UNIVERSIDAD TÉCNICA DE BABAHOYO

FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA.

PROCESO DE TITULACIÓN

DICIEMBRE 2022 – ABRIL 2023

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRÁCTICA

PREVIO A LA OBTENCIÓN DEL TÍTULO DE:

INGENIERO EN SISTEMAS

TEMA:

AUDITORIA DE LOS SISTEMAS INFORMATICOS APLICANDO EL SISTEMA COBIT 5 EN EL GOBIERNO AUTONOMO DESCENTRALIZADO MUNICIPAL DEL CANTON ALFREDO BAQUERIZO MORENO

EGRESADO

ALVARO EDUARDO PALMA MANCILA

TUTOR:

JORDÁN CORDONES FREDY MAXIMILIANO

AÑO 2023

INTRODUCCIÓN

El Gobierno Autónomo Descentralizado Municipal del cantón Alfredo Baquerizo Moreno se encarga de gestionar diferentes proyectos para brindar un bien común local, la atención prioritaria de las necesidades de la ciudad y de las parroquias rurales. El municipio cuenta con un departamento de TICs con algunas falencias las cuales serán expuestas en este documento.

Actualmente el departamento de TI no se encuentra organizado adecuadamente, lo cual provoca retraso en los proyectos y que los procesos que deberían estar automatizados sigan llevándose de forma manual, los procesos de encontrar información son difíciles y lentos. Esto provoca pérdida de productividad del departamento y de la institución. Los empleados no tienen acceso a las herramientas y recursos que necesitan para realizar sus tareas en forma eficiente, provocando un impacto negativo en el rendimiento general de la institución. Así mismo al no usar la tecnología en los procesos esto provoca mayor riesgo de errores y fallos, perdiendo información importante para la empresa, además esto provoca mayores gastos al tener que implementar procesos extras para recuperarse de los mismos.

Muchas empresas están sujetas a regulaciones y estándares de seguridad específicos, como la Ley de Protección de Datos o el Estándar de Seguridad de la Información ISO 27001. Una auditoría informática puede ayudar a las empresas a determinar si están cumpliendo con estos estándares y regulaciones, y si no lo están, les proporcionará recomendaciones para mejorar su cumplimiento.

En el municipio no se tiene una visión completa de los procesos de TI, no se han identificado los riesgos a los que está expuesta la información por lo tanto los gerentes o lideres no están tomando decisiones basadas en información real, que sean estratégicas y eficaces al mismo tiempo.

El objetivo principal del presente estudio es realizar un análisis usando el modelo COBIT en el municipio, el cual ayudaría a alinear las estrategias de TI con los objetivos de la institución, definiendo indicadores de rendimientos clave para poder medir el éxito o fracaso de los mismos. Aportando claridad en el valor que aporta del departamento de TI en la organización.

Con el fin de mejorar los problemas encontrados en el estado actual de los principales procesos de TI se propuso planes de acción a desarrollar según el estado actual de los procesos y de esta manera poder brindar un servicio de excelencia al usuario.

El presente caso de estudio se encuentra enlazado a la línea de investigación "Redes y tecnologías inteligentes de software y hardware", bajo el cual se realizó el análisis al departamento de TI del Gobierno Autónomo Descentralizado Municipal del cantón Alfredo Baquerizo Moreno.

Para el desarrollo del caso de estudio se utilizó la metodología descriptiva para poder detallar cada uno de los procesos que se analizaron, midiendo los niveles de cumplimiento para poder identificar las falencias de los procesos que se están llevando dentro de la institución.

Se realizo la observación para conocer la verdadera situación del departamento de TI y poder dar una evaluación transparente, el cual tiene una serie de problemas que al parecer llevan algunos años en la misma situación y los cuales detallo a continuación:

- Inexistencia de controles de seguridad de la información
- Tiempos de espera elevados en la atención de incidentes informáticos
- Escasez de talento humano, ya que solo existe el jefe de TI y la secretaria
- No se documentan las fallas
- Infraestructura tecnológica desactualizada
- Inventario de activos de TI desactualizados

DESARROLLO

Definición de COBIT

COBIT 5.0 es un marco de negocio para el gobierno y la gestión de las TI de la empresa, fue creado para ayudar a las organizaciones a obtener el valor óptimo de TI. Se puede aplicar tanto las organizaciones públicas como privadas. Su primera versión apareció en 1977 y en la actualidad su última versión es la 5.0 (ISACA, 2012).

Los principios de COBIT son en total 5:

1. Satisfacer las necesidades de las partes interesadas. Cobit provee los procesos necesarios para crear valor de negocio a través de un excelente servicio de TI.
2. Cubrir la empresa de extremo a extremo. Cobit no solo se enfoca en el departamento de TI también revisa la gestión de otros niveles de la empresa los cuales sean relevantes para el departamento de TI
3. Aplicar un marco de referencia único integrado. Existen algunos marcos y estándares orientados a garantizar las buenas prácticas de TI, sin embargo, el modelo COBIT sea alinea con los más relevantes convirtiéndose en un marco holístico.
4. Hacer posible un enfoque holístico. El modelo COBIT encierra todas las categorías relevantes dentro de una institución como son: principios y políticas de trabajo, procesos, estructuras organizativas, servicios e infraestructuras, personas y habilidades.
5. Separa el gobierno de la gestión. En muchas organizaciones el gobierno es responsabilidad de un comité general y las responsabilidades son distintas, mientras que la gestión es responsabilidad de otra dirección, por lo tanto, es importante para COBIT hacer la diferencia entre los departamentos de gobierno y gestión. (ISACA, 2012).

Se establecen 3 principios para un marco de gobierno:

Principio 1. Basado en un modelo conceptual, el cual debe identificar los componentes principales y sus relaciones para de esta manera facilitar su consistencia y automatización.

Principio 2. Abierto y flexible, debe ser posible incluir nuevos contenidos y abordar nuevas situaciones.

Principio 3. Alineado a los principales estándares. Es necesario que el marco de gobierno se encuentre alineado a los estándares, marcos y normativas. (ISACA, 2012).

Los procesos del Gobierno Corporativo de TI son: Evaluar, Dirigir y Monitorear (EDM), los cuales tienen cinco procesos internos que son EDM01 Asegurar el establecimiento y mantenimiento del marco de gobierno, EDM02 Asegurar la entrega de beneficios, EDM03 Asegurar la optimización del riesgo, EDM04 Asegurar la optimización de los recursos, EDM05 Asegurar la transparencia hacia las partes interesadas.

Y los procesos de gestión son:

- Planificar (APO), APO01 Gestionar el marco de gestión de TI, APO02 Gestionar la estrategia, APO03 Gestionar la arquitectura empresarial, APO04 Gestionar la innovación, APO05 Gestionar portafolio, APO06 Gestionar el presupuesto y los costes, APO07 Gestionar los recursos humanos, APO08 Gestionar las relaciones, APO09 Gestionar los Acuerdos de Servicio, APO10 Gestionar los proveedores, APO11 Gestionar la calidad, APO12 Gestionar el Riesgo, APO13 Gestionar la seguridad.

- Construir (BAI), BAI01 Gestionar los programas y proyectos, BAI02 Gestionar la definición de requisitos, BAI03 Gestionar la identificación y la construcción de soluciones, BAI04 Gestionar la disponibilidad y la capacidad, BAI05 Gestionar la introducción de cambios organizativos, BAI06 Gestionar los cambios, BAI07 Gestionar la aceptación del cambio y de la transición, BAI08 Gestionar el conocimiento, BAI09 Gestionar los activos, BAI010 Gestionar la configuración.

- Ejecutar (DSS), DSS01 Gestionar las operaciones, DSS02 Gestionar las peticiones y los incidentes del servicio, DSS03 Gestionar los problemas, DSS04 Gestionar la continuidad, DSS05 Gestionar los Servicios de Seguridad, DSS06 Gestionar los controles de los procesos de negocios.

- Supervisar (MEA). MEA01 Supervisar, evaluar y valorar rendimiento y conformidad, MEA02 Supervisar, evaluar y valorar el sistema de control interno, MEA03 Supervisar, evaluar y valorar la conformidad con los requerimientos externos.

LEVANTAMIENTO DE INFORMACION

Análisis preliminar del departamento

La presente información se obtuvo del departamento de TI del Gobierno Autónomo Descentralizado Municipal del cantón Alfredo Baquerizo Moreno durante el periodo de enero a marzo del 2023.

A continuación, se detalla el inventario de hardware y software, además de la arquitectura de redes que tiene la empresa.

Tabla 1

Inventario de Hardware

Cantidad de equipos de hardware	Sistema operativo	Licencia			Tipo	Modelo	Procesador	RAM	Disco
		Windows	Nod	Office					
1	Windows 10	X	X	X	Escritorio	Clon	Core i3	4Gb	1 Tera
4	Windows 10	X	X	X	Escritorio	Clon	Core i3	8Gb	1 Tera
5	Windows 10	X	X	X	Escritorio	Clon	Core i5	8Gb	1 Tera
17	Windows 10	X	X	X	Escritorio	Clon	Core i3	4Gb	500 Gb
3	Windows 10	X	X	X	Portátiles	Lenovo	Core i5	8Gb	1 Tera
30									

Como podemos observar en la Tabla Nro. 1 el Gobierno Autónomo Descentralizado Municipal(GADM) del Cantón Alfredo Baquerizo Moreno para enero del 2023 posee en total 30 equipos de hardware entre las cuales 27 son de tipo desktop clones y 3 son portátiles. La mayoría de estos equipos tienen procesador Core i3 y 4Gb de RAM. Todos cuentan con licencias del antivirus NOD como software de seguridad. Así mismo todos los equipos tienen Windows y Office con licencia, lo cual aporta en la estabilidad y seguridad de la información.

A continuación, se muestra la configuración del Servidor :

Figura 1

Información de equipo Servidor

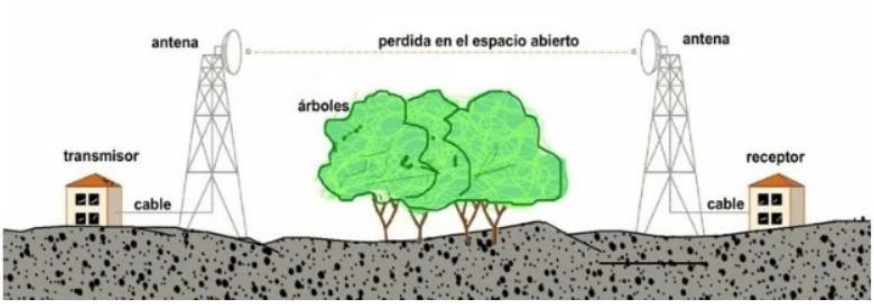
Fuente. Foto del servidor

ARQUITECTURA DE REDES

Después de la reunión sostenida con el encargado de sistemas este menciona que cuando asumió el cargo todos los equipos ya estaban funcionando y que la institución usa radio enlace wifi punto a punto.

Figura 2

Enlace punto a punto con antenas



Existen switches y routers CISCO en el Gobierno Autónomo Descentralizado Municipal del cantón Alfredo Baquerizo Moreno estos no están siendo realmente usados, nadie les da mantenimiento ni se implementan mejoras a los mismos.

Figura 3

Infraestructura de redes

Organigrama funcional del departamento de TI

Figura 4

Estructura funcional dentro de la institución del departamento de TI

METODOLOGIA

Se diseño un modelo de evaluación usando una matriz general de COBIT considerando los dominios, procesos, actividades de los procesos y su nivel de cumplimiento, además de un cuestionario de análisis de riesgos.

Se procedió a realizar un análisis de los riesgos a través de un cuestionario para el Jefe de TI, el cual se detalla a continuación:

Tabla 2

Criterio 1 Análisis de riesgos

I. Cumplimiento de procedimientos, normas y controles dictados. Vigilancia sobre el control de cambios y versiones de software			
Nº	Preguntas	Respuestas	
		Si	No
1	Existen procedimientos de control del software contratado bajo licencia?	X	
2	Existen procedimientos para la instalación de software en general y para el establecimiento de riesgos de virus y spam?	X	
3	Existen normativas para el desarrollo y adquisición de software en general?	X	
4	Existen manuales para el mantenimiento de hardware?		X
5	Existen manuales para el mantenimiento de software?	X	
	Total	4	1
	Porcentual	80%	20%

El no cumplimiento de procedimientos, normas y controles dictados en software puede tener consecuencias graves y costosas para las empresas y los usuarios finales. Esto puede incluir la pérdida de datos confidenciales, la violación de leyes y regulaciones, el daño a la reputación y la pérdida de clientes. Además, puede haber consecuencias legales y financieras, como multas y demandas. Por lo tanto, es crucial que las empresas tomen medidas proactivas para garantizar que sus sistemas y procesos cumplan con las normas y estándares relevantes, y que se realicen pruebas y auditorías periódicas para garantizar el cumplimiento continuo. Esto es especialmente importante en entornos de alta seguridad, como los sistemas financieros y de salud. En resumen, el cumplimiento de procedimientos, normas y controles es esencial para garantizar la seguridad, la confiabilidad y la integridad del software y proteger a las empresas y a los usuarios finales de consecuencias costosas y dañinas.

Tabla 3

Criterio 2 Análisis de riesgos

II. Control sobre la producción diaria			
Nº	Preguntas	Respuestas	
		Si	No
1	Existen políticas de la organización con respecto al uso del espacio de los discos duros	X	
2	Existe el plan de contingencia de TI		X
3	Existe mantenimiento preventivo en los equipos de TI	X	
4	Existen contratos de mantenimiento con proveedores externos	X	
5	Se han definido políticas de seguridad para los servidores	X	
	Total	4	2
	Porcentual	80%	20%

La implementación de un control efectivo sobre la producción diaria del departamento de TI es esencial para garantizar la continuidad del negocio y la satisfacción del cliente. La supervisión regular y la evaluación de la producción diaria pueden ayudar a detectar problemas temprano y evitar interrupciones costosas en el servicio. Además, establecer procedimientos claros y definir responsabilidades para el personal de TI puede garantizar la consistencia y la eficiencia en la producción diaria. También es importante documentar los procesos y los resultados para facilitar el seguimiento y la evaluación futura. En resumen, un control efectivo sobre la producción diaria del departamento de TI puede ayudar a mejorar la calidad del servicio, reducir los costos y aumentar la satisfacción del cliente.

Tabla 4

Criterio 3 Análisis de riesgos

III. Controles sobre la calidad y eficiencia del desarrollo y mantenimiento de software			
Nº	Preguntas	Respuestas	
		Si	No
1	Existen lineamientos para evitar las caidas del Sistema informatico?		X
2	Existen mantenimientos preventivos para el sistema informático?	X	
3	Se han realizado controles para comprobar el buen funcionamiento del sistema informático		X
4	Existen garantías por parte de los proveedores externos de software		X
5	Existen contratos de mantenimiento para los software de empresa externas		X
	Total	1	4
	Porcentual	20%	80%

No aplicar calidad y eficiencia en el desarrollo y mantenimiento de software puede resultar en productos de baja calidad, con errores y retrasos en la entrega, lo que a su vez puede generar costos adicionales y pérdida de clientes. Por lo tanto, es importante que las empresas apliquen prácticas de calidad y eficiencia en todo el ciclo de vida del software. Esto puede incluir la implementación de pruebas rigurosas, el uso de metodologías de desarrollo ágil y la documentación adecuada de los procesos de desarrollo y mantenimiento. Además, es importante involucrar a los usuarios finales en el proceso de desarrollo para garantizar que el producto final cumpla con sus necesidades y expectativas. La aplicación de la calidad y la

eficiencia también puede ayudar a las empresas a mejorar la productividad, reducir costos y aumentar la satisfacción del cliente. En resumen, la aplicación de la calidad y la eficiencia en el desarrollo y mantenimiento de software es fundamental para garantizar la entrega de productos de alta calidad que satisfagan las necesidades de los clientes de manera oportuna y eficiente.

Tabla 5

Criterio 4 Análisis de riesgos

IV. Controles en las redes de comunicaciones			
Nº	Preguntas	Respuestas	
		Si	No
1	Existen planes de implementación de las redes?		X
2	Existe personal asignado al control del tráfico de la red?	X	
3	Existen controles dentro de la red y el establecimiento de perfiles de usuario?		X
4	Las redes usan procedimientos de cifrado de información para salvaguardar la integridad de los datos		X
5	Existen controles para monitorear la eficiencia de la red?		X
	Total	1	4
	Porcentual	20%	80%

Las deficientes redes de comunicaciones pueden tener consecuencias graves para las empresas, incluyendo una reducción en la productividad, aumento de los costos operativos y pérdida de clientes. Las empresas dependen cada vez más de las redes de comunicaciones para operar de manera eficiente, y las interrupciones en el servicio pueden tener un impacto significativo en

la capacidad de la empresa para llevar a cabo sus operaciones diarias. Por lo tanto, es importante que las empresas implementen redes de comunicaciones sólidas y confiables, con redundancia y mecanismos de respaldo para minimizar el riesgo de interrupciones. Además, las empresas deben realizar pruebas periódicas y monitorear el rendimiento de sus redes para identificar y solucionar problemas temprano. La implementación de medidas de seguridad adecuadas, como el cifrado de datos y la autenticación de usuarios, también puede ayudar a proteger la integridad de la red y garantizar la privacidad de los datos de los clientes. Las empresas deben considerar las redes de comunicaciones como una inversión importante en su éxito a largo plazo.

Tabla 6

Criterio 5 Análisis de riesgos

V. Controles sobre el software base			
Nº	Preguntas	Respuestas	
		Si	No
1	Existen licencias para todos los equipos de hardware	X	
2	Existen controles sobre la caducidad de las licencias de software		X
	Total	1	1
	Porcentual	50%	50%

La falta de controles sobre el software puede tener varias implicaciones negativas para los usuarios, los desarrolladores y las empresas que utilizan el software. Algunas de las conclusiones que pueden ser extraídas son las siguientes:

1. Mayor riesgo de errores y fallos: La falta de controles puede resultar en software que no ha sido probado adecuadamente y que puede contener errores o fallos que pueden ser perjudiciales para los usuarios.
2. Menor seguridad: La falta de controles puede permitir que se introduzcan vulnerabilidades de seguridad en el software, lo que puede poner en riesgo la información confidencial y la privacidad de los usuarios.
3. Menor calidad: La falta de controles puede dar lugar a software de menor calidad que no cumple con los requisitos de los usuarios y que no satisface sus necesidades.
4. Menor confiabilidad: La falta de controles puede hacer que los usuarios pierdan confianza en el software, lo que puede llevar a una disminución en su uso y una pérdida de ingresos para las empresas que lo desarrollan y lo utilizan.

En conclusión, la falta de controles sobre el software puede tener un impacto negativo en la calidad, la seguridad y la confiabilidad del software, lo que puede perjudicar tanto a los usuarios

Tabla 7

Criterio 6 Análisis de riesgos

VI. Controles sobre los sistemas micro informáticos			
Nº	Preguntas	Respuestas	
		Si	No
1	Existen prevencion de robos de dispositivos informaticos	X	
2	Existen controles para desplazamientos de portatiles		X
	Total	1	1
	Porcentual	50%	50%

La falta de prevención de robos informáticos puede tener graves consecuencias para las empresas y los individuos. Sin medidas de seguridad adecuadas, los hackers pueden acceder a información confidencial, robar datos financieros y personales, interrumpir los sistemas de la empresa y causar daños irreparables. Es importante tomar medidas de seguridad proactivas, como implementar firewalls, utilizar software de seguridad actualizado y capacitar a los empleados en prácticas seguras de navegación web y correo electrónico, para minimizar los riesgos de los robos informáticos. La prevención es la mejor defensa contra los robos informáticos y puede ayudar a proteger la información valiosa y sensible de las empresas y de las personas.

Tabla 8

Criterio 7 Análisis de riesgos

VII. Seguridad Informática			
Nº	Preguntas	Respuestas	
		Si	No
1	Existen lineamientos de seguridad de la información?		X
2	Existen controles en el acceso a los servidores?		X
3	Tiene cámaras de seguridad donde se encuentran los servidores?		X
	Total	0	3
	Porcentual	0%	100%

No prever riesgos en TI puede llevar a consecuencias graves para una empresa. Los riesgos no identificados pueden resultar en interrupciones costosas, pérdida de datos, daño a la reputación y pérdida de clientes. Por lo tanto, es importante que las empresas lleven a cabo evaluaciones regulares de riesgos para identificar y mitigar posibles amenazas a la seguridad de sus sistemas

de TI. La implementación de medidas de seguridad adecuadas, como el cifrado de datos, la autenticación de usuarios y el monitoreo constante, también puede ayudar a reducir los riesgos. Además, es crucial que los empleados sean conscientes de los riesgos y reciban capacitación regular sobre las mejores prácticas de seguridad de TI. En resumen, prever los riesgos en TI es esencial para proteger los sistemas de una empresa y mantener su reputación y confianza en el mercado.

Tabla 9

Criterio 8 Análisis de riesgos

VIII. Usuarios, perfiles de uso de archivos, bases de datos			
Nº	Preguntas	Respuestas	
		Si	No
1	Existen funciones claramente definidas en el departamento de TI	X	
2	Existen controles físicos para garantizar el acceso no autorizado a las instalaciones del Departamento de TI		X
3	Existe el control de acceso a las computadoras mediante la asignación de usuarios y claves?		X
4	Existen normas que regulen el uso de los recursos informáticos?		X
5	Existen responsabilidades definidas en la dotación de activos de datos?		X
	Total	1	4
	Porcentual	20%	80%

El uso inadecuado de perfiles de usuario puede tener varias consecuencias negativas. Si los perfiles no se configuran correctamente, pueden permitir a usuarios no autorizados acceder a

información confidencial o realizar acciones que no deberían ser capaces de realizar. Además, si los perfiles no se actualizan adecuadamente, los usuarios pueden acceder a información obsoleta o irrelevante, lo que puede llevar a decisiones equivocadas y errores costosos. Por otro lado, la falta de control sobre los perfiles de usuario también puede dificultar la colaboración y el intercambio de información entre los miembros del equipo. En resumen, es importante utilizar los perfiles de usuario de manera adecuada y responsable para garantizar la seguridad, la eficiencia y la efectividad en el uso de los recursos informáticos.

Tabla 10

Criterio 9 Análisis de riesgos

IX. Normas de seguridad			
Nº	Preguntas	Respuestas	
		Si	No
1	Existen normas de seguridad para garantizar la confidencialidad e integridad de la información?		X
2	Existen normas que prohíban la utilización de los puertos de I/O en los equipos de hardware?		X
3	Existen normas que regulen el acceso a los recursos informáticos?		X
	Total	0	3
	Porcentual	0%	100%

La no aplicación de normas de seguridad en TI puede tener graves consecuencias para las empresas y organizaciones. Los riesgos de seguridad, como la pérdida de datos, el acceso no autorizado, el robo de información y los ataques cibernéticos, pueden causar daños financieros y reputacionales significativos. La falta de políticas y procedimientos de seguridad también

puede aumentar la probabilidad de errores humanos, lo que puede llevar a la pérdida de datos y a la interrupción de los sistemas críticos de la organización. Es importante que las empresas y organizaciones establezcan y apliquen medidas de seguridad adecuadas para proteger sus activos de información y garantizar la privacidad y seguridad de sus clientes. La aplicación de normas de seguridad en TI puede minimizar los riesgos y aumentar la confianza en la organización y sus sistemas informáticos.

Tabla 11

Criterio 10 Análisis de riesgos

X. Control de información clasificada			
Nº	Preguntas	Respuestas	
		Si	No
1	Existe una politica de clasificación de la información para saber dentro de la institucion que personas estan autorizadas y a que información	X	
2	Existen control de acceso físico a los datos y aplicaciones como almacenamiento de información?		X
	Total	1	1
	Porcentual	50%	50%

El poco control de la información clasificada puede tener consecuencias graves para la seguridad nacional, la privacidad de las personas y la competitividad de las empresas. La información clasificada puede incluir datos gubernamentales, militares, financieros o de propiedad intelectual que, si caen en manos equivocadas, pueden ser utilizados para fines

malintencionados. La falta de control sobre la información clasificada puede dar lugar a su divulgación no autorizada, lo que puede afectar a la seguridad nacional y la privacidad de las personas. Además, la falta de control sobre la información clasificada también puede tener un impacto negativo en la competitividad de las empresas, ya que la divulgación de información confidencial puede permitir a los competidores acceder a secretos comerciales valiosos. Por lo tanto, es importante que se establezcan y se apliquen medidas de seguridad adecuadas para proteger la información clasificada y garantizar que solo las personas autorizadas tengan acceso a ella.

Tabla 12

Criterio 11 Análisis de riesgos

XI. Control dual de la seguridad informática			
Nº	Preguntas	Respuestas	
		Si	No
1	Existe control dual en el acceso de los servidores?	X	
2	Existen control dual para la modificación de información debido a errores cometidos por los usuarios		X
3	Existe control dual para la asignación de perfiles de usuario		X
	Total	1	2
	Porcentual	33.33%	66.66%

El poco control dual en seguridad de TI puede poner en riesgo la seguridad y la integridad de los sistemas informáticos y los datos sensibles. El control dual es un método de seguridad que requiere que dos personas distintas autoricen una acción crítica antes de que se lleve a cabo, lo

que puede evitar errores y reducir el riesgo de fraude. Si el control dual no se implementa adecuadamente, los usuarios malintencionados pueden aprovechar las lagunas en el sistema de seguridad para realizar actividades no autorizadas, como el acceso a datos confidenciales, el robo de información o la interrupción del sistema. Además, la falta de control dual puede dificultar la detección de errores y la resolución de problemas, lo que puede afectar la eficiencia y la eficacia de la organización. Por lo tanto, es importante que las empresas y organizaciones implementen medidas de control dual en la seguridad de TI para garantizar la integridad de sus sistemas informáticos y la protección de sus datos sensibles.

Tabla 13

Criterio 12 Análisis de riesgos

XII. Licencias y relaciones contractuales con terceros			
Nº	Preguntas	Respuestas	
		Si	No
1	Existe seguimiento a los acuerdos previstos en los contratos de proveedores de servicios de software, internet?	X	
2	Existe seguimiento en los acuerdos de con los proveedores de hardware		X
3	Existe control en los tiempos de caducidad de las licencias de software		X
	Total	1	2
	Porcentual	33.33%	66.66%

La falta de licencias puede ser un problema grave para las empresas y organizaciones, ya que el uso no autorizado de software puede llevar a consecuencias legales y financieras negativas.

Las empresas que utilizan software sin licencia pueden estar violando los derechos de propiedad intelectual de los propietarios del software, lo que puede resultar en sanciones legales y multas significativas. Además, el uso no autorizado de software también puede poner en riesgo la seguridad de los sistemas de la empresa, ya que los parches y las actualizaciones de seguridad pueden no estar disponibles para el software sin licencia. Esto puede dejar a la empresa vulnerable a virus, malware y otros riesgos de seguridad. Por lo tanto, es importante que las empresas y organizaciones implementen medidas adecuadas para garantizar que todos los software que se utilizan estén debidamente licenciados, lo que puede ayudar a evitar problemas legales y de seguridad, y garantizar que la empresa esté protegida y en cumplimiento de la ley.

Tabla 14

Criterio 13 Análisis de riesgos

XIII. Asesorar y transmitir cultura sobre el riesgo informático			
Nº	Preguntas	Respuestas	
		Si	No
1	Existen capacitaciones al personal sobre los riesgos informáticos	X	
2	Existen sanciones para el personal que vulnera las seguridades en los equipos de hardware		X
	Total	1	1
	Porcentual	50%	50%

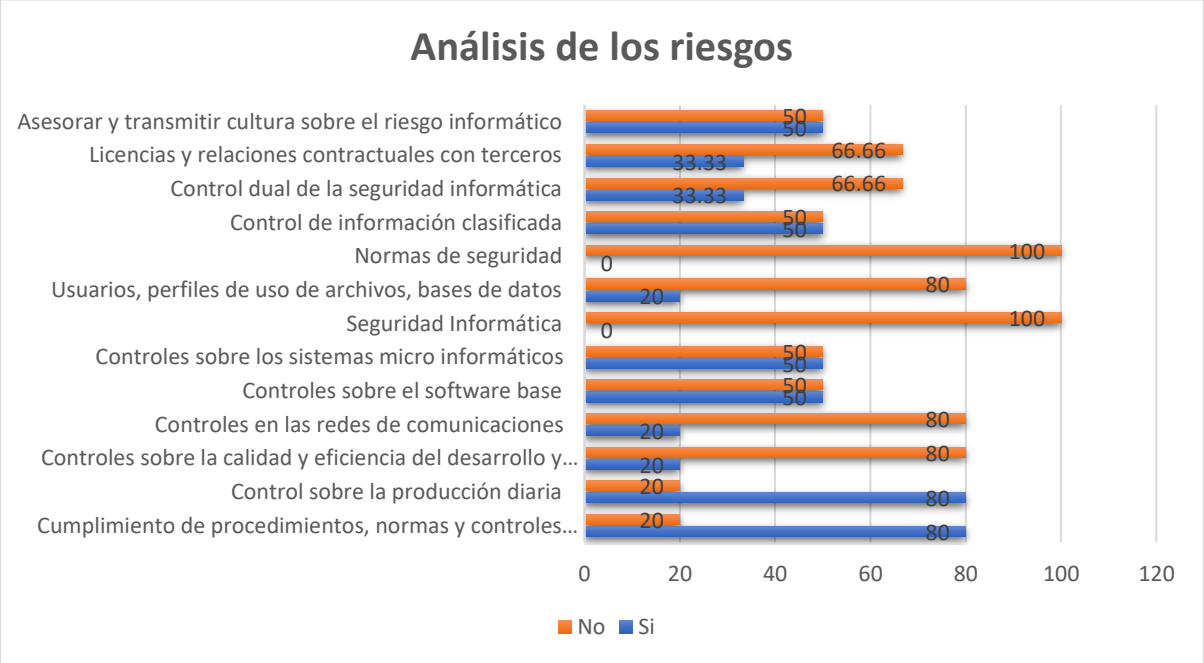
La falta de cultura del riesgo informático puede tener consecuencias graves para las empresas y organizaciones, ya que la seguridad informática es un componente crítico para la protección de los activos de información y la privacidad de los usuarios. La falta de comprensión y

conciencia de los riesgos informáticos puede llevar a decisiones equivocadas y a la toma de riesgos innecesarios, lo que puede poner en peligro la integridad y la seguridad de los sistemas informáticos. Además, la falta de cultura del riesgo informático también puede dificultar la implementación y la adopción de medidas de seguridad efectivas, lo que puede llevar a la exposición de los sistemas de la empresa a amenazas cibernéticas. Es importante que las empresas y organizaciones promuevan una cultura del riesgo informático mediante la educación y la formación de sus empleados en cuanto a los riesgos informáticos y la importancia de la seguridad informática. Esto puede ayudar a fomentar una cultura de responsabilidad y de conciencia del riesgo informático en toda la organización, lo que puede mejorar la protección de los activos de información y la privacidad de los usuarios.

Resumen de los resultados del cuestionario Análisis de los riesgos

Figura 5

Resultados del análisis de riesgos del departamento de TI



Es posible observar que de una manera generalizada no se cumplen los minimos criterios de seguridad de información en el departamento de TI, lo que implica un alto riesgo de robos de información o manipulación de la misma.

MATRIZ GENERAL DE COBIT 5

Tabla 15

Matriz General de COBIT 5

Dominio	Procesos	Actividades del proceso	Evaluado	Nivel objetivo	Nivel 0	Nivel 1	Nivel 2	Nivel 3	Nivel 4	Nivel 5
Evaluar, Orientar y Supervisar (EDM)	Gobierno de TI Empresarial	Asegurar y mantener el marco de referencia del gobierno de TI	Relacionar las metas de la institución con las de TI	Trabajar en pos de lograr las metas institucionales dando soporte desde el departamento de TI	N					
Alinear, Planificar y Organizar (APO)	Formular políticas de TI	Existen definidas las políticas de adquisiciones tecnológicas?	Analizar las tecnologías existentes para definir la dirección adecuada y crear oportunidades de negocio	Se planea cual es la dirección tecnológica apropiada para materializar la estrategia de TI?	N					

Construir, Adquirir e Implementar (BAI)	Análisis de negocios	Existen políticas de relaciones con proveedores	Existe un marco de trabajo definido para dar prioridades a la asignación de recursos de TI?	El proceso garantiza la inversión de TI en el presupuesto general de la institución	N					
Entregar, dar Servicio y Soporte (DSS)	Administración de la seguridad	Existen las políticas de continuidad del negocio en el departamento de TI?	Se identifica los estándares claves para los procesos de TI	Se monitorea la efectividad del departamento de TI?	N					
Supervisar, Evaluar y Valorar (MEA)	Revisión del cumplimiento	Existen lineamientos para realizar una revisión del cumplimiento del área de TI?	Existe un marco de trabajo que establezca el enfoque institucional hacia los riesgos?	Se mantiene un plan global de calidad que promueva la mejora continua?	N					

Leyenda: N (No logrado, 0-15%), P (Parcialmente logrado,> 15% -50%), L (En gran parte conseguido, 50% -85%), F (Totalmente Conseguido,> 85 a 100%)

DESARROLLAR UN PLAN DE MEJORA DE ACCIÓN

A continuación, se detallan los resultados de la evaluación de los niveles de capacidad:

Tabla 16

Medición de procesos

Total de procesos	Nivel 0	Nivel 1	Nivel 2	Nivel 3	Nivel 4	Nivel 5
5	5	0	0	0	0	0

Como es posible observar de los 5 procesos analizados ninguno se ha cumplido dentro del Gobierno Autónomo Descentralizado Municipal del cantón Alfredo Baquerizo Moreno por lo cual se propone el siguiente plan de mejoras:

Tabla 17

Nivel de madurez observado

Dominio	Procesos	Actividades del proceso	Evaluado	Nivel objetivo	Nivel de Madurez observado
Evaluar, Orientar y Supervisar (EDM)	Gobierno de TI Empresarial	Asegurar y mantener el marco de referencia del gobierno de TI	Relacionar las metas de la institución con las de TI	Trabajar en pos de lograr las metas institucionales dando soporte desde el departamento de TI	0 Proceso Incompleto No existe un marco del gobierno de TI Planes de acción relacionados Definir el modelo del Gobierno de TI

Alinear, Planificar y Organizar (APO)	Formular políticas de TI	Existen definidas las políticas de adquisiciones tecnológicas?	Analizar las tecnologías existentes para definir la dirección adecuada y crear oportunidades de negocio	Se planea cual es la dirección tecnológica apropiada para materializar la estrategia de TI?	0 Proceso Incompleto No existe un modelo estratégico de toma decisiones para que las TI sean efectivas y estén alineadas con el entorno externo e interno de la institución. Planes de acción relacionados Definir el plan estratégico de TI
Construir, Adquirire Implementar (BAI)	Análisis de negocios	Existen políticas de relaciones con proveedores	Existe un marco de trabajo definido para dar prioridades a la asignación de recursos de TI?	El proceso garantiza la inversión de TI en el presupuesto general de la institución	0 Proceso Incompleto Hay designaciones en el presupuesto para TI, sin embargo, no se hace en base a un estudio real de las necesidades ni se controlan los beneficios Planes de acción relacionados Definir un plan de adquisiciones de hardware y software
Entregar, dar Servicio y Soporte (DSS)	Administración de la seguridad	Existen las políticas de continuidad del negocio en el departamento de TI?	Se identifica los estándares claves para los procesos de TI	Se monitorea la efectividad del departamento de TI?	0 Proceso Incompleto No existe en la organización una visión de los riesgos y no se monitorea en ningún aspecto la efectividad del departamento de TI Planes de acción relacionados Definir el plan estratégico de TI
Supervisar, Evaluar	Revisión del	Existen lineamientos para realizar	Existe un marco de trabajo que	Se mantiene un plan global de	0 Proceso Incompleto No existe ninguna medición y elaboración de informes en cuanto a conformidad y

y Valorar (MEA)	cumplimiento	una revisión del cumplimiento del área de TI?	establezca el enfoque institucional hacia los riesgos?	calidad que promueva la mejora continua?	desempeño de TI en la institución con aprobaciones de partes a las que se les brindo el servicio Planes de acción relacionados Definir el plan estratégico de TI

CONCLUSIONES

Después de haber realizado la Auditoria de los Sistemas Informáticos Aplicando el sistema COBIT 5 en el Gobierno Autónomo Descentralizado Municipal del cantón Alfredo Baquerizo Moreno se obtuvo las siguientes conclusiones:

- Se realizó una revisión del departamento del TI en el Gobierno Autónomo Descentralizado Municipal del cantón Alfredo Baquerizo Moreno siguiendo los lineamientos del modelo COBIT 5.0 en el cual se pudo determinar que, en la evaluación de los atributos específicos para los procesos seleccionados en esta prueba piloto, ninguno pudo superar el nivel 0, es decir están incompletos.

- Según los resultados obtenidos en el cuestionario de análisis de riesgos, es posible observar que de una manera generalizada no se cumplen los mínimos criterios de seguridad de información en el departamento de TI, lo que implica un alto riesgo de robos de información o manipulación de la misma, sin ninguna protección a los delitos informáticos.

- Los planes de acción son específicos para cada uno de los procesos revisados en la evaluación piloto, los cuales deberían ser planificados por la nueva directiva cantonal que asumirá su mandato en el mes de mayo para de esta manera mejorar las debilidades detectadas en este análisis, sin embargo, es necesario una concientización de todo el personal para llegar a la consecución de los mismos.

BIBLIOGRAFIA

Aseguramiento, C. d. N. d. A. y. (2018). Guías de auditorÍa. México: Instituto Mexicano de Contadores Públicos.

Braz, M. M. R. (2017). Auditoria de Ti: O Guia de Sobrevivencia. Brasil: Ase Editorial.

Baca Urbina, G. (2016). Introducción a la seguridad informática. México: Grupo Editorial Patria.

Bernard, P. (2012). COBIT® 5 - A Management Guide. Países Bajos: van Haren Publishing.

Estupiñán Gaitán, R. (2022). Control interno y fraudes - 4ta edición: Análisis de Informe COSO I, II y III con base en los ciclos transaccionales. Colombia: Ecoe Ediciones.

Fundamentos de auditoría.: Aplicación práctica de las Normas Internacionales de Auditoría. (2019). (n.p.): IMCP.

GALLARDO VÁZQUEZ, S. (2019). Elementos de sistemas de telecomunicaciones 2.a edición. España: Ediciones Paraninfo, S.A.

ISACA. (2012). *COBIT 5: A business framework for the governance and management of enterprise IT*. Isaca.

Manual práctico de planeación estratégica. (2019). España: Ediciones Diaz de Santos S.A..

MODELO DE PLAN ESTRATÉGICO DE SISTEMAS PARA LA GESTIÓN Y ORGANIZACIÓN A TRAVÉS DE UNA PLATAFORMA INFORMÁTICA. (2017). (n.p.): 3Ciencias.

POSTIGO PALACIOS, A. (2020). Seguridad informática (Edición 2020). España: Ediciones Paraninfo, S.A.

Protección de Datos y Seguridad de la Información. (n.d.). (n.p.): Grupo Editorial RA-MA.

Ruggero, P. (2020). Seguridad Informática - Manual Principiantes: Un excelente manual para acercarse al mundo de la ciberseguridad personal. (n.p.): Independently Published.

Solís Salazar, C. (2012). Implantar Controles de Seguridad de la Información. (n.p.): Editorial Academica Espanola.

Vega Briceño, E. (2021). Seguridad de la información. España: 3Ciencias.

ANEXOS

UNIVERSIDAD TÉCNICA DE BABAHOYO
FACULTAD DE ADMINISTRACIÓN, FINANZAS E INFORMÁTICA
DECANATO

Babahoyo, 10 de marzo del 2023
D-FAFI-UTB-0098-2023

Ingeniera.
Angela Herrera Mendéz.
ALCALDESA DEL GOBIERNO AUTONÓMO DESCENTRALIZADO MUNICIPAL ALFREDO BAQUERIZO MORENO JUJAN.

Ciudad. -

De mis consideraciones:

Reciba un cordial saludo por parte de la Facultad de Administración, Finanzas e Informática de la Universidad Técnica de Babahoyo, donde formamos profesionales altamente capacitados en los campos de Tecnologías de la Información y de Administración, competentes, con principios y valores cuya practica contribuye al desarrollo integral de la sociedad, es por ello que buscamos prestigiosas Empresas e Instituciones Públicas y Privadas en las cuales nuestros futuros profesionales tengan la oportunidad de afianzar sus conocimientos.

El Señor, **PALMA MANCILLA ALVARO EDUARDO,** con cédula de identidad No. **092889043-3** Estudiante de la Carrera de Ingeniería en Sistemas, matriculado en el proceso de titulación en el periodo Diciembre 2022 – Mayo 2023, trabajo de titulación modalidad Estudio de Caso, previo a la obtención del grado académico profesional universitario de tercer nivel como **INGENIERO EN SISTEMAS,** solicita por intermedio del Decanato de esta Facultad el debido permiso para realizar el Estudio de Caso, el cual titula: **"AUDITORIA DE LOS SISTEMAS INFORMÁTICOS APLICANDO EL SISTEMA COBIT 5 EN EL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN ALFREDO BAQUERIZO MORENO".**

Atentamente,

Lcdo. Eduardo Galeas Guijarro MAE.
DECANO

GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL ALFREDO BAQUERIZO MORENO (JUJAN)
Fecha: 14-03-2023
Hora: 09:05
Recibido: SECRETARIA GENERAL

UNIVERSIDAD TÉCNICA DE BABAHOYO

Facultad de Administración, Finanzas e Informática

Alfredo Baquerizo Moreno Jujan , a 27 de FEBRERO del 2023

Ing. Angela Herrera Méndez
ALCALDESA DEL CANTÓN ALFREDO BAQUERIZO MORENO (JUJAN)

En su despacho. -

De mi consideración:

Reciba un cordial saludo, quien se suscribe **ALVARO EDUARDO PALMA MANCILLA**, cl. **092889043-3**, estudiante de la CARRERA DE **INGENIERÍA** EN SISTEMAS DE LA FACULTAD ADMINISTRACIÓN, FINANZAS E INFORMÁTICA. Me suscribo a usted en poder realizar mi caso de estudio para mi proyecto de titulación de la UNIVERSIDAD TECNICA DE BABAHOY0 el cual necesito realizarlo en el área de **SISTEMAS**, con su respectiva arquitectura de red con cada uno de sus departamentos, del gobierno autónomo municipal de Alfredo Baquerizo moreno jujan,

Es todo cuanto puedo informar para los fines correspondientes y seguros de contar con su favorable respuesta, reitero mis sinceros agradecimientos.

Atentamente,

Alvaro Palma.

ALVARO EDUARDO PALMA MANCILLA
C.I. 092889043-3

27-02-2023
Hora 12:00
SECRETARÍA GENERAL