



UNIVERSIDAD TÉCNICA DE AMBATO
FACULTAD DE CONTABILIDAD Y AUDITORÍA
CARRERA DE CONTABILIDAD Y AUDITORÍA

**Análisis de Caso, previo a la obtención del Título de Licenciada en Contabilidad
y Auditoría C.P.A.**

Tema:

**“Evaluación del sistema de control interno a los procesos de ciberseguridad en
la empresa Ecuatran S.A.”**

Autora: Flores Salazar, Diana Angely

Tutora: Dra. Jiménez Estrella, Patricia Paola

Ambato – Ecuador

2022

APROBACIÓN DEL TUTOR

Yo, Dra. Patricia Paola Jiménez Estrella con cédula de identidad No.180293423-0, en mi calidad de Tutora del análisis de caso sobre el tema: **“EVALUACIÓN DEL SISTEMA DE CONTROL INTERNO A LOS PROCESOS DE CIBERSEGURIDAD EN LA EMPRESA ECUATRAN S.A”**, desarrollado por Diana Angely Flores Salazar, de la Carrera de Contabilidad y Auditoría, modalidad presencial, considero que dicho informe investigativo reúne los requisitos, tanto técnicos como científicos y corresponde a las normas establecidas en el Reglamento de Graduación de Pregrado, de la Universidad Técnica de Ambato y en el normativo para presentación de Trabajos de Graduación de la Facultad de Contabilidad y Auditoría.

Por lo tanto, autorizo la presentación del mismo ante el organismo pertinente, para que sea sometido a evaluación por los profesores calificadores designados por el H. Consejo Directivo de la Facultad.

Ambato, marzo 2022.

TUTORA



.....
Dra. Patricia Paola Jiménez Estrella

C.I. 180293423-0

DECLARACIÓN DE AUTORÍA

Yo, Diana Angely Flores Salazar con cédula de identidad No. 185001283-0, tengo a bien indicar que los criterios emitidos en el análisis de caso, bajo el tema: **“EVALUACIÓN DEL SISTEMA DE CONTROL INTERNO A LOS PROCESOS DE CIBERSEGURIDAD EN LA EMPRESA ECUATRAN S.A”**, así como también los contenidos presentados, ideas, análisis, síntesis de datos, conclusiones, son de exclusiva responsabilidad de mi persona, como autora de este Análisis de Caso.

Ambato, marzo 2022.

AUTORA



.....
Diana Angely Flores Salazar

C.I. 185001283-0

CESIÓN DE DERECHOS

Autorizo a la Universidad Técnica de Ambato, para que haga de este análisis de caso, un documento disponible para su lectura, consulta y procesos de investigación.

Cedo los derechos en línea patrimoniales de mi análisis de caso, con fines de difusión pública; además apruebo la reproducción de este análisis de caso, dentro de las regulaciones de la Universidad, siempre y cuando esta reproducción no suponga una ganancia económica potencial; y se realice respetando mis derechos de autora.

Ambato, marzo 2022.

AUTORA



.....
Diana Angely Flores Salazar

C.I. 185001283-0

APROBACIÓN DEL TRIBUNAL DE GRADO

El Tribunal de Grado, aprueba el análisis de caso, sobre el tema: **“EVALUACIÓN DEL SISTEMA DE CONTROL INTERNO A LOS PROCESOS DE CIBERSEGURIDAD EN LA EMPRESA ECUATRAN S.A”**, elaborado por Diana Angely Flores Salazar, estudiante de la Carrera de Contabilidad y Auditoría, el mismo que guarda conformidad con las disposiciones reglamentarias emitidas por la Facultad de Contabilidad y Auditoría de la Universidad Técnica de Ambato.

Ambato, marzo 2022.



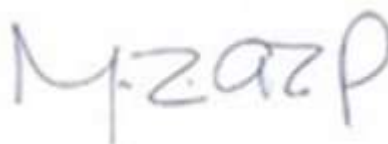
Dra. Mg. Tatiana Valle

PRESIDENTE



Dra. Rocío Cando

MIEMBRO CALIFICADOR



Dr. Mauricio Arias

MIEMBRO CALIFICADOR

DEDICATORIA

El presente trabajo lo dedico a Dios que está siempre junto a mí, iluminando mi camino, dándome las fuerzas necesarias para enfrentar las dificultades que se han presentado en la vida y por permitirme hacer posible este sueño, culminado con éxito mi carrera universitaria.

A mis padres Elji Flores y Rocío Salazar que han sido mi fuente de inspiración, que gracias a su dedicación, esfuerzo y amor me han acompañado a lo largo de mi formación, enseñándome a luchar por mis metas y nunca rendirme. A mis hermanitos que han estado junto a mí creciendo. A mis abuelitos que han sido amorosos conmigo y me han dado sus consejos de superación. A mi tía Ceci y mi tío Juanito que siempre han estado preocupándose por mí. Y a toda mi familia que ha estado pendientes de mí.

A mis docentes que han compartido conmigo sus enseñanzas. A la Dra. Patricia Jiménez por haberme guiado para la elaboración de mi trabajo de titulación y darme los consejos necesarios para una buena aplicación. A mis amigos que me han brindado su gran apoyo. A la empresa ECUATRAN S.A que me ha dado la oportunidad de realizar mi trabajo de titulación y a mis compañeros de trabajo que me han apoyado en el transcurso de este tiempo especialmente a la Ing. Angélica Tirado que ha estado pendiente de que todo salga con éxitos en esta etapa universitaria.

AGRADECIMIENTO

Mi agradecimiento profundo e infinito a Dios por permitirme llegar hasta este punto de mi vida iluminándome de sabiduría, logrando una meta de muchas más. A mis padres que gracias a su gran esfuerzo he llegado a donde estoy ahora. A toda mi familia que ha estado siempre pendiente, confiando en mí.

Mi profundo agradecimiento a la Universidad Técnica de Ambato a la facultad de Contabilidad y Auditoría a los docentes que en su momento formaron parte en mi formación tanto profesional como personal especialmente a mi tutora, la Dra. Patricia Jiménez por permitirme recurrir a sus capacidades y experiencias para la elaboración del presente trabajo.

Mis más sinceros agradecimientos a la prestigiosa empresa ECUATRAN S.A. y a cada uno de sus colaboradores por brindarme la información necesaria para la elaboración de este trabajo, ya que sin su apoyo no hubiese sido posible cumplir esta meta.

Y agradezco a cada una de las personas que me han apoyado incondicionalmente para que pueda culminar este ciclo con éxitos.

UNIVERSIDAD TÉCNICA DE AMBATO
FACULTAD DE CONTABILIDAD Y AUDITORÍA
CARRERA DE CONTABILIDAD Y AUDITORÍA

TEMA: “EVALUACIÓN DEL SISTEMA DE CONTROL INTERNO A LOS PROCESOS DE CIBERSEGURIDAD EN LA EMPRESA ECUATRAN S.A.”

AUTORA: Diana Angely Flores Salazar

TUTORA: Dra. Patricia Paola Jiménez Estrella

FECHA: Marzo 2022

RESUMEN EJECUTIVO

El presente trabajo investigativo acerca de la evaluación del sistema de control interno a los procesos de ciberseguridad en la empresa ECUATRAN S.A. consistió en diagnosticar la situación actual de la protección de la seguridad informática con respecto a la infraestructura computacional y todo lo vinculado con la información contenida en esta. Para lo cual fue necesario aplicar una entrevista, check list y cuestionarios que fueron fundamentales para la realización de las respectivas matrices con el análisis de la metodología COSO 2019 y las Normas ISO 27000. De tal manera, se obtuvo resultados que permitieron establecer estrategias de defensa ante las vulnerabilidades presentadas como es el caso de la administración segura, no constan de registros de auditorías pasadas lo cual dificultó el análisis de los procesos para hacer comparaciones la seguridad de información como ha ido evolucionando. Además, detectaron que el personal no poseía información de las medidas a tomar en caso exista un ciberataque en el ordenador. Finalmente, la empresa se encuentra dentro de los estándares de seguridad establecidas por la matriz realizada de la metodología COSO 2019 y normas ISO 27000. Siendo importante tomar en cuenta los riesgos altos que presenta para dar las posibles soluciones de acuerdo a las recomendaciones proporcionadas y el plan descrito.

PALABRAS DESCRIPTORAS: CIBERSEGURIDAD, CIBERDELITO,
CONTROL INTERNO, ATAQUES CIBERNÉTICOS.

TECHNICAL UNIVERSITY OF AMBATO
FACULTY OF ACCOUNTING AND AUDIT
ACCOUNTING AND AUDIT CAREER

TOPIC: "EVALUATION OF THE INTERNAL CONTROL SYSTEM TO THE CYBERSECURITY PROCESSES IN THE COMPANY ECUATRAN S.A."

AUTHOR: Diana Angely Flores Salazar

TUTOR: Dra. Patricia Paola Jiménez Estrella

DATE: March 2022

ABSTRACT

The present investigative work about the evaluation of the internal control system for cybersecurity processes in the company ECUATRAN SA consisted of the current situation of the protection of computer security with respect to the computing infrastructure and everything related to the information contained in it. For which it was necessary to apply an interview, check list and questionnaires that were fundamental for the realization of the respective matrices with the analysis of the COSO 2019 methodology and the ISO 27000 Standards. In this way, results were obtained that allowed establishing defense strategies. Given the vulnerabilities that may arise, such as the case of secure administration, they do not have records of past audits, which made it difficult to analyze the processes to make comparisons of information security as it has evolved. In addition, I detected that the staff did not have information on the measures to be taken in the event of a cyberattack on the computer. Finally, the company is within the security standards established by the matrix made of the COSO 2019 methodology and ISO 27000 standards. It is important to take into account the high risks that it presents to give possible solutions according to the recommendations provided and the described plan.

KEYWORDS: CYBER SECURITY, CYBER CRIME, INTERNAL CONTROL,
CYBER ATTACKS.

ÍNDICE GENERAL

CONTENIDO	PÁGINA
PÁGINAS PRELIMINARES	
PORTADA.....	i
APROBACIÓN DEL TUTOR.....	ii
DECLARACIÓN DE AUTORÍA.....	iii
CESIÓN DE DERECHOS	iv
APROBACIÓN DEL TRIBUNAL DE GRADO	v
DEDICATORIA	vi
AGRADECIMIENTO.....	vii
RESUMEN EJECUTIVO	viii
ABSTRACT	x
ÍNDICE GENERAL.....	xii
ÍNDICE DE TABLAS	xiv
ÍNDICE DE FIGURAS.....	xv
CAPÍTULO I.....	1
1. FORMULACIÓN DEL ANÁLISIS DE CASO.....	1
1.1. Tema.....	1
1.2. Antecedentes	1
1.3. Justificación.....	2
1.3.1. Justificación teórica científica.....	2
1.3.3. Justificación práctica.....	4
1.4. Objetivos	5
1.4.1. Objetivo general.....	5
1.4.2. Objetivos específicos	6
CAPÍTULO II.....	7
2. FUNDAMENTACIÓN CIENTÍFICA TÉCNICA	7
2.1. La incidencia de la tecnología a nivel mundial.....	7
2.1.1. La evolución informática, un enfoque en el ámbito empresarial	7

2.1.2. La realidad de la inseguridad de información tecnológica.....	8
2.1.3. Aplicación de la metodología COSO en Latinoamérica y el mundo	9
2.1.4. La importancia de las Normas ISO 27000 en las empresas	10
2.2. El control interno a la seguridad de información en el sector empresarial ecuatoriano.....	12
2.2.1. Casos de ciberdelincuencia detectada en el país y el efecto que conlleva al sector empresarial.....	12
2.2.2. Procesos de ciberseguridad aplicados en empresas nacionales.....	13
2.3. El desarrollo de la empresa Ecuatran S.A y la aplicación de la ciberseguridad en sus sistemas.....	14
2.3.1. El desarrollo de la ciberseguridad en los sistemas informáticos de Ecuatran..	14
2.4. Fundamentos teóricos.....	16
2.4.1. La teoría de sistemas de información y análisis de riesgos informáticos	16
CAPÍTULO III.....	17
3. METODOLOGÍA	17
3.1. Metodología e instrumentos de recolección de información	17
3.1.1. Unidad de análisis	17
3.1.2. Fuentes y técnicas de recolección de información.....	18
3.1.2.1. Fuentes de información primarias.....	18
3.2. Método de Análisis de Información.....	24
CAPÍTULO IV	30
4. DESARROLLO DEL ANÁLISIS DE CASO	30
4.1. Análisis y categorización de la información.	30
4.2. Narración del caso.....	36
CAPÍTULO V.....	51
5. CONCLUSIONES Y RECOMENDACIONES.....	51
5.1. Conclusiones	51
5.2. Recomendaciones.....	53
5.2.1. Plan de ciberseguridad	55
REFERENCIAS BIBLIOGRÁFICAS	62
ANEXOS	71

ÍNDICE DE TABLAS

CONTENIDO	PÁGINA
Tabla 1. Normas ISO 27000 aplicado en la ciberseguridad.....	11
Tabla 2. Preguntas de la entrevista categorizadas	18
Tabla 3. Preguntas del check list categorizado.....	19
Tabla 4. Personas encuestadas	21
Tabla 5. Preguntas del cuestionario categorizado y escalas.....	22
Tabla 6. Check List categorizado.....	24
Tabla 7. Tabulación general de la aplicación de encuestas.....	26
Tabla 8. Análisis de datos de la aplicación de encuestas	26
Tabla 9. Análisis del coeficiente de fiabilidad	27
Tabla 10. Matriz de riesgos con la aplicación del COSO 2017 e ISO 27000	29
Tabla 11. Análisis del Check List	30
Tabla 12. Análisis de las encuestas	32
Tabla 13. Análisis de las encuestas por categoría	33
Tabla 14. Análisis de fiabilidad de resultados.....	35
Tabla 15. El Riesgo según el Sistema COSO 2017 y la relación con las NORMAS ISO 27000.....	48
Tabla 16. El Riesgo según el Sistema COSO 2017 y la relación con las NORMAS ISO 27000.....	49
Tabla 17. Recomendaciones.....	61

ÍNDICE DE FIGURAS

CONTENIDO	PÁGINA
Figura 1. Ciclo Deming o PDCA	11
Figura 2. Análisis de datos del Check List.....	25
Figura 3. Análisis de datos de las encuestas	27
Figura 4. Verificación del cumplimiento de actividades del Check List	31
Figura 5. Verificación del cumplimiento de actividades de las encuestas	34
Figura 6. Flujograma de Mantenimiento Preventivo	40
Figura 7. Flujograma de Mantenimiento Correctivo	41
Figura 8. Flujograma de Solicitud de Hardware y Software.....	42
Figura 9. Flujograma de Adquisiciones	43
Figura 10. Flujograma de Solicitud de Consulta de Datos	44
Figura 11. Flujograma de Solicitud de Requerimiento de Desarrollo	45
Figura 12. Flujograma de Proyecto de Desarrollo de Software	46
Figura 13. Detalle análisis Check List	74
Figura 14. Tabulación Check List Categoría Sensibilizando.....	75
Figura 15. Tabulación Check List Categoría Conociendo el Sistema de Información.....	75
Figura 16. Tabulación Check List Categoría Autenticación de los accesos.....	75
Figura 17. Tabulación Check List Categoría Estaciones de Trabajo Seguras	76
Figura 18. Tabulación Check List Categoría Asegurando la Red.....	76
Figura 19. Tabulación Check List Seguridad para Equipos Portátiles.....	76
Figura 20. Tabulación Check List Mantener actualizado el sistema de información.....	77
Figura 21. Tabulación Check List Supervisar, Auditar y Reaccionar	77
Figura 22. Detalle análisis aplicación de encuestas	78
Figura 23. Tabulación por categorización.....	79
Figura 24. Escala de Impacto para aplicación matriz de riesgos	79
Figura 25. Escala de Probabilidad para aplicación matriz de riesgos	79

Figura 26. Escala de riesgo para aplicación matriz de riesgos.....	80
Figura 27. Definición del Riesgo	80

CAPÍTULO I

1. FORMULACIÓN DEL ANÁLISIS DE CASO

1.1. Tema

“Evaluación del sistema de control interno a los procesos de ciberseguridad en la empresa ECUATRAN S.A. “

1.2. Antecedentes

El presente análisis titulado la evaluación del sistema de control interno a los procesos de ciberseguridad en la empresa ECUATRAN S.A establece bases esenciales para el correcto procesamiento de la información. A través del, control interno permite la identificación y análisis de los riesgos, estableciendo medidas preventivas y correctivas. Además, la ciberseguridad permite que la empresa detecte debilidades en los sistemas de información. Por lo que, con estas dos variables establece mecanismos de apoyo para proteger el sistema de seguridad informática.

En este sentido, ECUATRAN considera a la ciberseguridad como un sistema importante al que se debe tomar en cuenta puesto que, toda su información se plasma en forma digital. Cabe señalar que a inicios de su actividad se realizaba registros manuales, pero con la evolución de más de 40 años de experiencia en el mercado se han ido integrando tecnologías, permitiendo el progreso eficiente de los procesos. Sin embargo, la empresa ha sufrido de ataque cibernético hace aproximadamente 2 años donde el servidor fue hackeado, siendo un impacto fuerte para el sistema informático. No obstante, la empresa poseía respaldo local que permitió la recuperación de la información.

La empresa posee una matriz de riesgos comprendida de tres elementos: el robo de la información, pérdida de la información y la confidencialidad de la información. Por consiguiente, ECUATRAN actualiza los antivirus constantemente como medida de prevención, mismos que poseen un costo por su funcionalidad para ser licenciados en

todos los equipos, Además dispone de un sistema de seguridad de la información desde hace ya un largo tiempo que aún sigue funcional, pero está por culminar su ciclo de vida.

A pesar de ello, el acceso a los datos del sistema informático ha generado ciertas vulnerabilidades que con el pasar del tiempo no han logrado ser monitoreadas de forma segura. Por esta razón, ECUATRAN requiere la implementación de un nuevo sistema de seguridad, teniendo en cuenta los recursos financieros necesarios, mismos que son plasmados en los presupuestos que entregados a gerencia para la respectiva aprobación. De tal forma, este sistema permitirá que la información se mantenga protegida ante cualquier vulnerabilidad.

1.3. Justificación

1.3.1. Justificación teórica científica

Durante años, los sistemas informáticos han permitido el fácil acceso a la información, gracias al avanzado sistema de software creado. En los últimos tiempos, el Ecuador y el mundo ha incrementado el uso de este sistema para la aplicación contable de las empresas. De hecho, el desarrollo tecnológico influye en las actividades de monitoreo de la información de las entidades.

De acuerdo a los resultados de Callery & Perkins (2021) los hallazgos demuestran que las empresas manipulan habitualmente las calificaciones intermedias con afirmaciones falsas, lo que socava los objetivos institucionales y sociales. En el mismo sentido, Tadesse & Murthy (2021) manifiestan que se ha hipotetizado y encontrado evidencia de presentaciones y los tipo de desagregación donde los inversionistas perciben las ICW como menos negativas cuando se generalizan de manera sobresaliente provocando que el efecto aumente cuando la debilidad material se desagrega en sus deficiencias de control individuales. En definitiva, el control interno obtendrá resultados precisos y correctos de los procesos de seguridad con la finalidad de tomar medidas correctivas.

A través del tiempo los sistemas informáticos presentan vulnerabilidades para el hurto de la información. En este sentido, los métodos de seguridad surgen con la necesidad de

protección de los datos. La señal negativa de un incidente de ciberseguridad posterior revierte las percepciones positivas de los inversores sobre la competencia del auditor y aumenta la sensibilidad de los inversores a posibles deterioros de independencia cuando la ciberseguridad se aprovisiona conjuntamente, lo que conduce a percepciones más bajas de la calidad de la auditoría (Perols & Murthy, 2021). En el mismo sentido, Para prevenir y detectar el fraude, es útil conocer sus causas. Sin embargo, los modelos de elección binaria (por ejemplo, logit y probit), de uso frecuente en la literatura, no tienen en cuenta los casos de fraude no detectado y, por tanto, presentan pruebas de hipótesis poco fiables (Wuerges et al., 2014).

En términos de Shakouri et al. (2021) afirma que los resultados de probar las hipótesis de este estudio indican que el modelo Beneish es exitoso en la separación de empresas involucradas en informes financieros fraudulentos y empresas saludables. En este sentido, los sistemas de información se ven vulnerables en las empresas. Por lo que, la importancia de tomar medidas de seguridad donde las claves de acceso sean configuradas constantemente y donde solo un cierto tipo de personal tenga acceso a la información.

El RapidMiner resultó de fácil aplicación para poder ejemplificar la detección de valores anómalos y el agrupamiento por clústeres de una data de prueba seleccionada de 1000 datos (Hernandez, 2015). Por lo que, el control interno se origina como un controlador de los procesos que realiza la empresa para así asegurar su desarrollo ante el sistema anormal de hackear la información. En el mismo sentido, uno de los objetivos finales de las instituciones que trabajan en transparencia y estandarización de estados financieros, y la publicación de estándares relacionados con la profesión de contabilidad y auditoría, ha sido poner en práctica un conjunto global uniforme de estándares que serán aplicables en finanzas (Bozkurt et al., 2013).

De acuerdo a Salas & Reyes (2015) la responsabilidad frente al fraude es de cada organización, que desde la administración debe implementar procedimientos de control interno fuertes para este propósito. Por otra parte, Barbadillo et al. (2007) afirma que las empresas que cambiaron hacia auditores menos conservadores y de menor tamaño obtuvieron una mayor probabilidad de mejorar su opinión, aunque su probabilidad de

recibir informes no limpios no se viera afectada, concluyéndose que existe compra de opinión con éxito entre las empresas. De este modo, los resultados muestran que la principal variable explicativa de las diferencias temporarias es, con mucho, la manipulación contable, encontrándose que las empresas que practican más discrecionalidad aplican ajustes menos positivos y más negativos para posponer o diferir la tributación (Fernández & Martínez, 2015).

Para el desarrollo del presente se apoyará en varios tipos de investigación, en primera instancia, documental-bibliográfica basada en la búsqueda de información, además de la recuperación de datos y análisis e interpretación de los mismos. Entre las principales fuentes tenemos los libros, revistas, documentos escritos (en general, todo medio impreso). Por consiguiente, esta investigación recabará información para los aportes significativos en el análisis de la misma.

Además, en una investigación de campo se conocerá la realidad y el funcionamiento de los sistemas de información. A través de, encuestas que reflejen el nivel de seguridad en los departamentos de ECUATRAN. De este modo, este método aportará con información relevante que beneficiará para el estudio de la entidad proporcionando un análisis crítico.

1.3.3. Justificación práctica

En la presente investigación se dará a conocer la importancia de la seguridad de los sistemas informáticos, para evitar el robo de información. Por tanto, el análisis permitirá establecer el nivel de seguridad de la empresa, En este sentido, la investigación evaluará los procesos relacionados a la ciberseguridad referente a la prevención, localización y reacción de los posibles ataques con el objeto de establecer procedimientos y herramientas que permitan proteger la información y proporcionar los resultados en beneficio de la entidad.

Por añadidura, este tipo de investigación es útil para la empresa ECUATRAN S.A. De hecho, permite la adecuada utilización de las herramientas y técnicas informáticas. De tal manera que, salvaguarde la información y el correcto manejo del sistema de información.

Para el desarrollo se cuenta con la información que proporciona la entidad y la recopilación de datos en la página web de la empresa. Cabe señalar que, la investigación contará con la aplicación de procedimientos de Control Interno, Auditoría en sistemas, Contabilidad, Tecnologías de información y comunicación. Inclusive, para el análisis se empleará los objetivos de los marcos de referencia en seguridad de la información en temas de ciberseguridad.

Se pretende con esta investigación detectar los puntos vulnerables, amenazas y riesgos de los sistemas de la entidad para la protección de la información. De tal manera, esta permita implementar un plan de seguridad como herramienta para prevenir y evitar la pérdida de información e infiltración no autorizada a los sistemas poniendo en riesgo los datos confidenciales e integridad de la entidad.

Como mejora del sistema de seguridad de la información se practicará las directrices que establece las Normas ISO 27000 como estándar esencial para la identificación de riesgos y vulnerabilidades de la entidad. De igual forma, se medirá los riesgos con base a la metodología COSO 2017.

Los resultados de la investigación establecerán parámetros de acción en la empresa para la correcta funcionalidad de los sistemas informáticos. Además, el investigador a través de un análisis crítico efectuará aportes profesionales y recomendaciones sobre el soporte tecnológico para la entidad. De esta manera, asegurar el buen control y la aplicación de buenas prácticas para salvaguardar la información, permitiendo que esta sea eficiente y eficaz, siendo beneficioso para la empresa.

1.4. Objetivos

1.4.1. Objetivo general

Evaluar el sistema de control interno a los procesos de ciberseguridad en la empresa ECUATRAN S.A para la implementación de acciones de mejora encaminadas al fortalecimiento y salvaguarda de la información.

1.4.2. Objetivos específicos

- Identificar los procesos de ciberseguridad que dispone la empresa ECUATRAN S.A. para el reconocimiento de las vulnerabilidades más relevantes con respecto a la seguridad de información.
- Emplear la metodología COSO 2017 para la evaluación del sistema de control interno a los procesos de ciberseguridad de la empresa ECUATRAN S.A.
- Contrastar los resultados obtenidos de la evaluación con una comparación de lo que propone las Normas ISO 27000 para efectos de la seguridad de la información.
- Plantear un Plan de Seguridad de la Información con enfoque a la ciberseguridad como herramienta de apoyo en la salvaguarda de la información.

1.5. Preguntas de reflexión

1. ¿Qué tan importante es la seguridad de información para ECUATRAN?
2. ¿Qué medidas de protección posee la empresa en cuanto a ciberseguridad?
3. ¿Cuán eficiente es el sistema de control interno aplicado a los procesos de ciberseguridad en la empresa ECUATRAN?
4. ¿Qué tipo de buenas prácticas en ciberseguridad ha adoptado la empresa para la salvaguarda de su información?
5. ¿Cómo se mejoraría la ciberseguridad en la empresa?

CAPÍTULO II

2. FUNDAMENTACIÓN CIENTÍFICA TÉCNICA

2.1. La incidencia de la tecnología a nivel mundial

2.1.1. La evolución informática, un enfoque en el ámbito empresarial

En el mundo actual, la tecnología ha trascendido con los tiempos, marcando en la sociedad su lugar. De hecho, ha generado aportes significativos para el progreso empresarial. En primer lugar, esta empieza con la necesidad de desarrollar un modelo capaz de responder a cambios operados, producidos por el progreso de la ciencia y tecnología. En el mismo sentido, (Cañedo et al., 2005) manifiesta que en el campo de las necesidades de información en la sociedad, ante las evidentes limitaciones de la Bibliotecología y la Documentación para responder con efectividad a los nuevos retos.

En términos de Aguirre & Pérez (2011) a partir de 1950 las TICS empezaron a desarrollarse notoriamente. Como consecuencia, estas han repercutido en las relaciones sociales, económicas, políticas y culturales en el mundo. Por lo que, la tecnología ha incrementado las necesidades de generar, sistematizar, compartir, transmitir, analizar y difundir información.

En USA, la revolución tecnológica se produjo en 1987, representada por los computadores personales y los programas ofimáticos (Pinzón, 2014). En este sentido, la información comenzaba a sistematizarse con los datos guardados en discos extraíbles o fijos. De este modo, la tecnología se adaptó en las grandes empresas, convirtiéndose en un punto esencial para el sistema operativo de las mismas. En este sentido, la Red de redes ha sido esencial para la información; ésta es un elemento que entrega información, como puede ser una persona hablando o un ordenador entregando datos (Rueda, 2007).

El avance tecnológico ha generado un impacto notorio a nivel mundial. En consecuencia, ha desencadenado procesos de globalización económica. De hecho,

Jiménez (2013) afirma que el desarrollo tecnológico a nivel de inserción en el marco de unidad económica diferencia a seis tipos de países.

- Desarrollados: Estructura productiva y con alto ingreso per cápita. Países de la OCDE, Corea del Sur, Taiwán, Singapur, Hong Kong e Israel.
- Super poderosos: Características similares a los desarrollados, pero con poder militar a escala planetaria. Estados Unidos de Norteamérica.
- Emergentes: Alta dinamismo económico e ingresos per cápita medio y bajo. Países como China, Brasil, Tailandia, Malasia, Filipinas, Brunei, Turquía, Hungría, Polonia, Arabia Saudita, Chile y México.
- Estancados: Ingreso per cápita bajo y poco dinamismo económico. Países como: Indonesia, Rusia, Sudáfrica, Yugoslavia, Ucrania, Armenia, Siria, Líbano, Egipto, Perú Ecuador, Bolivia, Paraguay y Kenia.
- Extremadamente pobres: Ingreso per cápita bajo y sin dinamismo económico. Haití
- Políticamente excluidos: Situaciones de guerra civil, fundamentalismo religioso y terrorista. Países como Iraq, Irán, Afganistán, Corea del Norte, Argelia, Sierra Leona y Somalia, entre otros.

2.1.2. La realidad de la inseguridad de información tecnológica

El acelerado crecimiento de las tecnologías en las últimas décadas ha generado un sinnúmero de oportunidades, al igual que amenazas. A nivel mundial ha existido una serie de acontecimientos que han violado la información de las empresas. Por ello, la importancia de diagnosticar adecuadamente los riesgos a los cuales se ven expuestos, permitiendo mitigar oportunamente la pérdida de información. Así mismo, Corda et al. (2017) plantea que el riesgo informático es aquella eventualidad de peligro o daño que afecta directamente al funcionamiento de los resultados esperados de un sistema informático.

En términos de Maza (2020) la seguridad internacional se encuentra cada vez más al asecho, con la aparición de vulnerabilidades, riesgos y amenazas propias de Estados,

al igual que alcances de organizaciones terroristas y redes de delincuencia organizada. En este sentido Ramírez (2021) afirma que el riesgo tecnológico que incursiona en las sociedades se debe a vulnerabilidades existentes de medidas de protección inapropiadas y los cambios constantes que evita las actualizaciones de medidas de seguridad. No obstante, Campos (2019) menciona que los delitos informáticos poseen dificultades para combatirlos, debido a la transnacionalizada e incompatibilidad de leyes a nivel mundial; considerando que en algunos países las carecen, provocando millonarias pérdidas de información.

Las pérdidas de información a nivel mundial por ataques cibernéticos han generado fuertes impactos en las organizaciones. De acuerdo a TI (2018) afirma que el robo de datos es constante donde un 77% a nivel mundial han tenido que enfrentar ataques al DNS (Sistemas de Nombres de Dominio) costando a las empresas europeas de 734.000 euros, donde el 39% de estas han sufrido el robo de información. Por lo tanto, la seguridad informática es esencial para la protección de información de las organizaciones para evitar ataques que perjudiquen su estado.

De acuerdo a estudios efectuados por Alvarado (2018) en países como Colombia se está utilizando la inteligencia artificial para agrupar cientos de denuncias, permitiendo la búsqueda de patrones y asociaciones criminales que antes eran imposibles de identificar. Sin embargo, la iniciativa de enfrentar desafíos permite a las organizaciones establecer normas de control interno para evitar vulnerabilidades en los sistemas informáticos. De esta manera, las empresas buscan programas de protección a los usuarios.

2.1.3. Aplicación de la metodología COSO en Latinoamérica y el mundo

En forma Internacional, el problema de vulnerabilidad en los sistemas informáticos ha generado gran controversia en la sociedad. Por tanto, se busca evitar cualquier tipo de fraude que ponga en riesgo la información de las empresas, Por consiguiente, a nivel mundial emplean la metodología COSO como un nuevo estándar aplicado para evitar el cibercrimen.

De acuerdo a (Quinaluisa et al., 2018) el sistema COSO posee cinco organismos profesionales financieros más importantes de los Estados Unidos definido en 1992, donde como marco de control interno permite integrar las operaciones de la empresa. De tal manera que se establezca acciones a seguir como sistema de protección de la misma. De la misma manera, Parra (2014) manifiesta que el modelo COSO pretende que las actividades de control se fundamenten en el grado de riesgo y no sobre la base de los posibles errores, de tal forma que exista una correlación entre la intensidad de riesgo y la actividad de control.

El COSO ha permitido en grandes países establecer medidas para las organizaciones, a través de sus componentes: Ambiente de control, Evaluación de Riesgo, Actividades de control, Información y Comunicación y Actividades de Cumplimiento. De igual manera, Galaz (2015) afirma que el COSO ayuda a reducir impactos negativos en las empresas, aportando confianza en el cumplimiento de los objetivos, provee feedback del funcionamiento del negocio. Por añadidura, este modelo es establecido en las organizaciones como un control interno para identificar acontecimientos potenciales.

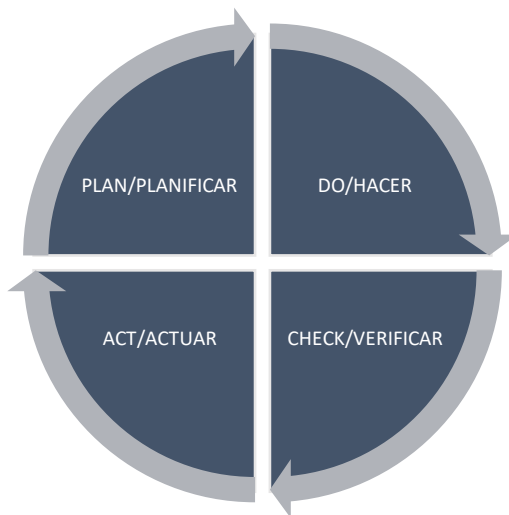
El control interno es aplicado en toda la organización, en cada nivel y unidad y a todos los miembros, para tomar conciencia de evaluar riesgos y aplicar controles (Castromán & Porto, 2005). De la misma manera, González (2007) manifiesta que el COSO permite alcanzar los objetivos, puesto que los controles internos permiten promoverlos para que los riesgos puedan ser superados. En tal forma que, en las organizaciones a nivel mundial poseen medidas correctivas para superar cualquier obstáculo o barrera que perjudique el bienestar de las entidades.

2.1.4. La importancia de las Normas ISO 27000 en las empresas

A nivel mundial ha existido un sinnúmero de aspectos que ha afectado el sistema de seguridad de información de las organizaciones por lo que se ha visto la necesidad de implementar normas que permitan proteger el sistema. De hecho, se ha creado las normas ISO 27000 que aportan a las empresas como estándares de seguridad. De esta manera, GlobalSUITE (2021) afirma que las normas 27000 permiten implementar un

Sistema de Gestión de Seguridad de la Información (SGSI) a través del proceso del Ciclo Deming o PDCA.

Figura 1. Ciclo Deming o PDCA



Fuente: Manay et al. (2019)

Elaborado por: Flores (2021)

Tabla 1. Normas ISO 27000 aplicado en la ciberseguridad

Norma	Detalle
27001	Proporciona establecimiento, implantación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información.
27002	Permite controlar la seguridad de información como buena práctica para las organizaciones.
27005	Proporciona directrices para la gestión de riesgos de la seguridad de la información de las empresas.
27007	Permite establecer, implementar, operar, monitorear, revisar, mantener y mejorar el SGSI.
27031	Proporciona métodos para mejorar la preparación de las Tecnologías de Información y Comunicación garantizando a continuidad de las empresas.
27701	Administra, gestiona y protege los datos personales de la compañía de acuerdo al Reglamento General de Protección de Datos (RGPD) para que exista confidencialidad en las organizaciones.

Fuente: Murillo et al. (2019)

Elaborado por: Flores (2021)

De acuerdo a Baena et al. (2019) afirma que ha utilizado los sistemas de seguridad de información no como un lujo sino como la necesidad de conocer y afrontar los riesgos para disminuir de manera significativa los ataques cibernéticos en las empresas. De la misma manera, Arévalo et al. (2015) menciona que SGSI permiten concientización de las esferas estratégicas que conducen a proteger los sistemas de información de las empresas como un proceso de mejora. De tal manera, permite que las organizaciones tomen medidas que ayuden con la protección de confidencialidad de la información personal de estas.

En Colombia el ISO 27000 son estándares de buenas prácticas que utilizan las empresas en las áreas tecnológicas que permiten fortalecer los sistemas de seguridad de información (Ladino et al., 2011). De tal manera que, Este país da ejemplo a las demás naciones que estas Normas permiten a las empresas tener un mejor control de seguridad de la información. De hecho, las buenas prácticas son perseguidas en las organizaciones por falta de la implementación de estas normas.

2.2. El control interno a la seguridad de información en el sector empresarial ecuatoriano

2.2.1. Casos de ciberdelincuencia detectada en el país y el efecto que conlleva al sector empresarial

En el Ecuador ha existido eventos peculiares de ciberataques a los servidores internos de las empresas. Inicialmente, este suceso apareció hace 10 años. De acuerdo a Navarrete (2020) afirma que una empresa reconocida en el sur del país dedicada a la importación de Equipos de China sufrió un ataque intermediario y suplantación de identidad al correo entre el dueño local y la exportadora asiática, motivando a realizar un pago vía transferencia Bancaria a una cuenta fraudulenta de Hong Kong por aproximadamente 40.000 USD, pudiendo ser el primer caso de fraude en el país. De tal manera esto desató la incertidumbre en el Ecuador con la inseguridad de la tecnología en las empresas.

De acuerdo a resultados de Vásconez (2015) el Ecuador registra más de 67.000 empresas de las cuales se ha presentado casos de ciberdelitos en 14, lo que llamo la atención puesto que se pensaba haber frenado el virus. De acuerdo a reportes fiscales existía clonaciones de tarjetas de crédito y robo de claves bancarias. En general, El Universo (2020) afirma que los delitos informáticos van creciendo en el país, desde el 2017 registraron 8421 casos, mientras que en el 2018 ascendió a 9571 y para el 2019 a 10279.

El Ecuador ha discutido ampliamente acerca de los problemas cibernéticos contraídos, enfocándose en lograr un modelo nacional de gobernanza y ciberdefensa De acuerdo a Chang (2020) manifiesta que Ecuador está en el puesto 82 de NCSI, calificado como una ciberseguridad deficiente en general. Sin embargo, la gestión de incidentes y crisis, dirigido por el Comando Cibernético del Comando Conjunto de las Fuerzas Armadas, le da una ventaja en la protección de los intereses del país, a través de estrategias de ciberdefensa.

De acuerdo a Vargas et al. (2017) el Ecuador (al igual que otros países) requieren de la implementación de un sistema de ciberdefensa como estrategia local y propia de gobernanza para la seguridad y defensa en el ciberespacio. De tal manera, este permitirá controlar la seguridad de la información en los procesos y las infraestructuras que dependen para la economía. A la vez, deferirá el correcto desarrollo de las organizaciones.

2.2.2. Procesos de ciberseguridad aplicados en empresas nacionales.

A nivel nacional, la ciberseguridad ha generado un gran impacto empresarial por la preocupación de la economía digital. Por lo que, han decidido hacerle frente al problema delictivo. De acuerdo a Becerra (2010) al fenómeno de globalización y la supresión de fronteras en internet ha surgido nuevas amenazas debido a la presencia global online y a la expansión en nuevos mercados de las organizaciones.

En términos de Dávalos (2020) en el país, el 3% de las empresas cuentan con herramientas que mitigan los riesgos cibernéticos. De tal manera, se busca estrategias para que la seguridad informática no padezca de vulnerabilidades que afecten el sistema operativo de las organizaciones. Del mismo modo, Almeida (2019) afirma que para proteger la seguridad de información de las empresas es necesario el resguardo de las redes y sistemas informáticos en el sector público y privado para fortalecer la confianza y las comunicaciones en el ciberespacio.

El país cuenta con empresas capacitadas en seguridad de información que brindan sus servicios para evitar los riesgos de robo de información, entre las más comunes se encuentra: Sertechma Cia. Ltda. Grupo Business IT. Ecuador VirtualIT. Procesos IQ. Corporación CISMO. Nube Digital. Binaria IT Services. Refundation. Kyrios Technologies. Kruger. GayaIT. RKLATAM. Byte atómico. Bi Solutions. Sin embargo, el Ecuador es uno de los últimos países en materia de ciberseguridad, ya que se encuentra en el séptimo lugar en América Latina (Espinosa, 2019). A pesar de ello, el interés de las empresas por salvaguardar la información ha creado la necesidad de establecer estrategias de ciberdefensa. En efecto, Infodefensa.com (2021) manifiesta que se inauguró el nuevo comando de ciberdefensa para contrarrestar ciberataques y ciberguerra para reforzar la seguridad y la defensa de la soberanía.

2.3. El desarrollo de la empresa Ecuatran S.A y la aplicación de la ciberseguridad en sus sistemas

2.3.1. El desarrollo de la ciberseguridad en los sistemas informáticos de Ecuatran

La empresa dispone de personal capacitado que se encarga de la seguridad tecnológica. Sin embargo, ha existido un ataque cibernético, provocando la pérdida de información. De acuerdo a Olmedo & Gavilánez (2018) afirma que los ataques cibernéticos ocurren por deficiencias en los mecanismos de defensa contra estas amenazas. Por otra parte, la empresa cuenta con un sistema de seguridad de información, pero requiere de uno más robusto que fortalezca la protección de los diferentes programas que maneja la entidad.

Los antivirus en los procesadores proporcionan de manera eficiente y eficaz el servicio de protección del equipo ante la detección de amenazas (Oberheide et al., 2008). Por lo tanto, la empresa actualiza constantemente los antivirus de todos los computadores en cada uno de los departamentos, De hecho, posee un antivirus con licencia de pago para que la protección sea la mejor. Sin embargo, Castro et al. (2018) afirma que las vulnerabilidades son fallos del sistema de seguridad o en los propios que el usuario utiliza para generar actividades de riesgo en el sistema informático. Por tanto, en el sistema pueden darse factores como páginas piratas que de una u otra forma requieran ingresar a los servidores, por esta razón la implementación de estrategias de seguridad.

ECUATRAN aplica los componentes del COSO como control interno En forma que, desarrollo de estrategias y el mejoramiento en el desempeño de la organización como una herramienta de gestión (Murillo et al., 2019). De esta manera busca adecuar los procesos de control en seguridad para evitar nuevamente acontecimientos que pongan en riesgo la integridad de la empresa.

La información de la empresa es manejada en: el RP, el sistema Financiero, sistema de producción, sistema de planificación, sistema de logística, sistemas de auditorías, sistema de calidad, I-SMART, WebPost, AXIS. Por lo tanto, las estrategias de seguridad aportarán con la protección eficiente su información. Así mismo, Gil & Gil (2017) mencionan que la seguridad informática trata de minimizar los riesgos asociados al acceso y utilización de determinados sistemas de forma no autorizada y en general malintencionada.

La evaluación del Control de riesgos en la empresa se rige a través de una serie de medidas como el mantenimiento continuo de cada equipo y el cambio de clave en los sistemas cada 3 meses. Además, el personal firma un acta de entrega recepción del usuario y contraseña. Por consiguiente, firman un documento de confidencialidad de la información para evitar hurto de la misma.

2.4. Fundamentos teóricos

2.4.1. La teoría de sistemas de información y análisis de riesgos informáticos

La teoría de sistemas de información es un esfuerzo de estudio interdisciplinario que combina de forma organizada a personas, hardware, software, redes de comunicaciones y recursos de datos que reúne, transforma y disemina información en una organización (Brien & Marakas, 2006). En este sentido, el sistema permite a la empresa establecer estándares de información de manera idónea. Esta teoría sirve para analizar la influencia de información en cada uno de los sistemas informáticos a través del uso del sistema de ciberseguridad, para verificar que los datos de la empresa se encuentren protegidos y que la confidencialidad de la información está segura, de tal manera que exista un mayor control de los datos.

CAPÍTULO III

3. METODOLOGÍA

3.1. Metodología e instrumentos de recolección de información

3.1.1. Unidad de análisis

La unidad de análisis escogida es la empresa ECUATRAN S.A, empresa ambateña dedicada a la producción de transformadores eléctricos, con más de 40 años de experiencia en el mercado nacional e internacional. Dicha institución al ser grande y reconocida posee información importante y valiosa para su productividad. Por ello, con el fin de salvaguardar sus datos requiere de la protección de los sistemas informáticos.

La empresa opera un sinnúmero de datos en varios sistemas que son utilizados por los departamentos. Por lo que, la protección de información es esencial para evitar la infiltración de usuarios no autorizados. De esta manera, el control de seguridad informática es importante para evitar ciberdelitos.

Se desarrolló una investigación de campo donde se determinó que, hace un par de años ECUATRAN sufrió de pérdida de información en los sistemas, provocando un gran impacto en su sistema operativo. Sin embargo, existía respaldos de información, lo que aportó significativamente para que las operaciones de la empresa no se vean afectados. Por esta razón, se vio la necesidad de implementar el control interno en ciberseguridad para prevenir que nuevos ataques cibernéticos ponga en riesgo la estabilidad de la entidad.

Además, existe el control de claves de los usuarios en los sistemas que utilizan. Puesto que, está diseñados para un cambio de contraseña cada 3 meses. Sin embargo, el sistema de seguridad requiere de más control puesto que la empresa ha visto la necesidad de tener un sistema más robusto que ayude a tener un mayor control de seguridad de los datos de cada área de la empresa.

3.1.2. Fuentes y técnicas de recolección de información

3.1.2.1. Fuentes de información primarias

Se aplicó una entrevista para conocer de forma general los aspectos de seguridad de la empresa. Además, el check list para verificar la seguridad de la empresa y una encuesta para conocer la perspectiva de los colaboradores de cómo está la protección de la información en la entidad. Cabe mencionar que, estos métodos fueron de gran ayuda para el análisis de los problemas de vulnerabilidades que posee la empresa

La entrevista con una duración aproximada de 5 minutos con 20 segundos fue efectuada al Analista Programador Senior de la empresa la Ing. Tannya Naranjo del departamento de sistemas, Cabe señalar, que fue aplicada el día viernes 29 de octubre del 2021 a las 10:22 am de forma presencial en la oficina de sistemas, para conocer a la entidad mediante la visita preliminar. De esta forma, se cumple con el proceso de investigación.

Tabla 2. Preguntas de la entrevista categorizadas

Pregunta	Dimensión o Categoría
1. ¿Qué sistemas informáticos son manejados en la empresa?	Sistemas Informáticos
2. ¿Cuáles son los problemas más comunes en tecnología de información que la empresa ha detectado?	Riesgos Informáticos
3. ¿Ha existido algún tipo de ciberdelito o problema similar en la empresa?	Riesgos Informáticos
4. ¿Qué tan importante es la seguridad informática para la empresa?	Seguridad Informática
5. ¿La empresa ha aplicado la metodología COSO 2017 para evaluar su sistema de control interno con respecto a la ciberseguridad?	Seguridad Informática
6. ¿Cuáles son las medidas de protección que aplica la empresa para evitar ciberdelitos?	Seguridad Informática
7. ¿Cada que tiempo se evalúa el control interno en la empresa?	Seguridad Informática
8. ¿Qué alternativas adicionales a los controles ha visto la empresa para dar solución al sistema de seguridad que maneja la entidad?	Seguridad Informática

Fuente: Flores (2021)

Elaborado por: Flores (2021)

De la misma manera, se aplicó el check list el 20 de diciembre del 2021 a nivel global de la empresa. A través de, la observación y evaluación para verificar que cada punto haya sido cumplido en base a la seguridad informática de acuerdo a las preguntas que se muestra a continuación.

Tabla 3. Preguntas del check list categorizado

Pregunta	Dimensión o Categoría
1. El personal operativo es capacitado sobre la seguridad en los sistemas de información.	Sensibilizando
2. Sensibiliza a los usuarios sobre buenas prácticas básicas de seguridad informática.	Sensibilizando
3. Controla riesgos sobre las maneras de compartir información.	Conociendo el sistema de información
4. Mantiene inventario de todas las cuentas, usuarios y permisos, siempre actualizado.	Conociendo el sistema de información
5. Existe procedimientos para el cambio de funciones de usuario y los controles de acceso.	Conociendo el sistema de información
6. Permite la conexión a la red de la empresa sólo a equipos controlados.	Conociendo el sistema de información
7. Existe identificación de los equipos que acceden a la red a través de claves de usuario/administrador.	Autenticando los accesos
8. Existe un control de acceso de los usuarios al sistema de información contable de la empresa.	Autenticando los accesos
9. Existe protección de las contraseñas de accesos a los sistemas informáticos contables de la empresa.	Autenticando los accesos
10. Cambia los elementos de autenticación por default sobre equipos y servicios.	Autenticando los accesos
11. Define y verifica la configuración de creación de contraseñas de usuario.	Autenticando los accesos
12. Privilegia alertas sobre la autenticación de contraseñas al momento del acceso.	Autenticando los accesos
13. Establece un nivel de seguridad mínimo para los equipos informáticos.	Estaciones de trabajo seguras
14. Existe un control de protección para las amenazas en medios extraíbles (memorias, USB).	Estaciones de trabajo seguras
15. Habilita y configura el firewall de las estaciones de trabajo.	Estaciones de trabajo seguras
16. Cifra datos confidenciales transmitidos por Internet.	Estaciones de trabajo seguras
17. Usa una herramienta de administración centralizada para estandarizar las políticas de seguridad.	Estaciones de trabajo seguras

18. Segmenta las redes por departamentos.	Asegurando la red
19. Garantiza la seguridad de las redes de acceso Wi-Fi.	Asegurando la red
20. Configura una puerta de acceso seguro a Internet.	Asegurando la red
21. Protege el servicio de correo electrónico profesional.	Asegurando la red
22. Controla y protege el acceso a la sala de servidores.	Asegurando la red
23. Usa protocolos de red seguros tan pronto como estén disponibles.	Asegurando la red
24. Existe fiabilidad con el servicio contratado de internet que utiliza la empresa.	Asegurando la red
25. Prohíbe el acceso a Internet desde las estaciones de trabajo o servidores utilizados para la administración del sistema de información.	Administración segura
26. Utiliza una red dedicada y separada para la administración del sistema de información.	Administración segura
27. Limita los permisos de administrador en las estaciones de trabajo.	Administración segura
28. Cuenta con medidas de protección físico para los equipos portátiles	Administración segura
29. Cifra datos confidenciales, especialmente en los equipos vulnerables al robo.	Seguridad para equipos portátiles
30. Asegura la conexión de red de estaciones de trabajo utilizadas en situación nómada.	Seguridad para equipos portátiles
31. Adopta políticas dedicadas a la seguridad de dispositivos portátiles.	Seguridad para equipos portátiles
32. Define políticas de actualización de los componentes del sistema de información.	Mantener actualizado el sistema de información
33. Anticipa la obsolescencia de software, hardware.	Mantener actualizado el sistema de información
34. Existe definida una política para copias de seguridad de la base de datos.	Supervisar, auditar y reaccionar
35. Designa un responsable para la seguridad del sistema de la información.	Supervisar, auditar y reaccionar
36. Tiene definido un procedimiento de gestión de incidentes de ciberseguridad.	Supervisar, auditar y reaccionar
37. Existe registros de auditorías informáticas realizadas a la entidad.	Supervisar, auditar y reaccionar
38. Los usuarios poseen respaldos individuales de sus equipos a cargo.	Supervisar, auditar y reaccionar

Fuente: Kippeo (2021)

Elaborado por: Flores (2021)

Además, las encuestas fueron aplicadas a varios miembros de los departamentos de ECUATRAN con un total 20 personas de acuerdo a como se muestra en la tabla.

Tabla 4. Personas encuestadas

Nombre	Cargo	Departamento
Jenrry Núñez	Asistente Programador	Departamento de Sistemas
Angélica Tirado	Analista de Logística y Exportaciones	Departamento de Logística
Carolina Arcos	Asistente Administrativa de Servicios y Garantías	Departamento de Garantías
Johanna Lagos	Asistente Administrativa Compras	Departamento de Compras
Ítalo Gaibor	Analista de Investigación y Desarrollo	Departamento de Investigación
Camila Martínez	Asistente Soporte Técnico	Departamento de Sistemas
Dennis Salazar	Auxiliar SIG	Departamento de Sistema Integral
Alexandra Ortiz	Asistente Financiera Contable	Departamento de Contabilidad
Eduardo Pacheco	Supervisor Seguridad Física	Departamento de Seguridad
Christian Montoya	Técnico de Servicios	Departamento Servicios
Xavier Gordillo	Líder de Ventas Internacionales	Departamento de Comercio Exterior
Gissela Medina	Analista de Producción	Departamento de producción
Erick Barrionuevo	Ingeniero de Diseño	Departamento de Diseño
Darío Campos	Ingeniero de Diseño Eléctrico	Departamento de Diseño
Paulina Adame	Analista Administrativa	Departamento Gerencial
Erick Manosalvas	Analista de Estructura	Departamento de Ingeniería
Valeria Baca	Auxiliar Contable	Departamento de Contabilidad
Santiago Carrasco	Subgerente de Ventas	Departamento de Ventas
Angela Freire	Líder SIG	Departamento de Sistema Integral
Jessica Mora	Asistente Administrativa Operaciones	Departamento de Producción

Fuente: Flores (2021)

Elaborado por: Flores (2021)

En la presente investigación se aplicó el cuestionario el 30-11-2021 de forma física para determinar la vulnerabilidades y riesgos que presenta en base a las preguntas que se muestra a continuación:

Tabla 5. Preguntas del cuestionario categorizado y escalas

Preguntas	Categoría	Escala
1.- ¿Ha firmado un acuerdo de confidencialidad?	Gobierno y Cultura	1. SI 2. NO 3. NO APLICA
2.- ¿Se han definido responsabilidades concretas para la seguridad de la información?	Modelo Operativo y de Negocios	1. SI 2. NO 3. NO APLICA
3.- ¿Existe una política que define cómo utilizar las tecnologías de la información y los datos de la empresa?	Modelo Operativo y de Negocios	1. SI 2. NO 3. NO APLICA
4.- ¿Existe una política para el uso privado de las tecnologías de la información de la empresa?	Modelo Operativo y de Negocios	1. SI 2. NO 3. NO APLICA
5.- ¿Está informado regularmente sobre las medidas de seguridad de la información?	Modelo Operativo y de Negocios	1. SI 2. NO 3. NO APLICA
6.- ¿Es capaz de identificar un virus o malware?	Modelo Operativo y de Negocios	1. SI 2. NO 3. NO APLICA
7.- ¿Gestiona el uso seguro de redes sociales y correo electrónico?	Modelo Operativo y de Negocios	1. SI 2. NO 3. NO APLICA
8.- ¿Conoce sobre la normativa pertinente de la seguridad de la información?	Modelo Operativo y de Negocios	1. SI 2. NO 3. NO APLICA
9.- ¿En caso de pérdida del dispositivo conoce el procedimiento a seguir?	Modelo Operativo y de Negocios	1. SI 2. NO 3. NO APLICA
10.- ¿Existe una política de la utilización de dispositivos móviles?	Modelo Operativo y de Negocios	1. SI 2. NO 3. NO APLICA
11.- ¿Conoce cómo actuar en caso de incidente de ciberseguridad?	Modelo Operativo y de Negocios	1. SI 2. NO 3. NO APLICA
12.- ¿Posee acceso a los sistemas como administrador?	Reporte y Tecnología	1. SI 2. NO 3. NO APLICA

13.- ¿Se revisan regularmente los perfiles de acceso y usuario de acuerdo a un ciclo definido previamente?	Reporte y Tecnología	1. SI 2. NO 3. NO APLICA
14.- ¿Los datos de los dispositivos se encuentran protegidos contra el acceso no autorizado?	Reporte y Tecnología	1. SI 2. NO 3. NO APLICA
15.- ¿Posee accesos a la infraestructura de las tecnologías de información solamente si son necesarios para el cumplimiento de las funciones?	Reporte y Tecnología	1. SI 2. NO 3. NO APLICA
16.- ¿Se ha capacitado acerca de la utilización de las Tecnologías de información, así como los datos de la empresa de forma segura?	Alineado con la Estrategia	1. SI 2. NO 3. NO APLICA
17.- ¿Se hacen copias de seguridad de los datos de la empresa?	Alineado con la estrategia	1. SI 2. NO 3. NO APLICA
18.- ¿Existe seguridad en caso de utilizar servicios de Cloud computing (nube)?	Alineado con la estrategia	1. SI 2. NO 3. NO APLICA

Fuente: Cepenven, (2021)

Elaborado por: Flores (2021)

3.2. Método de Análisis de Información

La entrevista fue realizada a una sola persona puesto que permitió conocer a la entidad con respecto a los sistemas de seguridad que aplicaban para el control tecnológico de los datos de la misma. Sin embargo, se aplicó el check list como verificación de las actividades de ciberseguridad que manejan en ECUATRAN. De esta forma, se logró obtener la información necesaria para el análisis del problema.

De acuerdo a la tabla 1.7 se fue tabulando las actividades que iba cumpliendo la empresa para el análisis pertinente.

Tabla 6. Check List categorizado

CATEGORÍA	PORCENTAJE DE CUMPLIMIENTO
SENSIBILIZANDO	
CONOCIENDO EL SISTEMA DE INFORMACIÓN	
AUTENTIFICACIÓN DE LOS ACCESOS	
ESTACIONES DE TRABAJO SEGURAS	
ASEGURANDO LA RED	
ADMINISTRACION SEGURA	
SEGURIDAD PARA EQUIPOS PORTÁTILES	
MANTENER ACTUALIZADO EL SISTEMA DE INFORMACIÓN	
SUPERVISAR, AUDITAR Y REACCIONAR	

Fuente: ECUATRAN (2021)

Elaborado por: Flores (2021)

Sin embargo, para el análisis comprensivo y la obtención de los resultados se procedió con el presente gráfico de líneas, donde se pudo observar los porcentajes de cumplimiento de acuerdo a la categoría. De tal manera, permitió detectar las vulnerabilidades en los procedimientos de seguridad. Siendo, este sistema un examinador potencial que aportó datos de interés a la empresa.

Figura 2. Análisis de datos del Check List



Fuente: ECUATRAN (2021)

Elaborado por: Flores (2021)

Para el tratamiento de los datos recolectados en las encuestas se tabuló las respuestas con el método de tablas de doble entrada. De acuerdo a (Justexw, 2018) afirma que este tipo de tabla registra datos de acuerdo a la recolección de la información en relación con las columnas y filas. De esta manera se analizó los resultados de forma clara y concisa.

Se utilizó de la tabla 1.8 para identificar las respuestas de acuerdo al cumplimiento de cada una de las preguntas que presentó la encuesta.

Tabla 7. Tabulación general de la aplicación de encuestas

PREGUNTA	CATEGORÍA	1 (SI)	2 (NO)	3 (NO APLICA)
Pregunta 1	Gobierno y Cultura			
Pregunta 2	Modelo Operativo y de Negocios			
Pregunta 3	Modelo Operativo y de Negocios			
Pregunta 4	Modelo Operativo y de Negocios			
Pregunta 5	Modelo Operativo y de Negocios			
Pregunta 6	Modelo Operativo y de Negocios			
Pregunta 7	Modelo Operativo y de Negocios			
Pregunta 8	Modelo Operativo y de Negocios			
Pregunta 9	Modelo Operativo y de Negocios			
Pregunta 10	Modelo Operativo y de Negocios			
Pregunta 11	Modelo Operativo y de Negocios			
Pregunta 12	Reporte y Tecnología			
Pregunta 13	Reporte y Tecnología			
Pregunta 14	Reporte y Tecnología			
Pregunta 15	Alineado con la estrategia			
Pregunta 16	Alineado con la estrategia			
Pregunta 17	Alineado con la estrategia			

Fuente: ECUATRAN (2021)

Elaborado por: Flores (2021)

Se requirió de la tabla 1.9 para analizar las respuestas de acuerdo al manejo de seguridad que efectuaba cada departamento según el cumplimiento.

Tabla 8. Análisis de datos de la aplicación de encuestas

CATEGORÍA	PORCENTAJE DE CUMPLIMIENTO
Gobierno y Cultura	
Modelo Operativo y de Negocios	
Reporte y Tecnología	
Alineado con la estrategia	

Fuente: ECUATRAN (2021)

Elaborado por: Flores (2021)

Se requirió de la figura 1.10 para el análisis pertinente de los datos recopilados en las encuestas de esta manera se localizó las fortalezas y vulnerabilidades de la entidad.

Figura 3. Análisis de datos de las encuestas



Fuente: ECUATRAN (2021)

Elaborado por: Flores (2021)

Para la fiabilidad de los datos se consideró el alfa de Cronbach que permitió que este análisis sea realizado con la seriedad que merita. Según Ruiz (2019) afirma que el alfa de Cronbach es un coeficiente que consiste en medir la fiabilidad de un instrumento o test. Así mismo, (García et al., 2010) manifiesta que es un modelo de consistencia interna que evalúa la fiabilidad de la prueba a través de un promedio de correlación entre ítems.

Tabla 9. Análisis del coeficiente de fiabilidad

ALFA	$\alpha=$	
NÚMERO DE PREGUNTAS	$K=$	
VARIANZA DE CADA ITEM	$V_i=$	
VARIANZA TOTAL	$V_t=$	

Fuente: ECUATRAN (2021)

Elaborado por: Flores (2021)

ISOTOOLS (2018) afirma que el COSO ERM 2017 es reconocido internacionalmente por ser un organismo regulador del riesgo y por cumplir procesos de control interno para la buena protección de las organizaciones. Por ello la importancia de la matriz de riesgos que permite la correcta evolución de los procesos efectuados. De igual forma la

aplicación de las Normas ISO 27000 que permite la fiabilidad y confidencialidad de la información. De acuerdo a NORMAS ISO (2022) manifiesta que estas normas consisten en medidas orientadas a la protección de la información garantizando la continuidad de la empresa preservando la confidencialidad, integridad y disponibilidad.

A través de los resultados obtenidos en las encuestas se realizó la tabla 1.11. matriz de riesgos en base a componente COSO 2017 y la determinación de la seguridad de la empresa con respecto a las vulnerabilidades que presenta de acuerdo a las NORMAS ISO 27000. De esta manera, se determinó el factor o nivel de riesgo, nivel de confianza, los controles inherentes y el enfoque de cumplimiento de las actividades de protección de información de la empresa. Finalmente, permitió establecer los resultados y las recomendaciones debidas para un mayor control de seguridad en la información.

Tabla 10. Matriz de riesgos con la aplicación del COSO 2017 e ISO 27000

NORMA ISO 27000	PRINCIPIO	COMPONENTE DEL COSO	PROCESO	TAREA	CONTROLES EXISTENTES			AMENAZA	RIESGO	EVALUACIÓN DE RIESGOS			TOTAL DEL RIESGO	TIPO DE RIESGO			SEMAFORIZACIÓN	TRATAMIENTO DEL RIESGO						
					DÉBIL	FUERTE	NO APLICA			NIVEL DE PROBABILIDAD	NIVEL DE IMPACTO	CLASIFICACIÓN DE RIESGOS		ALTO	MEDIO	BAJO		PREVENTIVO	DETECTIVO	CORRECTIVO	DESCRIPCIÓN DEL CONTROL	RESPONSABLE		
MONITOREO	CONFIDENCIALIDAD	GOBIERNO Y CULTURA	ÉTICA PROFESIONAL	FIRMA DE ACUERDO																				
MEDICIÓN	INTEGRIDAD		CONTROL DEL SISTEMA DE SEGURIDAD	RESPONSABILIDADES PARA LA SEGURIDAD DE INFORMACIÓN																				
MEDICIÓN	DISPONIBILIDAD	MODELO OPERATIVO Y DE NEGOCIOS	CONTROL DEL SISTEMA DE SEGURIDAD	POLÍTICAS DE LA UTILIZACIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y DATOS DE LA EMPRESA																				
MEDICIÓN	DISPONIBILIDAD		CONTROL DEL SISTEMA DE SEGURIDAD	POLÍTICA PARA EL USO PRIVADO DE TECNOLOGÍA DE INFORMACIÓN																				
MEDICIÓN	INTEGRIDAD		CONTROL DEL SISTEMA DE SEGURIDAD	PERSONAL INFORMADO SOBRE MEDIDAS DE SEGURIDAD DE INFORMACIÓN																				
MEDICIÓN	INTEGRIDAD		MANEJO DEL SISTEMA DE SEGURIDAD	PERSONAL CAPAZ DE DETECTAR MALWARE																				
MEDICIÓN	INTEGRIDAD		MANEJO DEL SISTEMA DE INFORMACIÓN	PERSONAL GESTIONA EL USO SEGURO DE REDES SOCIALES Y CORREO ELECTRÓNICO																				
MEDICIÓN	DISPONIBILIDAD		CONTROL DEL SISTEMA DE SEGURIDAD	PERSONAL CONOCE LA NORMATIVA DE SEGURIDAD DE INFORMACIÓN																				
MEDICIÓN	DISPONIBILIDAD		CONTROL DEL SISTEMA DE SEGURIDAD	PERSONAL CONOCE EL PROCEDIMIENTO EN CASO DE PERDIDA DE DISPOSITIVO																				
MEDICIÓN	DISPONIBILIDAD		CONTROL DEL SISTEMA DE SEGURIDAD	POLÍTICA DE LA UTILIZACIÓN DE DISPOSITIVOS MÓVILES																				
MEDICIÓN	INTEGRIDAD		CONTROL DEL SISTEMA DE SEGURIDAD	PERSONAL CONOCE COMO ACTUAR EN CASO DE INCIDENTE DE CIBERSEGURIDAD																				
ANÁLISIS	INTEGRIDAD		REPORTE Y TECNOLOGÍA	CONTROL DEL SISTEMA DE SEGURIDAD	REVISAN REGULARMENTE LOS PERFILES DE ACCESO Y USUARIOS																			
ANÁLISIS	INTEGRIDAD	CONTROL DEL SISTEMA DE SEGURIDAD		PROTEGEN LOS DATOS DE DISPOSITIVOS CONTRA ACCESO NO AUTORIZADO																				
EVALUACIÓN	INTEGRIDAD	REPORTE Y TECNOLOGÍA	MANEJO DEL SISTEMA DE INFORMACIÓN	ACCESOS A INFRAESTRUCTURAS DE LAS TI PARA EL CUMPLIMIENTO DE FUNCIONES NECESARIAS																				
EVALUACIÓN	INTEGRIDAD		CONTROL DEL SISTEMA DE SEGURIDAD	PERSONAL CAPAZ DE UTILIZAR LAS TECNOLOGÍAS DE INFORMACIÓN Y DATOS DE LA EMPRESA DE FORMA SEGURA																				
EVALUACIÓN	CONFIDENCIALIDAD		CONTROL DEL SISTEMA DE SEGURIDAD	EXISTENCIA DE COPIAS DE SEGURIDAD DE LOS DATOS DE LA EMPRESA																				
EVALUACIÓN	INTEGRIDAD		CONTROL DEL SISTEMA DE SEGURIDAD	UTILIZACIÓN SEGURA DE SERVICIOS DE CLOUD COMPUTING (NUBE)																				

Fuente: Ecuatran (2021)
 Elaborado por: Flores (2021)

CAPÍTULO IV

4. DESARROLLO DEL ANÁLISIS DE CASO

4.1. Análisis y categorización de la información.

ECUATRAN S.A. empresa industrial que maneja gran cantidad de información confidencial de sus actividades concentradas y almacenadas en su base de datos, la cual es gestionada por el centro de procesamiento informático que a más de dar soporte técnico se encargan de velar por la seguridad de dicha información, el análisis efectuado tanto al sistema de control interno como a los procesos de ciberseguridad empleando la metodología COSO 2017 y las NORMAS ISO 27000 han permitido verificar el cumplimiento de ciertos procesos y la identificación de ciertas vulnerabilidades, amenazas y riesgos en su sistema de ciberseguridad presentados a continuación:

De acuerdo a la tabla 1.12 se verificó el cumplimiento de las actividades de seguridad implementadas en ECUATRAN. A través de los porcentajes obtenidos de frecuencias como se detalla en el siguiente resumen.

Tabla 11. Análisis del Check List

CATEGORÍA	PORCENTAJE DE CUMPLIMIENTO
SENSIBILIZANDO	100
CONOCIENDO EL SISTEMA DE INFORMACIÓN	100
AUTENTIFICACIÓN DE LOS ACCESOS	100
ESTACIONES DE TRABAJO SEGURAS	100
ASEGURANDO LA RED	100
ADMINISTRACION SEGURA	60
SEGURIDAD PARA EQUIPOS PORTÁTILES	100
MANTENER ACTUALIZADO EL SISTEMA DE INFORMACIÓN	100
SUPERVISAR, AUDITAR Y REACCIONAR	80

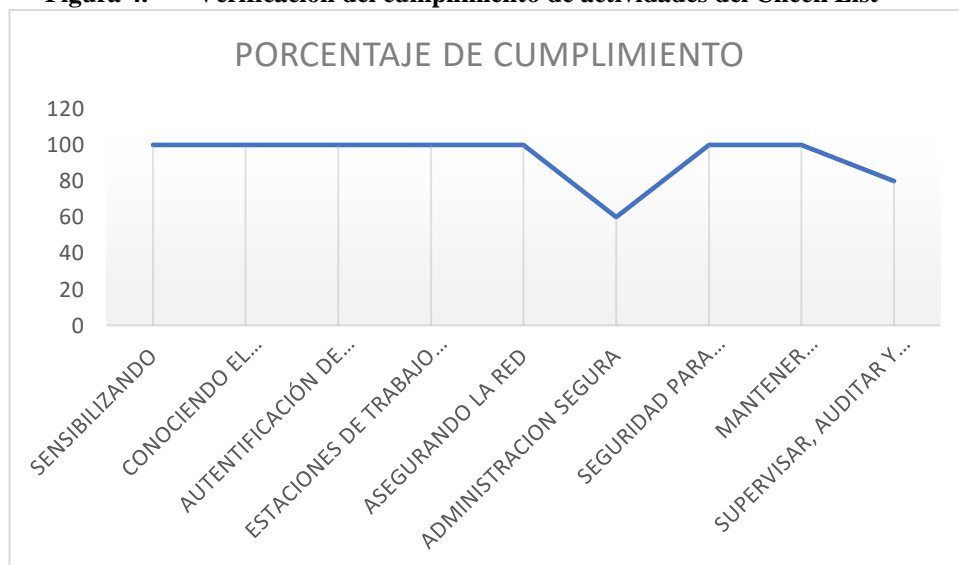
Fuente: ECUATRAN (2021)

Elaborado por: Flores (2021)

La empresa en la categoría de supervisión, auditoría y reacción cuentan con un 80% de cumplimiento. Puesto que, no poseen procedimientos de gestión de incidentes de ciberseguridad. De igual manera, no cuentan con registros de auditorías informáticas que reflejen como funciona la protección de los sistemas. Sin embargo, el personal del departamento informático se encarga de verificar personalmente y a través de su centro de operaciones, que no existan ciberdelitos en cada uno de los procesadores para evitar cualquier tipo de incidente cibernético.

La administración segura ha sido uno de los más importantes aspectos que toda organización debe tomar en cuenta. Puesto que, en el análisis del check list se ha detectado ciertas vulnerabilidades. Siendo, vulnerables a la toma de información por personal no autorizado o por malware que buscan el robo de información.

Figura 4. Verificación del cumplimiento de actividades del Check List



Fuente: ECUATRAN (2021)

Elaborado por: Flores (2021)

De esta manera, se identifican que la gran cantidad de actividades evaluadas en el check list se cumplen al 100%. Sin embargo, la administración segura posee un 60% de cumplimiento. Puesto que, no cuentan con medidas de protección físico para

equipos portátiles en caso de robo de información. Sin embargo, los miembros del departamento de TIC se encargan de dar soporte constante a los equipos.

Para el análisis exhaustivo, las encuestas reflejaron información como soporte de las prácticas de gestión de la protección de datos de la empresa. De esta manera, se detectó vulnerabilidades en los departamentos por falta de conocimiento de la defensa ante cualquier malware. Sin embargo, existen políticas definidas en ECUATRAN para contrastar dichos ataques pero que muchos aun no conocen.

Tabla 12. Análisis de las encuestas

PREGUNTA	CATEGORÍA	1 (SI)	2 (NO)	3 (NO APLICA)
Pregunta 1	Gobierno y Cultura	16	3	1
Pregunta 2	Modelo Operativo y de Negocios	15	5	0
Pregunta 3	Modelo Operativo y de Negocios	20	0	0
Pregunta 4	Modelo Operativo y de Negocios	18	0	2
Pregunta 5	Modelo Operativo y de Negocios	19	1	0
Pregunta 6	Modelo Operativo y de Negocios	11	9	0
Pregunta 7	Modelo Operativo y de Negocios	17	3	0
Pregunta 8	Modelo Operativo y de Negocios	9	11	0
Pregunta 9	Modelo Operativo y de Negocios	10	9	1
Pregunta 10	Modelo Operativo y de Negocios	10	7	3
Pregunta 11	Modelo Operativo y de Negocios	7	13	0
Pregunta 12	Reporte y Tecnología	12	5	3
Pregunta 13	Reporte y Tecnología	17	2	1
Pregunta 14	Reporte y Tecnología	12	7	1
Pregunta 15	Alineado con la estrategia	10	10	0
Pregunta 16	Alineado con la estrategia	17	1	2
Pregunta 17	Alineado con la estrategia	10	4	6

Fuente: ECUATRAN (2021)

Elaborado por: Flores (2021)

En el ámbito del uso de la tecnología la necesidad de revisar los accesos a los sistemas es fundamental para el control adecuado de personal autorizado a la información de la empresa. De esta manera, se centra en la importancia de la seguridad informática esencial donde la privacidad de la información esté protegida. De esta forma, se previene problemas financieros en la entidad.

El robo de la información es común en las organizaciones y más aún cuando no existe suficientes controles. Por ello, la tarea del departamento informático de que los funcionarios estén prevenidos en caso de ataques a su software. Así mismo, la protección de la empresa lo hacen todos para que la información no se vea vulnerable y afecte a la productividad de esta gran industria.

El soporte de seguridad que brinda el departamento TIC a los diferentes dispositivos, hace que la empresa posea grandes barreras ante los ciberdelincuentes. Por esta razón, la importancia de vigilar por un controlador que los usuarios no caigan en páginas fantasmas que provoquen virus a los procesadores. Así mismo, La importancia de las copias de seguridad en caso existen pérdida de la información.

Tabla 13. Análisis de las encuestas por categoría

CATEGORÍA	PORCENTAJE DE CUMPLIMIENTO
Gobierno y Cultura	80 %
Modelo Operativo y de Negocios	68 %
Reporte y Tecnología	68 %
Alineado con la estrategia	62 %

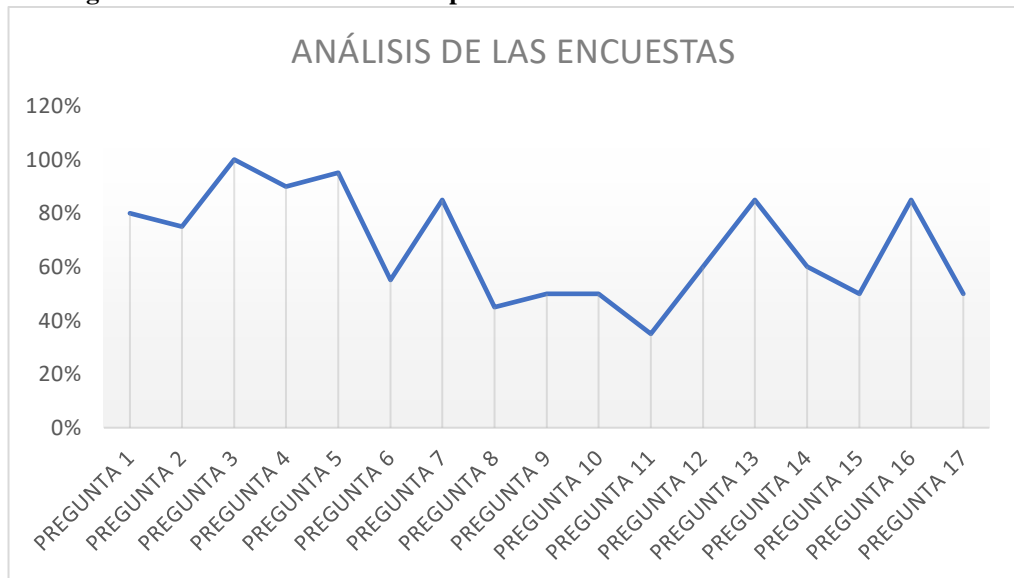
Fuente: ECUATRAN (2021)

Elaborado por: Flores (2021)

En la tabla 1.14. se identifican los porcentajes de cumplimiento por categoría. Sin embargo, existen actividades que no se cumplían al menos con el 50%. Por ello, la necesidad del análisis específico donde se muestre exactamente las vulnerabilidades de la institución.

La figura 1.12 indica el porcentaje de cumplimiento por actividad. De esta manera, se genera un mayor análisis de las vulnerabilidades en los procesos que maneja la institución para salvaguarda de la ciberseguridad. De tal forma, permite llegar a conclusiones exactas de los problemas suscitados.

Figura 5. Verificación del cumplimiento de actividades de las encuestas



Fuente: ECUATRAN (2021)

Elaborado por: Flores (2021)

De acuerdo al análisis de los datos que arrojan las encuestas se identifican que las actividades se cumplen moderadamente a excepción de las preguntas 8 y 11 que se efectúan con menos del 50%. Puesto que, varios de los colaboradores han manifestado que desconocen de la normativa de la seguridad de la información y la forma de actuar en caso existen incidentes de ciberseguridad. Siendo, un factor de vital importancia para contrastar el ataque y no permitir que se siga expandiendo puesto que podría provocar daños severos en el software y afectar directamente a todos los procesos generando pérdidas financieras a la entidad. Sin embargo, el departamento informático toma en consideración las respectivas medidas en el caso de ataques.

Para la confiabilidad y consistencia del análisis de datos recopilados, se efectuó el alfa de Cronbach como instrumento de investigación. Donde, se obtuvo un 0,65 representando como bueno el análisis, de acuerdo a como se describe a continuación.

Tabla 14. Análisis de fiabilidad de resultados

ALFA	$\alpha=$	0,65
NÚMERO DE PREGUNTAS	$K=$	17
VARIANZA DE CADA ITEM	$V_i=$	5,16
VARIANZA TOTAL	$V_t=$	13,35

Fuente: Flores (2021)

Elaborado por: Flores (2021)

Siendo un análisis donde cuyo coeficiente indica fiabilidad buena en la investigación de los datos obtenidos en las encuestas, ya que se tomó de fuentes confiables y las preguntas fueron planteadas de acuerdo a investigaciones anteriores que realizaban otros autores, dando veracidad y seriedad al análisis. Siendo, de esta investigación un instrumento importante para la obtención de resultados buenos que permitan dar fortalecimiento a la institución en aspectos de ciberseguridad con la finalidad de contribuir a la protección segura de la información.

4.2. Narración del caso

ECUATRAN S.A empresa que aplica los procesos de ciberseguridad para la protección de la información mediante los controles internos en los sistemas operativos. Debido a que, la seguridad de la información en la empresa es de gran importancia. Puesto que, la mala utilización de los sistemas de información privados y los recursos internos pueden provocar desastrosas consecuencias en todas las áreas, generando problemas productivos y financieros.

Hace aproximadamente dos años atrás la empresa sufrió de un ataque cibernético, donde el servidor fue hackeado a gran escala. Puesto que, existió la pérdida de la información del almacén de todo un rango. De tal manera que, la recuperación de esta fue exhausta significando un golpe muy fuerte en la organización. Sin embargo, gracias a los respaldos se logró la continuidad de los procesos.

Debido a estos acontecimientos la empresa aplica las debidas medidas de protección como es la aplicación de copias de seguridad de la información importante de la empresa. Puesto que, los sistemas que manejan son utilizados por varios usuarios por lo que efectúan controles en los accesos. Igualmente, para una mayor eficiencia y protección del software se manejan con antivirus licenciados y que son renovados constantemente. Asimismo, como otro sistema de control cuidan los puertos de entrada externa como es en el caso de insertar USB a los dispositivos.

Para un mejor manejo en los sistemas operativos de la información digital, la empresa ha creado instrumentos para que los sistemas sean protegidos. Como es el caso de la implementación de documentos donde a través de políticas el usuario se compromete a salvaguardar la información de la empresa. De esta manera, se demuestra las seguridades que toma la empresa al momento de entregar un dispositivo y un usuario.

La empresa aplica un acta de entrega recepción de usuario y contraseña, misma que consta del lugar y fecha de la entrega formal de credenciales de acceso al ERP, AXIS, correo y mas sistemas que requiera el funcionario, además del nombre y cargo al que

pertenece. Así mismo en el documento se da a conocer un acuerdo de confidencialidad y reserva de la información privilegiada o no de la compañía y/o de sus accionistas, empresas relacionadas y clientes.

Cabe mencionar que, la información confidencias incluye, pero no se limita a sistemas tecnológicos, software y programas informáticos. Además, el acta hace hincapié a los diseños, planos, información financiera, información contable, información patrimonial, información sobre bienes y propiedades, derechos de autor, marcas, nombres comerciales, procesos administrativos. Cabe mencionar que, la información técnica sobre productos o cualquier otro proceso de la compañía, información sobre clientes, actividades de la compañía, patentes de invención, políticas de ventas, información sobre programas, modelos, estrategias, objetivos, políticas, proyectos, procesos, presupuestos, cronogramas, investigaciones, manuales y reglamentos no deberán ser revelados.

Todo funcionario que maneje información de ECUATRAN y/o de sus accionistas y empresas relacionadas deberá ser secreta y confidencial como acuerdo entre las dos partes. Así mismo, adoptan medidas y seguridades de que la información que se observe o se tenga directamente se guarde a estricta confidencialidad de forma indefinida aun cuando dejare de prestar sus servicios para la empresa. Además, en el acta menciona el alcance de usuario y contraseña donde se responsabilice del buen uso de las credenciales de acceso, misma que no deberá ser compartida. También, los sistemas de información serán utilizados solo para fines de ECUATRAN S.A. Finalmente, se concluye dicho documento con las firmas de responsabilidad del representante TICS que entrega y el funcionario que recibe.

La empresa ha capacitado a los funcionarios sobre la importancia de la seguridad de los sistemas de información. Puesto que, los cibercrimes se cometen con frecuencia en las organizaciones con el fin de robar la información. Sin embargo, el departamento de sistemas toma las respectivas medidas ya que se ha difundido de las buenas prácticas para el desarrollo de la protección de datos.

El departamento de TIC se responsabiliza de velar que cada dispositivo funcione a cabalidad. Puesto que, si en algún departamento se ve afectado por errores en los servidores, rápidamente se encargan de dar soporte a tiempo para prevenir que cualquier malware se introduzca en los sistemas de la empresa. Además, se encargan de controlar los riesgos en caso se comparta la información.

Poseen un inventario de todas las cuentas de accesos siempre actualizados para verificación de los sistemas, además de controles a los sistemas informáticos contables de la empresa en caso personal no autorizado se introduzca a ver datos confidenciales de este departamento. Además, existen seguridad en todos los departamentos puesto que las funciones de los sistemas solo son habilitados de acuerdo a la necesidad del funcionario evitando así el acceso a todo el sistema empresarial.

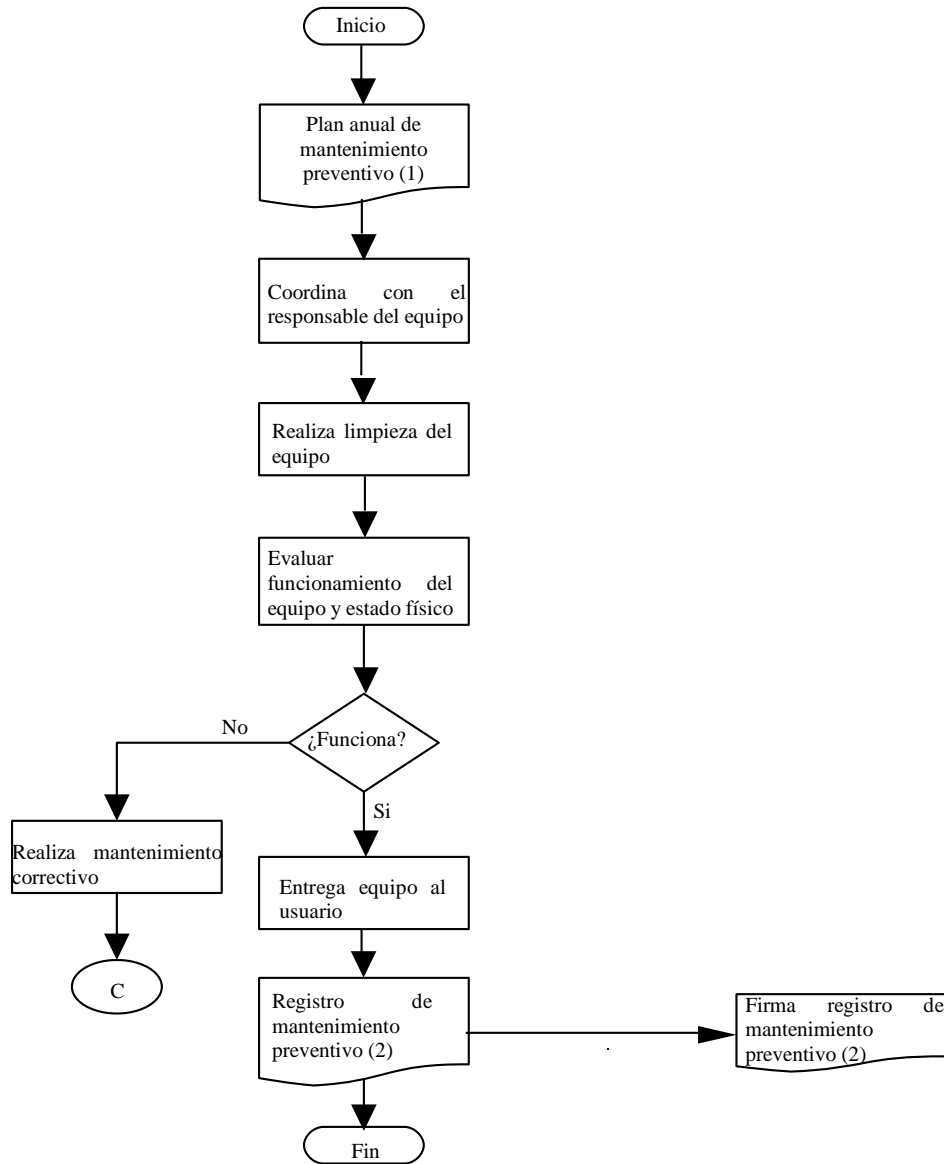
Con respecto a la conexión de internet se garantiza la seguridad de red, manteniendo un registro de los dispositivos conectados y a través del centro de operaciones siguen de cerca este proceso, Cabe mencionar que, la red de la empresa es para equipos controlados. Además, poseen alertas de ingresos de autenticación de contraseñas para el acceso de los sistemas. También, existen controles de cortafuegos que bloquean los accesos no autorizados a los sistemas, además de la protección a los correos electrónicos profesionales y el acceso a la sala de servidores

La empresa no cuenta medidas de protección físico para equipos portátiles en caso de robo de información. Además, los respaldos de información no poseen todos los usuarios, solo la alta gerencia lo que provoca gran dificultad en los departamentos al momento que la información se pierde puesto que no se puede recuperar. Tampoco, posee registros de auditorías informáticas para verificar el impacto de seguridad que posee ECUATRAN S.A. Sin embargo, el departamento de TIC toma en cuenta todos los procesos de ciberseguridad con las medidas de protección correspondientes aplicando los flujogramas para la realización de las actividades.

A continuación, se muestra los procesos creados por la empresa para un mejor control informático para evitar riesgos en la pérdida de información.

Figura 6. Flujograma de Mantenimiento Preventivo

Mantenimiento Preventivo	
TI	Entrada
Asistente Soporte Técnico	Usuario

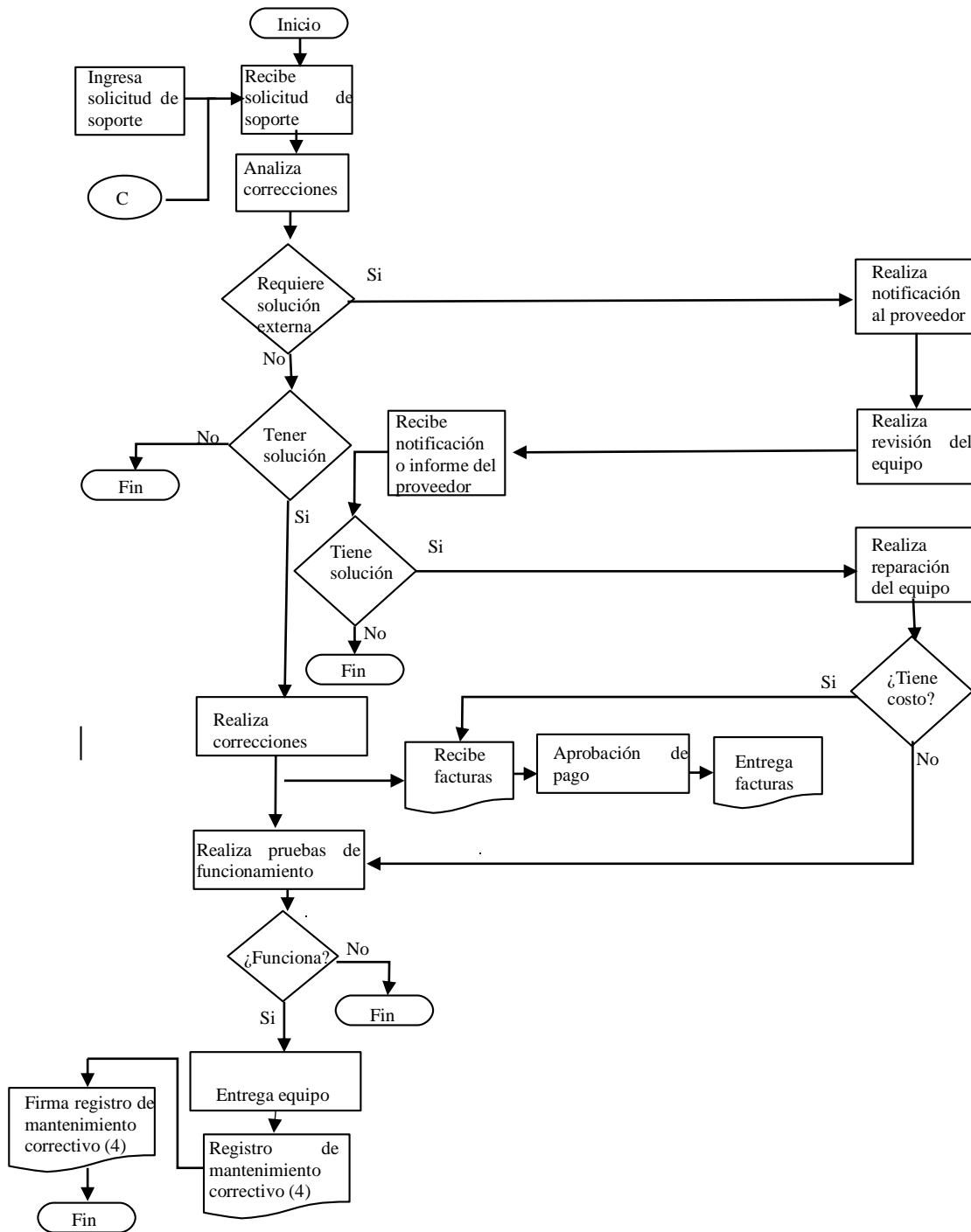


Fuente: ECUATRAN (2021)

Elaborado por: Flores (2021)

Figura 7. Flujograma de Mantenimiento Correctivo

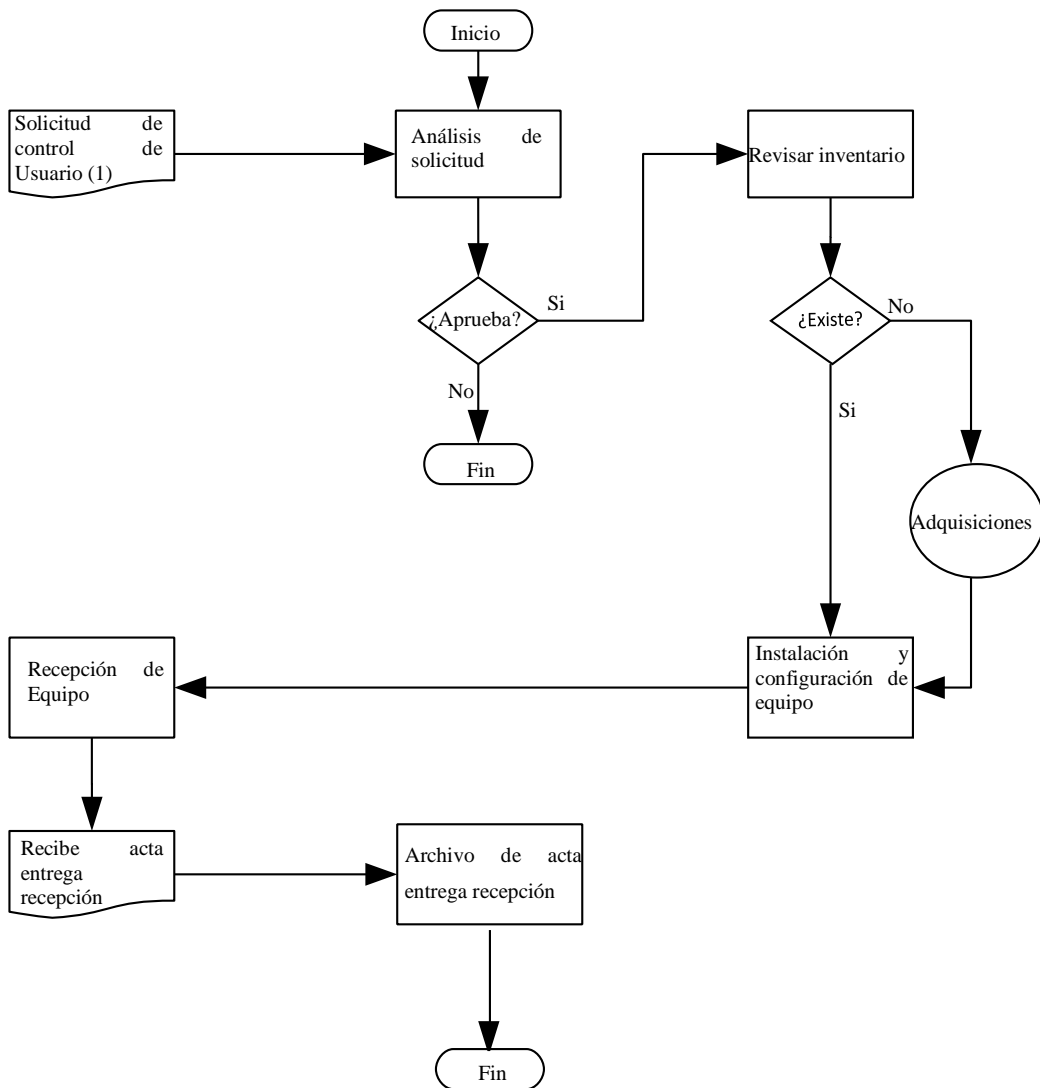
Mantenimiento Correctivo					
Entrada	TI		Financiero	Contabilidad	Proveedor
Usuario	Asistente Soporte Técnico	Representante TI	Sugerente General	Asistente Contabilidad	Proveedor



Fuente: ECUATRAN (2021)
 Elaborado por: Flores (2021)

Figura 8. Flujograma de Solicitud de Hardware y Software

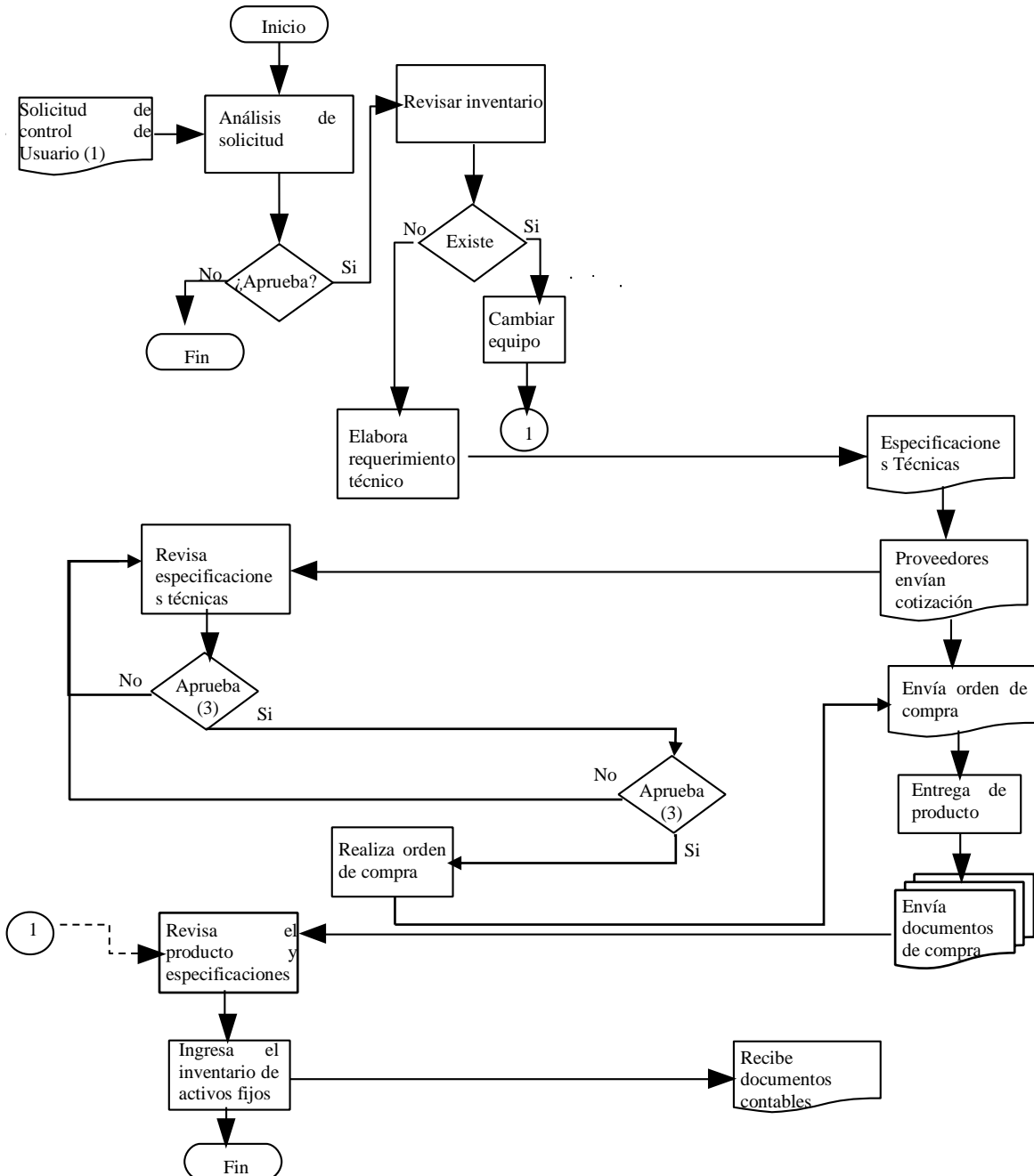
SOLICITUD DE HARDWARE Y SOFTWARE		
Usuario	TI	
Entrada	Representante TI	Asistente Soporte Técnico



Fuente: ECUATRAN (2021)
 Elaborado por: Flores (2021)

Figura 9. Flujograma de Adquisiciones

ADQUISICIONES					
Entrada	Sistemas Informáticos		Gestión Financiera		Proveedor
Usuario	Representante TI	Asistente Soporte Técnico	Sugerente General	Contabilidad	Proveedor

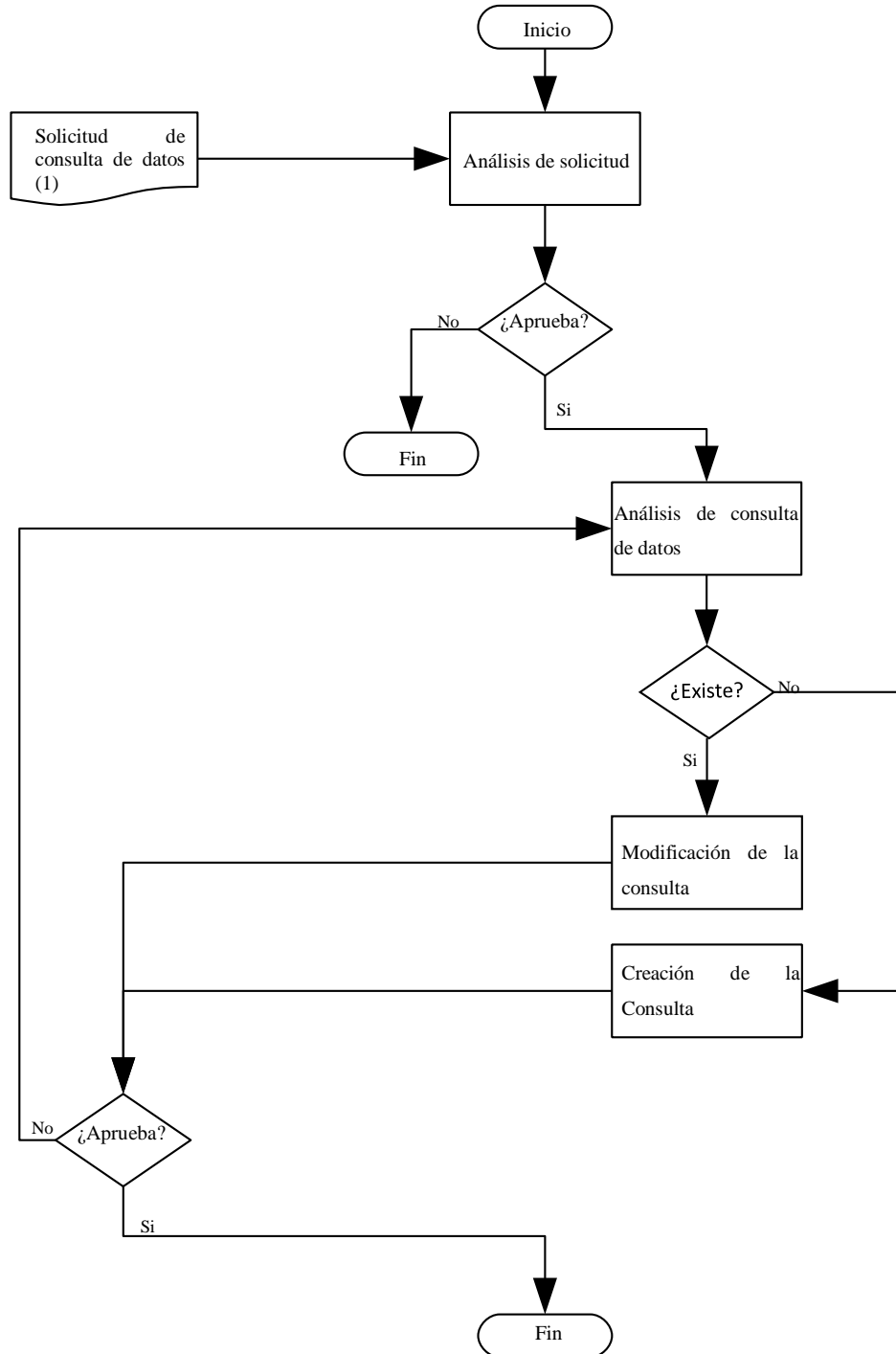


Fuente: ECUATRAN (2021)

Elaborado por: Flores (2021)

Figura 10. Flujograma de Solicitud de Consulta de Datos

SOLICITUD DE CONSULTA DE DATOS		
Usuario	TI	
Entrada	Representante de TI	Analista Programador

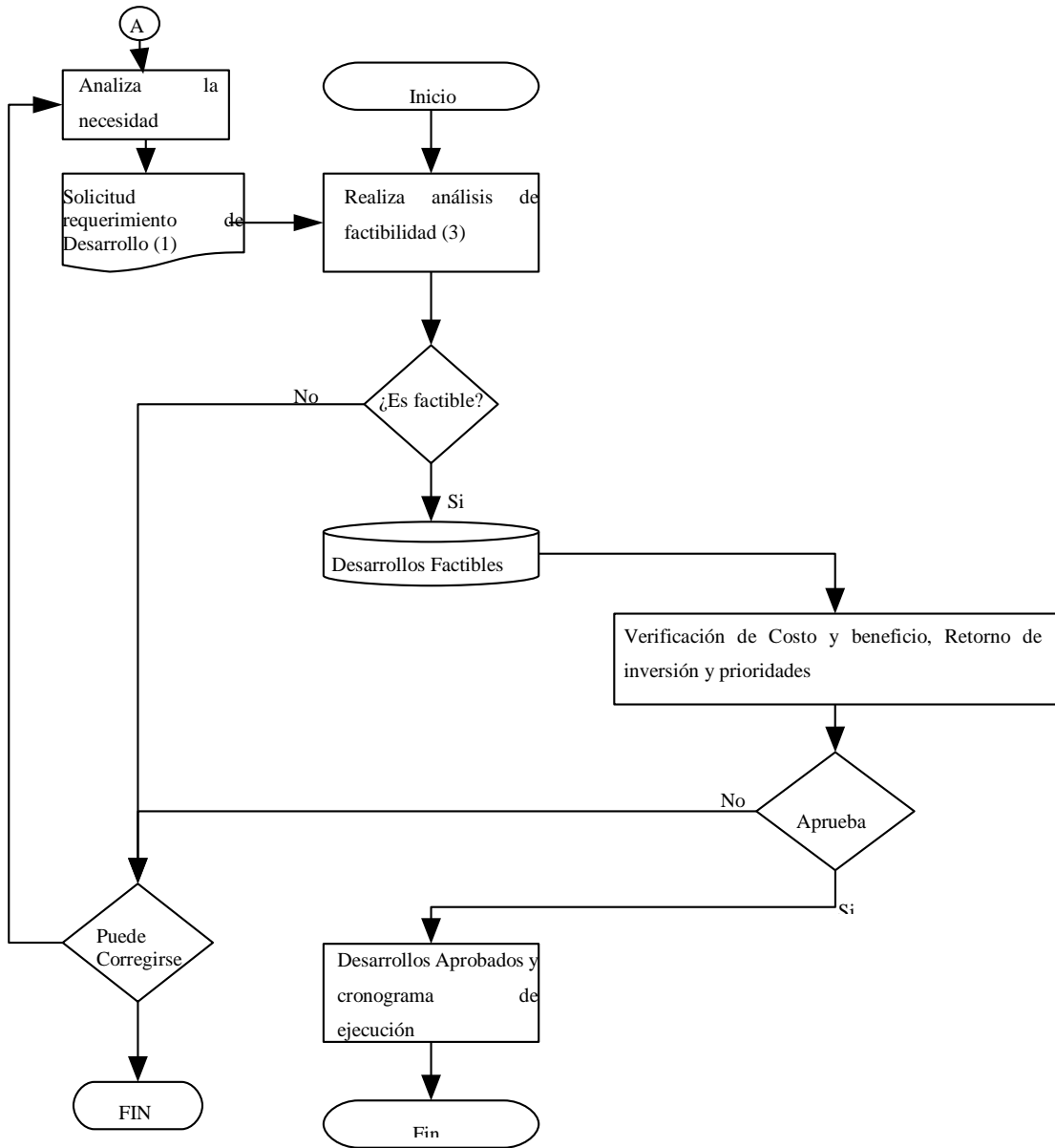


Fuente: ECUATRAN (2021)

Elaborado por: Flores (2021)

Figura 11. Flujograma de Solicitud de Requerimiento de Desarrollo

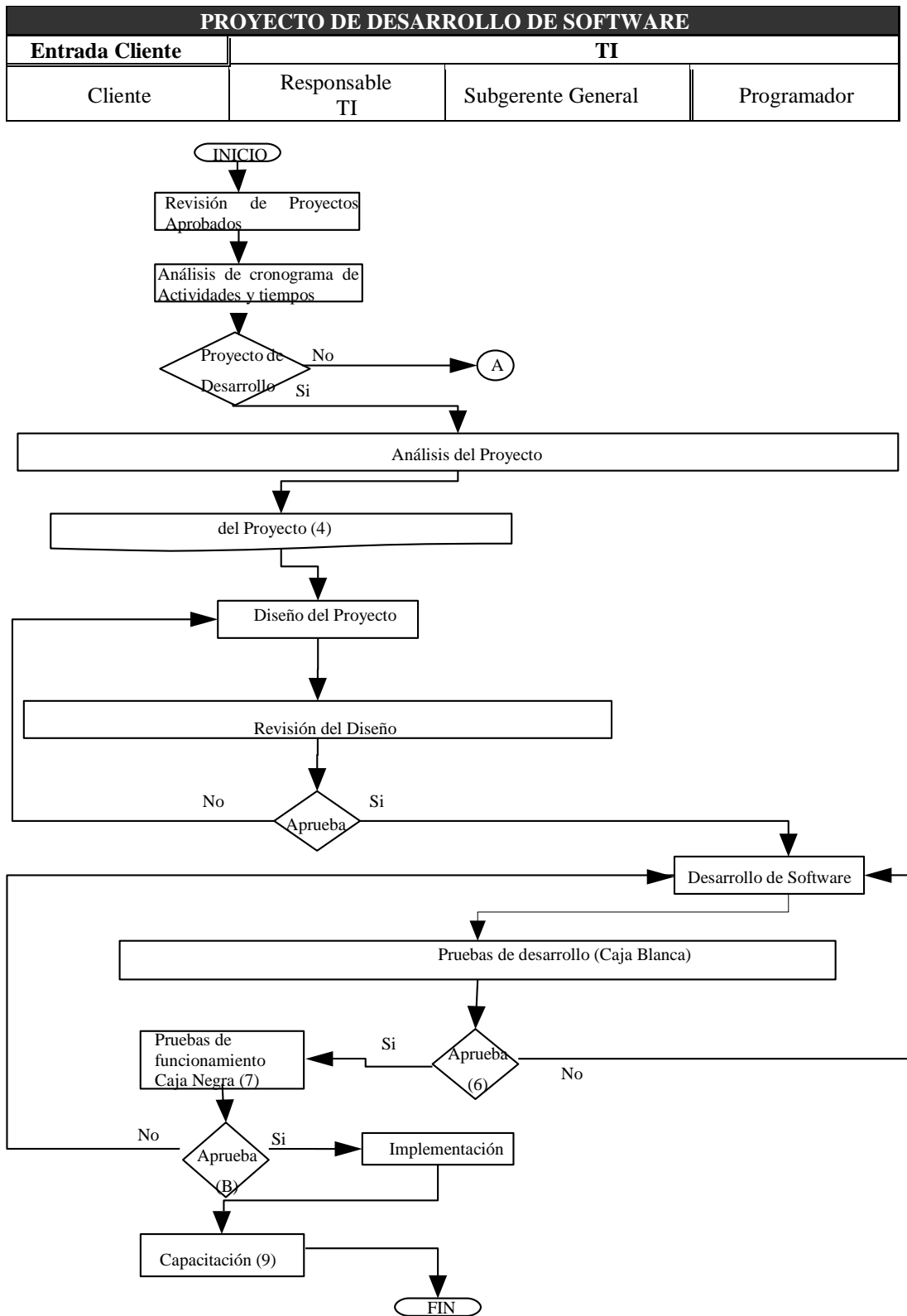
SOLICITUD DE REQUERIMIENTO DE DESARROLLO			
ENTRADA CLIENTE	SISTEMAS INORMÁTICOS	REVISIÓN GENERAL	GESTIÓN INANCIERA
Usuario	Representante de TI	Gerente General	Subgerente General



Fuente: ECUATRAN (2021)

Elaborado por: Flores (2021)

Figura 12. Flujograma de Proyecto de Desarrollo de Software



Fuente: ECUATRAN (2021)

Elaborado por: Flores (2021)

Los procesos de ciberseguridad que aplica la empresa son muy eficientes. Puesto que, el análisis realizado ha generado grandes resultados positivos con respecto a la protección de los ordenadores y su contenido. Es decir, el control y acceso a los sistemas y redes de internet por personal no autorizado, los robos informáticos y las modificaciones de información que causan los malware, son aspectos que la empresa previene para evitar futuros desastres, que perjudique el crecimiento laboral y económico de la misma.

En la presente matriz Tabla 1.14 y Tabla 1.15. se muestra un análisis detallado de las seguridades de información por actividades.

Tabla 15. El Riesgo según el Sistema COSO 2017 y la relación con las NORMAS ISO 27000

NORMA ISO 27000	PRINCIPIO	COMPONENTE DEL COSO	PROCESO	TAREA	CONTROLES EXISTENTES			AMENAZA	RIESGO	EVALUACION DE RIESGOS			TOTAL DEL RIESGO
					DÉBIL	FUERTE	NO APLICA			NIVEL DE PROBABILIDAD	NIVEL DE IMPACTO	CLASIFICACION DE RIESGOS	
MONITOREO	CONFIDENCIALIDAD	GOBIERNO Y CULTURA	ÉTICA PROFESIONAL	FIRMA DE ACUERDO		X		DIVULGACIÓN DE LA INFORMACIÓN	EMPRESA PIERDE PROPIEDAD INTELECTUAL, INGRESOS Y REPUTACIÓN DE LA MARCA	2	3	6	B: Bajo
MEDICIÓN	INTEGRIDAD	MODELO OPERATIVO Y DE NEGOCIOS	CONTROL DEL SISTEMA DE SEGURIDAD	RESPONSABILIDADES PARA LA SEGURIDAD DE INFORMACIÓN		X		VULNERABILIDAD DE LA INFORMACIÓN	FRAUDE CIBERNÉTICO	2	4	8	B: Bajo
MEDICIÓN	DISPONIBILIDAD	ESTRATEGIA Y OBJETIVOS	CONTROL DEL SISTEMA DE SEGURIDAD	POLÍTICAS DE LA UTILIZACIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y DATOS DE LA EMPRESA		X		INADECUADA PROTECCIÓN DE LA INFORMACIÓN	ROBO DE INFORMACIÓN Y MALA UTILIZACIÓN DE LAS TECNOLOGÍAS	1	1	1	NS: No significativo
MEDICIÓN	DISPONIBILIDAD	ESTRATEGIA Y OBJETIVOS	CONTROL DEL SISTEMA DE SEGURIDAD	POLÍTICA PARA EL USO PRIVADO DE TECNOLOGÍA DE INFORMACIÓN		X		INFORMACIÓN CONFIDENCIAL VULNERABLE	VANDALISMO EN LÍNEA	1	2	2	NS: No significativo
MEDICIÓN	INTEGRIDAD	DESEMPEÑO	CONTROL DEL SISTEMA DE SEGURIDAD	PERSONAL INFORMADO SOBRE MEDIDAS DE SEGURIDAD DE INFORMACIÓN		X		PÉRDIDA DE LA INFORMACIÓN	INFORMACIÓN UTILIZADA POR LA COMPETENCIA	1	2	2	NS: No significativo
MEDICIÓN	INTEGRIDAD		MANEJO DEL SISTEMA DE SEGURIDAD	PERSONAL CAPAZ DE DETECTAR MALWARE	X			SISTEMA INFECTADO DE SOFTWARE MALICIOSO	ROBO DE DATOS, DISMINUCIÓN DE LA VELOCIDAD DEL COMPUTADOR, INFILTRACIÓN DE LOS CORREOS ELECTRÓNICOS	3	4	12	A: Apreciable
MEDICIÓN	INTEGRIDAD		MANEJO DEL SISTEMA DE INFORMACIÓN	PERSONAL GESTIONA EL USO SEGURO DE REDES SOCIALES Y CORREO ELECTRÓNICO		X		REDES SOCIALES Y CORREOS VULNERABLES	ATAQUES DE PHISHING	1	2	2	NS: No significativo
MEDICIÓN	DISPONIBILIDAD		CONTROL DEL SISTEMA DE SEGURIDAD	PERSONAL CONOCE LA NORMATIVA DE SEGURIDAD DE INFORMACIÓN	X			INSEGURIDAD DEL SISTEMA DE INFORMACIÓN	AGUJERO DE SEGURIDAD	3	4	12	A: Apreciable
MEDICIÓN	DISPONIBILIDAD		CONTROL DEL SISTEMA DE SEGURIDAD	PERSONAL COONOCE EL PROCEDIMIENTO EN CASO DE PÉRDIDA DE DISPOSITIVO	X			INFORMACIÓN DISPONIBLE A PERSONAL NO AUTORIZADO	AUMENTO DE COMPETENCIA POR CONOCIMIENTO DE INFORMACIÓN	3	4	12	A: Apreciable
MEDICIÓN	DISPONIBILIDAD		ESTRATEGIA Y OBJETIVOS	CONTROL DEL SISTEMA DE SEGURIDAD	POLÍTICA DE LA UTILIZACIÓN DE DISPOSITIVOS MÓVILES	X			INADECUADA UTILIZACIÓN DE LOS DISPOSITIVOS MÓVILES DE LA EMPRESA	INFILTRACIÓN DEL SOFTWARE PERSONAL A LOS DATOS DE LA EMPRESA	3	4	12
MEDICIÓN	INTEGRIDAD	DESEMPEÑO	CONTROL DEL SISTEMA DE SEGURIDAD	PERSONAL CONOCE COMO ACTUAR EN CASO DE INCIDENTE DE CIBERSEGURIDAD	X			DESCONOCIMIENTO DE PROCEDIMIENTOS A SEGUIR EN CASO INCIDENTES CIBERNÉTICOS	ATAQUES DE PHISHING	4	4	16	I: Importante
ANÁLISIS	INTEGRIDAD	REVISIÓN	CONTROL DEL SISTEMA DE SEGURIDAD	REVISAN REGULARMENTE LOS PERFILES DE ACCESO Y USUARIOS	X			FILTRACIÓN DE BACKDOOR	ACCESOS NO AUTORIZADOS A SISTEMAS DE LA EMPRESA	3	4	12	A: Apreciable
ANÁLISIS	INTEGRIDAD		CONTROL DEL SISTEMA DE SEGURIDAD	PROTEGEN LOS DATOS DE DISPOSITIVOS CONTRA ACCESO NO AUTORIZADO	X			NO EXISTE CONTROL DE ACCESO A LOS SISTEMAS	PÉRDIDA DE INFORMACIÓN	1	2	2	NS: No significativo
EVALUACIÓN	INTEGRIDAD	INFORMACIÓN, COMUNICACIÓN Y REPORTE	MANEJO DEL SISTEMA DE INFORMACIÓN	ACCESOS A INFRAESTRUCTURAS DE LAS TI PARA EL CUMPLIMIENTO DE FUNCIONES NECESARIAS		X		INADECUADO MANEJO TECNOLÓGICO	DEFICIENCIA LABORAL	3	3	9	B: Bajo
EVALUACIÓN	INTEGRIDAD		CONTROL DEL SISTEMA DE SEGURIDAD	PERSONAL CAPAZ DE UTILIZAR LAS TECNOLOGÍAS DE INFORMACIÓN Y DATOS DE LA EMPRESA DE FORMA SEGURA	X			INADECUADA UTILIZACIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN	FUGA DE DATOS	3	4	12	A: Apreciable
EVALUACIÓN	CONFIDENCIALIDAD	CONTROL DEL SISTEMA DE SEGURIDAD	EXISTENCIA DE COPIAS DE SEGURIDAD DE LOS DATOS DE LA EMPRESA		X		RANSOMWARE	PÉRDIDA DE DATOS	1	4	4	NS: No significativo	
EVALUACIÓN	INTEGRIDAD	CONTROL DEL SISTEMA DE SEGURIDAD	UTILIZACIÓN SEGURA DE SERVICIOS DE CLOUD COMPUTING (NUBE)	X			SUPLANTACIÓN DE IDENTIDAD POR SPOOFING	INFORMACIÓN DE LA NUBE EXPUESTA A TERCEROS E INCLUSO ROBADA	3	4	12	A: Apreciable	

Fuente: ECUATRAN (2021)

Elaborado por: Flores (2021)

Tabla 16. El Riesgo según el Sistema COSO 2017 y la relación con las NORMAS ISO 27000

NORMA ISO 27000	PRINCIPIO	COMPONENTE DEL COSO	PROCESO	TAREA	TIPO DE RIESGO			SEM AFORIZACIÓN	CONTROL			DESCRIPCIÓN DEL CONTROL	RESPONSABLE	
					ALTO	MEDIO	BAJO		PREVENTIVO	DETECTIVO	CORRECTIVO			
MONITOREO	CONFIDENCIALIDAD	GOBIERNO Y CULTURA	ÉTICA PROFESIONAL	FIRMA DE ACUERDO			X	RIESGO MEDIO	X			IMPORTANCIA DE FIRMA DE ACUERDO DE RESPONSABILIDAD A TODOS LOS COLABORADORES DE A ENTIDAD	DEPARTAMENTO DE SISTEMAS	
MEDICIÓN	INTEGRIDAD	MODELO OPERATIVO Y DE NEGOCIOS	CONTROL DEL SISTEMA DE SEGURIDAD	RESPONSABILIDADES PARA LA SEGURIDAD DE INFORMACIÓN			X	RIESGO MEDIO	X			RESPONSABILIDADES DE LA PROTECCIÓN DE LA INFORMACIÓN	TODOS LOS DEPARTAMENTOS	
MEDICIÓN	DISPONIBILIDAD	ESTRATEGIA Y OBJETIVOS	CONTROL DEL SISTEMA DE SEGURIDAD	POLÍTICAS DE LA UTILIZACIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y DATOS DE LA EMPRESA			X	RIESGO BAJO	X			NO APLICA	NO APLICA	
MEDICIÓN	DISPONIBILIDAD	ESTRATEGIA Y OBJETIVOS	CONTROL DEL SISTEMA DE SEGURIDAD	POLÍTICA PARA EL USO PRIVADO DE TECNOLOGÍA DE INFORMACIÓN			X	RIESGO BAJO	X			IMPLEMENTACIÓN DE POLÍTICAS PARA EL USO PRIVADO DE LAS TECNOLOGÍAS DE INFORMACIÓN	TODOS LOS DEPARTAMENTOS	
MEDICIÓN	INTEGRIDAD	DESEMPEÑO	CONTROL DEL SISTEMA DE SEGURIDAD	PERSONAL INFORMADO SOBRE MEDIDAS DE SEGURIDAD DE INFORMACIÓN			X	RIESGO BAJO	X			CAPACITAR AL PERSONAL CONSTANTEMENTE SOBRE LAS MEDIDAS DE PREVENCIÓN DE LA INFORMACIÓN	TODOS LOS DEPARTAMENTOS	
MEDICIÓN	INTEGRIDAD		MANEJO DEL SISTEMA DE SEGURIDAD	PERSONAL CAPAZ DE DETECTAR MALWARE		X		RIESGO MEDIO			X		CAPACITAR AL PERSONAL ACERCA DE LA FORMA DE IDENTIFICAR UN MALWARE	TODOS LOS DEPARTAMENTOS
MEDICIÓN	INTEGRIDAD		MANEJO DEL SISTEMA DE INFORMACIÓN	PERSONAL GESTIONA EL USO SEGURO DE REDES SOCIALES Y CORREO ELECTRÓNICO			X	RIESGO BAJO	X				CAPACITAR AL PERSONAL DE LAS FORMAS SEGURAS DE LA UTILIZACIÓN DE REDES SOCIALES Y CORREOS ELECTRÓNICOS DE LA EMPRESA	TODOS LOS DEPARTAMENTOS
MEDICIÓN	DISPONIBILIDAD		CONTROL DEL SISTEMA DE SEGURIDAD	PERSONAL CONOCE LA NORMATIVA DE SEGURIDAD DE INFORMACIÓN		X		RIESGO MEDIO			X		IMPLEMENTACIÓN DE NORMATIVA DE LA SEGURIDAD DE INFORMACIÓN	TODOS LOS DEPARTAMENTOS
MEDICIÓN	DISPONIBILIDAD		CONTROL DEL SISTEMA DE SEGURIDAD	PERSONAL CONOCE EL PROCEDIMIENTO EN CASO DE PÉRDIDA DE DISPOSITIVO		X		RIESGO MEDIO			X		IMPLEMENTAR UN FLUJOGRAMA DE PROCEDIMIENTOS A SEGUIR EN CASO DE PÉRDIDA DE DISPOSITIVOS MÓVILES DE LA EMPRESA	TODOS LOS DEPARTAMENTOS QUE MANEJEN DISPOSITIVOS MÓVILES DEL TRABAJO
MEDICIÓN	DISPONIBILIDAD		CONTROL DEL SISTEMA DE SEGURIDAD	POLÍTICA DE LA UTILIZACIÓN DE DISPOSITIVOS MÓVILES		X		RIESGO MEDIO			X		IMPLEMENTAR POLÍTICAS DE LA ADECUADA UTILIZACIÓN DE LOS DISPOSITIVOS MÓVILES EMPRESARIALES	TODOS LOS DEPARTAMENTOS
MEDICIÓN	INTEGRIDAD		CONTROL DEL SISTEMA DE SEGURIDAD	PERSONAL CONOCE COMO ACTUAR EN CASO DE INCIDENTE DE CIBERSEGURIDAD		X		RIESGO ALTO				X	CAPACITAR AL PERSONAL LAS MEDIDAS DE PROTECCIÓN EN CASO DE ATAQUES DE CIBERSEGURIDAD	TODOS LOS DEPARTAMENTOS
ANÁLISIS	INTEGRIDAD	REVISIÓN	CONTROL DEL SISTEMA DE SEGURIDAD	REVISAN REGULARMENTE LOS PERFILES DE ACCESO Y USUARIOS	X			RIESGO MEDIO			X	REVISIÓN CONSTANTE DE LOS USUARIOS QUE INGRESAN A LOS SISTEMAS	DEPARTAMENTO DE SISTEMAS	
ANÁLISIS	INTEGRIDAD		CONTROL DEL SISTEMA DE SEGURIDAD	PROTEGEN LOS DATOS DE DISPOSITIVOS CONTRA ACCESO NO AUTORIZADO			X	RIESGO BAJO	X				PROTECCIÓN DE DATOS EMPRESARIALES A TRAVÉS DE CRIPTOGRAFÍA O FIREWALL	TODOS LOS DEPARTAMENTOS
EVALUACIÓN	INTEGRIDAD	INFORMACIÓN, COMUNICACIÓN Y REPORTE	MANEJO DEL SISTEMA DE INFORMACIÓN	ACCESOS A INFRAESTRUCTURAS DE LAS TI PARA EL CUMPLIMIENTO DE FUNCIONES NECESARIAS			X	RIESGO MEDIO		X		ACCESO A LAS TIC PARA EL CUMPLIMIENTO EFECTIVO DE FUNCIONES. EN DATOS CONFIDENCIALES ES NECESARIO SUPERVISIÓN Y APROBACIÓN A LA INFORMACIÓN	TODOS LOS DEPARTAMENTOS	
EVALUACIÓN	INTEGRIDAD		CONTROL DEL SISTEMA DE SEGURIDAD	PERSONAL CAPAZ DE UTILIZAR LAS TECNOLOGÍAS DE INFORMACIÓN Y DATOS DE LA EMPRESA DE FORMA SEGURA		X		RIESGO MEDIO		X			CAPACITACIÓN A PERSONAL DE LA CORRECTA UTILIZACIÓN DE LAS TIC Y EL MANEJO SEGURO DE LA INFORMACIÓN EMPRESARIAL	TODOS LOS DEPARTAMENTOS
EVALUACIÓN	CONFIDENCIALIDAD		CONTROL DEL SISTEMA DE SEGURIDAD	EXISTENCIA DE COPIAS DE SEGURIDAD DE LOS DATOS DE LA EMPRESA		X		RIESGO BAJO	X				DISEÑAR UNA COPIA DE SEGURIDAD O PLAN DE CONTINGENCIA EN LOS ARCHIVOS EMPRESARIALES	TODOS LOS DEPARTAMENTOS
EVALUACIÓN	INTEGRIDAD		CONTROL DEL SISTEMA DE SEGURIDAD	UTILIZACIÓN SEGURA DE SERVICIOS DE CLOUD COMPUTING (NUBE)		X		RIESGO MEDIO			X		IMPLEMENTAR UN PROTOCOLO CRIPTOGRÁFICO COMO EL TLS PARA LA COMUNICACIÓN SEGURA A TRAVÉS DE LA RED	DEPARTAMENTO DE SISTEMAS

Fuente: ECUATRAN (2021)

Elaborado por: Flores (2021)

De acuerdo al análisis de la matriz de riesgos se detecta que el personal no conoce las medidas a seguir en caso de incidente de ciberseguridad lo que provoca un riesgo alto. Puesto que, los malware avanzan hasta provocar severos daños en los sistemas y procesadores ya sea por ciberdelincuentes de phishing, pharming, keylogging o dependiendo la situación en la que se vea sometido el funcionario. Sin embargo, en los demás datos arrojados en la matriz se verifica que los riesgos no son de temer. Sin embargo, es importante tomarlos en cuenta.

La empresa ha adoptado como buenas prácticas los controles permanentes de cambios de configuraciones generales en toda la red, además de seguir con todas las medidas de seguridad implementadas. Cabe mencionar que, poseen un sistema de seguridad, el cual está perdiendo su vida útil, por lo que junto al equipo de TIC han generado un nuevo sistema más robusto que lo implementarán en la empresa apenas sea aprobado. Siendo para ECUATRAN la seguridad de información algo importante para el buen desarrollo de la organización y de sus colaboradores.

CAPÍTULO V

5. CONCLUSIONES Y RECOMENDACIONES

5.1. Conclusiones

- ECUATRAN S.A dispone de procedimientos de seguridad bien estructurados, los mismos que son aplicados de manera adecuada permitiendo que la información de la empresa se encuentre segura. Además de, contar con el personal suficientemente calificado que hace posible que el SGSI sea mejorado continuamente en la salvaguarda de la información. Sin embargo, se ha detectado que la institución no cuenta con registros de auditorías en seguridades de la información, lo cual fue un limitante para realizar una comparación del SGSI anteriormente implementado y sus cambios.

Por otro lado, las vulnerabilidades informáticas implican deficiencias por las que la infraestructura de la empresa está en riesgo de sufrir una amenaza de seguridad. La ausencia de las auditorías del sistema de información, el desconocimiento de la normativa o la ausencia de cualquier otro tipo de medida que no se ha socializado a su personal interno implica un alto riesgo de exposición de la compañía a brechas de seguridad. Por eso, los sistemas siempre deben garantizar la confidencialidad, la integridad y la disponibilidad de la información acorde a las directrices de los estándares establecidos.

- La metodología COSO 2017 aplicada para el análisis de la información permitió determinar los niveles de riesgo de la organización. De esta manera, se reflejó un nivel de riesgo alto por el desconocimiento de medidas que se deben tomar en cuenta en caso de que exista un ciberdelito. Puesto que, la gran mayoría de los funcionarios no conocen las normativas de seguridad ni las medidas de protección necesarias en caso de que se den

eventualidades de ciberdelito, reflejando en la matriz de riesgos aquellos que pueden provocar daños en la organización, siendo responsabilidad de todos conocer cómo proteger la información.

Existe un porcentaje del 35% correspondiente a una brecha roja debido al desconocimiento de casos a seguir en caso de incidentes cibernéticos. De esta manera se establece un riesgo (I) Importante de 16 considerado como alto. Para lo cual se determinó un control correctivo que favorezca a la institución para la solución del problema.

- De acuerdo a las normas 27001 y 27002 la ciberseguridad en la empresa cumple con las fases de monitoreo, medición, análisis y evaluación. Ya que, el personal informático hacía todo el trabajo de seguridades de información correcta y concretamente, pero los demás funcionarios desconocen de los temas de seguridades.

Mediante el monitoreo se ha firmado un acuerdo de confidencialidad representado un 80% de su cumplimiento. Sin embargo, la medición se lo representa con un 68% de su cumplimiento en relación con la integridad y disponibilidad de los controles y manejos de los sistemas. Además, el análisis generó un 73% de cumplimiento con respecto a las actividades de revisión de los sistemas. Finalmente, la evaluación que existe en la empresa posee el 61% de acuerdo a la comunicación, información y reporte del buen manejo y acceso a los sistemas de la empresa.

5.2. Recomendaciones

Desarrollar una cultura de seguridad de la información en toda la empresa que es de vital importancia para el cuidado de la misma, la implementación de normas y procedimientos para la utilización de dispositivos tecnológicos que encuentran conectados a internet deben considerar controles que den cumplimiento a dichas normas. Además, es importante realizar auditorías de la seguridad informática por lo menos una vez al año donde se registren datos que permitan tener un mejoramiento continuo en los procesos.

De acuerdo a los componentes del COSO 2017 ERM gobierno y cultura, modelo operativo y de negocios, estrategia y objetivos, desempeño, revisión información, comunicación y reporte, es recomendable que la empresa cuente con un plan de seguridad en que se establezcan las medidas y protocolos tanto de prevención y control en caso de producirse un incidente de tal magnitud. Además, es importante que su contenido delimite pasos a seguir para la gestión, mantenimiento y control de sus procesos informáticos y por ende de la salvaguarda de la información.

Una de las posiciones más importantes que se debe implementar en la empresa es el Cyber Security Analyst para el control del acceso, para planes de seguridad, evaluación de riesgo de red, etc. De esta manera, se pone en práctica el monitoreo, medición, análisis y evaluación según lo establece las normas ISO 27000.

Nunca proveer información confidencial a través de plataformas públicas en internet, no instalar programas si se desconoce al fabricante, siempre investigar la identidad de cada persona que solicite cualquier tipo de datos, evitar conectarse a redes de WiFi abiertas en computadoras de la empresa, utilizar un antivirus y mantenerlo actualizado, sacar copias de seguridad con frecuencia, mantener actualizado el software utilizado. Es importante que las empresas implementen soluciones de protección de la información.

La auditoría de ciberseguridad es una herramienta ideal para solventar estos problemas de seguridad y mantenerla a salvo. De esta manera, analizan la situación tecnológica a la misma, el rendimiento de la red, el cifrado de datos, las comunicaciones, las políticas de actualizaciones del hardware y el software y dan el aporte con una propuesta de seguridad perimetral. Además, detectar las vulnerabilidades de los sistemas para proponer mejoras tecnológicas aportando con las debidas recomendaciones para corregir errores en procedimientos y de configuración e identificación de las fortalezas, debilidades, amenazas y riesgos de ECUATRAN S.A. desde internet. Finalmente se logrará mitigarlos, compartiros, asumirlos según la gestión de riesgos que la empresa decida tomar como respuesta.

5.2.1. Plan de ciberseguridad

***PLAN
DE
CIBERSEGURIDAD***

ECUATRAN S.A.

Ambato, Parroquia Santa Rosa Calle Venezuela

3700100

ventas@ecuatran.com

INTRODUCCIÓN

El presente Plan estará enfocado al sistema de control interno a los procesos de ciberseguridad en la empresa ECUATRAN S.A. Además, consiste en dar las herramientas necesarias para la protección de la seguridad informática, brindando estrategias de defensa ante las vulnerabilidades que puedan presentarse. Para ello, es necesario partir del análisis situacional actual de la entidad.

Las medidas de control interno informático son importantes dentro de las empresas. Debido a que, el fraude abarca una serie de irregularidades y actos ilegales, también conocidos como engaños intencionales. Por esto, la situación informática en las organizaciones se ha visto amenazadas a través del tiempo.

Los datos que se aportará en el presente beneficiarán a los sistemas de información de la empresa ECUATRAN S.A. Puesto que, las estrategias recomendadas servirán como guía para establecer medidas de prevención o defensa ante los ataques cibernéticos. Permitiendo, fortalecer el nivel de ciberseguridad en la empresa como acción de la protección de información.

ALCANCE

El alcance del proyecto se enfoca principalmente al área de TIC, donde se pretende dar solución a los principales problemas como es la protección de activos intangibles y seguridad de la información, tratando de eliminar las principales debilidades y amenazas que tiene la actual infraestructura.

La evolución de las tecnologías de la información y comunicaciones, ha facilitado el cumplimiento de las actividades de la empresa. Y tienen tanta importancia la seguridad de información que sería imposible descuidarla.

OBJETIVOS

Objetivo general

Implementar acciones concretas en seguridad de la información con el propósito de lograr contrastar ciberataques en caso sea necesario.

Objetivos específicos

- Promover el adecuado bienestar de del sistema de seguridad a través de la aplicación de políticas
- Establecer medidas de protección de la seguridad de Información a través de las Normas ISO 27000
- Asegurar que las actividades de control se desarrollen a través de las normas y procedimientos de la seguridad de Información.

MARCO LEGAL

NORMAS ISO 27000

En palabras de Wang & Tsai (2009) Las series 27000 están enfocadas a la aplicación de buenas prácticas de acuerdo a la implantación, mantenimiento y gestión del Sistema de Gestión de Seguridad de la Información (SGSI) o por la denominación en inglés Information Security Management System (ISMS). En consecuencia, se dirigen a establecer las mejores prácticas en aspectos vinculados a la gestión de la seguridad de la información, direccionada a la mejora continua y a la mitigación de riesgos.

NORMAS ISO 27001

De acuerdo a Ladino et al. (2011) Especifica los requerimientos necesarios para la implantación y gestión en un SGSI, siendo certificable. Además, es considerada sencilla de implantar, automatizar y mantener con la Plataforma Tecnológica ISOTools. De esta manera, da cumplimiento a los requisitos basados en el ciclo PHVA (Planear – Hacer – Verificar – Actuar) para establecer, implementar, mantener y mejorar el SGSI, así como el cumplimiento oportuno y necesario de forma complementaria a las buenas prácticas o controles establecidos en ISO 27002.

NORMAS ISO 27002

De acuerdo a Ostec (2016) Señala que las Normas ISO 27002 son un conjunto de buenas prácticas para la implantación del SGSI, a través de 114 controles, estructurados en 14 dominios y 35 objetivos de controles. Además, establece ventajas por la certificación ISO 27002 que es representativa para las empresas, sobre todo porque son reconocidas mundialmente. Adicionalmente, señala beneficios asociados a la aplicación de la norma:

- Mejor concienciación sobre la seguridad de la información;
- Mayor control de activos e información sensible;
- Ofrece un enfoque para la implementación de políticas de control
- Oportunidad de identificar y corregir puntos débiles;

- Reducción del riesgo de responsabilidad por la no implementación de un SGSI o determinación de políticas y procedimientos;
- Se convierte en un diferencial competitivo para la conquista de clientes que valoran la certificación
- Mejor organización con procesos y mecanismos bien diseñados y gestionados;
- Promueve reducción de costos con la prevención de incidentes de seguridad de la información;
- Conformidad con la legislación y otras reglamentaciones.

NORMAS ISO 27018

De acuerdo a Mesquida et al. (2010) afirma que Permite el complemento de las normas 27001 y 27002 implantando procedimientos y controles como protección de los datos personales en aquellas organizaciones que proporcionan servicios en cloud para terceros.

Inspira confianza en su negocio: da una mayor seguridad a clientes y partes interesadas de que los datos y la información está protegida.

Ventaja competitiva:

- Permite diferenciarse de sus competidores mediante la protección de la información personal al más alto nivel.
- Protege su reputación de marca: Reduce el riesgo de publicidad negativa debido a las violaciones de datos.
- Reduce los riesgos: Garantiza la identificación de los riesgos y la aplicación de controles para su gestión o posible reducción
- Protege contra las multas: Garantiza que las normas locales se cumplan, lo cual implica una reducción del riesgo de multas por violaciones de datos.
- Ayuda a crecer a su negocio: Proporciona una guía común en diferentes países por lo que es más fácil hacer negocios a nivel mundial y obtener acceso como un proveedor preferido

RECOMENDACIONES

Tabla 17. Recomendaciones

ENFOQUE	POLÍTICA	PROCEDIMIENTO	DESCRIPCIÓN	CONTROLES	RESPONSABLES
DE REDES	instalación y actualización automática del software de protección.	Protección de Información	Aplicación de antivirus y cortafuegos o firewall.	Fortalecer la capacidad de los servicios digitales a través de la seguridad en el ciberespacio (VLAN)	Departamento TIC
	Copias de seguridad periódicas	Protección de Información	Respaldos de información en caso de ciberataque.	Fortalecer la seguridad de información	Departamento TIC
	Auditorías Internas de los procesos de ciberseguridad.	Protección de Información	Revisión de los procesos de seguridad de información.	Fortalecer los procesos SIG	Departamento TIC
	Auditoría de proveedores externos en servicios informáticos (PES)	Protección de Información	Delimitación de accesos a responsables de ciberataques	Fortalecer los puertos de acceso a los servidores	Departamento TIC
	Cumplimiento de las normativas legales que registra la empresa en seguridades de información.	Protección de Información	Desempeñar a cabalidad las normas dispuestas en la organización	Verificar que todo se cumpla de acuerdo a los procesos ya establecidos y aprobados	Departamento TIC
PERSONAL	Actuación prudente y preventiva en los equipos electrónicos, sistema de internet y medios de comunicación (correo electrónico)	Protección de Información	Identificar las medidas a seguir en caso de ciberataque.	Socializar las medidas a regir el personal en caso se enfrente a un ciberataque	Departamento TIC

Fuente: ECUATRAN (2021)

Elaborado por: Flores (2021)

REFERENCIAS BIBLIOGRÁFICAS

- Alvarado, N. (2018). *Tecnología Contra el Crimen: Entusiasmo con Cautela y Criterio*. Seguridad Ciudadana. <https://blogs.iadb.org/seguridad-ciudadana/es/tecnologia-contra-el-crimen-entusiasmo-con-criterio/>
- Arévalo, J., Bayona, R., & Rico, D. (2015). Implantación de un Sistema de Gestión de Seguridad de Información Bajo la ISO 27001: Análisis del Riesgo de la Información. *Revista Tecnura*, 19(46), 123-134.
<https://doi.org/10.14483/udistrital.jour.tecnura.2015.4.a10>
- Baena, G., Mendoza, R., & Dorantes, E. (2019). Importancia de la Norma ISO/EIC 27000 en la Implementación de un Sistema de Gestión de la Seguridad de la Información. *Contribuciones a la Economía*, 1-13. <https://doi.org/1696-8360>
- Barbadillo, E., Aguilar, N., & Trombetta, M. (2007). An Empirical Analysis of the Factors Explaining the Change in Audit Opinion: Opinion Shopping and Accounting Practices Improvements in Firms. *Spanish Journal of Finance and Accounting / Revista Española de Financiación y Contabilidad*, 36(134), 317-350. <https://doi.org/10.1080/02102412.2007.10779623>
- Becerra, D. (2010). La Globalización y el Crecimiento Empresarial a Través de Estrategias de Internacionalización. Globalization and Entrepreneurial Growth Through Internationalization Strategies. *Revista científica Pensamiento y Gestión*, 28, 1-25.

- Bozkurt, O., Slamolu, M., & Öz, Y. (2013). Percepciones de Profesionales Interesados en Contabilidad y Auditoría Acerca de la Aceptación y Adaptación de Normas Internacionales de Información Financiera. *Journal of Economics, Finance and Administrative Science*, 18(34), 16-23.
- Brien, J., & Marakas, G. (2006). *Sistemas de Informacion Gerencial*. 625.
- Callery, P. J., & Perkins, J. (2021). Detecting False Accounts In Intermediated Voluntary Disclosure. En *Academy OF Management Discoveries* (Vol. 7, Número 1, pp. 40-56). ACAD Managenent.
<https://doi.org/10.5465/amd.2018.0229>
- Cañedo, R., Ramos, R., & Guerrero, J. (2005). La Informática, la Computación y la Ciencia de la Información: Una Alianza para el Desarrollo. *ACIMED*, 13(5), 1-1.
- Castro, M., Morán, G., Navarrete, D., Cruzatty, J., Anzúles, G., Mero, C., Quimiz, Á., & Merino, M. (2018). *Introducción a la Seguridad Informática y el Análisis de Vulnerabilidades*. 3Ciencias.
- Castromán, J., & Porto, N. (2005, mayo 2). *Responsabilidad Social y Control Interno*. 1, 86-101.
- Cepreven. (2021). *Auditoria Informática. Seguridad Informática. Ciberseguridad Empresas*. <https://www.cepreven.com/cuestionario-ciberseguridad/>
- Chang, J. (2020). *Análisis de Ataques Cibernéticos Hacia el Ecuador*. 10.

- Corda, M., Viñas, M., & Coria, M. (2017). Gestión del Riesgo Tecnológico y Bibliotecas: Una Mirada Transdisciplinar para su Abordaje. *Palabra Clave*, 7, n.º 1. <https://doi.org/10.24215/18539912e032>
- Dávalos, N. (2020, julio 5). La Ciberseguridad en el País ha Mejorado, pero aún no es Suficiente. *Primicias*.
<https://www.primicias.ec/noticias/tecnologia/ciberseguridad-ecuador-mejorado-no-suficiente/>
- El Universo. (2020, septiembre 27). Los Delitos Informáticos Crecen en Ecuador; Cada Clic en la Web Deja su Rastro. *El Universo*.
<https://www.eluniverso.com/noticias/2020/09/27/nota/7991905/delitos-informaticos-internet-casos-reales-redes-sociales-ecuador>
- Espinosa, C. (2019, septiembre 22). *Ecuador Ocupa el Séptimo Lugar en Ciberseguridad en América Latina*. El Comercio.
<https://www.elcomercio.com/actualidad/seguridad/ecuador-ciberseguridad-region-informe-delitos.html>
- Fernández, E., & Martínez, A. (2015). La Discrecionalidad en las Diferencias Temporarias entre Contabilidad y Fiscalidad. *Spanish Journal of Finance and Accounting / Revista Española de Financiación y Contabilidad*, 44(2), 180-207. <https://doi.org/10.1080/02102412.2015.1006427>
- Galaz, Y. (2015). *Marco de Referencia para la Implementación, Gestión y Control de un Adecuado Sistema de Control Interno*. Deloitte.

<https://www2.deloitte.com/content/dam/Deloitte/mx/Documents/risk/COSO-Sesion1.pdf>

García, R., Gonzalez, J., & Jornet, J. (2010). *SPSS Análisis de Fiabilidad*. 6.

Gil, V., & Gil, J. (2017). Seguridad Informática Organizacional: Un Modelo de Simulación Basado en Dinámica de Sistemas. *Scientia et technica*, 22(2), 196. <https://doi.org/10.22517/23447214.11371>

GlobalSUITE. (2021, septiembre 3). Estándares y Normas ISO para Mejorar la Ciberseguridad. *GlobalSUITE Solutions*.
<https://www.globalsuitesolutions.com/es/normas-iso-para-mejorar-la-ciberseguridad/>

González, M. (2007). *Nuevo Paradigma del Control Interno y su Impacto en la Gestión Pública*. 141. <https://www.redalyc.org/pdf/4255/425541595009.pdf>

Hernandez, A. B. (2015). La Detección del Fraude Contable Utilizando Técnicas de Minería de Datos. *Revista Publicando*, 2(5), 103-113.

Infodefensa.com. (2021, marzo 5). *Ecuador Crea el Comando de Ciberdefensa para Blindar al País ante Ataques Cibernéticos*. Infodefensa.
<https://www.infodefensa.com/texto-diario/mostrar/3056658/ecuador-crea-comando-ciberdefensa-blindar-pais-ante-ataques-ciberneticos>

ISOTOOLS. (2018, febrero 7). *¿Cómo ha Cambiado el Nuevo COSO ERM 2017?*
ISOTOOLS. <https://www.isotools.org/2018/02/07/ha-cambiado-nuevo-coso-erm-2017/>

- Jiménez, A. (2013). Desarrollo Tecnológico y su Impacto en el Proceso de Globalización Económica: Retos y Oportunidades para los Países en Desarrollo en el Marco de la Era del Acceso. *Visión Gerencial*, 12(1), 123-150.
- Justexw. (2018, abril 16). Cómo Utilizar Tablas de Datos de Dos Entradas en Excel | Tablas en Excel. *Just EXW*. <https://es.justexw.com/como-utilizar-tablas-de-datos-de-dos-entradas-en-excel.html>
- Kippeo. (2021). *Home*. Kippeo Technologies. <https://kippeo.com/>
- Ladino, M., Villa, P., & López, A. (2011). Fundamentos de ISO 27001 y su Aplicación en las Empresas. *Scientia et Technica*, 1(47), 334-339. <https://doi.org/10.22517/23447214.1177>
- Manay, V., Cribillero, Y., & Pesantes, E. (2019). Aplicación de Ciclo Deming para la Mejora de la Productividad en una Empresa de Transportes. *Revista Científica EPígmalión*, 1(2), Article 2. <https://doi.org/10.51431/epigmalion.v1i2.538>
- Maza. (2020, septiembre 7). *El Impacto de las Tecnologías Exponenciales a la Seguridad Nacional e Internacional | Foreign Affairs Latinoamérica |*. <https://revistafal.com/el-impacto-de-las-tecnologias-exponenciales-a-la-seguridad-nacional-e-internacional/>
- Mesquida, A., Mas, A., Amengual, E., & Cabestrero, I. (2010). *Sistema de Gestión Integrado según las Normas ISO*. 3, 11.

- Michán, L., Alvarez, E., & Montoya, L. (2011). *La Revolución Informática en Biología: El Caso de la Genómica*. 16, 115-127.
- Murillo, L., Narváez, C., & Erazo, J. (2019). Sistema de Control Interno con Enfoque en la ISO 9001: 2015 en la Bananera Monterrey. *Revista Arbitrada Interdisciplinaria Koinonía*, 4(2), 241. <https://doi.org/10.35381/r.k.v4i2.474>
- Navarrete, J. (2020, septiembre 14). *Ecuador en Riesgo de Ciberataques*. BDO. <https://www.bdo.ec/es-ec/noticias/2020/ecuador-en-riesgo-ciberataques>
- NORMAS ISO. (2022, enero 23). ISO 27001 - Seguridad de la Información: Norma ISO IEC 27001/27002. *Normas ISO*. <https://www.normas-iso.com/iso-27001/>
- Oberheide, J., Cooke, E., & Jahanian, F. (2008). *CloudAV: N-Version Antivirus in the Network Cloud*. 91-106.
- Olmedo, J., & Gavilánez, F. (2018). Análisis de los Ciberataques Realizados en América Latina. *INNOVA Research Journal*, 3(9), 172-181. <https://doi.org/10.33890/innova.v3.n9.2018.837>
- Ortiz, N. (2019). Normativa Legal sobre Delitos Informáticos en Ecuador. *Revista Científica Hallazgos21*, 4(1), 100-111.
- Ostec. (2016, diciembre 30). ISO27002: Buenas Prácticas para Gestión de la Seguridad de la Información. *OSTEC / Segurança digital de resultados*. <https://ostec.blog/es/generico/iso-27002-buenas-practicas-gsi/>

- Parra, L. (2014). Los Sistemas de Control Interno en las Mipymes y su Impacto en la Efectividad Empresarial. *En-Contexto Revista de Investigación en Administración, Contabilidad, Economía y Sociedad*, 2, 129-146.
- Perols, R. R., & Murthy, U. S. (2021). The Impact of Cybersecurity Risk Management Examinations and Cybersecurity Incidents on Investor Perceptions and Decisions. *Auditing*, 40(1), 73-89.
<https://doi.org/10.2308/AJPT-18-010>
- Pinzón, L. (2014). Tecnología e Informática de la Historia. *Journal of Human Sciences*, 10, 26.
- Quinaluisa, N., Ponce, V., Muñoz, S., Ortega, X., & Pérez, J. (2018). El Control Interno y sus Herramientas de Aplicación entre COSO y COCO. *Cofin Habana*, 12(1), 268-283.
- Ramírez, A. (2021). *Riesgo Tecnológico y su Impacto para las Organizaciones parte I / Revista Seguridad*. Revista Seguridad.
<https://revista.seguridad.unam.mx/numero-14/riesgo-tecnol%C3%B3gico-y-su-impacto-para-las-organizaciones-parte-i>
- Rueda, J. (2007). *La Tecnología de la Sociedad del Siglo XXI: Albores de una Nueva Revolución Industrial*. 1-28.
- Ruiz, L. (2019). *Alfa de Cronbach (α): Qué es y Cómo se Usa en Estadística*.
<https://psicologiaymente.com/miscelanea/alfa-de-cronbach>

- Salas, J. A. S., & Reyes, N. M. (2015). Modelo Propuesto para la Detección de Fraudes por Parte de los Auditores Internos Basado en las Normas Internacionales de Auditoría. *Cuadernos de Contabilidad*, 16(SPE42), 579-623. <https://doi.org/10.11144/Javeriana.cc16-42.mpdf>
- Shakouri, M. M., Taherabadi, A., Ghanbari, M., & Jamshidinavid, B. (2021). Explaining the Beneish Model and Providing a Comprehensive Model of Fraudulent Financial Reporting(FFR). En *International Journal of Nonlinear Analysis and Applications* (Vol. 12, Número SI, pp. 39-48). SEMNAN UNIV. <https://doi.org/10.22075/IJNAA.2021.4793>
- Tadesse, A. F., & Murthy, U. S. (2021). Does the Format of Internal Control Disclosures Matter? An Experimental Investigation of Nonprofessional Investor Behavior. *Auditing*, 40(1), 91-106. <https://doi.org/10.2308/AJPT-17-171>
- Tates, C., & Herrera, L. (2019). *La Ciberseguridad en Ecuador, una Propuesta de Organización. IV*, 156-169.
- TI, R. B. (2018). *Un 39% de las Empresas de la UE Sufre Robo de Datos* [Revista]. Revista byte. <https://revistabyte.es/actualidad-it/empresas-sufre-robo-de-datos/>
- Vargas, R., Reyes, R., & Recalde, L. (2017). Ciberdefensa y Ciberseguridad, más Allá del Mundo Virtual: Modelo Ecuatoriano de Gobernanza en Ciberdefensa/ Cyber-Defense and Cybersecurity, Beyond the Virtual World: Ecuadorian Model of Cyber-Defense Governance. *URVIO - Revista*

Latinoamericana de Estudios de Seguridad, 20, 31.

<https://doi.org/10.17141/urvio.20.2017.2571>

Vásconez, L. (2015). Cibermafias Atacaron a 17 Empresas Ecuatorianas. *El Comercio*. <https://www.elcomercio.com/actualidad/seguridad/cibermafias-ciberataque-17empresas-ecuador-seguridadinformatica.html>

Wang, C., & Tsai, D. (2009). Integrated Installing ISO 9000 and ISO 27000 Management Systems on an Organization. *43rd Annual 2009 International Carnahan Conference on Security Technology*, 265-267.

<https://doi.org/10.1109/CCST.2009.5335527>

Wuerges, A. F. E., Borba, J. A., Wuerges, A. F. E., & Borba, J. A. (2014). Fraudes Contábeis: Uma Estimativa da Probabilidade de Detecção. *Revista Brasileira de Gestão de Negócios*, 16(52), 466-483.

<https://doi.org/10.7819/rbgn.v16i52.1555>

ANEXOS

Anexo 1

6.1. Entrevista

Persona: Tannia Naranjo **Cargo:** Líder de Sistemas

¿Qué sistemas informáticos son manejados en la empresa?

Respuesta: El RP, el sistema financiero, se maneja el AXIS que es el complementario para producción, planificación, logística e.... se tiene también el sistema de calidad, el sistema de laboratorio, el sistema de auditoría, esos son los más comunes.

¿Cuáles son los problemas más comunes en tecnología de información que la empresa ha detectado?

Respuesta: Ya, los problemas más comunes que se tiene es respecto a la infraestructura, porque cuando iniciaron la empresa no tenían mucha tecnología, por lo cual no estaban distribuidos los puntos de red o no estaban distribuidos e... en general todo lo que es la infraestructura, eso se fue acoplando poco a poco con el paso de los años, sin embargo como van pasando personas a nivel de todo el tiempo van dejando a medias a medias a medias y la otra persona no conoce hasta donde llegó el punto anterior y lo vuelve a iniciar, entonces es un.... Ese es uno de los mayores problemas que existe en la empresa con el tema de la infraestructura.

¿Ha existido algún tipo de ciberdelito o problema similar en la empresa?

Respuesta: Se tuvo es un ataque cibernético me parece que hace dos años exactamente, en donde e... literalmente nos hackearon el servidor, el almacén en todo un rango y fue difícil recuperar la información, pero como tenemos los respaldos acá, estamos preparados para esas eventualidades, aunque si fue un golpe muy duro.

¿Qué tan importante es la seguridad informática para la empresa?

Respuesta: La seguridad informática es bastante importante en... general en la empresa y en todo, ya que ahora la mayor parte de documentos se manejan digitalmente, toda la información también es digital, así que hay que tener mucho cuidado con eso.

¿La empresa ha aplicado la metodología COSO 2017 para evaluar su sistema de control interno con respecto a la ciberseguridad?

Respuesta: Si de hecho nosotros estamos en la.... En la matriz de riesgos, tenemos me parece que hay tres riesgos desencadenados, el uno es el robo de información, el otro es la pérdida de la información como tal y la otra es la confidencialidad de la información.

¿Cuáles son las medidas de protección que aplica la empresa para evitar ciberdelitos?

Respuesta: La medida principal es tener el antivirus actualizado, nosotros manejamos un antivirus que no es gratuito es de paga, ya que los gratuitos también tienen sus Book internos, tenemos licenciados en todos los equipos y el control de los puertos que no cualquiera tiene el acceso por ejemplo a los puertos USB.

¿Cada que tiempo se evalúa el control interno en la empresa?

Respuesta: Nosotros estamos constantemente haciendo los controles en informática de hecho e..... hace un mes y medio más o menos hicimos el cambio de la configuración general de todo lo que es la red y ahí se implementó un nuevo equipo que está haciendo ahorita el peso del..... como se puede decir de la seguridad tanto de afuera como la interna de aquí.

¿Qué alternativas adicionales a los controles ha visto la empresa para dar solución al sistema de seguridad que maneja la entidad?

Respuesta: Si, de hecho, estamos trabajando en ello, nos falta la aprobación del equipo para la nueva adquisición, estamos buscando es un equipo más robusto para... para complementar la seguridad. Este sistema lo venimos planificando desde hace unos

cuatro, cinco meses, el que tenemos actualmente todavía esta funcional pero ya está saliendo de su ciclo de vida útil.

Anexo 2

Figura 13. Detalle análisis Check List

CATEGORÍA	PREGUNTA	CUMPLE
SENSIBILIZANDO	1	1
SENSIBILIZANDO	2	1
SENSIBILIZANDO	3	1
CONOCIENDO EL SISTEMA DE INFORMACIÓN	4	1
CONOCIENDO EL SISTEMA DE INFORMACIÓN	5	1
CONOCIENDO EL SISTEMA DE INFORMACIÓN	6	1
AUTENTIFICACIÓN DE LOS ACCESOS	7	1
AUTENTIFICACIÓN DE LOS ACCESOS	8	1
AUTENTIFICACIÓN DE LOS ACCESOS	9	1
AUTENTIFICACIÓN DE LOS ACCESOS	10	1
AUTENTIFICACIÓN DE LOS ACCESOS	11	1
AUTENTIFICACIÓN DE LOS ACCESOS	12	1
ESTACIONES DE TRABAJO SEGURAS	13	1
ESTACIONES DE TRABAJO SEGURAS	14	1
ESTACIONES DE TRABAJO SEGURAS	15	1
ESTACIONES DE TRABAJO SEGURAS	16	1
ESTACIONES DE TRABAJO SEGURAS	17	1
ASEGURANDO LA RED	18	1
ASEGURANDO LA RED	19	1
ASEGURANDO LA RED	20	1
ASEGURANDO LA RED	21	1
ASEGURANDO LA RED	22	1
ASEGURANDO LA RED	23	1
ASEGURANDO LA RED	24	1
ADMINISTRACIÓN SEGURA	25	1
ADMINISTRACIÓN SEGURA	26	1
ADMINISTRACIÓN SEGURA	27	1
ADMINISTRACIÓN SEGURA	28	2
SEGURIDAD PARA EQUIPOS PORTÁTILES	29	1
SEGURIDAD PARA EQUIPOS PORTÁTILES	30	1
SEGURIDAD PARA EQUIPOS PORTÁTILES	31	1
MANTENER ACTUALIZADO EL SISTEMA DE INFORMACIÓN	32	1
MANTENER ACTUALIZADO EL SISTEMA DE INFORMACIÓN	33	1
SUPERVISAR, AUDITAR Y REACCIONAR	34	1
SUPERVISAR, AUDITAR Y REACCIONAR	35	1
SUPERVISAR, AUDITAR Y REACCIONAR	36	1
SUPERVISAR, AUDITAR Y REACCIONAR	37	1
SUPERVISAR, AUDITAR Y REACCIONAR	38	2

Fuente: ECUATRAN (2021)

Elaborado por: Flores (2021)

Anexo 3

Figura 14. Tabulación Check List Categoría Sensibilizando

	SENSIBILIZANDO				
	X	F	FR	%	F
SI	1	3	1	100	3
NO	2			0	3
	TOTAL	3	1	100	

Fuente: ECUATRAN (2021)

Elaborado por: Flores (2021)

Anexo 4

Figura 15. Tabulación Check List Categoría Conociendo el Sistema de Información

	CONOCIENDO EL SISTEMA DE INFORMACIÓN				
	X	F	FR	%	F
SI	1	3	1	100	3
NO	2			0	3
	TOTAL	3	1	100	

Fuente: ECUATRAN (2021)

Elaborado por: Flores (2021)

Anexo 5

Figura 16. Tabulación Check List Categoría Autenticación de los accesos

	AUTENTICACIÓN DE LOS ACCESOS				
	X	F	FR	%	F
SI	1	6	1	100	6
NO	2			0	6
	TOTAL	6	1	100	

Fuente: ECUATRAN (2021)

Elaborado por: Flores (2021)

Anexo 6

Figura 17. Tabulación Check List Categoría Estaciones de Trabajo Seguras

	ESTACIONES DE TRABAJO SEGURAS				
	X	F	FR	%	F
SI	1	5	1	100	5
NO	2			0	5
	TOTAL	5	1	100	

Fuente: ECUATRAN (2021)

Elaborado por: Flores (2021)

Anexo 7

Figura 18. Tabulación Check List Categoría Asegurando la Red

	ASEGURANDO LA RED				
	X	F	FR	%	F
SI	1	7	1	100	7
NO	2			0	7
	TOTAL	7	1	100	

Fuente: ECUATRAN (2021)

Elaborado por: Flores (2021)

Anexo 8

Figura 19. Tabulación Check List Seguridad para Equipos Portátiles

	SEGURIDAD PARA EQUIPOS PORTÁTILES				
	X	F	FR	%	F
SI	1	3	1	100	3
NO	2			0	3
	TOTAL	3	1	100	

Fuente: ECUATRAN (2021)

Elaborado por: Flores (2021)

Anexo 9

Figura 20. Tabulación Check List Mantener actualizado el sistema de información

	MANTENER ACTUALIZADO EL SISTEMA DE INFORMACIÓN				
	X	F	FR	%	F
SI	1	2	1	100	2
NO	2			0	2
	TOTAL	2	1	100	

Fuente: ECUATRAN (2021)

Elaborado por: Flores (2021)

Anexo 10

Figura 21. Tabulación Check List Supervisar, Auditar y Reaccionar

	SUPERVISAR, AUDITAR Y REACCIONAR				
	X	F	FR	%	F
SI	1	4	0,8	80	4
NO	2	1		0	5
	TOTAL	5	0,8	80	

Fuente: ECUATRAN (2021)

Elaborado por: Flores (2021)

Anexo 11

Figura 22. Detalle análisis aplicación de encuestas

N°	CARGO	PERSONAS	PREGUNTA 1	PREGUNTA 2	PREGUNTA 3	PREGUNTA 4	PREGUNTA 5	PREGUNTA 6	PREGUNTA 7	PREGUNTA 8	PREGUNTA 9	PREGUNTA 10	PREGUNTA 11	PREGUNTA 12	PREGUNTA 13	PREGUNTA 14	PREGUNTA 15	PREGUNTA 16	PREGUNTA 17	SUMA
1	Líder de Ventas Internacionales	Xavier Gordillo	1	1	1	1	1	2	1	1	2	2	2	3	2	3	2	1	3	29
2	Asistente Administrativa de Operaciones	Jessica Mora	1	1	1	1	1	1	1	1	1	1	1	2	2	2	1	1	1	20
3	Analista de Producción	Gissela Medina	1	1	1	1	1	2	1	1	1	1	2	1	1	1	1	1	1	19
4	Asistente Soporte Técnico	Camila Martínez	1	1	1	3	1	1	1	2	2	1	2	1	1	2	2	1	3	26
5	Analista de Investigación y Desarrollo	Italo Gaibor	1	1	1	1	1	1	1	2	2	1	2	3	1	1	2	3	3	27
6	Ingeniero de Diseño	Erick Barrionuevo	2	1	1	1	1	1	1	2	1	2	1	1	1	2	2	1	3	24
7	Técnico de Servicios	Christian Montoya	2	2	1	1	1	2	1	2	1	2	2	1	1	2	2	1	1	25
8	Auxiliar SIG	Dennis Salazar	1	2	1	1	1	1	1	2	2	2	2	1	1	2	2	1	1	24
9	Analista de Logística y Exportación	Angélica Tirado	1	2	1	1	1	2	1	2	2	1	2	1	1	1	2	1	2	24
10	Ingeniero de Diseño Eléctrico	Dario Campos	1	1	1	3	1	2	2	2	2	1	2	2	3	1	2	3	3	32
11	Asistente Servicios y Garantías	Carolina Arcos	3	1	1	1	1	1	1	1	2	1	2	1	1	1	2	1	1	22
12	Analista Administrativa	Paulina Adame	1	1	1	1	1	1	1	1	1	2	1	1	1	2	1	2	1	20
13	Analista de Estructuras- Ingeniería	Erick Manosalvas	1	1	1	1	1	2	1	2	2	3	2	1	1	1	1	1	1	23
14	Asistente Programador	Jenny Núñez	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	3	20
15	Asistente Financiera	Alexandra Ortiz	1	1	1	1	2	2	2	2	1	1	2	2	1	1	1	1	2	24
16	Auxiliar Contable	Valeria Baca	2	2	1	1	1	1	2	2	1	3	2	2	1	1	2	1	2	27
17	Asistente Administrativa de Compras	Johanna Lagos	1	1	1	1	1	1	1	1	2	1	2	1	1	1	1	1	1	19
18	Supervisor de Seguridad Física	Eduardo Pacheco	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	17
19	Subgerente de Ventas	Santiago Carrasco	1	2	1	1	1	2	1	1	1	2	1	2	1	1	1	1	2	22
20	Líder SIG	Angela Freire	1	1	1	1	1	2	1	2	3	3	1	3	1	2	1	1	1	26
ANÁLISIS DE DE DATOS			16	15	20	18	19	11	17	9	10	10	7	12	17	12	10	17	10	
PORCENTAJE DE ANÁLISIS			80%	75%	100%	90%	95%	55%	85%	45%	50%	50%	35%	60%	85%	60%	50%	85%	50%	

Fuente: ECUATRAN (2021)

Elaborado por: Flores (2021)

Anexo 12

Figura 23. Tabulación por categorización

CATEGORÍA	1 (SI)	2 (NO)	3 (NO APLICA)
Gobierno y Cultura	16,000	3,000	1,000
Modelo Operativo y de Negocios	13,600	5,800	0,600
Reporte y Tecnología	13,667	4,667	1,667
Alineado con la estrategia	12,333	5,000	2,667

Fuente: ECUATRAN (2021)

Elaborado por: Flores (2021)

Anexo 13

Figura 24. Escala de Impacto para aplicación matriz de riesgos

<i>ESCALA VALORATIVA DEL IMPACTO</i>	
N°	IMPACTO
5	MA: Muy Alto
4	A: Alto
3	M: Medio
2	B: Bajo
1	MB: Muy Bajo

Fuente: ECUATRAN (2021)

Elaborado por: Flores (2021)

Anexo 14

Figura 25. Escala de Probabilidad para aplicación matriz de riesgos

<i>ESCALA VALORATIVA DE PROBABILIDAD</i>		
N°	PROBABILIDAD	
5	PS: Paráticamente seguro	1 A 20
4	S: Probablemente Seguro	21 A 40
3	P: Probable	41 A 60
2	PP: Poco probable	61 A 80
1	MR: Muy raro	81 A 100

Fuente: ECUATRAN (2021)

Elaborado por: Flores (2021)

Anexo 15

Figura 26. Escala de riesgo para aplicación matriz de riesgos

<i>ESCALA VALORATIVA DEL RIESGO</i>		
N°	RIESGO	
21-25	C: Crítico	1 A 20
16-20	I: Importante	21 A 40
11-15	A: Apreciable	41 A 60
6-10	B: Bajo	61 A 80
1-5	NS: No significativo	81 A 100

Fuente: ECUATRAN (2021)

Elaborado por: Flores (2021)

Anexo 16

Figura 27. Definición del Riesgo

1	MB: No significativo
2	MB: No significativo
3	MB: No significativo
4	MB: No significativo
5	MB: No significativo
6	B: Bajo
7	B: Bajo
8	B: Bajo
9	B: Bajo
10	B: Bajo
11	M: Apreciable
12	M: Apreciable
13	M: Apreciable
14	M: Apreciable
15	M: Apreciable
16	A: Importante
17	A: Importante
18	A: Importante
19	A: Importante
20	A: Importante
21	MA: Crítico
22	MA: Crítico
23	MA: Crítico
24	MA: Crítico
25	MA: Crítico

Fuente: ECUATRAN (2021)

Elaborado por: Flores (2021)