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

## PROCESO DE TITULACIÓN

**PERIODO DICIEMBRE 2022 - MAYO 2023**

**EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA**

**PRUEBA PRÁCTICA**

**PREVIO A LA OBTENCIÓN DEL TITULO DE INGENIERÍA EN SISTEMAS**

## TEMA:

**DIAGNOTICO Y ESTRUCTURA DE LAS BUENAS PRACTICAS EN LA GESTION DE LA SEGURIDAD DE LA INFORMACION BASADOS EN LA NORMA ISO /IEC 27001 PARA LA EMPRESA AVCAMNET S.A EN BABAHOYO**

## EGRESADA:

**MICHELL MARIA PAZ CAICEDO**

## TUTOR:

**ING. GERSON DAMACIO LEDESMA ALVAREZ. MUFI**

**AÑO:**

**2023**

# INTRODUCCIÓN

En la actualidad digital, la gestión de la seguridad de la información es un aspecto crítico para cualquier empresa, incluyendo AVCAMNET S.A, ya que es esencial proteger sus activos más valiosos. Para lograr esto, es importante contar con un sistema de gestión de la seguridad de la información eficiente y efectivo. La norma ISO/IEC 27001 proporciona un marco de referencia para establecer, implementar, mantener y mejorar continuamente la gestión de la seguridad de la información en una organización. Por lo tanto, el objetivo de esta investigación es explorar y describir las mejores prácticas en la gestión de la seguridad de la información basadas en la norma ISO/IEC 27001, para que AVCAMNET S.A pueda implementarlas en su sistema de gestión de seguridad de la información.

La síntesis de la investigación incluirá la identificación de los principales aspectos a considerar para una gestión eficiente de la seguridad de la información en AVCAMNET S.A, tales como la evaluación de riesgos, la implementación de controles de seguridad, la formación del personal y la monitorización continua. En definitiva, El objetivo principal de esta investigación es evaluar la aplicación de las buenas prácticas de seguridad de la información basadas en la norma ISO / IEC 27001 en AVCAMNET S.A.

Este trabajo se centra en dos áreas de investigación cruciales en el mundo actual: “Sistemas de información y comunicación, emprendimiento e innovación”, y “Redes y tecnologías inteligentes de software y hardware”. La gestión eficiente de las tecnologías de la información y comunicación es esencial para el éxito de las organizaciones y empresas en la era digital actual. Además, el emprendimiento y la innovación son fundamentales para mantenerse competitivo en un entorno empresarial en constante evolución. Por otro lado, las redes y tecnologías inteligentes de software y hardware permiten a las empresas y organizaciones optimizar sus procesos, mejorar su eficiencia y aumentar su productividad.

Las preguntas de reflexión que se plantean en esta investigación para AVCAMNET S.A son: ¿Cómo puede su empresa garantizar la efectividad de su sistema de gestión de seguridad de la información? ¿Qué retos enfrenta AVCAMNET S.A.? en la implementación de la norma ISO/IEC 27001 y cómo pueden superarlos? ¿Cómo pueden adaptarse a los cambios y evoluciones constantes en la gestión de la seguridad de la información para seguir protegiendo sus activos más valiosos?

Para ello, se utilizarán métodos de investigación como la documental o bibliográfica con un enfoque cualitativo de la investigación permite al autor comprender de manera adecuada el sistema informático de la empresa, que permitan recopilar y analizar información relevante, incluyendo la revisión de la literatura especializada y el estudio de casos prácticos. La integración de los conocimientos adquiridos en la investigación permitirá establecer recomendaciones para AVCAMNET S.A.

## DESARROLLO

La empresa AVCAMNET S.A con RUC #1703204722001 inicio sus actividades en el 2022, se encuentra ubicada en la parroquia Turubamba en la provincia de Pichicha, en las calles E41 y calle S dentro del centro comercial ACHOMEC del cantón Quito, cuyo representante legal es el Sr. Valle Riofrio Arturo Alberto, tiene como actividad comercial ventas de computadoras al por mayor y menor en locales especializados, supervisión remota de los sistemas electrónicos de seguridad como alarma contra robos o incendios, suministra internet a través de la estructura de telecomunicaciones alámbricos, venta al por menor de accesorios y equipos de telecomunicaciones y también opera y realiza mantenimiento o facilita los accesos a servicios de trasmisión de punto a punto.

La seguridad de AVCAMNET S.A. se ve comprometida por diversas amenazas, que podrían exponer información valiosa y poner en riesgo sus activos críticos. La empresa depende en gran medida de sus sistemas de información, lo que la hace vulnerable a posibles vulnerabilidades y ataques cibernéticos. También debe tener en cuenta posibles incidentes causados por el personal de la organización o desastres naturales que podrían afectar la continuidad del negocio. Por lo tanto, es importante que la empresa tome medidas proactivas para mitigar estas amenazas y proteger sus activos y la información confidencial.

Por lo tanto, el diagnostico de las políticas basadas en el estándar de la norma ISO 27001 permitirá a AVCAMNET S.A. identificar posibles riesgos y elaborar procedimientos adecuados para mitigarlos y responder adecuadamente en caso de que ocurran. De esta manera, la empresa podrá garantizar la confidencialidad, integridad y disponibilidad de su información, lo que a su vez permitirá mantener los niveles de competencia y alcanzar los objetivos establecidos.

La norma ISO / IEC 27001 establece los requisitos para un sistema de gestión de seguridad de la información, y su aplicación puede mejorar significativamente la gestión de la seguridad de la información en las empresas. Por esta razón, esta investigación justifica la necesidad de evaluar las buenas prácticas de seguridad de la información basadas en la norma ISO / IEC 27001, y su aplicación en AVCAMNET S.A.

El objetivo central de esta investigación es analizar la implementación de las buenas prácticas de seguridad de la información, que se basan en la norma ISO / IEC 27001, en AVCAMNET S.A. Esta evaluación es esencial para garantizar la protección de la información confidencial y los activos críticos de la empresa, y reducir el riesgo de posibles amenazas y vulnerabilidades. Para tener una mejor comprensión del tema a estudiar se describen varios conceptos bibliográficos a continuación:

**SGSI**

Según Fernández (2022), un SGSI gestiona la seguridad de la información de una organización mediante el establecimiento, operación, revisión y mejora de contramedidas para las vulnerabilidades. Aborda el comportamiento de los empleados, así como los datos y la tecnología.

Para AVCAMNET S.A., es importante definir el alcance del SGSI considerando sus características como organización, actividad empresarial, ubicación, activos y tecnología involucrados, así como las posibles interacciones con otros sistemas y organizaciones. El SGSI puede ser implementado en toda la organización o en secciones específicas identificadas dentro de ella y puede estar enfocado en un tipo particular de datos, como los de sus clientes.

**Norma ISO / IEC 27001**

Según Russell**,** La norma internacional ISO 27001 establece los requisitos para los (SGSI):

> Proporciona un marco sólido para proteger la información de cualquier tipo y tamaño de organización. Cada vez más, las organizaciones que son más vulnerables a los riesgos relacionados con la seguridad de la información optan por implementar un SGSI que cumpla con la norma ISO 27001. (Russell, 2023)**.**

**Enfoque de la ISO / IEC 27001**

La forma de abordar el procedimiento para la seguridad de la información que se presenta en este estándar, hace que los usuarios pongan mayor énfasis en los siguientes aspectos:

Conoce los requisitos de seguridad de la información de la compañía y determina la importancia de establecer políticas y objetivos para garantizar la seguridad de la información.

- Ejecutar y supervisar los controles para mitigar los peligros de la seguridad de la información.
- Supervisar y evaluar el desempeño y la efectividad del SGSI.
- Implementación de mejoras continuas que se basen en la medición de los resultados. (Sordo, 2021)

**Procesos para certificar un SGSI basado en la norma ISO / IEC 27001.**

Según Leal (2020), comenta que se establece una evaluación de riesgos para lograr los objetivos del SGSI, basada en las amenazas, activos, vulnerabilidades e impactos en la organización. Luego, se seleccionan los dominios de control y controles para el tratamiento de riesgos.

Según Villamar (2021) afirma que “el estándar ISO / IEC 27001 garantiza la seguridad de la información empresarial de manera estructurada mediante procesos y políticas. Es

aplicable a todas las organizaciones y es una referencia para cumplir con leyes y regulaciones internacionales" (p. 85).

El proceso de adopción de ISO 27001 implica una descripción de los controles seleccionados y su implementación, seguida de la medición de su efectividad para evaluar el cumplimiento de los objetivos del SGSI. Se deben asignar responsabilidades para la implementación y medición del SGSI, y la alta gerencia debe tomar decisiones importantes y motivar a los empleados para cumplir con las políticas de seguridad de la información.

**Funcionamiento ISO / IEC 27001**

La ISO / IEC 27001 también considera a las partes interesadas y los auditores internos seleccionados para realizar auditorías internas periódicas. Los usuarios finales son los principales ejecutores de las políticas y normas de ISO / IEC 27001, y se requiere una cultura organizacional que coincida con la cultura de seguridad de la información deseada. La asignación de presupuesto y recursos humanos es crucial para el éxito del SGSI, y se requiere la implementación de acciones correctivas y preventivas sistemáticas para mantener y mejorar el SGSI.

Según Calder y Watkins (2019) menciona que "las precauciones que se van a tomar (o implementar) se describen comúnmente como políticas, procedimientos y métodos para llevarlas a cabo" (p. 45).

**Confidencialidad en un SGSI**

Para Calder y Watkins (2020) la propiedad que impide la divulgación de información a personas o sistemas no autorizados. Sintetizando, asegura el acceso a la información solo a quienes estén autorizados.

**Disponibilidad en un SGSI**

Es la propiedad de la información de ser accesible para quienes deben tener acceso a ella, ya sean personas, procesos o aplicaciones. En términos generales según Chilán y Pionce (2019) define “la disponibilidad es la capacidad de acceder a la información y a los sistemas de forma autorizada por parte de las personas en el momento que lo consideren necesario” (p. 45).

**Integridad en un SGSI**

Según Almeida *et al.* (2018) es la propiedad que se encarga de resguardar los datos que no puedan ser alterados de manera no autorizada. Es decir, la integridad es la exactitud de la información, sin alteraciones o manipulaciones no autorizadas.

**Beneficios de un SGSI**

Según Arreaga (2020), la Auditoria de seguridad de información de ISO / IEC 27001 puede ofrecer varios beneficios a una organización.

> En primer lugar, puede ayudar a proteger la información crítica y sensible, y cumplir con los requerimientos legales y regulaciones en materia de seguridad de la información. Además, la obtención de una certificación de cumplimiento puede mejorar la reputación de la organización y ofrecer una ventaja comercial sobre sus competidores. Por último, un SGSI puede ayudar a mejorar la eficiencia y reducir los costos asociados con incidentes de seguridad. (págs. 11-15).

**El alcance de un SGSI**

Según Iso27000 (2021) define “alcance del SGSI establece los límites del sistema en relación con el contexto, la importancia y la ubicación de los activos críticos de información de la organización”, así como los riesgos internos o externos asociados, como leyes y

regulaciones, obligaciones contractuales, y estrategias y políticas establecidas por organismos centrales.

### Política del SGSI

Según iso27000 (2023) menciona que: “es un documento que establece los objetivos y principios generales de seguridad de la información de una organización. Esta política es la base para el diseño, implementación, mantenimiento y mejora continua del SGSI en una organización”. En la política del SGSI se establecen las responsabilidades de la dirección y de los empleados en relación a la seguridad de la información, se identifican los activos críticos de información, se establecen las medidas de seguridad a aplicar y se definen los procedimientos y controles necesarios para proteger la información de la organización.

### Evaluacion de riesgos

Para De Freitas (2009), esta evaluación permite identificar los riesgos que pueden afectar a la seguridad de la información de una organización, evaluar su probabilidad de ocurrencia y su impacto en los activos de información, y determinar las medidas de seguridad necesarias para mitigar o reducir dichos riesgos.

### Dominios de la ISO/IEC 27001

Las áreas clave destinadas a la protección en un (SGSI) son los dominios de control. Los controles de seguridad de la información se implementan con el objetivo de proteger estos dominios que se basan en el estándar ISO / IEC 27001. Este estándar especifica catorce dominios de control e incluye operaciones y comunicaciones, gestión de acceso, seguridad de recursos humanos, seguridad de la información, seguridad física y ambiental, gestión de

activos, seguridad en el desarrollo y mantenimiento de sistemas, y varios otros. Según ISOTools son:

1. La política de seguridad de la información: se refiere a la creación de un conjunto de directrices que guíen la gestión de la seguridad de la información, proporcionando así una orientación clara y un marco de referencia.
2. La gestión de activos: consiste en identificar y categorizar los activos de información de la organización, y establecer responsabilidades claras para su protección. Esto implica la elaboración de un inventario y una clasificación de dichos activos.
3. Seguridad en recursos humanos: asegurar que los empleados, contratistas y terceros entiendan y cumplan con las políticas de seguridad de la información.
4. Gestión de accesos: controlar el acceso a los sistemas y aplicaciones de información, garantizando que los usuarios solo tengan acceso a lo que necesitan.
5. Seguridad física y del entorno: proteger los recursos físicos y entornos en los que se manejan los activos de información de la organización.
6. Gestión de operaciones y comunicaciones: garantizar la correcta operación y mantenimiento de los sistemas y la protección de la información durante las comunicaciones.
7. Control de sistemas de información: implementar controles técnicos y de seguridad para garantizar que los sistemas de información estén protegidos contra amenazas.
8. La gestión de incidentes de seguridad de la información implica la planificación y respuesta a eventos de seguridad para reducir al mínimo su impacto.
9. Gestión de la continuidad del negocio: planificar y preparar la respuesta de la organización a situaciones de interrupción del negocio.

10. Conformidad: cumplir con los requisitos legales y regulaciones relacionadas con la seguridad de la información.

11. Adquisición, desarrollo y mantenimiento de sistemas de información: asegurar que los sistemas de información sean seguros durante su adquisición, desarrollo y mantenimiento.

12. Relaciones con proveedores: garantizar que los proveedores y terceros cumplan con los requisitos de seguridad de la información.

13. Seguridad en la gestión de la información: proteger la información en todo el ciclo de vida de su gestión.

14. Aspectos de seguridad de la gestión de proyectos: considerar la seguridad de la información en la planificación y gestión de proyectos. (ISOTools Excellence, 2023)

**Modelo PHVA**

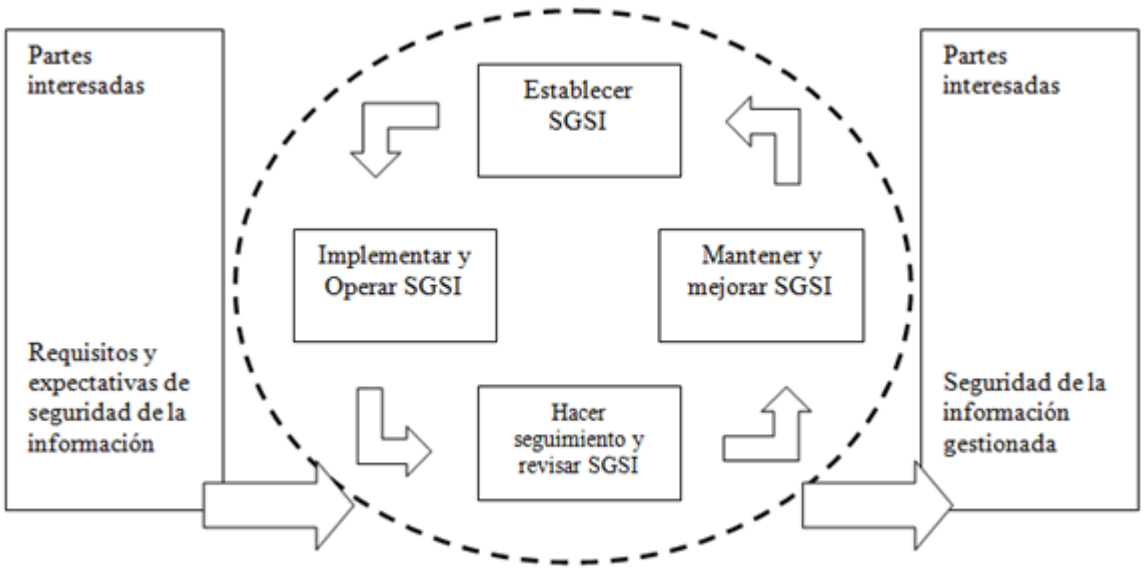



***Ilustración 1. Modelo PHVA. Fuente:*** *(Nicolas, 2019)*

Con el propósito de llevar a cabo un adecuado proceso metodológico, se recolectó la información en los diferentes puntos que se explican a continuación. Para este estudio, el enfoque metodológico fue cualitativo, ya que se enfocó en las cualidades de la investigación. Como resultado, el enfoque cualitativo de la investigación permite al autor comprender de manera adecuada el sistema informático de la compañía AVCAMNET S.A. Basándose en la norma ISO / IEC 27001 sobre seguridad informática, el estudio se enfocó en encontrar las debilidades del sistema que pudiesen ser corregidas.

Una investigación descriptiva podría ser útil para especificar las propiedades y características de la situación actual de gestión de la seguridad de la información en la empresa AVCAMNET S.A. Este método permitiría la observación de los eventos que ocurren en la empresa y la identificación de patrones y tendencias en la gestión de la seguridad de la información.

Por otro lado, una investigación bibliográfica que, a través de la búsqueda, recuperación y análisis de datos secundarios de autores literarios, se podrían identificar las mejores prácticas que podrían ser aplicables a la empresa AVCAMNET S.A.

Finalmente, una investigación explicativa podría ser útil para identificar las causas y consecuencias de los problemas del SGSI en la empresa AVCAMNET S.A. Este método permitiría la identificación de la causa raíz de los problemas y la búsqueda de posibles soluciones a través del análisis de la relación causa-efecto.

En la presente investigación que se realizará en el departamento tecnológico de la empresa AVCAMNET S.A. La meta primordial es evaluar el peligro de la compañía a través de la norma ISO / IEC 27001. No se llevará a cabo un proceso de muestreo, ya que no se empleará la técnica de la entrevista, sino que será esta última la que sirva como instrumento para analizar el riesgo.

La técnica de investigación aplicada implica la realización de entrevistas, que son preguntas verbales que conducen a respuestas que permiten entender las opiniones, conocimientos, habilidades y deseos de la persona que se está investigando. Las entrevistas estarán direccionadas al jefe del departamento de sistemas y al coordinador de tecnología.

**Análisis de las encuestas realizadas**

*Tabla 1. Tiempo laborando*

| Descripción | Frecuencia | Porcentaje |
|---|---|---|
| 0-3 meses | 2 | 28,57% |
| 6-9 meses | 2 | 28,57% |
| 1 año o mas | 3 | 42,86% |
| Total | 7 | 100,00% |

*Elaborado por la autora.*

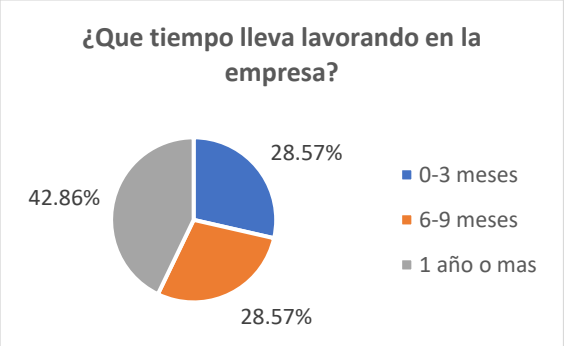



*Gráfico 1. Tiempo laborando.*

**Analisis**

Los datos muestran que el 28,57% de los empleados ha estado trabajando en la empresa durante 0-3 meses y el mismo porcentaje ha estado trabajando en la empresa durante 6-9 meses. El 42,86% de los trabajadores ha estado trabajando en la empresa durante 1 año o más.

*Tabla 2. Conoce los sistemas APS.*

| Descripción | Frecuencia | Porcentaje |
|---|---|---|
| Si | 3 | 42,86% |
| No | 4 | 57,14% |
| Total | 7 | 100,00% |

*Elaborado por la autora.*

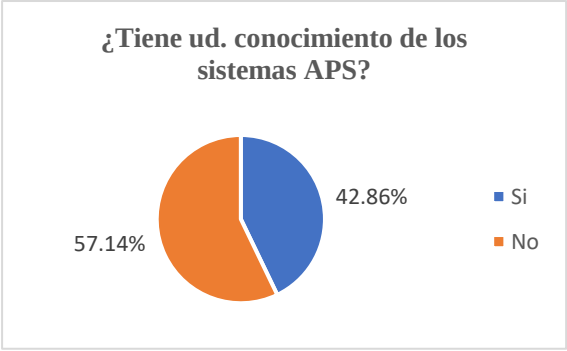



*Gráfico 2. Conoce el sistema APS.*

**Analisis**

Según la encuesta se pudo identificar que solo 3 que corresponde al 42,86% tienen conocimiento de dichos programas, mientras que el 57,14% no tienen conocimiento.

*Tabla 3. Maneja el sistema APS.*

| Descripción | Frecuencia | Porcentaje |
|---|---|---|
| Si | 1 | 14,29% |
| Más o Menos | 2 | 28,57% |
| No | 4 | 57,14% |
| Total | 7 | 100,00% |

*Elaborado por la autora.*

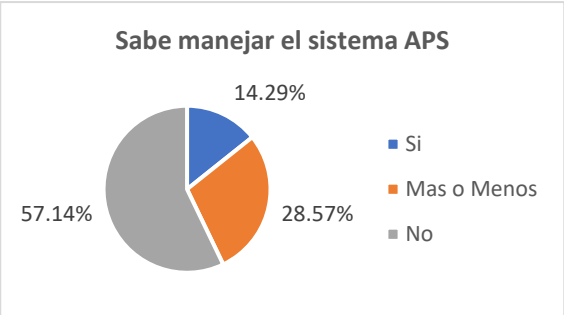



*Gráfico 3. Maneja el sistema APS.*

**Analisis** En esta pregunta cabe señalar que solo 3 respondieron que tenían conocimiento del tema, del cual solo uno de los encuestados sabe usarlo perfectamente y los otro dos más o menos que corresponde al 42,86%, mientras que el 57,14% no tiene conocimiento.

*Tabla 4. Conoce la norma ISO/IEC 27001*

| Descripción | Frecuencia | Porcentaje |
|---|---|---|
| Si | 2 | 28,57% |
| Más o Menos | 2 | 28,57% |
| No | 3 | 42,86% |
| Total | 7 | 100,00% |

*Elaborado por la autora.*

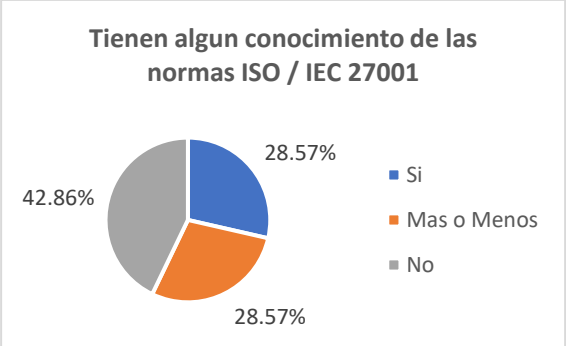



*Gráfico 4. Conoce la norma ISO/IEC 27001*

**Analisis**

El 28,57% de los encuestados que mencionaron que si conocian las normas ISO / IEC 27001, de igual porcentaje estan los que saben mas o menos sobre estas normas, mientras que 42,86% afirmaron que no conocían estas normas.

*Tabla 5. Información confidencial.*

| Descripción | Frecuencia | Porcentaje |
|---|---|---|
| Si | 5 | 71,43% |
| No | 2 | 28,57% |
| Total | 7 | 100,00% |

*Elaborado por la autora.*

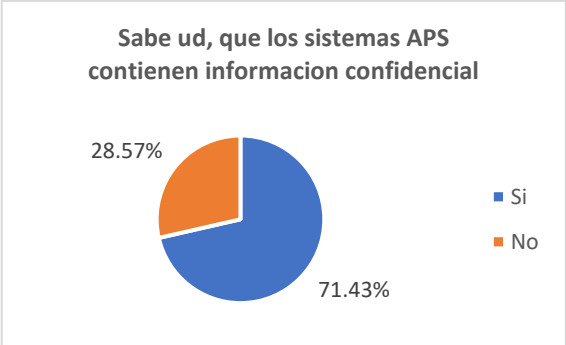



*Gráfico 5. Información confidencial.*

**Analisis**

Cinco colaboradores de la empresa, lo que representa el 71,43%, indicaron que eran conscientes de que el sistema de planificación avanzada (APS) contiene información confidencial de la empresa. Por otro lado, dos colaboradores, lo que corresponde al 28,57%, afirmaron no saber que el sistema incluye información confidencial de la empresa.

Este estudio se clasifica como una investigación cualitativa con una cuestión abierta. Sin embargo, se incluyó un número mínimo de preguntas cerradas en la encuesta aplicada para obtener la opinión directa de los siete colaboradores de la empresa AVCAMNET S.A. acerca de la gestión del sistema APS.

El propósito de la encuesta fue determinar el nivel de conocimiento de cada empleado sobre el sistema de planificación avanzada y el porcentaje de ellos que tiene conciencia de la existencia de una norma destinada a la seguridad de la información.

**Análisis de entrevista**

*Tabla 6. Entrevista al jefe del departamento de sistemas*

| Orden | Preguntas | Datos relevantes encontrados |
|---|---|---|
| 1 | ¿Existe algún tipo de control interno de TI? | No se tiene un control interno formal para la gestión de la información, pero se está trabajando en el desarrollo de un sistema de control. |
| 2 | ¿Cómo aplica la empresa las políticas de seguridad? | Hay un equipo de auditoría interna encargado de comprobar que las políticas de cada sector de la empresa se estén cumpliendo. Este proceso se lleva a cabo utilizando métricas de desempeño externas. |
| 3 | | La política de seguridad de la información comienza en el momento en que un nuevo empleado se incorpora a la |

| | | |
|---|---|---|
| | ¿Qué filtros de seguridad de la información tiene la empresa? | empresa. Se evalúa al personal y se le asignan perfiles de usuario para proteger la información generada y que puede ser ingresada o descargada. Para ello, a cada perfil se le asignan funciones específicas y se restringen sus derechos de acceso. |
| 4 | ¿Cómo se realiza el control de seguridad de la información de sistema APS? | Se lleva a cabo mediante la utilización de cuestionarios que incluyen una lista de verificación de los puntos clave de la política de seguridad de la empresa. Después, se otorga una calificación para evaluar si se están implementando las estrategias destinadas a reducir los riesgos en la gestión de la información. |
| 5 | ¿Qué tipo de mecanismos se aplican en los sistemas de seguridad de información? | La información se asegura mediante la asignación de perfiles y el control de accesos y cambios. |
| 6 | ¿Existe algún tipo de control interno informático en el departamento de tecnología de la empresa? | Si estamos en la etapa inicial de trabajo, mantenemos reuniones regulares con el personal encargado para supervisar el progreso del proceso. |
| 7 | ¿La empresa ha realizado simulacros de caídas de sistema? | No |
| 8 | ¿La empresa realiza monitoreo constante de los mecanismos aplicados? | Si |
| 9 | ¿Cuál es el procedimiento de control post simulacro? | No se han realizado simulacros. |
| 10 | ¿Cómo se aseguran que el sistema de información realiza una correcta gestión de seguridad? | Se comprueba si un colaborador cuyo perfil no tenía permiso para acceder a información confidencial o realizar cambios ha llevado a cabo alguna actividad sospechosa. |

***Elaborado por la autora.***

*Tabla 7. Entrevista al coordinador de tecnología.*

| Orden | Preguntas | Datos relevantes encontrados |
|---|---|---|
| 1 | ¿Cuáles son las políticas de seguridad de la empresa? | La empresa no tiene políticas de seguridad establecidas. |
| 2 | ¿Cómo se aseguran de que las políticas mencionadas se estén aplicando adecuadamente? | Se llevan a cabo revisiones mensuales para verificar si hay información cruzada entre perfiles que no tienen las autorizaciones correspondientes. |
| 3 | ¿Cómo se realiza el control de seguridad de la información? | Se realizan pruebas para cada perfil, simulando fallos, para determinar si los perfiles sin autorización pueden realizar transacciones que no se les permiten. |
| 4 | ¿Cómo se aseguran de que el sistema de información gestione adecuadamente la seguridad? | Se realizan pruebas para cada usuario. |
| 5 | ¿La empresa tiene algún tipo de control interno informático? | La empresa no tiene un control interno formal. |
| 6 | ¿La empresa ha realizado simulacros de caídas de sistema? | No se han llevado a cabo simulacros. |
| 7 | ¿Cuál es el procedimiento de control posterior a los simulacros? | No se han realizado simulacros. |
| 8 | ¿La empresa realiza monitoreo constante de los mecanismos aplicados? | Si |
| 9 | ¿La empresa realiza monitoreo constante de los mecanismos aplicados? | Se llevan a cabo reuniones periódicas para identificar cualquier debilidad en el sistema de información. |
| 10 | ¿Qué mecanismos se aplican en los sistemas de seguridad de la información? | No se cuenta con mecanismos autorizados. |

*Elaborado por la autora.*

Los resultados de las encuestas y entrevistas se basan en la norma ISO / IEC 27001 y en la información obtenida mediante técnicas metodológicas y controles aplicados. Estos resultados permitieron obtener información importante para confirmar la necesidad de establecer directrices de seguridad para el sistema de información APS. De esta manera, se pretende disminuir los posibles riesgos de seguridad en el sistema utilizado por la empresa objeto de estudio.

Se puede afirmar que la empresa no cuenta con políticas de seguridad establecidas, lo que puede generar debilidades en la gestión de la seguridad de la información. A pesar de llevar a cabo revisiones mensuales y pruebas para verificar la correcta aplicación de las políticas, no se cuenta con mecanismos autorizados para garantizar la seguridad de la información. Además, la empresa no tiene un control interno formal y no ha realizado simulacros de caídas de sistema. Aunque se realizan reuniones periódicas para identificar debilidades, es necesario implementar mecanismos adecuados de gestión y mejorar los procedimientos de control y monitoreo para garantizar una adecuada protección de los datos.

Aunque la empresa no cuenta con un control interno formal para la gestión de la información, se están llevando a cabo esfuerzos para implementarlo. La empresa aplica políticas de seguridad a través de un equipo de auditoría interna y filtros de seguridad para el personal y la gestión de la información. El control de seguridad de la información de sistema APS se realiza mediante cuestionarios y se asegura la información mediante la asignación de perfiles y control de accesos. La empresa realiza monitoreo constante y comprueba la correcta gestión de seguridad del sistema a través de la detección de actividades sospechosas.

Luego de las entrevistas se determinó la situación actual de los dominios de control, con la evaluación de su grado de cumplimiento y se estima el porcentaje de cumplimiento de cada control respecto al número total de controles necesarios en el dominio, cuyos resultados se muestran a continuación.

Se puede notar que solamente cumple con el 21,4% de los procedimientos y políticas relacionados con la seguridad de la información que posee. Esto indica que no cumple con el 78,6% de los requisitos de control. La tabla 16 se utiliza para evaluar el sistema de información de AVCAMNET S.A en relación con el estándar ISO 27001 y describe el estado actual de cumplimiento sugerido.

## CONCLUSIONES

Tras la realización de encuestas entre los empleados de AVCAMNET S.A., se ha llegado a la conclusión de que existe una situación de vulnerabilidad en la información debido a la falta de capacitación adecuada del personal en el manejo del sistema de planificación avanzada. La recopilación de datos mediante encuestas ha sido clave para obtener una visión más completa y precisa de la problemática actual. De esta forma, se podrá establecer un plan de acción que permita mejorar la capacitación del personal, a fin de garantizar una gestión de la información segura y efectiva en la empresa.

Durante la entrevista con el departamento de Sistemas, se identificaron varias fallas críticas en los procedimientos de administración de la información en el sistema de planificación avanzada que AVCAMNET S.A. utiliza. Estas fallas han tenido un impacto negativo en la eficiencia y eficacia del sistema, lo que ha llevado a errores y retrasos en la toma de decisiones empresariales importantes. Entre las fallas detectadas, se encontró una falta de controles adecuados en los procedimientos de gestión de la información, lo que ha permitido la entrada de datos incorrectos y la manipulación indebida de la información.

La empresa AVCAMNET S.A. no cuenta con un control interno formal para la gestión de la información, pero se están llevando a cabo esfuerzos para implementarlo. El control de seguridad de la información de sistema APS se realiza mediante cuestionarios y se asegura la información mediante la asignación de perfiles y control de accesos. Entre los riesgos más importantes que afectan al sistema de planificación avanzada utilizado por la empresa AVCAMNET S.A., se destaca la vulnerabilidad continua al acceso y control de cambios en la información. Es por ello que resulta necesario aplicar los principios presentados en la norma ISO / IEC 27001 con el objetivo de reducir dichos riesgos.

## BIBLIOGRAFÍA


Almeida, R., Lourinho, R., Mira da Silva, M., & Pereira, R. (2018). *A model for assessing COBIT 5 and ISO 27001 simultaneously.* New Jersey: IEEE. Obtenido de file:///C:/Users/Eliseo/Downloads/A%20Model%20for%20Assessing%20COBIT%205%20and%20ISO%2027001.pdf

Arreaga P. (2020). *ISO 27001 – Where to Start?* Obtenido de Advisera: http://www.iso27001standard.com/es/que-es-iso-27001/

Calder, A., & Watkins, S. (2019). *IT Governance: An International Guide to Data Security and ISO27001/ISO27002.* Estados Unidos: Fifth.

Calder, A., & Watkins, S. (2020). *IT Governance: An International Guide to Data Security and ISO27001/ISO27002.* Londres: koganpage. Obtenido de https://books.google.com.ec/books?id=qSCyDwAAQBAJ&printsec=frontcover&hl=es&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false

Chilán, S. E., & Pionce, P. W. (2019). Apuntes teóricos introductorios sobre la seguridad de la información. *Dominio de las Ciencias*, 284-295. Obtenido de file:///C:/Users/Eliseo/Downloads/Dialnet-ApuntesTeoricosIntroductoriosSobreLaSeguridadDeLaI-6174477.pdf

De Freitas, V. (25 de 3 de 2009). Análisis y evaluación del riesgo de la información: caso de estudio Universidad Simón Bolívar. *Scielo Venezuela*, 43-55. Obtenido de http://ve.scielo.org/scielo.php?script=sci_arttext&pid=S1690-75152009000100004

Fernández, O. G. (2022). *"Análisis y diseño de un sistema de gestión de la seguridad de la información basado en la norma ISO 27001, orientado a la disminución de riesgos".* Sangolqui: Universidad de las Fuerzas Armadas.

Iso27000. (15 de 11 de 2021). *SGSI*. Obtenido de Iso27000.es: https://www.iso27000.es/sgsi.html

ISO27000. (25 de 3 de 2023). *Política del SGSI*. Obtenido de ISO27000: https://www.iso27000.es/sgsi.html

ISOTools Excellence. (12 de 3 de 2023). *NTP ISO 27001: Los Dominios de Seguridad de la Información*. Obtenido de ISOTools Excellence: https://www.isotools.pe/ntp-iso-27001-dominios/#:~:text=Estos%20son%20los%20dominios%20incluidos,provisi%C3%B3n%20de%20bienes%20y%20servicios.

Leal, R. Y. (2020). *Buenas prácticas de seguridad informática aplicado al comercio electrónico para las Pymes colombianas asociada a la norma ISO 27001.* Bogotá: Universidad Nacional Abierta y a Distancia.

Nicolas, S. (2019). *Modelo de procesos "Planear-Hacer-Verificar-Actuar".* Madrid: Esic. Obtenido de http://blogsgsi.blogspot.com/2016/07/v-behaviorurldefaultvmlo.html

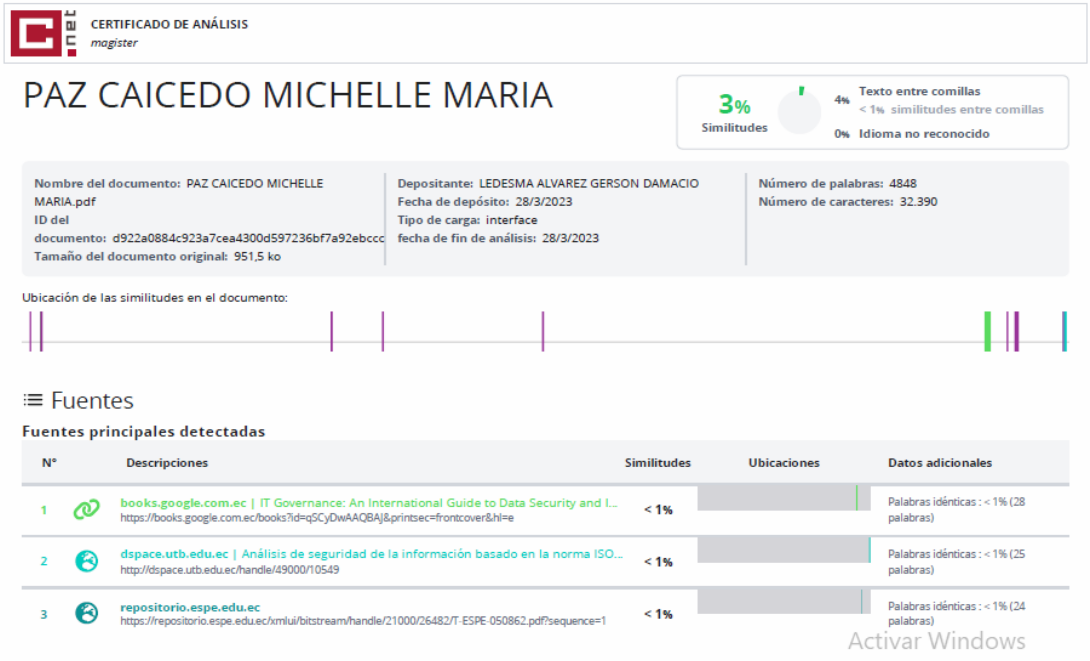
Russell, J. (18 de 03 de 2023). *Introduccion a la norma ISO*. Obtenido de https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf

Sordo, A. I. (08 de Diciembre de 2021). *Sistemas de información en las empresas: tipos, funciones y ejemplos*. Obtenido de Hubspot: https://blog.hubspot.es/marketing/sistema-informacion

Villamar, S. C. (2021). *Análisis de seguridad de la información basado en la norma ISO 27001 en el Área Técnica de Reparación e Instalación de la Corporación Nacional de Telecomunicaciones.* Babahoyo: Universidad Técnica de Babahoyo .

# ANEXOS

## Informe Compilatio



CERTIFICADO DE ANÁLISIS
*magister*

PAZ CAICEDO MICHELLE MARIA

3% Similitudes

4% Texto entre comillas
< 1% similitudes entre comillas
0% Idioma no reconocido

Nombre del documento: PAZ CAICEDO MICHELLE MARIA.pdf
ID del documento: d922a0884c923a7cea4300d597236bf7a92ebccc
Tamaño del documento original: 951,5 ko

Depositante: LEDESMA ALVAREZ GERSON DAMACIO
Fecha de depósito: 28/3/2023
Tipo de carga: interface
fecha de fin de análisis: 28/3/2023

Número de palabras: 4848
Número de caracteres: 32.390

Ubicación de las similitudes en el documento:

Fuentes

Fuentes principales detectadas

| N° | Descripciones | Similitudes | Ubicaciones | Datos adicionales |
|---|---|---|---|---|
| 1 | books.google.com.ec \| IT Governance: An International Guide to Data Security and I... https://books.google.com.ec/books?id=q5CyDwAAQBAJ&printsec=frontcover&hl=e | < 1% | | Palabras idénticas : < 1% (28 palabras) |
| 2 | dspace.utb.edu.ec \| Análisis de seguridad de la información basado en la norma ISO... http://dspace.utb.edu.ec/handle/49000/10549 | < 1% | | Palabras idénticas : < 1% (25 palabras) |
| 3 | repositorio.espe.edu.ec https://repositorio.espe.edu.ec/xmlui/bitstream/handle/21000/26482/T-ESPE-050862.pdf?sequence=1 | < 1% | | Palabras idénticas : < 1% (24 palabras) |

Activar Windows

## Análisis del sistema de información APS en base a los dominios de control de la norma ISO / IEC 27001.

*Tabla 8. Análisis Políticas de seguridad de la información y organización.*

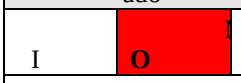
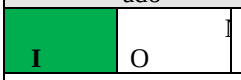
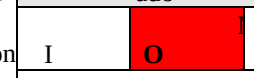
| | | | |
|---|---|---|---|
| **A.5 Políticas de seguridad de la información** | | | |
| **A.5.1 Orientación de la dirección para la gestión de la seguridad de la información** | | | |
| **Objetivo: Brindar orientación y apoyo por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.** | | | |
| A.5.1.2 | Revisión de la política de Seguridad de la información. | Control: Las políticas para seguridad de la información, Se deberían revisar aintervalos planificados o si ocurren cambios significativos para asegurar su conveniencia, adecuación y eficacia continua. | Implementado<br>I O<br>El proceso de tecnología de la empresa no lleva a cabo revisiones periódicas a la política de seguridad de la información, ya que no se tiene definida dicha política. |
| **A.6 Organización de la seguridad de la información**<br>**6.1 Organización interna**<br>**Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementacióny la operación de la seguridad de la información dentro de la organización.** | | | |
| A.6.1.2 | Separación de deberes. | Control: Los deberes y áreas de responsabilidad en conflicto se deberían separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización. | Implementado<br>I O<br>En el proceso de tecnología de la empresa no se lleva a cabo la separación de deberes. |
| A.6.1.4 | Contacto con grupos de interés especial. | Control: Es conveniente mantener contactos apropiados con grupos deinterés especial u otros foros y asociaciones Profesionales especializadas en seguridad. | Implementado<br>I O<br>No se mantienen contactos apropiados con grupos de interés. |
| **7.2 Durante la ejecución del empleo** | | | |
| **Objetivo: Asegurarse de que los empleados tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.** | | | |
| .7.2.1 | Responsabilidades dela dirección. | Control: La dirección debería exigir a todos los empleados la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización. | Implementado<br>I O<br>No se tiene implementado. |
| .7.2.2 | Toma de conciencia,educación y formación en la seguridad de la información. | Control: Todos los empleados de la organización, y en donde sea pertinente, deberían recibir la educación y la formación en toma de conciencia apropiada, y actualizacionesregulares sobre las políticas yprocedimientos pertinentes para su cargo. | Implementado<br>I O<br>No se llevan a cabo campañas de formación y actualización. |

***Fuente: Información obtenida de los instrumentos de investigación.***
***Elaborado por la autora.***

*Tabla 9. Análisis cambio de empleo y Gestión de activos.*

| | | | |
|---|---|---|---|
| **7.2 Durante la ejecución del empleo** | | | |
| **Objetivo: Asegurarse que los empleados tomen conciencia de sus responsabilidades de seguridad dela información y las cumplan.** | | | |
| .7.2.3 | Proceso disciplinario | Control: Se debería contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contraempleados que hayan cometido una violación a la seguridad de la información. | Implementado<br>I **O**<br>No se cuenta con un proceso disciplinario documentado. |
| **7.3 Terminación o cambio de empleo** | | | |
| **Objetivo: Proteger los intereses de la organización como parte del proceso de cambio oterminacióndel contrato.** | | | |
| .7.3.1 | Terminación o cambiode responsabilidades de empleo. | Control: Las responsabilidades y los deberes de seguridad de la información que Permanecen validos después de la terminación o cambio de contrato se deberían definir, comunicar al empleado y se deberían hacer cumplir. | Implementado<br>**I** O<br>Cada que se presenta un cambio de cargo, reemplazo o finalización de un contrato se lleva a cabo la validación del acceso a la información de la persona que presenta dicho cambio de responsabilidades. |
| **A.8 Gestión de activos** | | | |
| **8.1 Responsabilidad por los activos** | | | |
| **Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protecciónapropiadas.** | | | |
| .8.1.1 | Inventario de activos. | Control: Se deberían identificar los activos asociados con la informacióny las instalaciones de Procesamiento de información, y se debería elaborar y mantener un inventario de estos activos. | Implementado<br>**I** O<br>Se tiene un inventario de los activos de información de forma básica. |
| **8.2 Clasificación de la información** | | | |
| **Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con suimportancia para la organización.** | | | |
| .8.2.1 | Clasificación de la información. | Control: La información se debería clasificar en función de los requisitoslegales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada. | Implementado<br>I **O**<br>No se clasifica la información como lo indica el control. |
| .8.2.2 | Etiquetado de la información. | Control: Se debería desarrollar e implementar un conjunto adecuadode procedimientos para el etiquetadode la información de acuerdo con elesquema de clasificación de información adoptado por la organización. | Implementado<br>I **O**<br>No se etiqueta la información en función de su clasificación. |

| | | | |
|---|---|---|---|
| A.8.2.3 | Manejo de activos. | Control: Se deberían desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con elesquema de clasificación de información adoptado por la organización. | Implementado<br>I **O**<br>No se cuenta con procedimientos de manejo de activos en función de la clasificación de la información. |
| **8.3 Manejo de medios** | | | |
| **Objetivo: Evitar la divulgación, modificación, el retiro o la destrucción no autorizados de información almacenada en los medios.** | | | |
| A.8.3.1 | Gestión de medios removibles. | Control: Se deberían implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización. | Implementado<br>I **O**<br>No se tienen implementados procedimientos para los medios removibles. |
| A.8.3.2 | Disposición de los medios. | Control: Se debería disponer en formasegura de los medios cuando ya no se requieran, utilizando procedimientos formales. | Implementado<br>**I** O<br>Se cuenta con un procedimiento para la disposición final de equipos tecnológicos. |
| A.8.3.3 | Transferencia de medios físicos. | Control: Los medios que contienen información se deberían proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte. | Implementado<br>I **O**<br>No se cuentan con procedimientos que aseguren el acceso no autorizado a los medios durante su transporte. |
| **A.9 Control de acceso** | | | |
| **9.1 Requisitos del negocio para control de acceso** | | | |
| **Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.** | | | |
| | | | Implementado<br>I **O** |
| A.9.1.1 | Política de control de acceso. | Control: Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información. | No se cuenta con una política para el control de acceso. |
| **9.2 Gestión de acceso de usuarios** | | | |
| **Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemasy servicios.** | | | |
| A | Registro y cancelacióndel | Control: Se debería implementar un proceso formal de registro y decancelación de registro | Implementado<br>**I** O |

| | | | |
|---|---|---|---|
| .9.2.1 | registro de usuarios. | de usuarios, para posibilitar la asignación de los derechos de acceso. | Se cuenta con un software que lleva a cabo el registro y cancelación de acceso de los usuarios, así mismo se administran los derechos deacceso. |
| .9.2.2 | Suministro de acceso de usuarios. | Control: Se debería implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios. | Implemento<br>  <br>No hay un proceso que defina formalmente el acceso de los usuarios a los sistemas, puestoque estos son definidos segúnsus funciones y su cargo. |
| .9.2.3 | Gestión de derechosde acceso privilegiado. | Control: Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado. | Implemento<br>  <br>Se lleva a cabo los procedimientos necesarios para limitar el acceso a los sistemas a través del perfilamiento de los cargos. |
| .9.2.4 | Gestión de información de autenticación secreta de usuarios. | Control: La asignación de la información secreta se debería controlar por medio de un proceso de gestión formal. | Implemento<br>  <br>No se cuenta con el proceso de gestión formal. |

***Fuente: Información obtenida de los instrumentos de investigación.***
***Elaborado por la autora.***

*Tabla 10. Análisis del sistema, aplicaciones y criptografía.*

| | | | |
|---|---|---|---|
| **9.4 Control de acceso a sistemas y aplicaciones** | | | |
| **Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones** | | | |
| .9.4.3 | A Sistema de gestión de contraseñas. | Control: Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas. | Implementado<br>SI **O**<br>Las aplicaciones corporativas cuentan con su sistema gestor de contraseñas, en el que se exige unminino de características en las contraseñas. |
| .9.4.4 | A Uso de program as utilitario s privilegia dos | Control: Se debería restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones. | Implementado<br>SI **O**<br>Se lleva a cabo la restricción a utilitarios |
| .9.4.5 | A Cont rol de acceso acódigos fuente de programas. | Control: Se debería restringir el acceso a los códigos fuente de los programas. | Implementado<br>**SI** O<br>Se tiene restringido el acceso alos códigos fuente de las aplicaciones corporativas. |
| **A.10 Criptografía** | | | |
| **10.1 Controles criptográficos** | | | |
| **Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger laconfidencialidad,la autenticidad y/o la integridad de la información.** | | | |
| .10.1.1 | A Política sobre el uso de controles criptográficos. | Control: Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información. | Implementado<br>SI **O**<br>Existe la política de controles criptográficos. |
| .10.1.2 | A Gestión de llaves. | Control: Se debería desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida. | Implementado<br>SI **O**<br>Existe política para la gestión de llaves criptográficas. |
| **A.11 Seguridad física y del entorno** | | | |
| **11.1 Áreas seguras** | | | |
| **Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a lasinstalaciones de procesamiento de información de la organización.** | | | |
| .11.1.1 | A Perímetro de seguridad física. | Control: Se deberían definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o critica, e instalaciones de manejo de información. | Implementado<br>**SI** O<br>Se tienen definidos perímetros de seguridad en instalaciones de manejo de información. |
| | | Control: Las áreas seguras se deberían proteger | Implementado<br>**SI** O |

| | | | |
|---|---|---|---|
| A.11.1.2 | Controles físicos de entrada. | mediante controles de entrada apropiados para asegurar que solamente se permite el accesoa personal autorizado. | Se cuenta con un sistema de control de acceso físico a través de tarjetas de proximidad, en el que se limita el acceso a ciertos perímetros de la compañía. |
| A.11.1.3 | Seguridad de oficinas, recintos e instalaciones. | Control: Se debería diseñar y aplicar seguridad física a oficinas, recintos e instalaciones | Implementado<br>**I** O<br>Dentro del edificio en el que la compañía desarrolla su actividad administrativa se cuenta con el control de acceso a oficinas y sectores específicos y en oficinas críticas, como gerencia, dirección y entre otras se cuenta con chapas físicas que limitan elacceso a solo el personal autorizado, pero en las tiendas no es implementado y es ahí donde son vulnerables. |
| A.11.1.4 | Protección contra amenazas externasy ambientales. | Control: Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes. | Implementado<br>I **O**<br>No se cuenta con controles específicos para amenazas extremas y ambientales. |
| A.11.1.5 | Trabajo en áreas seguras. | Control: Se deberían diseñar y aplicar procedimientos para trabajo en áreas seguras. | Implementado<br>**SI** O<br>La compañía cuenta con procedimientos dentro de su sistema de gestión de calidad de trabajo en áreas seguras. |
| A.11.1.6 | Áreas de despacho y carga. | Control: Se deberían controlarlos puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado. | Implementado<br>**SI** O<br>Cerca del perímetro en donde se lleva a cabo procesamiento de información no se ejecutanprocesos de despacho o carga. |
| **11.2 Equipos** | | | |
| **Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.** | | | |
| A.11.2.1 | Ubicación y protección de los equipos. | Control: Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado. | Implementado<br>**SI** O<br>Los equipos se encuentran ubicados de forma tal que su acceso sea únicamente para los usuarios autorizados, es decir, ubicados después de los controles de acceso por tarjeta de proximidad y monitoreada por CCTV. |
| | | Control: Los equipos se deberían proteger | Implementado<br>**SI** O |

| | | | |
|---|---|---|---|
| A .11.2.2 | Servicios de suministro. | contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro. | El edificio administrativo cuenta con un sistema de respaldo eléctrico a través de UPS y plantaeléctrica que satisface la perdidade suministro de energía. |

***Fuente: Información obtenida de los instrumentos de investigación.***
***Elaborado por la autora.***

*Tabla 11. Análisis Gestión de la vulnerabilidad técnica.*

| | | | |
|---|---|---|---|
| **12.6 Gestión de la vulnerabilidad técnica** | | | |
| **Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas** | | | |
| A.12.6.1 | Gestión de las vulnerabilidades técnicas. | Control: Se debería obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado. | Implementado<br>I **O**<br>Se lleva a cabo la gestión de vulnerabilidades técnicas. |
| A.12.6.2 | Restricciones sobre lainstalación de software. | Control: Restricciones sobre la instalación de software. | Implementado<br>**I** O<br>Se cuenta con una restricción para la instalación de software, en el que el sistema operativo solicita por obligatoriedad la contraseña del administrador para ejecutar la instalación, en donde dicha contraseña solo la tiene el área de tecnología. |
| **12.7 Consideraciones sobre auditorias de sistemas de información** | | | |
| **Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operacionales.** | | | |
| A.12.7.1 | Información controles de auditoría de sistemas. | Control: Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deberían planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio. | Implementado<br>I **O**<br>Se ejecutan auditorías a los sistemas de información de manera periódica. |
| **13. Seguridad de las comunicaciones** | | | |
| **13.1 Gestión de la seguridad de las redes** | | | |
| **Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte** | | | |
| A.13.1.1 | Controles de redes. | Control: Las redes se deberían gestionar y controlar para proteger la información ensistemas y aplicaciones. | Implementado<br>**I** O<br>Se gestiona a través de firewall,IDS e IPS controles sobre la red. |
| **13.2 Transferencia de información** | | | |
| **Objetivo: Mantener la seguridad de la información transferida dentro de una organización ycon cualquier entidad externa** | | | |
| A | Acuerdos | Control: Se deberían identificar, revisar regularmente y | Implementado<br>**I** O |

| | | | |
|---|---|---|---|
| .13.2.4 | de confidencialidad o de nodivulgación. | documentar los requisitos para los acuerdos de confidencialidad y no divulgación que reflejen las necesidades de la organización para la protección de la información. | Se cuentan con acuerdos de confidencialidad entre los empleados y los terceros externos. |
| **14 adquisición, desarrollo y mantenimientos de sistemas** | | | |
| **14.1 Requisitos de seguridad de los sistemas de información** | | | |
| **Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios en redes públicas.** | | | |
| A .14.1.1 | Análisis y especificación de requisitos de seguridadde la información. | Control: Los requisitos relacionados con seguridad de la información se deberían incluir en nuevos sistemas de información para mejoras a los sistemas de información existentes. | Implementado<br>I **O**<br>Se lleva a cabo el respectivo análisis y especificación de los requisitos de seguridad de la información para los nuevos sistemas. |
| A .14.1.2 | Seguridad de servicios de las aplicaciones en redes públicas. | Control: La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debería proteger de actividades fraudulentas, disputas contractuales, divulgación y modificación no autorizada. | Implementado<br>I **O**<br>No se tiene implementado el control para la seguridad de servicios de las aplicaciones en redes públicas porque es una empresa privada y el sistema queutilizan es externo. |
| **14.2 Seguridad en los procesos de desarrollo y soporte** | | | |
| **Objetivo: Asegurar de que la seguridad de la información esté diseñada e implementada dentro delciclo de vida de desarrollo de los sistemas de información.** | | | |
| A .14.2.4 | Restricciones en los cambios a los paquetes de software. | Control: Se deberían desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deberían controlarestrictamente. | Implementado<br>I **O**<br>Hay restricción a cambios en elárea de tecnología. |
| | | Control: Se deberían establecer, | Implementado<br>I **O** |
| A .14.2.5 | Principios de construcción de sistemas seguros. | documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información. | Se tienen claros los principios de construcción de sistemasseguros. |
| A .14.2.6 | Ambiente de desarrollo seguro. | Control: Las organizaciones deberían establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas. | Implementado<br>I **O**<br>Se tienen claros los principios de construcción de sistemas seguros. |
| | Desarrollo | Control: La organización | Implementado<br>I **O** |

| | | | |
|---|---|---|---|
| A.14.2.7 | contratado externamente. | debería supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externa mente. | Se tiene del software contratadoexternamente. |
| A.14.2.8 | Pruebas de seguridad de sistemas. | Control: Durante el desarrollo sedeberían llevar a cabo pruebas de funcionalidad de la seguridad. | Implementado<br>I **O**<br>La compañía no lleva a cabo el desarrollo de la aplicación. |
| A.14.2.9 | Prueba de aceptación de sistemas. | Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deberían establecer programas de prueba para aceptación y criterios de aceptación relacionados. | Implementado<br>I **O**<br>La compañía no lleva a cabo el desarrollo de la aplicación ya que es contratada manera externa. |
| **14.3 Datos de Prueba** | | | |
| **Objetivo: Asegurar la protección de los datos usados para pruebas.** | | | |
| A.14.3.1 | Protección de datos de prueba. | Control: Los datos de ensayo se deberían seleccionar, proteger y controlar cuidadosamente | Implementado<br>I **O**<br>La compañía no lleva a cabo eldesarrollo del sistema. |
| **15. Relación con los proveedores** | | | |
| **15.1 Seguridad de la información en las relaciones con los proveedores** | | | |
| **Objetivo: Asegurar la protección de los activos de la organización que sean accesibles alos proveedores.** | | | |
| | | Control: Los requisitos de seguridad de la información para | Implementado<br>I **O** |
| A.15.1.1 | Política de seguridad de la información para las relaciones con proveedores. | mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deberían acordar con estos y se deberían documentar. | No se tiene implementado una política de seguridad de la información para las relaciones con proveedores. |
| A.15.1.2 | Tratamiento de la seguridad dentro de los acuerdos con proveedores. | Control: Se deberían establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización. | Implementado<br>I **O**<br>Se lleva a cabo tratamiento de seguridad de la información dentro de los acuerdos con proveedores. |
| **16. Gestión de incidentes de seguridad de la información** | | | |
| **16.1 Gestión de incidentes y mejoras en la seguridad de la información** | | | |
| **Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.** | | | |
| | Evaluación | Control: Los eventos de | Implementado<br>I **O** |

| | | | |
|---|---|---|---|
| A.16.1.4 | de eventosde seguridad de la información y decisiones sobre ellos. | seguridad de la información se deberían evaluar y se debería decidir si se van a clasificar como incidentes de seguridad de la información. | La compañía cuenta con gestión a incidentes de sistema. |
| A.16.1.5 | Respuesta a incidentesde seguridad de la información. | Control: Se debería dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados. | Implementado<br>I **O**<br>La compañía cuenta congestión a incidentes de sistema. |
| A.16.1.6 | Aprendizaje obtenidode los incidentes de seguridad de la información. | Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debería usar para reducir la posibilidad o el impacto de incidentes futuros. | Implementado<br>I **O**<br>La compañía no cuenta con gestión a incidentes de sistema. |
| A.16.1.7 | Recolección de evidencia. | Control: La organización debería definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia. | Implementado<br>I **O**<br>La compañía no cuenta con gestión a incidentes de sistema. |
| **18. Cumplimiento** | | | |
| **18.1 Cumplimiento de requisitos legales y contractuales** | | | |
| **Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquierrequisito de seguridad.** | | | |
| A.18.1.4 | Reglament ación decontroles criptográficos. | Control: Se deberían usar controles criptográficos, encumplimiento de todos los acuerdos, legislación y reglamentación pertinentes. | Implementado<br>I **O**<br>Se utilizan controles criptográficos. |
| **18.2 Revisiones de seguridad de la información** | | | |
| **Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdocon laspolíticas y procedimientos organizacionales.** | | | |
| A.18.2.1 | Revisión independiente de la seguridad de la información. | Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deberían revisar independientemente a intervalos planificados o cuando ocurran cambios significativos. | Implementado<br>I O<br>No se lleva a cabo revisión sobre la gestión de la seguridad de la información. |
| | Cumplim | Control: Los directores deberían revisar con regularidad el | Implementado<br>I **O** |

| | | | |
|---|---|---|---|
| .18.2.2 | A iento conlas políticas y normas de seguridad. | cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad. | Teniendo en cuenta que no se posee una política de seguridad de la información no se valida sucumplimiento. |

***Fuente: Información obtenida de los instrumentos de investigación.***
***Elaborado por la autora.***

*Tabla 12. Dominios de control del sistema de información APS de la empresa AVCAMNET S.A.*

| | | |
|---|---|---|
| A5. Políticas de la seguridad de la información | % | 00% |
| A6. Organización de la seguridad de la información | % | 00% |
| A7. Seguridad de los recursos humanos | 1<br>6.7% | 3.3% |
| A8. Gestión de activos | 3<br>7.5% | 2.5% |
| A9. Control de acceso | 3<br>5.7% | 4.3% |
| A10. Criptografía | 0<br>.0% | 00.0% |
| A11. Seguridad física y del entorno | 7<br>3.3% | 6.7% |
| A12. Seguridad de las operaciones | 3<br>5.7% | 4.3% |
| A13. Seguridad de las comunicaciones | 4<br>2.9% | 7.1% |
| A14. Adquisición, desarrollo y mantenimiento de sistemas | 7<br>.7% | 2.3% |
| A15. Relaciones con los proveedores | 0<br>.0% | 00.0% |
| A16. Gestión de incidentes de seguridad de la información | 1<br>2.5% | 7.5% |
| A17. Aspectos de seguridad de la información de la gestión de la continuidad del negocio | 0<br>.0% | 00.0% |
| A18. Cumplimiento | 3<br>7.5% | 2.5% |

***Adaptado de AVCAMNET S.A (2022).***
***Elaborado por la autora.***

## ANEXO 2: RUC de la empresa

**Representante legal**

- VALLE RIOFRIO ARTURO ALBERTO

| Estado | Régimen | |
|---|---|---|
| ACTIVO | RIMPE - EMPRENDEDOR | |
| **Fecha de registro** | **Fecha de actualización** | **Inicio de actividades** |
| 01/03/2023 | No registra | 01/03/2023 |
| **Fecha de constitución** | **Reinicio de actividades** | **Cese de actividades** |
| 27/02/2023 | No registra | No registra |
| **Jurisdicción** | | **Obligado a llevar contabilidad** |
| ZONA 9 / PICHINCHA / QUITO | | NO |
| **Tipo** | **Agente de retención** | **Contribuyente especial** |
| SOCIEDADES | NO | NO |

## Domicilio tributario

**Ubicación geográfica**

**Provincia:** PICHINCHA **Cantón:** QUITO **Parroquia:** TURUBAMBA

**Dirección**

**Calle:** E 4I **Número:** 49 **Intersección:** CALLE S **Número de piso:** PB **Referencia:** DENTRO DEL CENTRO COMERCIAL ACHOMEC

## Medios de contacto

**Email:** avalleisp2012@gmail.com **Celular:** 0968604987

## Actividades económicas

- G47411101 - VENTA AL POR MENOR DE COMPUTADORAS EN ESTABLECIMIENTOS ESPECIALIZADOS.
- N80200101 - ACTIVIDADES DE SUPERVISIÓN A DISTANCIA DE SISTEMAS ELECTRÓNICOS DE SEGURIDAD, COMO LOS DE ALARMA CONTRA ROBOS Y CONTRA INCENDIOS, INCLUIDO SU INSTALACIÓN Y MANTENIMIENTO. LA UNIDAD QUE LLEVA A CABO ESTA ACTIVIDAD PUEDE DEDICARSE TAMBIÉN A LA VENTA DE ESTOS SISTEMAS DE SEGURIDAD.
- J61100401 - ACTIVIDADES DE SUMINISTRO EN ACCESO A INTERNET POR LOS OPERADORES DE LA INFRAESTRUCTURA DE TELECOMUNICACIONES ALAMBRICAS.
- G47411301 - VENTA AL POR MENOR DE EQUIPOS DE TELECOMUNICACIONES: CELULARES, TUBOS ELECTRÓNICOS, ETCÉTERA. INCLUYE PARTES Y PIEZAS EN ESTABLECIMIENTOS ESPECIALIZADOS.
- J61100101 - ACTIVIDADES DE OPERACIÓN, MANTENIMIENTO O FACILITACIÓN DEL ACCESO A SERVICIOS DE TRANSMISIÓN DE VOZ, DATOS, TEXTO, SONIDO Y VÍDEO UTILIZANDO UNA INFRAESTRUCTURA DE TELECOMUNICACIONES ALAMBRICAS, COMO: OPERACIÓN Y MANTENIMIENTO DE SISTEMAS DE CONMUTACIÓN Y TRANSMISIÓN PARA SUMINISTRAR SERVICIOS DE COMUNICACIONES DE PUNTO A PUNTO POR LÍNEAS ALAMBRICAS, POR MICROONDAS O POR UNA COMBINACIÓN DE LÍNEAS ALAMBRICAS Y CONEXIONES POR SATÉLITE.





| Razón Social | Número RUC |
|---|---|
| AVCAMNET S.A.S | 1793204722001 |

## Establecimientos

| Abiertos | Cerrados |
|---|---|
| 1 | 0 |

## Obligaciones tributarias

- 2021 - DECLARACIÓN SEMESTRAL IVA
- 1021 - DECLARACIÓN DE IMPUESTO A LA RENTA SOCIEDADES
- ANEXO RELACIÓN DEPENDENCIA
- ANEXO TRANSACCIONAL SIMPLIFICADO
- ANEXO ACCIONISTAS, PARTÍCIPES, SOCIOS, MIEMBROS DEL DIRECTORIO Y ADMINISTRADORES – ANUAL
- ANEXO DE DIVIDENDOS, UTILIDADES O BENEFICIOS - ADI
- 9090 - IMPUESTO DE PATENTE MUNICIPAL

## ANEXO 3: Carta de Autorización

**Anexo 4: Reporte de plagio**