	**Fecha:** 17/01/2018
Periodo:	Enero 2016-octubre 2017	**Revisado por:** Ing. Christian Vaca	**Fecha:** 18/01/2018
Objetivo:	Identificar el personal a entrevistar	**Aprobado por:** Ing. Christian Vaca	**Fecha:** 18/01/2018

Procedimientos:

1.Se realizo una visita in situ, a la Dirección Distrital se procedió a recorrer las instalaciones.

2.Previamente el 14 de Diciembre del 2014 se obtuvo la respuesta del Sr. Director Distrital, para la realización de la Auditoría a la Seguridad Informática

Conclusiones:

Se determino que el personal objeto de la entrevista, son:

Nombres y Apellidos	**Cargo**
1.Lcdo. David Galarza Luna	Director Distrital
2.Lcdo. Carlos Aroca Benítez	Analista Distrital TICS

Anexo: img.-Autorización_Auditoría

ANEXO 7

Papel de Trabajo. - Identificación de los Procesos TIC's a Auditar

PAPEL DE TRABAJO

Tema de Auditoría:	Auditoría a la Seguridad Informática en la Dirección Distrital 02d03 Chimbo-San Miguel-Educación, durante el periodo enero 2016 - octubre 2017; utilizando el marco de referencia Cobit 5.	**Referencia:**	PA_EN_002
Entidad Auditada:	DIRECCION DISTRITAL 02D03 CHIMBO-SAN MIGUEL-EDUCACION	**Elaborado por:** Angel Palacios	**Fecha:** 19/01/2018
Periodo:	Enero 2016-octubre 2017	**Revisado por:** Ing. Christian Vaca	**Fecha:** 22/01/2018
Objetivo:	Identificar los Procesos de la Unidad de Tecnologías de la Información y Comunicaciones	**Aprobado por:** Ing. Christian Vaca	**Fecha:** 22/01/2018

Procedimientos:	
	Solicitud de documentos de los Procesos de la Unidad de Tecnologías de la Información y Comunicaciones
Responsable:	Lcdo. Carlos Aroca Benitez
Cargo:	Analista Distrital TICS
Fuente:	Sistema de Gestión de Calidad ISO 9001 (SGC)
Conclusiones:	
	Se entrego en formato digital los documentos de los Procesos de la Unidad de Tics

Procesos de la Unidad de Tics-Distrital
1.Contratación o Adquisición de Bienes y Servicios Tecnológicos.
2.Creación de cuentas de usuarios y perfiles
3.Soporte Técnico (Distrital)
4.Instalación de enlaces de internet Datos y Telefonía (Distrital)
5.Cierre de cuentas de Sistemas de Información
6.Habilitación de Servicios Tecnológicos Restringidos

Anexo:	Procesos Adjetivos Tics

ANEXO 8

Papel de Trabajo. – Selección del Enfoque de trabajo-Metodología

PAPEL DE TRABAJO

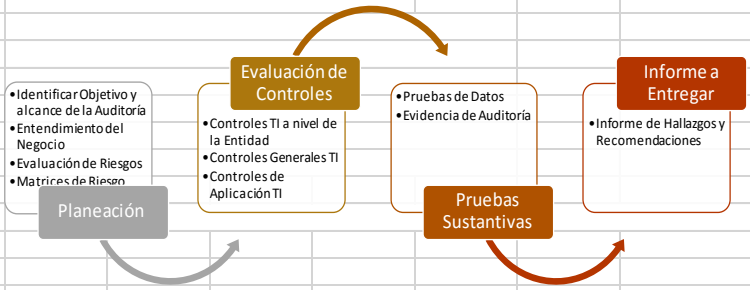
Tema de Auditoría:	Auditoría a la Seguridad Informática en la Dirección Distrital 02d03 Chimbo-San Miguel-Educación, durante el periodo enero 2016 - octubre 2017; utilizando el marco de referencia Cobit 5.	**Referencia:**	PA_EN_003
Entidad Auditada:	DIRECCION DISTRITAL 02D03 CHIMBO-SAN MIGUEL-EDUCACION	**Elaborado por:** Angel Palacios	**Fecha:** 23/01/2018
Periodo:	Enero 2016-octubre 2017	**Revisado por:** Ing. Christian Vaca	**Fecha:** 25/01/2018
Objetivo:	Selección del Enfoque de Trabajo (Metodología)	**Aprobado por:** Ing. Christian Vaca	**Fecha:** 25/01/2018

Procedimientos:

Investigación Bibliográfica sobre: Metodologías de Auditoría Informática, Marcas de Auditoría y Umbrales de Riesgo

Fuente: Google Académico

Hallazgos:



METODOLOGIA

1. Índice

PA - Planificación	Referencia
Entendimiento del Negocio	PA_EN_001
Identificacion de Riesgos	PA_RSK_2
Elaboración de los programas y procedimientos de auditoria	PA_PRO_3
EJ -Ejecución	
Pruebas de Controles	EJ_PC_1
Controles Generales	EJ_CG_2
Controles de Aplicación	EJ_CA_3
Pruebas Sustantivas	EJ_PS_4
IF - Informes - Entregables	
Informe y Seguimiento	IF_1

2. Marcas de Auditoría

Descripción	Marca
Cumple	✓
No cumple	✗
No aplica	N/A

3. Umbrales de Riesgo

Descripción	Ponderación
Riesgo Alto	67 % - 100 %
Riesgo Moderado	34 % - 66 %
Riesgo Bajo	1 % - 33 %

Conclusión: La metodología propuesta, las marcas de auditoría y la escala de valoración del riesgo, serán utilizadas durante todo el desarrollo del trabajo investigativo.

ANEXO 9

Papel de Trabajo. – Identificación de las Normas, Políticas, Reglamentos.

PAPEL DE TRABAJO

Tema de Auditoría:	Auditoría a la Seguridad Informática en la Dirección Distrital 02d03 Chimbo-San Miguel-Educación, durante el periodo enero 2016 - octubre 2017; utilizando el marco de referencia Cobit 5.	**Referencia:**	PA_EN_004
Entidad Auditada:	DIRECCION DISTRITAL 02D03 CHIMBO-SAN MIGUEL-EDUCACION	**Elaborado por:** Angel Palacios	**Fecha:** 26/01/2018
Periodo:	Enero 2016-octubre 2017	**Revisado por:** Ing. Christian Vaca	**Fecha:** 31/01/2018
Objetivo:	Identificar las: Normas, Políticas o Reglamentos con los que opera la Dirección Distrital.	**Aprobado por:** Ing. Christian Vaca	**Fecha:** 31/01/2018

Procedimientos:	
	Entrevista
Responsable:	Lcdo. David Galarza Luna
Cargo:	Director Distrital
Fuente:	Sistema de Gestión de Calidad ISO 9001 (SGC)
Conclusiones:	
	La Dirección Distrital 02d03 Chimbo San Miguel-Educación, opera a nivel de Gestión Administrativa en base a los procesos del Manual de Gestión Administrativa Distrital.
	También en los diferentes Departamentos, se trabaja con el Marco Legal Educativo.
	Reglamento General a la Ley Orgánica de Educación Intercultural

Normativa Sobre Temas Educativos

ANEXO 10

Papel de Trabajo. – Diseño de herramientas de recolección y validación de Datos

PAPEL DE TRABAJO

Tema de Auditoría:	Auditoría a la Seguridad Informática en la Dirección Distrital 02d03 Chimbo-San Miguel-Educación, durante el periodo enero 2016 - octubre 2017; utilizando el marco de referencia Cobit 5.	**Referencia:**	PA_EN_005
Entidad Auditada:	DIRECCION DISTRITAL 02D03 CHIMBO-SAN MIGUEL-EDUCACION	**Elaborado por:** Angel Palacios	**Fecha:** 01/02/2018
Periodo:	Enero 2016-octubre 2017	**Revisado por:** Ing. Christian Vaca	**Fecha:** 07/02/2018
Objetivo:	Formular las preguntas de las Entrevistas a fin de conocer el contexto organizacional y el entorno Tecnológico de la Unidad de Tecnologías de la Información y Comunicaciones y	**Aprobado por:** Ing. Christian Vaca	**Fecha:** 07/02/2018

Procedimientos:

Se diseño:

1 Entrevistas para la máxima Autoridad de la Dirección Distrital de Educación y Analista Distrital TICS

2 Encuestas para funcionarios y usuarios de los servcios de la Dirección Distrital de Educación

a.Director Distrital de Educación

Objetivo: : Conocer el contexto organizacional de la Dirección Distrital 02D03-Chimbo-San Miguel-Educación.

Formulación de Preguntas:

1)¿Desde qué fecha se encuentra como Director Distrital?

2)¿Describa la situación organizacional, cuando llego a formar parte del Distrito Educativo?

3)¿Cuáles considera que son los activos más importantes de la Dirección Distrital de Educación?

4)¿Podría mencionar en que debería mejorar el Distrito Educativo?

5)¿Qué sucedería si se materializara algún incidente informático, relacionandose con los activos más importantes del

6)¿Qué medidas de seguridad tiene el distrito?

7)¿Cómo es la comunicación interna y externa del Distrito Educativo?

8)¿Que piensa de la Auditoría Informática que se esta realizando en el Distrito Educativo?

b.Jefe de la Unidad de Tecnologías de la Información y Comunicaciones

Objetivo: Comprender la problemática del Distrito Educativo, a nivel de Tics y sus factores.

Formulación de Preguntas:

1)¿Cuáles han sido los principales problemas informáticos que usted ha tenido en su departamento?

2) ¿Cómo ha solucionado los problemas informáticos?

3) ¿Qué controles de seguridad informática aplica la Unidad de Tics?

4)¿Cuáles considera los activos más importantes de la Dirección Distrital de Educación?

5)¿Qué medios utiliza para proteger la información?

Encuesta a Funcionarios de la Dirección Distrital 02d03 Chimbo-San Miguel-Educación.

1.¿Seleccione el nivel con el que usted se identifica en el tema Seguridad Informática?

Elemental…….Básico……Avanzado

2.¿El control de acceso a la estación de trabajo es…?

Contraseña en la BIOS | Contraseña en la Cuenta de Usuario | Ninguno

3.¿Con que frecuencia se ha presentado indisponibilidad de equipos o servicios Informáticos?

Mensualmente | Trimestralmente | Semestralmente | Ninguna

4.¿Dispone de Inventario Actualizado?

Si ( ) | No ( )

5. ¿Considera que los equipos Informáticos deben ser remplazados por nuevos y de mejores características a fines de realizar un trabajo eficiente y confiable?

Si ( ) | No ( )

Encuesta a Usuarios de la Dirección Distrital 02d03 Chimbo-San Miguel-Educación.

1. ¿Considera que los servicios ofrecidos por la Dirección Distrital 02D03 Chimbo-San Miguel-Educación son eficientes?

Si ( ) | No ( )

2.¿La comunicación entre Distrito Educativo e Institución Educativa es?

Buena ( ) | Mala ( ) | Regular ( )

3.¿La información solicitada es a traves de:?

Correo electrónico Personal ( ) | Quipux ( )

Correo electrónico Institucional ( ) | Otro…….. ( )

Conclusiones: Tambien se diseñaron: Papeles de Trabajo, Matrices de Riesgo y Matrices de Control.

ANEXO 11

Papel de Trabajo. – Elaboración del Plan de Auditoría

PLAN DE AUDITORIA	
Antecedentes	
Como trabajo de investigación, se realizará una auditoría a la Seguridad Informática del periodo enero 2016-octubre 2017 en la Unidad de Tecnologías de la Información y Comunicaciones de la Dirección Distrital 02d03 Chimbo-San Miguel-Educación.	
Objetivos de Alto Nivel y Alcance del trabajo General	
Realizar una auditoría a la Seguridad Informática en la Unidad de Tecnologías de la Información y Comunicaciones de la Dirección Distrital 02d03 Chimbo-San Miguel-Educación.	
Específicos:	
Realizar un estudio preliminar, a fin de comprender la dinámica de la Unidad de Tecnologías de la Información y Comunicaciones de la Dirección Distrital 02d03 Chimbo-San Miguel-Educación.	
Aplicar los procedimientos de Auditoría, considerando el Marco de Referencia COBIT 5	
Proponer soluciones para la Seguridad Informática de la unidad de Tics, en base a los resultados generados.	
Alcance	
Procesos de la Unidad de Tecnologías de la Información y Comunicaciones:	
1. Contratación o Adquisición de Bienes y Servicios Tecnológicos.	
2. Creación de cuentas de usuarios y perfiles	
3. Soporte Técnico (Distrital)	
a) Respaldos y Recuperación de Datos	
b) Continuidad del Negocio	
c) Licenciamiento de Software	
4. Instalación de enlaces de internet Datos y Telefonía (Distrital).	
a) Redes de Área local	
Metodología	
Investigación Preliminar	
Visitas in situ a la unidad de Tics, a fin de comprender el contexto tecnológico	
Recolección de Información	Preparar instrumentos como formulación de encuestas y entrevistas
Toma de entrevistas a realizar para descubrir hechos	Director de la Dirección Distrital 02d03 Chimbo-San Miguel-Educación.
	Analista Distrital de la Unidad de Tecnologías de la Información y Comunicaciones

Ejecución de Pruebas							
	Ejecutar pruebas de seguridad a los procesos de la Unidad de Tics Distrital.						
Proceso de Análisis y Evaluación de Riesgos.	a Unidad de Tecnologías de la Información y Comunicaciones de la Dirección Dis						
Tratamiento de Riesgos	Proponer los controles, para el tratamiento de los riesgos, en base al marco de referencia COBIT 5.						
Tipo de Informe	Informativo						
A quien va dirigido	Director Distrital 02D03 Chimbo-San Miguel-Educación.						
	Analista Distrital de la Unidad de Tecnologías de la Información y Comunicaciones						
Entregables	Informe de Auditoría						
	Evidencia fotográfica						
	Capturas de pantallas						
	Fichas.						
	Grabaciones						
Recursos:							
	Recursos Técnicos			**Recursos Humanos**			
	Cámara fotográfica			Un auditor conocedor del ambiente tecnológico y del contexto del Distrito			
	Grabadora de Sonidos.			Un Supervisor de Auditoría Informática.			
	Computador Portátil.						
	Internet, Software de red.						
	Recursos Físicos						
	Instalaciones de la Dirección Distrital 02d03 Chimbo-San Miguel-Educación.						
	Instalaciones de la Unidad de Tecnologías de la Información y Comunicaciones						
Temas generales	Presupuesto	(Autofinanciamiento)					
Criterios de evaluación a utilizar	Cualitativa y Cuantitativa						
Requisitos y distribución de los informes	Validar el informe						
Otros aspectos generales del trabajo	Factor tiempo, la Auditoría se realizará a partir de las 14h00, según el cronograma establecido.						
Fechas Planificadas	16 de enero, al 10 de agosto del 2018						

ANEXO 12

Papel de Trabajo. – Elaboración del Programa de Auditoría

Ministerio de Educación			***PROGRAMA DE AUDITORIA***			
					Ref: PRG_A_001	
Tema de Auditoria:	Auditoría a la Seguridad Informática en la Dirección Distrital 02d03 Chimbo-San Miguel-Educación, durante el periodo enero 2016 - octubre 2017; utilizando el marco de referencia Cobit 5.					
Objetivos de la Auditoria:	1.Contar con información sobre el cumplimiento de requisitos legales relacionados con el uso de la información y la tecnología, de tal manera que se apoye a la alta Dirección en la toma de decisiones.					
	2.Optimizar los recursos tecnológicos y plantear las prioridades de atención.					
	3.Comprender el estado de los procesos que gestionan las TIC, con la finalidad de establecer el nivel adecuado					
Alcance de la Auditoría:	Procesos de la Unidad de Tecnología de Información y Comunicaciones					
1	Contratación o Adquisición de Bienes y Servicios Tecnológicos.					
2	Creación de cuentas de usuarios y perfiles.					
3	Soporte Técnico (Distrital)					
a	Respaldos y Recuperación de Datos					
b	Continuidad del Negocio					
c	Licenciamiento de Software					
4	Instalación de enlaces de internet Datos y Telefonía (Distrital)					
a	Redes de Área local					
Planificación Previa:						
Recursos:						
	Humanos:	1 Auditor , 1 Supervisor				
	Técnicos:	Cámara fotográfica, Grabadora se Sonidos, Cuaderno de Notas, Laptop.				
	Económicos:	Autofinanciamiento por el Autor				
	Fuentes de Información:	Director Distrital de Educación, Analista Distrital de la Unidad de Tics, Analistas departamentales y usuarios.				
	Revisión:	Procesos de la Unidad de Tecnologías de la Información y Comunicaciones.				
	Instalaciones:	Unidad de Tics, de la Dirección Distrital 02d03 Chimbo-San Miguel-Educación.				

Área	Procedimientos de Auditoría	Realizado Por: Fecha:	Ref. PT.
Dirección Distrital 02d03 Chimbo-San Miguel-Educación.	Identificación del Personal a Entrevistar	Angel Palacios. 17-01-2018	PA_EN_001
	Identificación de los Procesos de la Unidad de Tics	Angel Palacios. 19-01-2018	PA_EN_002
	Selección del Enfoque de trabajo (Metodología)	Angel Palacios. 23-01-2018	PA_EN_003
	Identificación de Políticas, Normas o Marco de Referencia.	Angel Palacios. 26-01-2018	PA_EN_004
	Diseño de herramientas para recolectar datos, probar y verificar controles	Angel Palacios. 01-02-2018	PA_EN_005
	Elaboración del Plan de Auditoría.	Angel Palacios. 08-02-2018	PLA_001
Unidad de Tecnologías de la Información y Comunicaciones.	Identificación de Riesgos	Angel Palacios. 23-02-2018	PA_RSK_001
	Diseño de Programas de Auditoría	Angel Palacios. 01-03-2018	PRG_A_001
Dirección Distrital 02d03 Chimbo-San Miguel-Educación.	Aplicación de Entrevista a Director Distrital de Educación.	Angel Palacios. 16-03-2018	EJ_001
Unidad de Tecnologías de la Información y Comunicaciones.	Aplicación de Entrevista a Jefe de la Unidad de Tecnologías de la Información y Comunicaciones.	Angel Palacios. 21-03-2018	EJ_002
	Evaluación del Proceso de Contratación o Adquisición de Bienes y Servicios Tecnológicos.	Angel Palacios. 28-03-2018	PA_TICS_001
	Evaluación del Proceso de Creación de Cuentas de Usuarios y Perfiles.	Angel Palacios. 19-04-2018	PA_TICS_002
	Evaluación del Proceso de Soporte Técnico (Distrital)	Angel Palacios. 14-05-2018	PA_TICS_003
	Evaluación del Proceso de Instalación de enlaces de internet Datos y Telefonía (Distrital)	Angel Palacios. 11-06-2018	PA_TICS_004
Dirección Distrital 02d03 Chimbo-San Miguel-Educación.	Revisión de los Papeles de Trabajo	Angel Palacios. 04-07-2018	N/A
	Elaboración del Informe (Borrador)	Angel Palacios. 12-07-2018	N/A
	Elaboración del Informe Final (Comunicación de Resultados)	Angel Palacios. 23-07-2018	N/A

ANEXO 13

Papel de Trabajo. – Evaluación del Proceso de Contratación o Adquisición de Bienes y Servicios Tecnológicos.

					PAPEL DE TRABAJO						
					Auditoría a la Seguridad Informática						
Entidad Auditada:	DIRECCION DISTRITAL 02D03 CHIMBO-SAN MIGUEL-EDUCACION				**Ref. P/T:**		PA_TICS_001				
Periodo:	Enero 2016-octubre 2017				**Elaborado por:** Angel Palacios					**Fecha:** 28/03/2018	
Nombre del proceso:	Contratación o Adquisición de Bienes y Servicios Tecnológicos				**Revisado por:** Ing. Christian Vaca					**Fecha:** 02/04/2018	
					Aprobado por: Ing. Christian Vaca					**Fecha:** 02/04/2018	
Objetivos											
	Comprender la actividad del Proceso de Contratación o adquisición de Bienes y Servicios Tecnológicos.										
	Verificar el cumplimiento del Proceso de Contratación y Adquisición de Bienes y Servicios Tecnológicos.										
Procedimientos:											
	Entrevista										
	Solicitud de documentos del Proceso										
Responsable: **Cargo:**	Lcdo. Carlos Aroca Benitez Jefe de la Unidad de Tics										
Estatuto:	Manual de Gestión Administrativa Distrital										
						VERIFICACIONES					**Ref. P/T**
A	Ha realizado contrataciones durante el periodo de enero 2016-octubre 2017.				A	B	C	D	E		PA_EN_1.1.1
B	Existe una bitácora de las peticiones del proceso				×	×	×	×	×		
C	Se ha realizado informes de análisis de mercado										
D	Se ha elaborado las especificaciones técnicas de										
E	Existen informes que corroboren que los bienes adquiridos cumplan con las especificaciones técnicas solicitadas.										
Hallazgos											
Las adquisiciones durante el periodo de auditoría, se han realizado directamente por la Unidad Administrativa, en los meses de agosto de cada año, en algunas ocasiones el administrativo ha preguntado a TICS que necesita; en otras ocasiones han comprado directamente suministros tecnológicos, sin previa consulta a TICS de requerimientos.											
No se han realizado adquisiciones o contrataciones de bienes o servicios durante el periodo de auditoría por el departamento de Tics, conforme a los lineamientos del Manual de Gestión Administrativa Distrital; debido a que las adquisiones han sido realizadas directamente por la Unidad Administrativa en los meses de agosto de cada año; de tal manera que en algunas ocasiones el Departamento Administrativo ha preguntado a TICS que necesita; mientras en otras ocasiones han comprado directamente suministros tecnológicos, sin previa consulta a TICS; por lo tanto se incumple el Manual de Gestión de Administrativa Distrital, generando un impacto negativo en el Proceso de Tics en relación a las Auditorías que realiza el MINEDUC.											
El entrevistado manifiesta que se ha gestionado adquisiciones, pero debido a la falta de presupuesto las adquisiciones. No s ehan realizado.											
Tambien manifiesta, que la Directora Distrital Saliente si daba seguimiento a los Procesos del Manual de Gestión de Calidad: mientras el nuevo Director Distrital no.											
Observaciones	No ha dado cumpliemiento con el Manual de Gestión Administrativa Distrital.										
Riesgos	Baja puntuación en las Auditorías , que realiza el Ministerio de Educación.										
Conclusiones:											
No se han realizado compras dando cumplimiento al proceso de contratación o adquisición de bienes o servicios tecnológicos, durante el periodo de auditoría.											

ANEXO 14

Papel de Trabajo. – Creación de cuentas de usuarios y perfiles para sistemas de información.

PAPEL DE TRABAJO											
Auditoría a la Seguridad Informática											
Entidad Auditada:	DIRECCION DISTRITAL 02D03 CHIMBO-SAN MIGUEL-EDUCACION				**Ref. P/T:**	PA_TICS_002					
Periodo:	Enero 2016-octubre 2017				**Elaborado por:** Angel Palacios				**Fecha:** 19/04/2018		
Nombre del proceso:	Creación de cuentas de Usuarios y Perfiles				**Revisado por:** Ing. Christian Vaca				**Fecha:** 20/04/2018		
					Aprobado por: Ing. Christian Vaca				**Fecha:** 20/04/2018		
Objetivo											
Comprender las actividades del Proceso de Creación de cuentas de Usuarios y Perfiles											
Procedimiento de Auditoría	Revisión de Documentos del Proceso.										
Fuente de Información:	Lcdo. Carlos Aroca Benitez - Jefe de la Unidad de Tecnologías de la Información y Comunicaciones.										
Estatuto:	Manual de Gestión Administrativa Distrital										
Muestra:	Se reviso la documentación fisica entregada y se encontro 34 formularios de creación de cuentas de usuario para Quipux y 63 formularios de Creación/Modificación de acceso a plataformas, las cuales se procedió a analizar:										**Ref. P/T**
						VERIFICACIONES					PA_EN_1.1.1
A	Existe documentos del proceso, del periodo de Auditoría.				A	B	C	D	E		
B	Los documentos se encuentran organizados				✓	×	×	✓	✓		
C	Los documentos se encuentran etiquetados										
D	Al menos un 70 % de los documentos cuentan con firmas de responsabilidad.										
E	Al menos un 70% de los documentos cuentan con sellos.										
Hallazgos											
1.Creación de cuentas de usuarios de QUIPUX. Se encontró 11 formularios sin sello del Despacho de Direción Distrital, 17 formularios sin sello de la Unidad de Talento Humano, 2 sin firma de responsabilidad de la Directora Distrital, 1 sin firma de responsabilidad de la Unidad de Talento Humano, 1 sin firma del Usuario y 1 formulario sin fecha, 1 formulario sin correo electronico personal de la Directora Distrital. 2. De la creación/ modificación de acceso a plataformas se encontro: 34 peticiones de creación de correo institucional, 27 de habilitación del correo institucional de MOGAC y 2 de habilitación del correo institucional de gestión docente, también se ha utilizado una matriz llenada a mano para el proceso de creación de cuentas de usuario.											
Observaciones	Solo reposan archivos en formato físico.										
Riesgos	Pérdida , Modificación de la Información										
Conclusiones:											
Se sigue el flujo del proceso, pero se incumple las normas de seguridad como sello, firmas.											
	El proceso no especifica, por que medio debe hacer llegar el formulario a la Unidad de Tics										

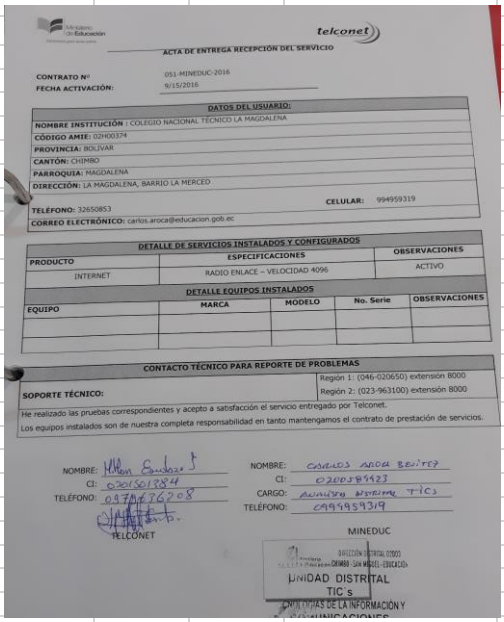
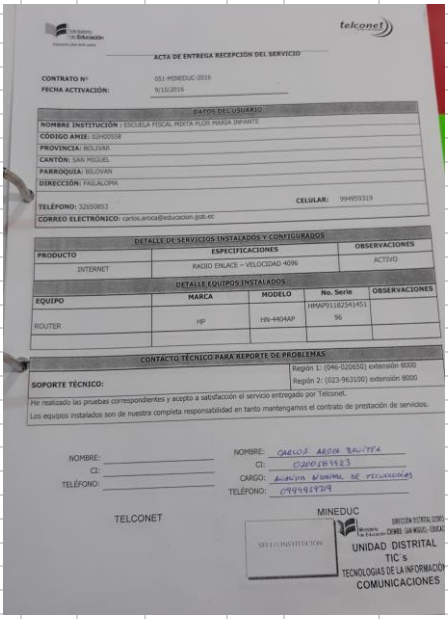
ANEXO 15

Papel de Trabajo. – Evaluación del Proceso de Soporte Técnico Distrital

PAPEL DE TRABAJO									
Auditoría a la Seguridad Informática									
Entidad Auditada:	DIRECCION DISTRITAL 02D03 CHIMBO-SAN MIGUEL-EDUCACION			**Ref. P/T:**	PA_TICS_003				
Periodo:	Enero 2016-octubre 2017			**Elaborado por:** Angel Palacios				**Fecha:** 14/05/2018	
Nombre del proceso:	Soporte Técnico.			**Revisado por:** Ing. Christian Vaca				**Fecha:** 15/05/2018	
				Aprobado por: Ing. Christian Vaca				**Fecha:** 15/05/2018	
Objetivo									
Comprender las actividades del Proceso de Soporte Técnico.									
Procedimiento de Auditoría	Revisión de Documentos del Proceso.								
Fuente de Información:	Lcdo. Carlos Aroca Benitez - Jefe de la Unidad de Tecnologías de la Información y Comunicaciones.								
Estatuto:	Manual de Gestión Administrativa Distrital - Cobit 5								
Muestra:	Se encontraron 59 registros físicos de Soporte Técnico del periodo de auditoria enero 2016-octubre 2017, de los cuales: 2 corresponden a Mantenimiento preventivo, 2 registros de mantenimiento preventivo durante el periodo de la auditoría, 6 registros de mantenimiento correctivo, 19 registros entre cambio de toner y carga de tinta de impresoras, 4 de configuraciones de cuentas de correo, 4 carpetas para almacenar información, 3 respaldos de la cuenta de correo institucional y se complementa con cambios de teclado e instalación de punto eléctrico, 1 instalación de 1 switch, 1 implementación de módulo de memoria RAM.								**Ref. P/T**
					VERIFICACIONES				PA_EN_1.1.1
A	Existe documentos del proceso del periodo de Auditoría.			A	B	C	D	E	
B	Los documentos se encuentran debidamentprotegidos			✓	×	✓	✓	✓	
C	Los documentos se encuentran ordenados y etiquetados								
D	Los documentos cuentan con sellos del departamento								
E	Los documentos cuentan con firmas de responsabilidad								
Hallazgos									
1. Los registros de Soporte Técnico, solo se los ha realizado solo hasta enero del 2017, a partir de esa fecha manifiesta el jefe de la unidad de Tics, que debido al cambio de Director Distrital, no se ha dado seguimiento al cumplimiento de los procesos.									
Observaciones	Solo reposan archivos en formato digital en una carpeta de red interna compartida.								
Riesgos	Pérdida , Modificación, Acceso no autorizado a la Información.								
Conclusiones:									
Se sigue el flujo del proceso, pero se incumple las normas de seguridad como sello, firmas.									

ANEXO 16

Papel de Trabajo. – Instalación de enlaces de Internet, datos y telefonía

PAPEL DE TRABAJO				
Auditoría a la Seguridad Informática				
Entidad Auditada:	DIRECCION DISTRITAL 02D03 CHIMBO-SAN MIGUEL-EDUCACION	**Ref. P/T:**	PA_TICS_004	
Periodo:	Enero 2016-octubre 2017	**Elaborado por:** Angel Palacios		**Fecha:** 16/05/2018
Nombre del proceso:	Instalación de Enlaces de Internet Datos y Telefonía (Distrital)	**Revisado por:** Ing. Christian Vaca		**Fecha:** 17/05/2018
		Aprobado por: Ing. Christian Vaca		**Fecha:** 17/05/2018
Objetivo				
	Analizar los documentos del proceso de Instalación de Enlaces de Internet Datos y Telefonía (Distrital)			
Procedimiento de Auditoría	Revisión de documentación entregada por el Departamento de Tecnologías de la Información y Comunicaciones.			
Fuente:	Lcdo. Carlos Aroca Benitez-Jefe de la Unidad de Tics			
Estatuto:	Manual de Gestión Administrativa Distrital			
Desarrollo:	El Lcdo. Carlos Aroca proveeo varios archivos digitales del Proceso de Instalación de Enlaces de Internet, Datos y Telefonía, de los cuales se procedió a revisar, contabilizary contrastar la existencia de firmas y sellos de los documentos.			
Conclusiones:	Solo se cuenta con 15 registros del Proceso, durante el periodo de Auditoría.			
Anexo	 			
			Sin Firma	

ANEXO 17

Comunicación de Resultados de la Auditoría a la Seguridad Informática.

EDUCACIÓN

San Miguel de Bolívar 18 de agosto del 2018

Señores
UNIVERSIDAD TECNOLÓGICA ISRAEL
De mi consideración

Por medio del presente reciban un cordial saludo; a la vez pongo en conocimiento que el Sr. **ANGEL RAMIRO PALACIOS BAYAS**, con C.C. **0201780038**, realizo la Auditoría a la Seguridad Informática en la Dirección Distrital 02D03 Chimbo-San Miguel-Educación del periodo enero 2016 a octubre 2017 y entregó el respectivo informe de Auditoría.

Particular que comunico, para los fines pertinentes.

Atentamente.

Carlos Aroca Benítez
Analista Distrital TIC´s

DIRECCIÓN DISTRITAL 02D03
CHIMBO - SAN MIGUEL - EDUCACIÓN

UNIDAD DISTRITAL
TIC´s
TECNOLOGÍAS DE LA INFORMACIÓN Y
COMUNICACIONES

Dirección: Av. El Maestro y Loja. Barrio 13 de Abril **Teléfono:** 593-03-2650853 www.educacion.gob.ec

ANEXO 18

Aplicación de Encuestas a Servidores Públicos y Usuarios del Distrito Educativo 02d03.

ANEXO 19

Formato del Plan de Auditoría

PLAN DE AUDITORIA

Evaluación de riesgo

Áreas a auditar

……

Referencia: ……

Tipo de trabajo planificado

Objetivos de alto nivel y alcance del trabajo

……

Entrevistas a realizar para descubrir hechos

……

Información relevante a obtener

……

Procedimientos para verificar o validar la información obtenida y su uso como evidencia de auditoría

……

Temas generales

……

Disponibilidad y asignación de recursos

……

Fechas Planificadas

……

Tipo de Informe

……

A quien va dirigido

……

Entregables

……

Temas específicos

Identificación de las herramientas necesarias para obtener las evidencias, pruebas realizadas y preparación/resumen de la información, para el informe

……

Criterios de evaluación a utilizar

……

Requisitos y distribución de los informes

……

Otros aspectos generales del trabajo……

ANEXO 20

Formato del Papel de Trabajo

PAPEL DE TRABAJO								
Nombre de la Auditoría:	.....							**Ref PT: .....**
Nombre del Proceso o del Area Auditada:	.....					**Elaborado por:**	.....	**Fecha: .....**
Periodo:	.....					**Revisado por:**	.....	**Fecha: .....**
						Aprobado por:	.....	**Fecha: .....**
Objetivo del Papel de Trabajo								
.....								
Procedimientos de Auditoria								
A.....								
B.....								
C.....								
D.....								
E.....								
F.....								
Verificaciones								
A	B	C	D	E	F	Observaciones		
						.....		
Marcas De Auditoria			Hallazgos		Riesgos		Información	
✓	Cumple		.....		.....		.....	
✗	No cumple		.....		.....		.....	
N/A	No aplica		.....		.....		.....	
Conclusiones:	.....							