UNIVERSIDAD DE EL SALVADOR

FACULTAD DE CIENCIAS ECONÓMICAS

ESCUELA DE CONTADURÍA PÚBLICA

"GUÍA PARA LA PLANEACIÓN E IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN, BASADO EN LA ISO 27001 APLICADAS A CLÍNICAS Y HOSPITALES VETERINARIOS DEL ÁREA METROPOLITANA DE SAN SALVADOR"

TRABAJO DE INVESTIGACIÓN PRESENTADO POR:

DÍAZ RAMÍREZ, KARLA BEATRIZ

ESCAMILLA MARTÍNEZ, MARIO ANTONIO

VELÁSQUEZ CARBALLO, DAVID ERNESTO

PARA OPTAR EL GRADO DE:

LICENCIATURA EN CONTADURÍA PÚBLICA

FEBRERO 2020

SAN SALVADOR, EL SALVADOR, CENTROMÉRICA

AUTORIDADES UNIVERSITARIAS

Rector	Msc. Roger Armando Arias Alvarado
Secretario General	Lic. Cristóbal Hernán Ríos Benítez
Decano de la Facultad de Ciencias Económicas	Lic. Nixon Rogelio Hernández Vásquez
Vice Decano de la Facultad de Ciencias Económicas	Msc. Mario Wilfredo Crespín Elías
Secretario de la Facultad de Ciencias Económicas	Lic. Francisco Antonio Alarcón Sandoval
Director de la Escuela de Contaduría Pública	Lic. Gilberto Díaz
Coordinador General de Seminario de Graduación	Lic. Mauricio Ernesto Magaña Menéndez
Jurado Examinador	

Febrero 2020

San Salvador, El salvador, Centroamérica

AGRADECIMIENTOS

En primer lugar, agradezco a mis padres, José y Reina por haberme apoyado en diferentes etapas de mi formación académica y que siempre mostraron su confianza que concluiría mi sueño; a mi esposa Fátima y mi hijo José David que me han impulsado y ayudado a concluir este proceso; a mis hermanos que de alguna u otra manera me apoyaron a llegar lejos y no rendirme; y a mis amigos y compañeros de trabajo de graduación que han estado en los buenos y en los no tan buenos momentos, pero siempre dando ánimos para salir adelante, independientemente las dificultades que tuviéramos por delante.

David Ernesto Velásquez Carballo

Agradecer primeramente a Dios por permitirme culminar este propósito tan importante en mi vida. A mis padres Nohemy y Juan que han sido mi apoyo moral, espiritual, económico e incondicional desde mi infancia hasta el día de hoy y en especial durante mi etapa universitaria. A mis amigos y compañeros de trabajo de graduación por todo el apoyo, paciencia, y aprecio brindada durante tanto tiempo y que nos ha permitido llegar hasta acá. A todos los demás familiares y amigos que de una u otra manera me motivaron a seguir adelante y me han acompañado durante este proceso.

Mario Antonio Escamilla Martínez

Primeramente, agradecer a Dios por brindarme vida, sabiduría y fuerza para salir adelante cada día y permitirme finalizar una de mis principales metas. A mi Madre por ser siempre un pilar fundamental en vida, por su apoyo incondicional en todas las áreas de mi vida y porque no importando las circunstancias, siempre ha velado por darme las herramientas necesarias para garantizar mi formación académica desde mi niñez hasta ahora en día. A mi familia y amigos en general, por creer siempre en mí y animarme a no darme por vencida. A nuestro asesor por orientarnos durante el transcurso de este proceso y regalarnos de su tiempo y conocimiento, y compañeros y amigos de trabajo de graduación por su apoyo ante las adversidades y paciencia durante este proceso.

Karla Beatriz Díaz Ramírez

CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN EJECUTIVO

En la actualidad el avance tecnológico que se está presentando trae consigo desafíos que generan preocupaciones a los altos directivos organizacionales. Garantizar un máximo nivel de disponibilidad, integridad y confidencialidad de la información manejada diariamente en las organizaciones es un aspecto de gran importancia que se procura tener en cuenta dentro de las labores empresariales hoy en día. En el mundo de las redes y comunicaciones se presentan diferentes amenazas tales como los ataques de ciberdelincuentes en busca de datos confidenciales y de gran interés comercial, sabotajes, modificación de información altamente confidencial, entre otras, que se realizan con algún interés económico, comercial, competitivo o con el fin de que el atacante obtenga alguna reputación.

Por lo anterior, es de gran utilidad para las organizaciones la implementación de un SGSI (Sistema de Gestión de Seguridad de la Información) el cual está fundamentado sobre la norma ISO27001 y establece un proceso sistemático para la protección ante cualquier amenaza que podría llegar afectar la confidencialidad, integridad o disponibilidad de la información.

Para el caso de El Salvador, la metodología propuesta a fin de implementar el SGSI es la NTS ISO/IEC 27001:2013 que constituye la adopción realizada por parte del OSN(Organismo Salvadoreño de Normalización) y que permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos. La aplicación de ésta norma significa una diferenciación respecto al resto, que mejora la competitividad y la imagen de una organización.

El tipo de estudio que se utilizó es el método hipotético deductivo que consiste en hacer observaciones del contexto, para conocer las características del problema en la gestión de los principales riesgos de la información, para ello la investigación se apoya en los resultados obtenidos en las encuestas dirigidas a contadores de las clínicas y/o hospitales veterinarios, por lo tanto y según el análisis de la información proporcionada al menos la mitad del universos estudiado no tiene implementado un SGSI pero reconocen que la importancia de contar con uno es relevante dentro de la empresas para las cuales laboran.

De acuerdo a los resultados de la investigación y con el propósito de mejora se recomienda a las clínicas y hospitales veterinarios lo siguiente: llevar cabo el proceso de implementación de un SGSI basado en la NTS ISO/IEC 27001:2013 siguiendo los pasos y lineamientos establecidos en el presente trabajo de investigación y adaptándolo a las necesidades de cada entidad, además se debe garantizar la realización de capacitaciones periódicas al personal correspondiente para que el seguimiento de los procesos se realice de la manera más adecuada y eficiente.

INTRODUCCIÓN

Las compañías crecen y se desarrollan en un ambiente dominado por la tecnología, en los últimos años se han implementado desarrollos importantes en la materia, que ayudan a agilizar procesos y disminuir costos. De esta forma las empresas dedicadas a brindar servicios veterinarios han implementado sistemas de información que ayude a manejar mejor la información de sus clientes.

Resultado de esto es la necesidad de las empresas que prestan servicios veterinarios gestionar los riesgos a los que está expuesta la información de los sistemas informáticos, tales como, el manejo, la filtración y pérdida de datos, con el fin de asegurar la integridad de la información.

El trabajo tiene como objetivo desarrollar una guía para la planeación e implementación de un sistema de gestión de la seguridad de la información para empresas dedicadas a prestar servicios veterinarios basados en la ISO 27001 y otras normas conexas, manteniendo la fiabilidad y seguridad de la información.

Para su desarrollo, el trabajo está estructurado en capítulos, en el capítulo I, se aborda la situación actual de las clínicas y hospitales veterinarios, también se conocen los objetivos planteados, así como las hipótesis referentes a la investigación.

En el capítulo II, se desarrolla un marco teórico que incluye información referente a las clínicas y hospitales veterinarios, guías y procedimientos aplicados a la gestión de la seguridad de la información, además, se conocen el marco legal donde se analiza el surgimiento del Organismo Salvadoreño de Normalización, leyes como la Ley de Firma

Electrónica y Ley Especial Contra Delitos Informáticos y Conexos, técnico y normativo a tener en cuenta para la implementación de un SGSI basado en la NTS ISO/IEC 27001:2013.

Seguidamente, en el capítulo III, se detalla el diseño metodológico como respaldo de proceso investigativo que define el tipo de estudio, unidad de análisis, universo, muestra, instrumentos y técnicas utilizadas en la investigación, procesamiento de la información, análisis e interpretación de los datos procesados y diagnóstico de la misma.

Finalmente, en el capítulo IV se desarrolla un caso práctico en el cual es aplicado un SGSI a la veterinaria “ABC”, que viene a dar solución a la problemática descrita en el desarrollo del trabajo, esto para realizar las conclusiones y recomendaciones de los resultados obtenidos.

1 CAPÍTULO I. PLANTEAMIENTO DEL PROBLEMA

1.1 Situación de las clínicas y hospitales veterinarios

En El Salvador el sector comercial de las clínicas y hospitales veterinarios es un rubro que ha ido creciendo con el pasar de los años, a medida que la profesión veterinaria se va proliferando y cada vez más personas deciden estudiar ésta carrera. Muchas veterinarias han sido establecidas en distintos puntos del país y principalmente en la capital. Teniendo en cuenta dicho crecimiento se puede afirmar que, como cualquier otro tipo de empresas, también están expuestos a diversos riesgos de índole informático, tales como los ataques cibernéticos o pérdida de información por eventos externos. A pesar de su importancia la administración de dichos establecimientos no ha considerado la implementación de un sistema de gestión para dichos riesgos, pues lo consideran irrelevante y prefieren enfocar sus esfuerzos y estrategias a otras áreas como el incremento de ventas.

La seguridad de la información comprende tres aspectos fundamentales: confidencialidad, integridad y disponibilidad; así como otros de importancia significativa; comunicación, identificación de problemas, análisis de riesgos y recuperación de los mismos. Es necesario señalar que su manejo está basado en la tecnología y que puede tener un elevado valor para las empresas, por lo que está expuesta a ser divulgada, mal utilizada, robada, borrada o saboteada.

Ahora bien, se estableció que el crecimiento del sector veterinario (entendiendo tanto clínicas como hospitales) lo expone a diversos riesgos, incluido el de la seguridad de su información, por lo tanto, es necesario elaborar y diseñar un sistema de gestión de riesgos

(para la seguridad de la información) que permita identificar las amenazas específicas que dicho sector afronta en el día a día con todas las operaciones que realizan.

Las clínicas y hospitales veterinarios manejan una amplia gama de información sensible y valiosa: datos personales de sus clientes (nombres, domicilio particular, lugar de trabajo, números de identificación personal, números telefónicos), registro clínico de sus pacientes (consultas, vacunas, seguimiento de enfermedades), recetas, entre otros además de la información contable y administrativa (libros de IVA, partidas contables, controles de inventario, cortes de caja, listado de proveedores, reportes de cuentas por cobrar y por pagar), es evidente que ésta información comprende un conjunto de elementos significativamente importantes que la convierten en un activo más dentro de las entidades y por ende requiere una adecuada gestión para garantizar su seguridad a corto y largo plazo.

El ISO/IEC 27001 es un estándar para la seguridad de la información (Sistema de Gestión de Seguridad de la Información (SGSI)) aprobado y publicado como estándar internacional, por primera vez en 2005. La gestión de la seguridad de la información ofrece la seguridad necesaria al crecer, innovar y ampliar su negocio y su base de clientes, teniendo la certeza que toda su información conservará su calidad de "confidencial". La norma ISO 27001 es la herramienta para enfrentar el reto.

1.2 Enunciado del Problema

El equipo de investigación plantea la siguiente interrogante:

¿En qué medida la falta de un Sistema de Gestión de Seguridad de la Información afecta el triángulo de la seguridad (CID) de los hospitales y clínicas veterinarias ubicadas el área metropolitana de San Salvador?

1.3 Justificación de la investigación

1.3.1 Novedoso

La investigación se considera novedosa debido a que muchas veterinarias establecidas en el área de metropolitana de San Salvador no cuentan en la actualidad con un SGSI y menos que esté basado en una norma ISO. Además, no existen otras investigaciones con un enfoque similar aplicado dirigido a éste sector en la Universidad de El Salvador u otras universidades.

1.3.2 Factible o Viable

La factibilidad de la investigación es considera bajo cuatro aspectos fundamentales:

Documental

Se cuenta con documentos bibliográficos válidos y vigentes que abordan la temática en cuestión y pueden ayudar a sustentar la investigación propuesta. Además, existen normas técnicas (emitidas internacionalmente y tropicalizadas regionalmente) que servirán como base técnica, principalmente la NTS ISO-IEC 27001:2013 y cuyo objetivo es el establecimiento, implementación, mejora y certificación de los SGSI para todo tipo de empresas.

De Campo

Toda la información necesaria se obtendrá de parte de los contadores en los hospitales y clínicas veterinarias (objetos de análisis), de igual manera será posible llevar a cabo las encuestas (o cualquier otro instrumento) que permitirán formular las respectivas conclusiones de la investigación.

Recursos Financieros y Materiales

La investigación se realizará con recursos económicos y materiales propios tales como laptops e impresoras, así como de la participación activa y propositiva del personal encargado (egresados). Se prevé realizar inversión considerable de tiempo (horas-hombre).

Apoyo institucional

La Escuela de Contaduría Pública de la Universidad de El Salvador ha asignado docentes asesores encargados de impartir el seminario, y que tienen como objetivo coordinar y guiar adecuadamente la realización de los trabajos de graduación en las áreas especiales siguiendo los objetivos y directrices planteados por la alta dirección.

1.3.3 Utilidad Social

Con ésta investigación se pretende brindar a los hospitales y clínicas veterinarias una adecuada y precisa guía que le permita a la administración la implementación de un SGSI y mejorar así sus procesos internos a nivel gerencial y operativo.

1.4 Objetivos

1.4.1 Objetivo General

Diseñar una guía integral que le permita a la administración implementar un Sistema de Gestión de Seguridad de la Información en los hospitales y clínicas veterinarias ubicadas en el área Metropolitana de San Salvador, basada en la NTS ISO-IEC 27001-2013

1.4.2 Objetivos Específicos

- Definir un proceso de evaluación de riesgos de la seguridad de información que permita establecer criterios e identificar dichos riesgos.

- Elaborar un manual de políticas de seguridad riguroso que permita resguardar la información de las empresas objeto de estudio.
- Plantear el diseño de un SGSI acorde a las necesidades de los objetos de estudio.
- Elaborar una guía de pasos para lograr la implementación del SGSI previamente diseñado.

Establecer un listado de verificación del cumplimiento de las políticas diseñadas para llevar a cabo un control y seguimiento de los SGSI que implementen las clínicas y hospitales veterinarios.

1.5 Formulación de hipótesis

1.5.1 Hipótesis de Trabajo

La implementación de un SGSI mejorará los procesos de seguridad informática y ciberseguridad de los hospitales y clínicas veterinarias del área metropolitana de San Salvador.

1.5.2 Determinación de Variables

- **Variable independiente**

Implementación de un Sistema de Gestión de la Seguridad de la Información.

- **Variable dependiente**

Mejora en los hospitales y clínicas veterinarias del área metropolitana de San Salvador.

2 CAPÍTULO II. MARCO TEÓRICO

2.1 Antecedentes

2.1.1. Antecedentes del sector veterinario

En El Salvador, la Universidad de El Salvador fundó la Facultad de Ciencias Agronómicas el 21 de agosto de 1964 por acuerdo del Consejo Superior Universitario 29-8-64, esto a raíz de una reforma universitaria que comenzó en 1963. Pero no fue hasta el 26 de noviembre de 1998 que se crea la carrera de Veterinaria y Zootecnia como tal, según acuerdo de Consejo Superior Universitario No. 126-95-99; es inaugurada el 16 de febrero de 1999 y su creación obedece a la necesidad de formar profesionales que enfrenten y solucionen los problemas del sector pecuario que limita la producción. (Universidad de El Salvador, 2008). Éste viene siendo el poco antecedente que existe sobre el sector veterinario en el país.

Junta de Vigilancia de la Profesión Médico Veterinaria de El Salvador

A principios del año 1985, el gremio médico veterinario con la finalidad que la carrera de Medicina Veterinaria fuera reconocida a nivel nacional y contribuir a la excelencia de la misma, por tener un papel muy importante dentro de la economía nacional, solicitó a la Asamblea Legislativa, la creación de la Junta de Vigilancia de la Profesión Médico Veterinaria para ser incorporada al Consejo Superior de Salud Pública, quedando oficialmente establecida, en el Decreto Legislativo No. 357 con fecha 21 de marzo de 1985, publicado en el Diario Oficial Número 75 Tomo No. 287 del día martes 23 de abril de 1985.

La Junta de Vigilancia tiene como finalidad vigilar por el buen ejercicio de todos los Médicos Veterinarios que se dedican a esa profesión en el país.(Consejo Superior de Salud Pública)

2.1.2. Antecedentes de la norma ISO 270001:2013

En el año 2000 el estándar BS 7799-1 pasa a ser identificado como ISO 17799. Durante el período 2001 a 2004 la norma ISO 17799 pasó por una amplia revisión, resultando en una nueva versión ISO/IEC 17799: 2005, publicada en junio de 2005. En ese mismo año el BS 7799-2 es adoptado por la ISO, recibiendo la numeración 27000, dando inicio a la serie dirigida a la estandarización de normas para el segmento de seguridad de la información, lanzado como norma ISO/IEC 27001. En julio de 2007 el estándar 17799:2005 recibe nueva numeración (ISO/IEC 27002:2005), integrando la serie ISO 27000.

Las organizaciones ISO (*The International Organization for Standardization*) e IEC (*International Electrotechnical Commission*) mantienen equipos de expertos dedicados al desarrollo de normas internacionales, posibilitando que las organizaciones implementen estructuras adecuadas para la gestión de sus activos de información, tales como información financiera, de propiedad intelectual, datos de empleados, clientes o terceros, o sea, toda información que traiga valor para las corporaciones.

Las normas ISO 27000 posibilitan que organizaciones de todos los tipos y tamaños implementen y operen un Sistema de Gestión de Seguridad de la Información (SGSI).(Pandini, 2019)

2.1.3. Antecedentes de la NTS ISO/IEC 270001:2013

En El Salvador, a partir de la creación del OSN en el 2011 como el organismo competente para realizar las actividades de Normalización, y con el auge de las tecnologías de información, es necesario aplicar una normativa técnica internacional vigente la cual es la Norma Técnica Salvadoreña ISO/IEC 27001:2013.

En el 2014, la OSN desarrolla un taller de interpretación de la Norma Técnica Salvadoreña ISO/IEC 27001, con el objetivo de dar a conocer los requisitos y alcances de la norma, para el establecimiento y certificación de un sistema de gestión de seguridad de la información.

Posteriormente en el 2015, el OSN realiza un evento de difusión de normas en tecnología de la información entre las cuales se encuentran la Norma Técnica Salvadoreña ISO/IEC 27001:2013, Norma Técnica Salvadoreña ISO/IEC 27003:2010, Norma Técnica Salvadoreña ISO/IEC 27004:2009 y Norma Técnica Salvadoreña ISO 27006:2011. Esto con el fin de dar a conocer al público en general, las normas técnicas que son aplicables a las tecnologías de información en El Salvador.

2.2 Marco teórico

2.2.1. Principales definiciones

Entre los principales conceptos relacionados con la temática del SGSI y la ISO 27001 se pueden enlistar los siguientes:

Seguridad de la información: Es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la

información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma.

Tríada CID: Es un concepto de ciberseguridad que hace referencia a tres principios que deben trabajar en conjunto para garantizar la seguridad de un sistema informático: confidencialidad, integridad y disponibilidad.

Confidencialidad: Se refiere a que los datos deben estar solo al alcance de los usuarios autorizados.

Integridad: Comprende la correctitud y completitud de la información que se ha almacenado.

Disponibilidad: Implica que la información tiene que ser accesible para los usuarios autorizados dentro de un tiempo razonable.

Evaluación de riesgos: Es el estudio de las causas de las posibles amenazas y probables eventos no deseados y los daños y consecuencias que éstas puedan producir en un ambiente de TI.

2.2.2 ¿Qué es un SGSI?

El SGSI (Sistema de Gestión de Seguridad de la Información, ISMS por sus siglas en inglés *Information Security Management System*) es el concepto central sobre el cual se construye la ISO 27001. Comprende el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.

Se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente la forma en que se guarde

o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de su fecha de elaboración.

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información: confidencialidad, integridad y disponibilidad.

Para garantizar que la seguridad de la información es gestionada correctamente, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI.

2.2.3. ¿Para qué sirve un SGSI?

La información, junto a los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización. La confidencialidad, integridad y disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos.

Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo.

El Sistema de Gestión de la Seguridad de la Información (SGSI) ayuda a establecer estas políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir.

Con un SGSI, la organización conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o controla mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente.

2.2.4. ¿Qué incluye un SGSI?

En el ámbito de la gestión de la calidad según ISO 9001, siempre se ha mostrado gráficamente la documentación del sistema como una pirámide de cuatro niveles. Es posible trasladar ese modelo a un Sistema de Gestión de la Seguridad de la Información basado en ISO 27001 de la siguiente forma:

Documentos de Nivel 1

Manual de seguridad: por analogía con el manual de calidad, aunque el término se usa también en otros ámbitos. Sería el documento que inspira y dirige todo el sistema, el que expone y determina las intenciones, alcance, objetivos, responsabilidades, políticas y directrices principales, etc., del SGSI.

Documentos de Nivel 2

Procedimientos: documentos en el nivel operativo, que aseguran que se realicen de forma eficaz la planificación, operación y control de los procesos de seguridad de la información.

Documentos de Nivel 3

Instrucciones, checklists y formularios: documentos que describen cómo se realizan las tareas y las actividades específicas relacionadas con la seguridad de la información.

Documentos de Nivel 4

Registros: documentos que proporcionan una evidencia objetiva del cumplimiento de los requisitos del SGSI; están asociados a documentos de los otros tres niveles como output que demuestra que se ha cumplido lo indicado en los mismos.

2.3 Marco legal

Actualmente la información que se maneja dentro de las empresas ha adquirido mucha importancia en el desarrollo de sus actividades, por lo que siempre se busca resguardarla. La legislación salvadoreña atendiendo esta necesidad ha emitido normativa que ayude a las empresas a proteger esta información.

Durante el 2011 se dio la aprobación de la Ley de Creación del Sistema Salvadoreño para la Calidad, esto debido a la alta competitividad en el entorno económico a nivel nacional e internacional, siendo necesario mantener estándares de calidad y niveles altos de productividad, dando origen al Organismo Salvadoreño de Normalización (OSN) que vendría a regular lo concerniente a normas que establezcan parámetros para la mejora de productividad.

Esta ley define las atribuciones que vendría a desarrollar la OSN

1. Elaborar, actualizar, adoptar, adaptar, derogar y divulgar normas que faciliten la evaluación de la conformidad, así como conocer el desarrollo de los productores y proporcionar bases para la mejora de la calidad de los productos o servicios

prestados, siendo esta atribución la que pone la primera piedra para la implementación de la ISO 27001:2013

2. Ser participe constante en el desarrollo de normas nacionales como internacionales.
3. Elaboración y desarrollar programas anuales de normalización.
4. Promover la creación de comités interesados en el desarrollo de la normalización
5. Sera representante del país ante organismos internacionales de normalización
6. Proporcionar una base de datos de las normas técnicas vigentes y actualizadas disponible al público.
7. Mantener un constante esfuerzo para la implementación de la norma en los sectores productivos.

En el 2016 se emitió la Ley Especial Contra Delitos Informáticos y Conexos, en la cual se especifican tipos de delitos como sus sanciones por acciones contra la información confidencial, entre ellos se encuentra el acceso indebido a sistemas informáticos. Esta ley busca mantener la integridad y confidencialidad de la información, así como evitar la divulgación no autorizada. En su artículo 3, establece que los delitos informáticos se cometen cuando se haga uso de las Tecnologías de la Información y Comunicación, teniendo por objeto la realización de la conducta típica y antijurídica para la obtención, manipulación o perjuicio de la información. (Asamblea Legislativa de El Salvador)

Otra reciente ley que resguarda la información personal es la Ley de Firma Electrónica, que busca la certificación de transmisión de datos, para mantener la autenticidad, integridad y confidencialidad de la misma. En ella se abordan parámetros para asegurar envío de información o el almacenamiento de esta. Basándose en una serie de requisitos que deben cumplirse para mantener la calidad.

Para tener una mejor comprensión, la ley establece las principales definiciones (ver Tabla 1)

La información electrónica representa uno de los principales activos de una empresa que necesita tener organizada la información de sus clientes, proveedores y empleados, así como el manejo responsable de la misma. La ley en su artículo 5, define tres reglas a tener en cuenta para el almacenamiento de datos personales, tratándose de las veterinarias información sensible del personal encargado del manejo de la información.

La primera regla se enfoca en la obtención de información únicamente de los firmantes. Y la prohibición de ceder la información de los usuarios a terceros.

Tabla 1Principales definiciones de la Ley de la Firma Electrónica.

Acreditación:	Es la autorización que otorga la autoridad competente establecida en la presente Ley, a los proveedores de servicios de certificación, para operar y proporcionar certificados electrónicos, y a los proveedores de servicios de almacenamiento de documentos electrónicos, una vez cumplidos los requisitos y condiciones establecidos en la presente Ley.
Certificado Electrónico:	Documento proporcionado por un proveedor de servicios de certificación que otorga certeza a la firma electrónica certificada, garantizando la asociación de la persona con dicha firma.
Datos Personales:	Cualquier información numérica, alfabética, gráfica, fotográfica o de cualquier otro tipo, concerniente a personas naturales identificadas o identificables.
Documento Electrónico:	Todo mensaje de datos, enviado, recibido o archivado por medios electrónicos, ópticos o de cualquier otra tecnología, que forman parte de un expediente electrónico.
Firma Autógrafa:	Marca o signo, que una persona escribe de su propia mano en un instrumento o documento para asegurar o autenticar la identidad de una persona como prueba del consentimiento y verificación de la información contenida en dicho instrumento.
Firma Electrónica Simple:	Son los datos en forma electrónica, consignados en un mensaje de datos o lógicamente asociados al mismo, que puedan ser utilizados para identificar al firmante en relación con el mensaje de datos, e

	indicar que el firmante aprueba la información recogida en el mensaje de datos.
Firma Electrónica Certificada:	Son los datos en forma electrónica, consignados en un mensaje de datos o lógicamente asociados al mismo, que permiten la identificación del signatario, y que los datos de creación de la firma se encuentran en exclusivo control del signatario, lo que permite que sea detectable cualquier modificación ulterior al contenido del mensaje de datos
Firmante:	La persona que posee los datos de la creación de la firma y que actúa en nombre propio o de la persona que representa.

(Asamblea Legislativa de El Salvador, 2015)

Por otra parte, en su segunda regla establece que los datos obtenidos de los usuarios de la firma electrónica serán solamente los necesarios para el mantenimiento del certificado electrónico.

Por último, se tiene que los encargados del registro de datos y otras personas que intervengan en su tratamiento, están obligados a la confidencialidad de los mismos, así como a su almacenamiento seguro. Esto incluso cuando se hayan dado por concluidas la relación entre las partes.

Cabe mencionar que la firma electrónica simple tendrá la misma validez que una firma autógrafa, siempre que no se trate de documentos para efectos jurídicos, tal como se define en el artículo 6 de esta ley.

La firma electrónica certificada tendrá la misma validez que un documento tradicional (físico), incluso tratándose de procesos jurídicos, tal como se establece en el artículo 24.

Resulta necesaria su implementación para el manejo de datos para las veterinarias que manejan información sensible por medios electrónicos o que se requiera verificar su autenticidad. Además de tener debidamente almacenada la información.

2.4 Marco técnico y normativo

La ISO 27001 es una norma internacional emitida por La Organización Internacional de Normalización, en donde se describe cómo gestionar la seguridad de la información en una empresa. Una característica cualitativa de esta normativa es que puede ser utilizada para cualquier tipo de organización con o sin fines de lucro, tanto pequeña y grande.

La información en una entidad es un activo muy vital para el éxito y la continuidad en el mercado de cualquier organización, por lo que el aseguramiento de dicha información y de los sistemas que los procesan, es de interés primordial en las organizaciones. Para garantizar una adecuada gestión en la seguridad de la información, es necesario implementar un sistema que aborde esta tarea de una forma metódica, documentada y basada en unos objetivos claros de seguridad y evaluación de los riesgos a los que se encuentra sometida la información de la organización.

2.4.1 Función de la normativa ISO 27001

El objetivo principal de ISO 27001 es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa donde se centraliza en la investigación de cuáles son los potenciales problemas que podrían afectar la información, es decir la evaluación de los riesgos y de tal manera definir lo que es necesario para poder evitar que estos problemas se produzcan.

2.4.2 ISO 27001:2013

"El objeto de la ISO 27001:2013 es especificar los requerimientos para establecer, implementar, mantener y mejorar continuamente un sistema de seguridad de la información dentro del contexto de la información".(OSN, 2013)

Las medidas de controles que se van a implementar se presentan por lo general, bajo la forma de políticas, procedimientos e implementación técnica. Por ejemplo (software y equipos). En algunas empresas tienen todo el software y hardware necesario, pero no lo utilizan de una manera eficiente y segura.

La norma ISO/IEC 27001:2013 ofrece las herramientas necesarias para la implementación de un Sistema de Gestión de Seguridad de la Información. Esta norma permite que la empresa gestione y aplique de forma adecuada todas las medidas de seguridad necesarias para controlar el estado y la utilización de la información, entre otras muchas funciones.

Cada empresa debe conocer los diferentes tipos de datos de los que dispone para realizar sus actividades y así, conocer las medidas que necesita aplicar para que éstos se mantengan perfectamente protegidos y asegurarse de que no son utilizados de una forma inadecuada.

Esta norma permite generar una sensibilización del personal de una organización en relación con la importancia de la correcta manipulación de la información, y su aplicación adecuada de las medidas de seguridad a implementar, así como hacer conciencia al personal sobre la responsabilidad obtenida en relación a la información que se dispone.

2.4.3 Aspectos claves de un SGSI basado en la norma ISO 27001

La norma ISO 27001 es una solución de mejora continua o mejor conocido como "Ciclo de mejora continua o Ciclo metodológico de Deming", en base al cual puede desarrollarse un Sistema de Gestión de Seguridad de la Información (SGSI) que permita evaluar todo tipo de riesgos o amenazas susceptibles de poner en peligro la información de una organización tanto propia como datos de terceros. Asimismo, permite establecer los controles y estrategias más adecuadas para eliminar o minimizar dichos peligros. Dicho ciclo consiste en cuatro pasos importantes; Planificar, Hacer, Verificar y Actuar, por lo que se le conoce también como ciclo PDCA (acrónimo de sus siglas en inglés Plan-Do-Check-Act). Cada paso se encuentra ligado a una seria de acciones, las cuales se presentan en la Tabla 2.

2.4.4 Fases de la norma ISO 27001 para la implementación de un SGSI

El Sistema de Gestión de La Seguridad de la Información que propone la Norma ISO 27001 se puede resumir en las siguientes fases que se detallan en la figura 1, la cual debe iniciar con la obtención de la aprobación de la Dirección, para dar inicio a un proyecto de SGSI, culminando con la implementación de dicho proyecto.

2.4.5 Ventaja, en la implementación de La NTS 1SO.TEC 27001:2013

Las ventajas comerciales esenciales que una empresa puede obtener con la implementación de la 1SO 27001:2013, son las siguientes:

- Cumplir con requerimientos legales: cada vez hay más y más leyes, normativas y requerimientos contractuales relacionados con la seguridad de la información. La mayoría de ellos se pueden resolver implementando ISO 27001, ya que esta norma proporciona una metodología perfecta para cumplir con todos ellos.

Tabla 2 Ciclo PDCA basado en norma ISO 27001

Planificar	- Definir la política de seguridad
	- Establecer al alcance del SGSI
	- Realizar el análisis de riesgo
	- Seleccionar los controles
	- Definir competencias
	- Establecer un mapa de procesos
	- Definir autoridades y responsabilidades
Hacer	- Implantar el plan de gestión de riesgos
	- Implantar el SGSI
	- Implantar los controles
Controlar	- Revisar internamente el SGSI
	- Realizar auditorías internas del SGSI
	- Poner en marcha indicadores y métricas
	- Hacer una revisión por parte de la Dirección
Actuar	- Adoptar acciones correctivas
	- Adoptar acciones de mejora

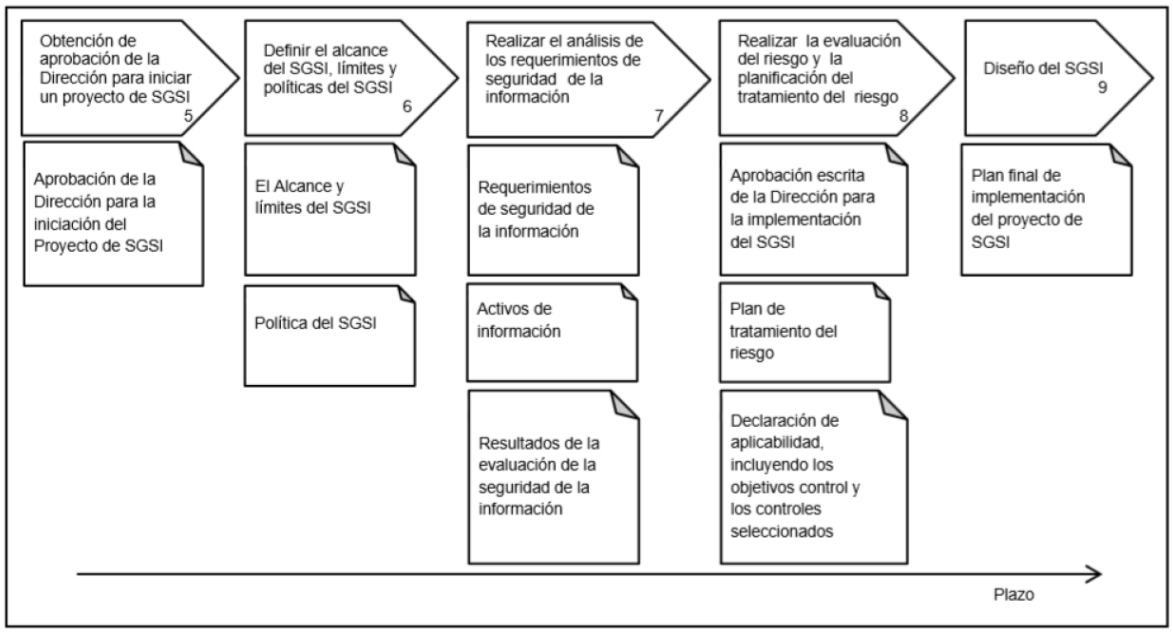
(OSN, 2005).

- Obtener una ventaja comercial: si la empresa obtiene la certificación y sus competidores no, es posible que obtenga una ventaja sobre ellos ante los ojos de los clientes a los que les interesa mantener en forma segura su información.
- Menores costos: la filosofas principal de ISO 27001 es evitar que se produzcan incidentes de seguridad, y cada incidente, ya sea grande o pequeño, cuesta dinero; por

lo tanto, evitándolos la empresa ahorra mucho dinero. La inversión en ISO 27001 es mucho menor que el ahorro que obtendrá.

- Una mejor organización: en general las empresas de rápido crecimiento no tienen tiempo para hacer una pausa y definir sus procesos y procedimientos; como consecuencia, muchas veces los empleados no saben qué hay que hacer, cuándo y quién debe hacerlo. La implementación de la ISO 27001 ayuda a resolver este tipo de situaciones ya que alienta a las empresas a escribir sus principales procesos (incluso los que no están relacionados con la seguridad), lo que les permite reducir el tiempo perdido de sus empleados.
- Garantía de los controles internos y cumplimiento de requisitos de gestión corporativa y de continuidad de la actividad comercial.
- Poner de manifiesto el respeto a las leyes y normativas que sean de aplicación.

Figura 1 Fases de la Norma para la implementación de un SGSI



(OSN, 2005)

3 CAPÍTULO III. METODOLOGÍA DE LA INVESTIGACIÓN

3.1 Delimitación de la Investigación

3.1.1 Temporal

La investigación se realizó a partir de octubre 2015, que es donde quedó únicamente certificada la ISO 27001:2013.

3.1.2 Espacial

Para realizar la investigación se tomó como referencia las empresas dedicadas a prestar servicios veterinarios ubicados en el área metropolitana de San Salvador

3.1.3 Tipo de estudio.

El método de estudio se utilizó es el hipotético deductivo, ya que a través de éste se puede observar el problema en estudio, operar hipótesis y sus variables, deducir las causas y medir sus efectos, lo que se tomó como base para proporcionar un modelo de gestión de seguridad de la información que sirva como orientación para las clínicas veterinarias ubicadas en el área metropolitana de San Salvador.

3.2 Unidades de análisis

Las unidades de análisis consideradas en la investigación fueron contadores las veterinarias autorizadas ubicadas en el área metropolitana de San Salvador.

3.3 Universo y muestra

El universo estuvo conformado por las clínicas veterinarias ubicadas en el área metropolitana de San Salvador, obteniendo un universo de 39 clínicas veterinarias y 5 hospitales veterinarios

En la determinación de la muestra se utilizó la fórmula estadística para poblaciones infinitas o desconocidas, la selección de la muestra se realizó por medio del método aleatorio simple.

$$n = \frac{Z^2 . P . Q .}{e^2}$$

Donde:

n = Tamaño de la muestra

Z = Coeficiente de confianza

p = Probabilidad de éxito de que la problemática exista

q = Probabilidad de fracaso

e = Margen de error

Se tomó un nivel de confianza 85%, indicando que de cada 100 respuestas obtenidas se espera que 85 estén dentro de las expectativas de la investigación. El margen de error dispuesto a aceptar es del 15%.

Sustituyendo:

n =?

Z = 1.44 nivel de confianza 85%

p = 50% (probabilidad de éxito)

q = 50% (probabilidad de fracaso)

e = 15% nivel de error

$$n = \frac{1.44^2 x 0.50 x 0.50}{0.15^2}$$

$$n = \frac{0.5184}{0.0225}$$

n= 23.04

La muestra resultó de 23 clínicas veterinarias ubicadas en el área metropolitana de San Salvador.

3.4 Instrumentos y técnicas de medición

El instrumento que se utilizó para la recolección de información es la encuesta, la cual se enviará a los contadores de las clínicas veterinarias vía correo electrónico. Dicho instrumento está estructurado con una serie de preguntas tanto cerradas como abiertas enfocadas a la gestión de seguridad de la información.

3.5 Procesamiento de la información

La información obtenida por medio de las encuestas es procesada en el programa de Microsoft Excel, ya que es la herramienta que se utiliza para el diseño de gráficos, estadísticas, análisis e interpretación de los datos.

3.6 Análisis de los resultados.

El análisis de los datos se realizó por medio de la tabulación de los datos, destacando la frecuencia en términos absolutos y porcentuales con sus respectivos gráficos, con la intención de medir porcentualmente si la problemática estipulada existe, y si hay gestión de riesgos en seguridad de la información por parte de los contadores o encargados de TI o en su defecto por los administradores o gerentes de las clínicas veterinarias. La mencionada tabulación se muestra en la sección de Anexos.

4 CAPÍTULO IV: DESARROLLO DE CASO PRACTICO

PROPUESTA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NTS ISO/IEC 27001:2013 APLICADA A CLÍNICAS Y HOSPITALES VETERINARIOS DEL ÁREA METROPOLINA DE SAN SALVADOR

4.1 Introducción

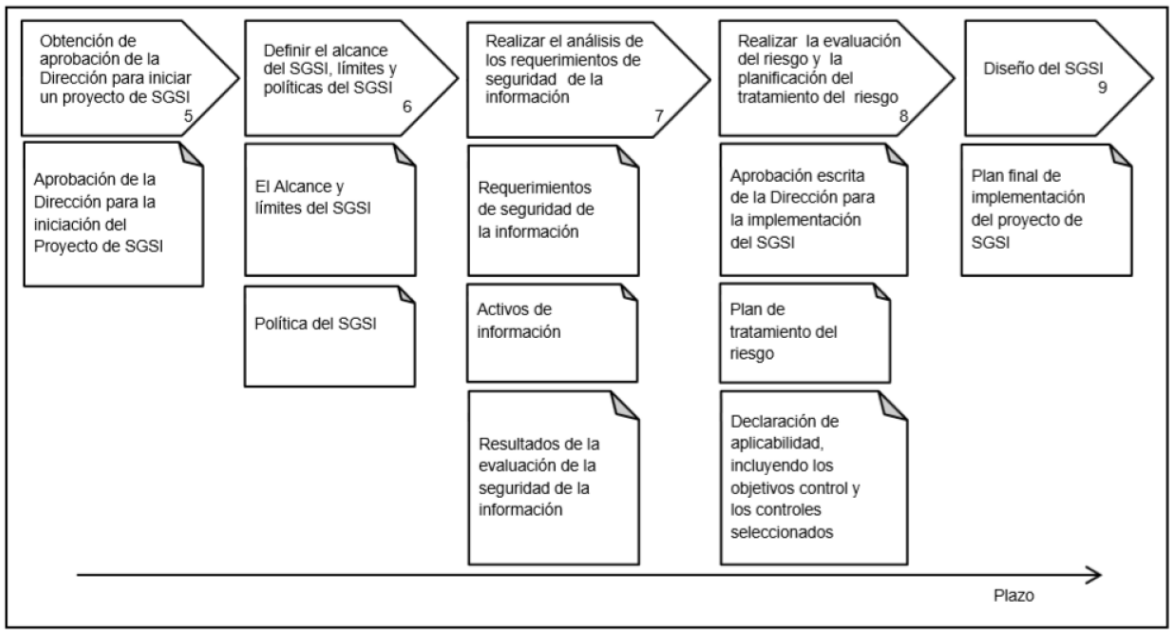
Los servicios y productos que comercializan las clínicas y hospitales veterinarios en área metropolitana de San Salvador, han tomado importancia dentro de la economía salvadoreña en los últimos años, puesto que se ha incrementado la demanda las actividades que estas desarrollan y en consecuencia incrementado sus riesgos informáticos, es por eso que se ha visto la necesidad de planear e implementar un Sistema de Seguridad de la Información, que le permita prevenir y detectar de manera oportuna pérdida o fuga de la información que afecten los objetivos empresariales,

En este capítulo se desarrolló una guía para la planeación e implementación de un Sistema de Seguridad de la Información en base a la ISO/EC 27001:2013, en la empresa Veterinaria ABC, S.A. de C.V. Las técnicas de evaluación utilizadas fueron las encuestas; que fueron aplicadas a los contadores generales de cada departamento para conocer las causas, riesgos y controles identificados a nivel de la seguridad de la información en los diferentes departamentos e instalaciones de la clínica veterinaria.

Flujograma para la Implementación de un SSGI

Figura 2

Fases de la Norma para la implementación de un SGSI



Tomado de NTS ISO/IEC 27001:2005

4.2 Generalidades Veterinaria "ABC"

Veterinaria "ABC" se encuentra ubicada en el municipio de San Salvador, departamento de San Salvador, y se especializa en las siguientes áreas:

Clínica

Cuenta con el equipo adecuado y el personal capacitado para brindar los siguientes servicios:

- Consulta general, de control y urgencias

- Vacunas y desparasitaciones
- Aplicaciones
- Cirugías menores y mayores
- Eutanasias
- Pruebas de laboratorio

Sala de Belleza

Posee un área de Peluquería Canina y Felina especial y una amplia gama de opciones de baños, cortes de pelo, corte de uñas, cepillado dental, arreglos etc.

Pet Shop

Es una de las Farmacias Veterinarias más grandes a nivel nacional, y una tienda, con más de 1,000 diferentes productos para usted y su Mascota: Concentrado, artículos para aseo canino y felino, medicamentos, accesorios, entre otros

Misión

Dar el mejor servicio de atención clínica y estética para especies menores, así como proveer de la mejor calidad de alimentos y accesorios para mascotas en El Salvador.

Visión

Convertirnos en el más completo centro veterinario de atención clínica, estética y sala de ventas para especies menores en El Salvador, para satisfacer todas las necesidades de nuestros clientes.

Valores

Integridad: Comprometerse con un servicio honesto y ético. Siempre a actuar en el mejor interés de los pacientes y sus propietarios. La base de la práctica es la confianza e integridad.

Experiencia: Responsabilizarse en estar en continua formación, para estar al día de las últimas novedades clínicas y poder ofrecer los tratamientos más actualizados a su mascota.

Comunicación: Priorizar el tipo de comunicación que se tenga con los propietarios, por lo que incentivan aquellas acciones que permitan al propietario de ABC, entender de forma didáctica, el proceso que sufre su mascota.

Cuidado: Preocuparse por el bienestar y la comodidad de los pacientes y sus familias, así como brindar un cuidado compasivo y un servicio excelente.

4.2.1 Obtención de la Aprobación de la Dirección para iniciar un proyecto SSGI - Nombramiento de Comité de Seguridad de la Información

ACTA NÚMERO CATORCE. En la ciudad de San Salvador, a las diez horas del día doscientos treinta de julio de dos mil diecinueve, en las oficinas ubicadas en Calle ABC, número treinta y seis, Colonia ABC, San Salvador. ASISTENCIA. Se encuentran presentes en las oficinas de la sociedad VETERINARIA ABC, S.A. DE C.V., los señores Giovanni Salvador Cornejo Cruz, Director Propietario; Amalia Hernández, Director Propietario y Juan Ernesto Ángeles, Director Propietario; de acuerdo a lo establecido en el Código de Comercio y el Pacto Social, fueron convocados por el Lic. Giovanni Salvador Cornejo Cruz, la totalidad de los miembros propietarios de la sociedad, por lo que se hace constar, según se ha indicado anteriormente, que se encuentran presentes en esta sesión, la totalidad de los Directores Propietarios, existiendo el quórum legal suficiente para celebrar la sesión, la cual fue declarada abierta y se desarrolló literalmente de la manera siguiente: “”””””Luego de dar la bienvenida a la Junta Directiva, se sometió a aprobación de estos la agenda siguiente: 1. Verificación de QUORUM. 2. Elección de presidente y secretario de la Sesión. 3. Lectura y Verificación de la Agenda 4. Aprobación de Comité de Seguridad de la Información. DESARROLLO DE LA SESIÓN: PUNTO PRIMERO: VERIFICACIÓN DEL QUÓRUM: Tal y como se estableció al inicio de la sesión se encuentran presentes en las oficinas de la sociedad y a través de videoconferencia la unanimidad de los Directores Propietarios por lo que existe quórum suficiente para celebrar la sesión y tomar resoluciones. PUNTO SEGUNDO: ELECCIÓN DEL PRESIDENTE Y SECRETARIO DE LA SESION. Se hizo del conocimiento de los miembros de la Junta Directiva que es necesario que la sesión sea conducida por un presidente y un secretario de la sesión, por lo que se sometió aprobación de los Directores, que esta sesión sea presidida por la Licda. Amalia Hernández y el Lic. Giovanni Cornejo, como secretario, de la sesión, lo cual fue aprobado por unanimidad de los

miembros de la Junta Directiva. PUNTO TERCERO: LECTURA Y VERIFICACIÓN DE LA AGENDA: El secretario de la sesión procedió a dar lectura de la agenda de la sesión, la cual una vez leída se sometió aprobación y fue aprobada por unanimidad de los Directores presentes. PUNTO CUARTO: APROBACIÓN DEL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN. El secretario de la sesión cedió la palabra al Licenciado Carlos Alberto Figueroa, miembro del equipo TI, para que desarrolle el punto CUARTO de la agenda referente a la Aprobación del Comité de Seguridad de la Información. El secretario de la junta cedió la palabra al Lic. Carlos Figueroa para que desarrolle el punto CUARTO de la agenda referente a la Aprobación del Comité de Seguridad de la Información. El Licenciado Figueroa expone al pleno la necesidad de nombrarse un comité de Seguridad el cual estará conformado por: El gerente General, el director del hospital, un miembro del área de finanzas y un miembro del equipo de TI, el cual tendrá entre las funciones principales las siguiente:

1. Dentro del flujo de aprobación de las Políticas de Seguridad de la Información, el Comité de Seguridad de la Información es el primer nivel de aprobación, revisión, rechazo, modificación o eliminación de éstas;

2. El Comité de Seguridad de la Información aprueba normas y procedimientos de seguridad de la Información.

3. Revisa y valida normas y procedimientos en general, a fin de verificar que se estén cumpliendo los aspectos de seguridad dentro de los procesos.

4. Por medio del Comité de Seguridad de la Información se supervisa y controla el Plan de Seguridad de la Información para analizar temas tales como:

5. Revisar el avance del plan y dar directrices en caso de atrasos;

6. Establecer recursos para administrar los incidentes de seguridad u otras vulnerabilidades;

7. Velar por el cumplimiento de las políticas, normas, procedimientos y demás documentos relacionados en Seguridad de la Información dentro de la organización;

8. Definir proyectos de tecnología que impliquen la aplicación de Seguridad de la Información en el contexto del negocio (Servicio, Producto e Información);

9. Generar resúmenes de actividades englobadas en el marco de la Seguridad de la Información para ser presentadas ante las máximas autoridades de la organización.

10. Monitorear cambios significativos en los riesgos que afectan a los recursos de la información de la Organización frente a posibles amenazas, sean internas o externas.

11. Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes, relativos a la seguridad, que se produzcan en el ámbito de la Organización.

12. Por medio del Comité de Seguridad de la Información se instruirá al Oficial de Seguridad de la Información el inicio del proceso de revisión anual de las políticas vigentes. Dicha instrucción se dará en la sesión de diciembre de cada año.

13. Aprobar las principales iniciativas para incrementar la Seguridad de la Información de acuerdo a las competencias y responsabilidades asignadas a cada gerencia, así como acordar y aprobar metodologías y procesos específicos relativos a la Seguridad de la Información.

14. Evaluar y coordinar la implementación de controles específicos de Seguridad de la Información para los sistemas o servicios de la Organización, sean preexistente o nuevos.

15. Promover la difusión y apoyo a la Seguridad de la Información dentro de la Organización, así como también, coordinar el proceso de administración de la continuidad de las actividades.

16. Entre otras

El Licenciado Figueroa propone que el comité de seguridad sea conformado por las siguientes personas:

- Gerente General: Dr. Giacomo Zappalá
- Director del hospital: Dr Adrian Abarca
- Administrador Contable: Ricardo Domínguez
- Gerente de IT: Carlos Figueroa

El comité es aprobado por unanimidad y no habiendo más asuntos que tratar, se da por finalizada la sesión a las dice horas del día doscientos treinta de julio de dos mil diecinueve.

4.3 Definición de información requerida y plazos

Fase	Documento requerido	Plazo en semanas.
A.5 Política de seguridad de la información		
A.5.1 Gestión de la dirección para la seguridad de la información		
A.5.1.1 Políticas para la seguridad de la información.	Manual de políticas para la seguridad de la información, aprobado por la dirección.	4
A.5.1.2 Revisión de las políticas de la seguridad de la información		

A.6 Organización de la seguridad de la información		
A.6.1 Organización interna		
A.6.1.1 Roles y responsabilidades de la seguridad de la información	Manual de funciones y jerarquización de puestos de trabajo	1
A.6.2 Dispositivos móviles y trabajo remoto		
A.6.2.1 Política de dispositivos móviles	Manual de políticas para la seguridad de la información, aprobado por la dirección.	4
A.6.2.2 Trabajo remoto	Registro y control de dispositivos y usuarios con acceso remoto.	1
A.7 Seguridad de recursos humanos		
A.7.1 Antes del empleo		
A.7.1.1 Selección de personal	Manual de reclutamiento, selección y contratación de personal.	1
A.7.1.2 Términos y condición de empleo	Contrato de trabajo	1
A.7.2 Durante el empleo		
A.7.2.1 Responsabilidades de la dirección	Acuerdo de confidencialidad y no divulgación postcontractual	1
A.7.2.2 Capacitación, educación y concientización sobre la seguridad de la información.	Programa de capacitaciones sobre las políticas de la seguridad de la información.	2

A.7.2.3 Proceso disciplinario	Reglamento interno de personal	1
A.7.3 Terminación y cambio del empleo		
A.7.3.1 Responsabilidades de terminación o cambio de empleo	Acuerdo de confidencialidad y no divulgación postcontractual	1
A.8 Gestión de activos		
A.8.1 Responsabilidades sobre los activos		
A.8.1.1 Inventario de activos A.8.1.2 Propiedad de los activos	Estatuto sobre el registro y control de activos relacionados con el procesamiento y almacenamiento de la información.	2
A.8.1.3 Uso aceptable de los activos A.8.1.4 Devolución de los activos	Reglamento para la asignación y utilización de activos	1
A.8.2 Clasificación de la información		
A.8.2.1 Clasificación de la información	Sistema de clasificación y etiquetado de la información	1
A.8.2.2 Etiquetado de la información		
A.8.2.3 Manejo de activos	Reglamento para la asignación y utilización de activos	1
A.8.3 Manejo de medios		
A.8.3.1 Gestión de medios removibles A.8.3.2 Eliminación de medios A.8.3.3 Transferencia de medios físicos	Manual de procedimientos para la gestión de medios de almacenamiento de información	1
A.9 Control de acceso		
A.9.1 Requerimiento del negocio para el control de acceso		
A.9.1.1 Política del control de acceso A.9.1.2 Acceso a redes y servicios de red	Política - Manual de usuarios y seguridad de la información	2
A.9.2 Requerimiento del negocio para el control de acceso		
A.9.2.1 Gestión del acceso de usuarios A.9.2.2 Provisión de accesos de usuarios A.9.2.4 Gestión de la información de	Manual de usuarios y acceso seguridad de la información	2

autenticación secreta de usuarios		
A.9.2.4 Remover o ajustar derechos de acceso		
A.9.3 Responsabilidades del usuario		
A.9.3.1 Uso de información de autenticación secreta	Manual descripción de puestos de trabajo	1
A.9.4 Control de acceso a sistemas y aplicaciones		
A.9.4.1 Restricción del acceso a la información		
A.9.4.2 Procedimientos seguros de inicio de sesión		
A.9.4.3 Sistema de gestión de la contraseña	Manual de usuarios y acceso seguridad de la información	2
A.9.4.4 Uso de programas utilitarios privilegiados		
A.9.4.5 Control de acceso al código fuente de los programas		
A.11 Seguridad física y ambiental		
A.11.1 Áreas seguras		
A.11.1.1 Perímetro de seguridad física		
A.11.1.3 Seguridad de oficinas, habitaciones e instalaciones		
A.11.1.4 Protección contra amenazas externas y ambientales	Manual de procedimientos de seguridad física para el resguardo de la información	3
A.11.1.5 Trabajo en áreas seguras		
A.11.1.6 Áreas de carga y descarga		
A.11.2 Equipo		
A.11.2.1 Ubicación y protección de equipo	Manual de procedimientos de seguridad física para el resguardo de la información	2

A.11.2.2 Herramientas de soporte A.11.2.3 Seguridad en el cableado A.11.2.4 Mantenimiento de equipo A.11.2.5 Retiro de activos A.11.2.6 Seguridad del equipo y activos fuera de las instalaciones A.11.2.7 Seguridad en la reutilización o eliminación de equipos		
A.12 Seguridad de las operaciones		
A.12.2 Protección contra software malicioso A.12.2.1 Controles contra software malicioso A.12.3 Copias de seguridad A.12.4. Registro y monitoreo A.12.4.1 Registro de eventos A.12.4.2 Protección de la bitácora de información A.12.4.3 Bitácoras del administrador y operador A.12.6 Gestión de vulnerabilidades técnicas	Manual de usuarios y acceso seguridad de la información Informes de auditoría sobre operaciones dentro del sistema de información.	2 4
A.13 Seguridad de las comunicaciones		
A.13.1 Gestion de la seguridad de red A.13.1.1 Controles de red A.13.1.2 Seguridad de los servicios de red	Manual de usuarios y acceso seguridad de la información	3

A.13.1.3 Segmentación de redes		
A.13.2 Transferencia de la información		
A.13.2.1 Procedimientos y políticas de transferencia de información		
A.13.2.2 Acuerdos de transferencia de información	Manual para el manejo y transferencia de información	1
A.13.2.3 Mensajes electrónicos		
A.13.2.4 Acuerdos de confidencialidad y no divulgación		
A.15 Relaciones con los proveedores		
A.15.1 Seguridad de la información en las relaciones con los proveedores		
A.15.1.1 Política de seguridad de la información para las relaciones con los proveedores	Reglamento para el establecimiento de relaciones con proveedores de bienes o servicios	1
A.15.1.2 Abordar la seguridad dentro de los acuerdos con los proveedores		
A.15.2 Gestión del servicio de entrega del proveedor		
A.15.2.1 Monitoreo y revisión de los servicios del proveedor	Política para el seguimiento de las relaciones con los proveedores	1
A.16 Gestión de incidentes de seguridad de la información	Manual de procedimiento para la gestión de incidentes de seguridad de la información	3
A.18 Cumplimiento		
A.18.1 Cumplimiento con requerimientos legales y contractuales	Informe de auditoría de sistemas	4
A.18.2 Revisiones de seguridad de la información		

4.4 Identificación de Riesgos de Activos de Información

Activo de información	Riesgo identificado	Consecuencia asociada
Información de clientes	Filtración de información sensible (nombres de clientes, números telefónicos, domicilio, correos electrónicos) hacia personas ajenas a la veterinaria	Consecuencias del tipo reputacional o económicas por daños y perjuicios en contra de los afectados(clientes)
Información contable-administrativa	Pérdida de información provocada por bajones de energía e inexistencia de back-ups recientes	Atraso en las operaciones diarias y reorientación de prioridades administrativas para la reconstrucción de la información perdida
Software para historial clínico: MEDVET	Caída del sistema al momento de tomar alguna orden del área de peluquería o clínica (generalmente por problemas de red)	Quejas y reclamos de los clientes por el atraso generado al procesar los servicios que ha solicitado
Software contable-administrativo: SAC	Caída del sistema SAC	• En facturación, quejas de parte de los clientes debido a atrasos al momento de dar ingreso a la factura por el servicio o producto que está pagando • Respecto a la parte contable-administrativa, atrasos en el procesamiento de la información lo cual no permitiría presentar resultados oportunamente ante la alta dirección
Instalaciones	Daños provocados por algún tipo desastre natural, principalmente terremotos que son bastante comunes en nuestro país	Detrimento económico para la empresa pues tendría que destinar fondos a la reparación de la infraestructura para reestablecer el buen funcionamiento de las operaciones
Internet	Caída del servicio de internet	Atraso en las actividades empresariales así como perdida

		de comunicación entre los mismos empleados, con los proveedores y hasta con los clientes.
Infraestructura de red	Daños en el cableado interno de red de la empresa por deterioro del tiempo u otro agente externo	Consecuencias económicas pues afecta las actividades normales de la empresa
Sistema de videovigilancia	Falta de funcionamiento	Posibilidad de sufrir algún tipo de robo o hurto tanto en los alrededores de la veterinaria como adentro de la misma que a su vez provocaría detrimento económico
Página web	Caída del servidor que soporta el sitio web	Disminución de clientes potenciales que a su vez deriva en pérdidas económicas
Servidor de red	Daño parcial o permanente por mala manipulación de los empleados	Atraso en las actividades diarias de la empresa al afectar directamente a los demás equipos que se encuentran conectados a dicho servidor
Equipo de computo	Daño parcial o total por mal uso de parte del personal asignado	Atraso en las actividades diarias de la empresa pues es un recurso que interviene de manera directa
Impresoras	Dejar de imprimir cuando se lleve a cabo alguna actividad urgente (reportes de clínica)	Atraso en las actividades normales del área correspondiente

Lineamientos establecidos por la ISO 27001:2013

4.4.1 Comprensión de la organización y su contexto

La organización debe determinar asuntos internos y externos que son relevantes a su propósito y que afectan Su habilidad para alcanzar los resultados esperados de su sistema de gestión de seguridad de la información.

Nota 1: Determinar estos asuntos se refiere a establecer el contexto interno y externo de la organización considerado en la cláusula 5.3 de ISO 31000:2009.

4.4.2 Comprensión de las necesidades y expectativas de las partes interesadas

La organización debe determinar:	**a) partes interesadas que son relevantes al sistema de gestión de seguridad de la información; y**
	b) los requerimientos de esas partes interesadas relevantes para la seguridad de la información.
	Nota 2: Los requerimientos de las partes interesadas pueden incluir requerimientos y Obligaciones contractuales.
1.1.1 Determinar el alcance del sistema de gestión de seguridad de la información	La organización debe determinar los límites y aplicabilidad del sistema de gestión de seguridad de la información para establecer su alcance.
	Cuando se determine el alcance, la organización debe considerar:
	a) los asuntos internos y externos referidos en 4.1;
	b) los requerimientos referidos en 4.2; y
	c) interfaces y dependencias entre actividades desempeñadas por la organización, y aquellas que son desempeñadas por Otras organizaciones.
	El alcance debe estar disponible como información documental.
1.1.2 Sistema de gestión de seguridad de la información	La organización debe establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información, en concordancia con los requerimientos de esta Norma Técnica Salvadoreña.
1.1.3 Liderazgo y Compromiso	La alta dirección debe demostrar liderazgo y compromiso con respecto al sistema de gestión de seguridad de la información a través de:
	a) asegurar que la política de seguridad de la información y los objetivos de seguridad de la información están establecidos y son compatibles con la dirección estratégica de la organización;
	b) asegurar la integración de los requerimientos del sistema de gestión de seguridad de la información dentro de los procesos de la organización;
	c) asegurar que los recursos necesarios para el sistema de gestión de Seguridad de la información están disponibles;
	d) comunicar la importancia de la efectividad de la gestión de seguridad de la información y del cumplimiento de los requerimientos del sistema de gestión de seguridad de la información;
	e) asegurar quo el sistema de gestión de seguridad de la información logra el(los) resultado(s) esperado(s);
	f) dirigir y apoyar a las personas que contribuyen a la efectividad del sistema de gestión de seguridad de la información
	g) promover la mejora continua; y

	h) apoyar otros roles pertinentes de la administración para mostrar liderazgo según aplique en sus áreas de responsabilidad.
1.2 Política	La alta dirección debe establecer una política de seguridad de la información que:
	a) sea apropiada para el propósito de la organización;
	b) incluya objetivos de seguridad de la (ver 6.2) o provea el para establecer los objetivos de seguridad de la información;
	c) incluya un compromiso para satisfacer los requerimientos aplicables relacionados a la seguridad de la información; e
	d) incluya un compromiso mejora continua del sistema de gestión de seguridad de la información.
	La política de seguridad de la información debe:
	a) estar disponible como información documental:
	b) ser comunicada dentro de la organización: y
	c) disponible a las partes interesadas, de manera apropiada.
1.2.1 Roles, responsabilidades y autoridades organizacionales	La alta dirección debe asegurar que las responsabilidades y autoridades para los roles relevantes a la seguridad de la información son asignados y comunicados.
	La ata dirección debe asignar la responsabilidad y autoridad para:
	a) asegurar que el sistema de gestión de seguridad de la Información esté conforme con los requerimientos de esta Norma Técnica Salvadoreña; e
	b) informar el desempeño del sistema de gestión de seguridad de información a la alta dirección.
	Nota 3: La alta dirección puede también asignar dentro de organización responsabilidades y autoridades para informar el desempeño del sistema de gestión de seguridad de la información.
1.3 Acciones para abordar riesgos y oportunidades	
1.3.1 General	Cuando se esté planeando para el sistema de gestión de seguridad de la información, la organización debe considerar los elementos referidos en 4.1 y los requerimientos referidos en 4.2 y determinar los riesgos y oportunidades que necesitan ser abordados para:
	a) asegurar que el sistema de gestión de seguridad de la información pueda obtener los resultados esperados;
	b) prevenir o reducir los efectos no deseados; y
	c) lograr mejora continua.
	La organización debe planear:
	a) acciones para abordar estos riesgos y oportunidades: y
	b) como:
	- integrar e implementar las acciones dentro de procesos del sistema de gestión de seguridad de información; y
	- evaluar la efectividad de estas acciones.

1.3.2 Evaluación del riesgo de seguridad de la información	La organización debe definir y aplicar un proceso de evaluación del riesgo de seguridad de la información que:
	a) establezca y mantenga criterios de riesgo de seguridad de la información que incluyan:
	- el criterio de aceptación de riesgo; y
	- criterio de desempeño de la evaluación de riesgo de seguridad de la información;
	b) asegure que repetidas evaluaciones de riesgo de seguridad de la información producen resultados consistentes, válidos y comparables;
	c) identifique los riesgos de seguridad de la información:
	d) generar una declaración de aplicabilidad que contenga los controles necesarios (ver 6.1.3 b) y c)) y justificación para inclusiones, ya sea que sean implementadas o no. y la justificación de exclusiones de control del Anexo A;
	e) formular un plan de tratamiento de riesgo de seguridad de la información; y
	f) obtener aprobación del plan de tratamiento del riesgo de seguridad de la información y aceptación de los riesgos residuales por parte de los propietarios del riesgo.
	La organización debe retener información documental acerca del proceso de tratamiento de riesgo de seguridad de la información.
	Nota 7: Los procesos de tratamiento y evaluación del riesgo de seguridad de la información en esta Norma Técnica Salvadoreña se alinean con los principios y guías genéricas provistas en ISO 310001.
1.3.3 Objetivos de seguridad de la información y planeación para lograrlos	La organización debe establecer objetivos de seguridad de la información en niveles y funciones
	pertinentes.
	Los objetivos de seguridad de la información deben:
	a) ser consistentes con la política de seguridad de la información;
	b) ser medibles (si aplica);
	c) tomar en cuenta los requerimientos aplicables a la seguridad de la información, y los resultados de la evaluación y tratamiento del riesgo;
	d) ser comunicados; y
	e) ser actualizados apropiadamente.
	La organización debe conservar información documental sobre los objetivos de seguridad de la información.
	Cuando se planee como alcanzar los objetivos de seguridad de la información, organización debe determinar:
	a) qué será realizado;
	b) qué recursos serán requeridos:

	c) quién será responsable;
	d) cuándo se completará; y
	e) cómo se evaluarán los resultados.
1.3.4 Recursos	La organización debe determinar y proveer los recursos necesarios para el establecimiento, implementación, mantenimiento y la mejora continua del sistema de gestión de seguridad de la información.
1.3.5 Competencia	La organización debe:
	a) determinar la competencia necesaria de la(s) persona(s) desarrollando trabajos bajo su control que afectan el desempeño de seguridad de la información;
	b) asegurar que estas personas son competentes sobre la base de una educación, entrenamiento o experiencia apropiada;
	c) donde sea aplicable, tomar acciones para adquirir las competencias necesarias y evaluar la efectividad de las acciones tomadas; y retener la información documental apropiada como evidencia de la competencia:
	Nota 8: Acciones aplicables pueden incluir, ejemplo: proveer de entrenamiento, tutorías, o la reasignación de empleados actuales: o la contratación o sub contratación de personas competentes.
1.3.6 Conciencia	Las personas desarrollando trabajo bajo el control de la organización deben estar conscientes de:
	a) la política de seguridad de la información;
	b) su contribución a la efectividad del sistema de gestión de seguridad de la información. incluyendo los beneficios del desempeño mejorado de seguridad de la información; y
	c) las implicaciones de no conformidad con los requerimientos del sistema de gestión de seguridad de la información.
1.3.7 Comunicación	La organización debe determinar la necesidad de comunicaciones internas y externas pertinentes al sistema de gestión de seguridad de la información que incluyan:
	a) qué comunicar;
	b) cuándo comunicar;
	c) a quién comunicar;
	d) quién debe comunicar; y
	e) los procesos por los cuales la comunicación debe ser efectuada.
1.4 Información documental	
1.4.1 General	El sistema de gestión de seguridad de la información de la organización debe incluir:
	a) información documental requerida por esta Norma Técnica Salvadoreña; e

	b) información documental determinada por la organización como necesaria para la efectividad del sistema de gestión de seguridad de la información.
	Nota 9: La extensión de la información para el sistema de gestión de seguridad de la información puede diferir de una organización a otra debido a:
	a) el tamaño de la organización y su tipo de actividades, procesos. y servicios;
	b) la de los procesos y sus interacciones; y
	c) las competencias de las personas.
1.4.2 Creación y actualización	Cuando se cree y actualice información documental, la organización debe asegurar su apropiada:
	a) identificación y descripción (p. ej. un título, fecha, autor o número de referencia);
	b) formato (p. ej. lenguaje, versión de software, gráficos) y medio (p. ej. papel, electrónico); y
	c) revisión y aprobación para su idoneidad y adecuación.
1.4.3 Control de información documental	La información documental requerida por el sistema de gestión de seguridad de la información y por la Norma Técnica Salvadoreña debe ser controlada para asegurar:
	a) que esté disponible y sea idónea para su uso, donde y cuando sea necesario; y
	b) esté adecuadamente protegida (p. ej. de pérdida de confidencialidad, uso inapropiado, o pérdida de integridad).
	Para el control de la información documental. la organización debe alinear las siguientes actividades, como aplicables:
	a) distribución, acceso. recuperación y uso;
	b) almacenamiento y conservación. incluyendo la conservación de la legibilidad;
	c) control de cambios (p. ej. control de versiones); y
	d) retención y disposición.
	La información documental de origen externo, determinada por la organización como necesaria para la planificación y operación del sistema de gestión de seguridad de la información, debe ser oportunamente identificada y controlada.
	Nota 10: El acceso implica una decisión con respecto al permiso para únicamente consultar la información documental, o autorización para cambiar la información
	documental, etc.
1.5 Operación	
1.5.1 Planeación y control operacional	La organización debe planificar, implementar y controlar los procesos necesarios para cumplir los requerimientos de seguridad de la información, y para implementar las acciones determinadas en

	6.1. La organización también debe implementar planes para lograr los objetivos de la seguridad de la información determinados en 6.2.
	La organización debe mantener información documental en la medida necesaria que proporcione la confianza que los procesos han sido ejecutados como fueron planeados.
	La organización debe controlar los cambios planificados y revisar las consecuencias de los cambios no previstos, tomando acción para mitigar cualquier efecto adverso donde sea necesario.
	La organización debe asegurar que los procesos sub contratados estén determinados y controlados.
1.5.2 Evaluación del riesgo de seguridad de la Información	La organización debe desarrollar evaluaciones de riesgo de seguridad de la información planificadas periódicamente o cuando ocurran o sean propuestos cambios significativos. tomando en cuenta el criterio establecido en 6.12 a).
	La organización debe retener información documental de los resultados de las evaluaciones del riesgo de seguridad de la información.
1.5.3 Tratamiento del riesgo de seguridad de la información	La organización debe implementar el plan de tratamiento del riesgo de seguridad de la información.
	La organización debe retener información documental de los resultados del tratamiento del riesgo de seguridad de la información.
1.6 Evaluación del desempeño	
1.6.1 Monitoreo, medición, análisis y evaluación	La organización debe evaluar el desempeño de la seguridad de la información y la efectividad del sistema de gestión de seguridad de la información.
	La organización debe determinar.
	a) qué necesita ser monitoreado y medido, incluyendo procesos y controles de seguridad de la información;
	b) los métodos para monitorear, medir, analizar y evaluar, según sean aplicables para asegurar la validez de los resultados;
	Nota 11: Los métodos seleccionados deberían producir resultados comparables y ser como válidos.
	c) cuándo el monitoreo y la medición deben ser ejecutados;
	d) quién debe monitorear y medir;
	e) cuándo los resultados del monitoreo y la medición deben ser analizados y evaluados; y
	f) quién debe analizar y evaluar estos resultados.
	La organización debe retener información documental apropiada como evidencia de los resultados del monitoreo y revisión.

1.6.2 Auditoría interna	La organización debe ejecutar auditorías internas planificadas periódicamente para proveer información sobre Si el sistema de gestión de seguridad de la información:
	a) está conforme a:
	- los requerimientos propios de la organización para su sistema de gestión de seguridad de la información; y
	- requerimientos de esta Norma Técnica Salvadoreña,
	b) es efectivamente implementado y mantenido.
	La organización debe:
	a) planificar, establecer, implementar y mantener uno o más programas de auditoria, incluyendo la frecuencia. métodos. responsabilidades, requerimientos de planificación e informes. El o los programas de auditoria deben considerar la importancia de los procesos concernientes y los resultados de auditorías previas;
	b) definir el criterio de la auditoria y el alcance para cada auditoria;
	c) seleccionar los auditores y ejecutar auditorias que aseguren la objetividad e imparcialidad del proceso de auditoría
	d) asegurar que los resultados de las auditorías son informados a la administración pertinente: y
	e) retener información documental como evidencia del o de los programas de auditoria y los resultados de la auditoria.
1.6.3 Revisión de la Dirección	La Alta Dirección debe revisar el sistema de gestión de seguridad de la información de la organización a períodos planificados para asegurar su continua idoneidad. adecuación y efectividad.
	La revisión de la Dirección debe incluir consideraciones de:
	a) estado acciones de previas revisiones de la Dirección;
	b) cambios en asuntos internos y externos que sean relevantes al sistema de gestión de seguridad de la información
	c) retroalimentación del desempeño de la seguridad de la información, incluyendo tendencias en:
	- no conformidades y acciones correctivas
	- resultados del monitoreo y medición;
	- resultados de auditoria;
	- cumplimiento de objetivos de seguridad de la información;
	d) retroalimentación de partes interesadas
	e) resultados de evaluación de riesgo y estado del plan de tratamiento de riesgos: y
	f) oportunidades de mejora continua.
	Los resultados de la revisión de la Dirección deben incluir decisiones relacionadas a oportunidades de mejora continua y

	cualquier necesidad cambios del sistema de gestión de seguridad de la información
	La organización debe retener información documental como evidencia de los resultados de la revisión de la Dirección
1.7 Mejora	
1.7.1 No conformidad y acción correctiva	Cuando una no conformidad ocurre, la organización debe:
	a) reaccionar a la no conformidad. y según aplique:
	- tomar acción para controlarla y corregirla; y
	- lidiar con las consecuencias:
	b) la necesidad de acciones para eliminar las causas de la no conformidad. de tal forma que esta no sea recurrente o se de en otros lugares. a través de:
	- revisar la no conformidad;
	- determinar las de las causas de la no conformidad; y
	- determinar si no conformidades similares existen o podrían ocurrir potencialmente;
	c) implementar cualquier acción necesaria
	d) revisar la efectividad de cualquier acción correctiva tornada; y
	e) realizar cambios al sistema de gestión de seguridad de la información, de ser necesario.
	Las acciones correctivas deben de corresponder a los efectos de las no conformidades encontradas.
	La organización debe retener información documental como evidencia de:
	a) naturaleza de las conformidades y cualesquiera sean las acciones subsecuentes tomadas; y
	b) los resultados de cualquier acción correctiva.
1.7.2 Mejora continua	La organización debe continuamente mejorar la idoneidad, adecuación y efectividad del sistema de gestión de seguridad de la información.

4.5 Política general de seguridad de la información

Veterinaria ABC, S.A de C.V., reconoce la importancia de identificar y proteger los activos de información de la organización, evitando la destrucción, divulgación, modificación y utilización no autorizada de toda información relacionada con clientes, empleados, precios, estrategia, gestión, y otros conceptos relacionados.

La información es el activo más preciado de las empresas y entidades en general, por tanto, se deben tomar todas las precauciones necesarias, para mantener y preservar información, para ello Veterinaria ABC, S.A de C.V., ha venido desarrollando y evolucionando su modelo de seguridad de la información, así como adoptando buenas prácticas en cuanto a la gestión y administración de las Tecnologías de la Información. En consecuencia, se compromete a desarrollar, implantar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información (SGSI) con el objetivo de asegurar la confidencialidad, disponibilidad e integridad de la información.

Introducción

Veterinaria ABC, S.A de C.V. consiente de los riesgos actuales decidió adoptar el modelo de gestión de seguridad de la información que le permite, identificar y minimizar los riesgos a que está expuesta la información y los procesos y elementos asociados a ella.

Dado el gran esfuerzo y recursos que demanda el SGSI, la entidad ha venido adoptando transicionalmente una serie de políticas y medidas que le permitan ir avanzando hasta alcanzar el nivel de madurez necesario.

Por lo anterior, la política y el desarrollo del SGSI serán revisadas con regularidad como parte del proceso de revisión gerencial, o en la medida que se sugieran cambios en el desarrollo del negocio, estructura, objetivos o estrategias que involucren aspectos afines.

Políticas generales de seguridad de la información

La Política de Seguridad de la Información es la declaración general que representa la posición de la administración de Veterinaria ABC, S.A de C.V. con respecto a la protección de los activos de información (los funcionarios, la información, los procesos, las tecnologías

de información incluido el hardware y el software), a la implementación del Sistema de Gestión de Seguridad de la Información y al apoyo, generación y publicación de sus políticas, procedimientos e instructivos.

Veterinaria ABC, S.A de C.V. para el cumplimiento de su misión, visión, objetivo estratégico y apegado a sus valores corporativos, establece la función de Seguridad de la Información en la Entidad, con el objetivo de:

1. Minimizar el riesgo en las funciones más importantes y críticas de la entidad.
2. Cumplir con los principios de seguridad de la información.
3. Cumplir con los principios de la función administrativa.
4. Mantener la confianza de sus clientes, socios y empleados.
5. Apoyar la innovación tecnológica.
6. Implementar el sistema de gestión de seguridad de la información ajustado a las necesidades y dimensión de la entidad.
7. Proteger los activos tecnológicos.
8. 8. Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
9. Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de Veterinaria ABC, S.A de C.V.
10. Garantizar la continuidad del negocio frente a incidentes.

Alcance

Esta política aplica a toda la entidad, sus funcionarios, terceros, aprendices, practicantes, proveedores, clientes de Veterinaria ABC, S.A de C.V.; artesanos de Colombia y ciudadanía en general.

Objetivos

a) Proteger, preservar y administrar objetivamente la información de la Veterinaria ABC, S.A de C.V., junto con las tecnologías utilizada para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de las características de confidencialidad, integridad, disponibilidad, legalidad, confiabilidad y no repudio de la información.
b) Mantener la Política de Seguridad de la Información actualizada, vigente, operativa y auditada dentro del marco determinado por los riesgos globales y específicos de la Veterinaria ABC, S.A de C.V. para asegurar su permanencia y nivel de eficacia.
c) Definir las directrices de la Veterinaria ABC, S.A de C.V. Distrital para la correcta valoración, análisis y evaluación de los riesgos de seguridad asociados a la información y su impacto, identificando y evaluando diferentes opciones para su tratamiento con el fin de garantizar la continuidad e integridad de los sistemas de información.

Responsabilidades

Comité de Seguridad de la Información

-Gerente General: Dr. Giacomo Zappalá

-Director del hospital: Dr Adrian Abarca

-Administrador Contable: Ricardo Domínguez

-Gerente de IT: Carlos Figueroa

Funciones Principales

a) Dentro del flujo de aprobación de las Políticas de Seguridad de la Información, el Comité de Seguridad de la Información es el primer nivel de aprobación, revisión, rechazo, modificación o eliminación de éstas;
b) El Comité de Seguridad de la Información aprueba normas y procedimientos de seguridad de la Información.
c) Revisa y valida normas y procedimientos en general, a fin de verificar que se estén cumpliendo los aspectos de seguridad dentro de los procesos.
d) Por medio del Comité de Seguridad de la Información se supervisa y controla el Plan de Seguridad de la Información para analizar temas tales como:
e) Revisar el avance del plan y dar directrices en caso de atrasos;
f) Establecer recursos para administrar los incidentes de seguridad u otras vulnerabilidades;
g) Velar por el cumplimiento de las políticas, normas, procedimientos y demás documentos relacionados en Seguridad de la Información dentro de la organización;
h) Definir proyectos de tecnología que impliquen la aplicación de Seguridad de la Información en el contexto del negocio (Servicio, Producto e Información);
i) Generar resúmenes de actividades englobadas en el marco de la Seguridad de la Información para ser presentadas ante las máximas autoridades de la organización.
j) Monitorear cambios significativos en los riesgos que afectan a los recursos de la información de la Organización frente a posibles amenazas, sean internas o externas.

k) Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes, relativos a la seguridad, que se produzcan en el ámbito de la Organización.

l) Por medio del Comité de Seguridad de la Información se instruirá al Oficial de Seguridad de la Información el inicio del proceso de revisión anual de las políticas vigentes. Dicha instrucción se dará en la sesión de diciembre de cada año.

m) Aprobar las principales iniciativas para incrementar la Seguridad de la Información de acuerdo a las competencias y responsabilidades asignadas a cada gerencia, así como acordar y aprobar metodologías y procesos específicos relativos a la Seguridad de la Información.

n) Evaluar y coordinar la implementación de controles específicos de Seguridad de la Información para los sistemas o servicios de la Organización, sean preexistente o nuevos.

o) Promover la difusión y apoyo a la Seguridad de la Información dentro de la Organización, así como también, coordinar el proceso de administración de la continuidad de las actividades.

p) Entre otras

Nivel de cumplimiento

Todas las personas cubiertas por el alcance y aplicabilidad se esperan adhieran en un 100% la política.

A continuación, se establecen las políticas de seguridad que soportan el SGSI de Veterinaria ABC, S.A de C.V.

1. Veterinaria ABC, S.A de C.V. ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.
2. Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, socios de negocio o terceros.
3. Veterinaria ABC, S.A de C.V. protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.
4. Veterinaria ABC, S.A de C.V. protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
5. Veterinaria ABC, S.A de C.V. protegerá su información de las amenazas originadas por parte del personal.
6. Veterinaria ABC, S.A de C.V., protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
7. Veterinaria ABC, S.A de C.V., controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
8. Veterinaria ABC, S.A de C.V., implementará control de acceso a la información, sistemas y recursos de red.

9. Veterinaria ABC, S.A de C.V., garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
10. Veterinaria ABC, S.A de C.V., garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
11. Veterinaria ABC, S.A de C.V. garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos. Veterinaria ABC, S.A de C.V. garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecida.

4.6 Matriz de Riesgo

Para obtener la matriz de riesgos se tienen en cuenta los diferentes escenarios a los que se enfrenta el proyecto y su impacto

a) El analista determina los posibles riesgos, a partir del "Listado de Riesgos" que se puede ampliar y adaptar a cada caso concreto.
b) Asigna una probabilidad de ocurrencia (1, 2, 3, 4, y 5), correspondiendo 1 a un suceso excepcional y 5 a la máxima probabilidad
c) Asigna el impacto (1, 2, 3, 4 y 5), siendo 1 un impacto insignificante y 5 una catástrofe
d) El modelo calcula el riesgo (bajo, medio, alto y muy alto) de acuerdo con la matriz de riesgos.

Figura 3 Matriz de Riesgos para Seguridad Lógica y Seguridad Física

	IMPACTO				
PROBABILIDAD	1–Insignificante	2–Pequeño	3–Moderado	4–Grande	5–Catastrofe
5- Casi seguro que sucede	Medio (5)	Alto (10)	Alto (15)	Muy alto (20)	Muy alto (25)
4- Muy probable	Medio (4)	Medio (6)	Alto (12)	Alto (16)	Muy alto (20)
3- Es posible	Bajo (3)	Medio (5)	Medio (9)	Alto (12)	Alto (15)
2- Es raro que suceda	Bajo (2)	Bajo (4)	Medio (6)	Medio (8)	Alto (10)
1- Sería excepcional	Bajo (1)	Bajo (2)	Bajo (3)	Bajo (4)	Medio (5)

Figura 3. Elaboración propia

Tabla 3 Evaluación de Riesgos

Tipo de riesgo	Probabilidad	X	Impacto
Filtración de información sensible (nombres de clientes, números telefónicos, domicilio, correos electrónicos) hacia personas ajenas a la veterinaria	4- Muy probable		3–Moderado
Pérdida de información provocada por bajones de energía e inexistencia de back-ups recientes	2- Es raro que suceda		3–Moderado
Caída del sistema al momento de tomar alguna orden del área de peluquería o clínica (generalmente por problemas de red)	3- Es posible		4–Grande

Caída del sistema SAC	3- Es posible	4–Grande
Daños provocados por algún tipo desastre natural, principalmente terremotos que son bastante comunes en nuestro país	3- Es posible	5–Catástrofe
Caída del servicio de internet	4- Muy probable	4–Grande
Daños en el cableado interno de red de la empresa por deterioro del tiempo u otro agente externo	3- Es posible	3–Moderado
Falta de funcionamiento	1- Sería excepcional	4–Grande
Caída del servidor que soporta el sitio web	3- Es posible	4–Grande
Daño parcial o permanente por mala manipulación de los empleados	3- Es posible	4–Grande
Daño parcial o total por mal uso de parte del personal asignado	3- Es posible	4–Grande
Dejar de imprimir cuando se lleve a cabo alguna actividad urgente (reportes de clínica)	3- Es posible	3–Moderado

Tabla 3. Elaboración propia

Tabla 4 Resultado de Matriz de Riesgos

Activo de información	**Riesgo identificado**	**Consecuencia asociada**	**Resultado**	**Periodicidad de revisión**
Información de clientes	Filtración de información sensible (nombres de clientes, números telefónicos, domicilio, correos electrónicos) hacia personas ajenas a la veterinaria	Consecuencias del tipo reputacional o económicas por daños y perjuicios en contra de los afectados(clientes)	Alto	Mínimo de 3 veces al año
Información contable-administrativa	Pérdida de información provocada por bajones de energía e inexistencia de back-ups recientes	Atraso en las operaciones diarias y reorientación de prioridades administrativas para la reconstrucción de la información perdida	Medio	Mínimo de 3 veces al año
Software para historial clínico: MEDVET	Caída del sistema al momento de tomar alguna orden del área de peluquería o clínica (generalmente por problemas de red)	Quejas y reclamos de los clientes por el atraso generado al procesar los servicios que ha solicitado	Alto	Mínimo de 4 veces al año
Software contable-administrativo: SAC	Caída del sistema SAC	• En facturación, quejas de parte de los clientes debido a atrasos al momento de dar ingreso a la factura por el servicio o producto que está pagando	Alto	Mínimo de 6 veces al año

		• Respecto a la parte contable-administrativa, atrasos en el procesamiento de la información lo cual no permitiría presentar resultados oportunamente ante la alta dirección		
Instalaciones	Daños provocados por algún tipo desastre natural, principalmente terremotos que son bastante comunes en nuestro país	Detrimento económico para la empresa pues tendría que destinar fondos a la reparación de la infraestructura para reestablecer el buen funcionamiento de las operaciones	Alto	Mínimo de 6 veces al año
Internet	Caída del servicio de internet	Atraso en las actividades empresariales, así como perdida de comunicación entre los mismos empleados, con los proveedores y hasta con los clientes.	Alto	Mínimo de 12 veces al año
Infraestructura de red	Daños en el cableado interno de red de la empresa por deterioro del tiempo u otro agente externo	Consecuencias económicas pues afecta las actividades normales de la empresa	Medio	Mínimo de 4 veces al año
Sistema de videovigilancia	Falta de funcionamiento	Posibilidad de sufrir algún tipo de robo o hurto tanto en los alrededores de la veterinaria como adentro de la misma que a	Bajo	Mínimo de 12 veces al año

		su vez provocaría detrimento económico		
Página web	Caída del servidor que soporta el sitio web	Disminución de clientes potenciales que a su vez deriva en pérdidas económicas	Alto	Mínimo de 12 veces al año
Servidor de red	Daño parcial o permanente por mala manipulación de los empleados	Atraso en las actividades diarias de la empresa al afectar directamente a los demás equipos que se encuentran conectados a dicho servidor	Alto	Mínimo de 3 veces al año
Equipo de computo	Daño parcial o total por mal uso de parte del personal asignado	Atraso en las actividades diarias de la empresa pues es un recurso que interviene de manera directa	Alto	Mínimo de 4 veces al año
Impresoras	Dejar de imprimir cuando se lleve a cabo alguna actividad urgente (reportes de clínica)	Atraso en las actividades normales del área correspondiente	Medio	Mínimo de 4 veces al año

Tabla 4 Elaboración propia

Riesgo identificado	Controles	Periodicidad de revisión
Filtración de información sensible (nombres de clientes, números telefónicos, domicilio, correos electrónicos) hacia personas ajenas a la veterinaria	-Establecer niveles de acceso a la información según la jerarquía organizacional. -Restringir el uso de USB para gestionar el manejo de la información	Mensual
Pérdida de información provocada por bajones de energía e inexistencia de back-ups recientes	-Colocar UPS que permitan apagar los equipos de manera correcta y evitar así la perdida de información	Anual
Caída del sistema al momento de tomar alguna orden del área de peluquería o clínica (generalmente por problemas de red)	-Mantenimiento a las conexiones de red de la empresa	Mensual
Caída del sistema SAC	-Revisión y mantenimiento rutinario del sistema de parte del proveedor respectivo	Mensual
Daños provocados por algún tipo desastre natural, principalmente terremotos que son bastante comunes en nuestro país	-Contratación de un seguro contra daños que minimice el impacto económico en caso se suscite algún evento fortuito.	Renovación anual y pago mensual
Caída del servicio de internet	-Revisión y mantenimiento del router	Mensual
Daños en el cableado interno de red de la empresa por deterioro del tiempo u otro agente externo	-Revisión del cableado y reparaciones en caso de ser necesario	Mensual
Falta de funcionamiento	-Mantenimiento correctivo y preventivo del sistema de cámaras	Mensual
Caída del servidor que soporta el sitio web	-Contratar un plan de hosting acorde a la demanda del sitio y solicitar mantenimiento periódico	Mensual
Daño parcial o permanente por mala manipulación de los empleados	-Capacitaciones a los empleados que manipulan los servidores	Anual o cada vez que se cambien los servidores
Daño parcial o total por mal uso de parte del personal asignado	-Capacitaciones a los empleados que manipulan los equipos(computadoras de escritorio o laptops)	Anual o cada vez que se cambien los equipos
Atraso en las actividades normales del área correspondiente	-Mantenimiento preventivo y correctivo y limpieza interna de las impresoras	Mensual

5 CONCLUSIONES

a) Las clínicas y hospitales veterinarios que actualmente cuentan con un SGSI no está diseñado bajo la metodología de la NTS ISO/IEC 27001:2013 sino más bien son implementados basados en la propia experiencia de las empresas y en el conocimiento mínimo de algunos aspectos básicos por lo que no se garantiza la confidencialidad, integridad y disponibilidad de la información.

b) Si bien es cierto, una buena parte de clínicas y/o hospitales veterinarios se han preocupado por las capacitaciones sobre SGSI aún se tiene mucho camino por recorrer en este tema sobre todo en la frecuencia con que son realizadas las mencionadas capacitaciones.

c) Los principales riesgos a los que las veterinarias están expuesta son el robo de la información y a los virus informáticos. A pesar de esto, la mayor parte los controles aplicados para el resguardo de la información se limita a realizar back-up en discos de almacenaje físicos, dejando de lado riesgos como robo de información de carácter confidencial.

d) La mejora continua es parte esencial del desarrollo de un SGSI, las empresas veterinarias enfocan sus esfuerzos en mantener su información segura de riesgos que puedan provocar su perdida, por ejemplo, fallo en el servidor, daños en discos duros, etc. Si bien es cierto, esto es parte fundamental a tener en cuenta para aplicar políticas de seguridad de la información, también la NTS ISO/IEC 27001:2013 aborda temas relacionados a la mantener la confidencialidad de la información, esto debido a las amenazas que surgen a partir de los avances tecnológicos, como lo son ataques de secuestro y filtración de información confidencial.

6 RECOMENDACIONES

De acuerdo a conclusiones anteriores se recomienda:

a) A las clínicas y hospitales veterinarios tanto a los que cuentan con un SGSI como las que no ha implementado alguno, hacerlo basándose en la NTS ISO/IEC 27001:2013, pues proporciona una reducción del riesgo de sufrir incidentes además establece una metodología para gestionar la seguridad de la información de forma clara y concisa.

b) Definir políticas de seguridad de la información, las cuales deben reflejar los objetivos de seguridad que se persiguen, respondiendo a la interrogante de ¿Qué voy a hacer?, sin tocar el tema de implementación, por lo tanto hay que tener el cuidado de no relacionar procesos operativos en este punto.

c) Establecer de qué manera se va a gestionar la seguridad del recurso humano, tomando en consideración dos tiempos: Antes de la contratación (Verificación de hojas de vida y referencias tanto personales como laborales) y Durante la contratación (Firma de acuerdos de confidencialidad y de no divulgación).

d) Realizar capacitaciones al personal correspondiente sobre los SGSI, su implementación y seguimiento con una mayor frecuencia, por lo menos dos veces al año. Hay que tomar en cuenta que las tecnologías y los sistemas de información evolucionan a un ritmo acelerado y la necesidad de emitir normativas que regulen la gestión de dichos sistemas se vuelve imperante por lo tanto se debe buscar ir a la vanguardia para no caer en la obsolescencia de conocimiento.

e) Evitar el incumplimiento de obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con la seguridad de la información, es de suma importancia para que la entidad (en este caso las clínicas veterinarias), no incurran en demandas, multas u otra clase de afectación tanto a la imagen como a las finanzas de la misma. Es necesario tomar en cuenta este aspecto, ya que no se sabe con certeza en qué momento, las actuales leyes serán aplicadas con mayor rigurosidad o si se emitirán nuevas regulaciones en el futuro.

f) Redactar procedimientos documentados de cada uno de los elementos de procesamiento de la información, tales como servicios, aplicativos, dispositivos de red y de infraestructura. La documentación por cada elemento debe incluir al menos: Información y configuración de los sistemas, procedimientos de encendido y apagado y procedimientos de respaldo de los datos.

g) Mantener un plan de mejora continua para el SGSI, que vaya acorde los nuevos riesgos que surgen con las nuevas tecnologías, además establecer revisiones periódicas sobre el mencionado plan, para corregir desviaciones que puedan surgir en el camino.

BIBLIOGRAFÍA

Asamblea Legislativa de El Salvador. (s.f.). Ley especial contra delitos informáticos y conexos. San Salvador.

Consejo Superior de Salud Pública. (s.f.). Obtenido de www.cddp.gob.sv

OSN. (2013). NTS ISO/IEC 27001:2013.

Universidad de El Salvador. (2008). Periódico El Universitario.

ANEXOS

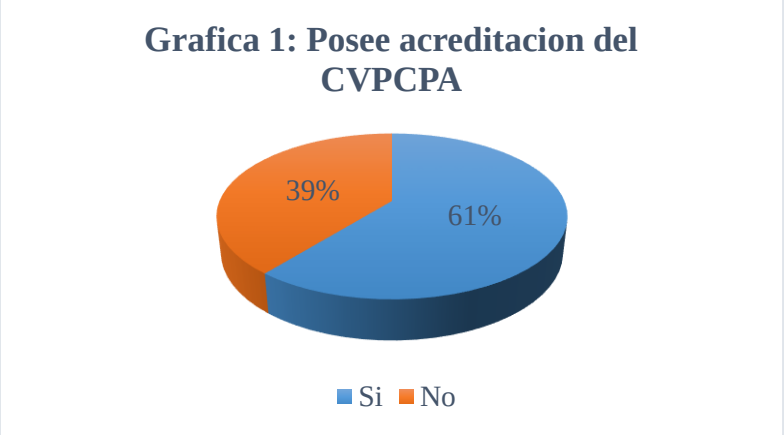
Anexo 1. ANALISIS Y PROCESAMIENTO DE DATOS

Pregunta 1:

¿Posee acreditación del Consejo de Vigilancia de la Profesión de Contaduría Pública y Auditoria, para ejercer como contador?

Objetivo: Determinar el porcentaje de contadores que están autorizados para ejercer la Profesión de Contaduría Pública.

Opción	Frecuencia absoluta	Frecuencia relativa
Si	14	61%
No	9	39%
Total	**23**	**100%**



Análisis e interpretación:
Del 100% de contadores encuestados que conforman la muestra (23), el 61% posee actualmente acreditación del CVPCPA para ejercer la profesión mientras que el 39% restante no posee la mencionada acreditación (o probablemente está en trámite).

Pregunta 2:

¿La entidad para la cual trabaja ha implementado un Sistema de Gestión de Seguridad de la Información (SGSI)?

Objetivo: Identificar si en las clínicas y hospitales veterinarios consideran importante la implementación de un SGSI para mejorar el triángulo CID (Confidencialidad, Integridad y Disponibilidad)

Tabla de resultados 2: la entidad ha implementado un SGSI

Opción	Frecuencia absoluta	Frecuencia relativa
Si	9	39%
No	14	61%
Total	**23**	**100%**

Análisis e interpretación:
Solo el 39% de los contadores encuestados indicaron que la clínica veterinaria en la cual trabajan ha implementado un SGSI contrarrestado con un 61% que mencionaron que no poseen un SGSI en la entidad.

Pregunta 3:

¿Ha recibido capacitaciones relacionadas a los Sistema de Gestión de Seguridad de la Información?

Tabla de resultados 3: Ha recibido capacitaciones relacionadas a SGSI

Opción	Frecuencia absoluta	Frecuencia relativa
Si	12	52%
No	11	48%
Total	**23**	**100%**

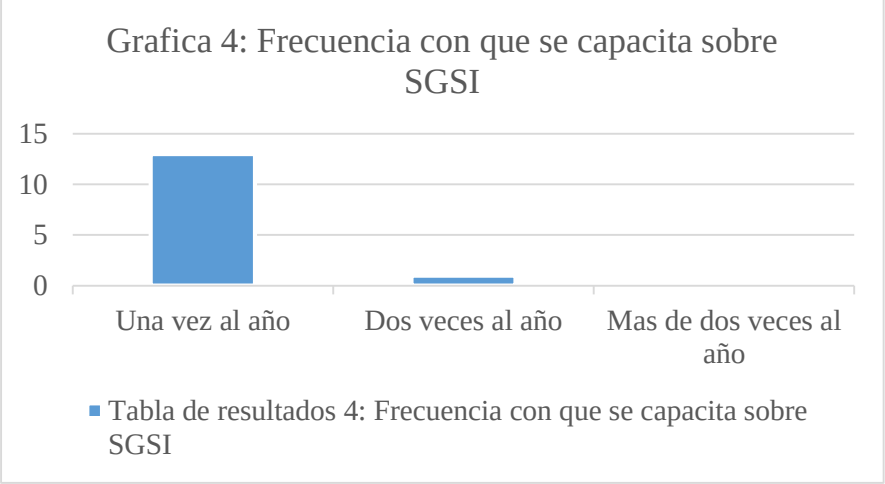
Análisis e Interpretación:
De los 23 encuestados, 12 mencionaron que han recibido capacitaciones relacionados a los SGSI representando un 52% del total de la muestra, lo que indica que al menos la mitad de clínicas veterinarias le han tomado importancia a este aspecto.

Pregunta 4:

¿Con qué frecuencia ha recibido capacitaciones sobre un SGSI?

Tabla de resultados 4: Frecuencia con que se capacita sobre SGSI

Opción	Frecuencia absoluta	Frecuencia relativa
Una vez al año	13	93%
Dos veces al año	1	7%
Más de dos veces al año	0	0%
Total	**14**	**100%**



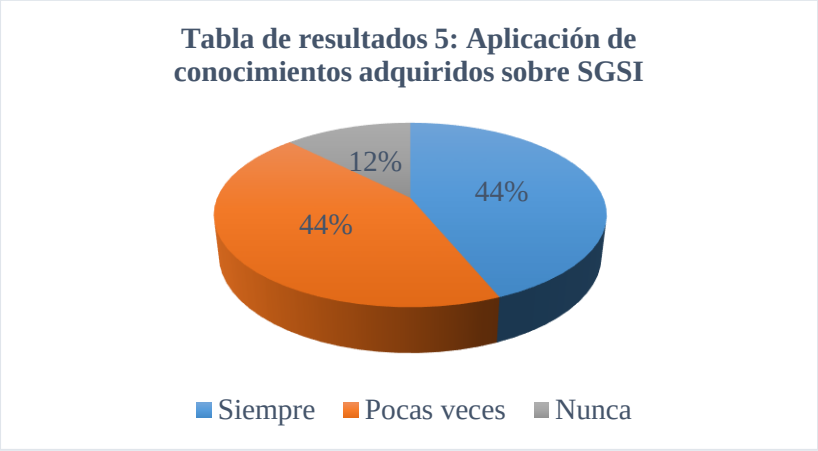
Análisis e Interpretación:
De los 12 contadores que han recibido capacitaciones relacionadas con los SGSI, 11 la han recibido una vez al año (91.67%) y 1 persona la ha recibido dos veces al año (8.33%), las otras dos personas que mencionaron la frecuencia, respondieron negativamente la pregunta anterior por lo que no se tomarán en cuenta para el análisis de ésta pregunta.

Pregunta 5:

¿Ha aplicado los conocimientos adquiridos en las capacitaciones recibidas sobre los SGSI en sus labores como contador?

Objetivo: identificar si el profesional aplica los conocimientos adquiridos en las capacitaciones

Opción	Frecuencia absoluta	Frecuencia relativa
Siempre	7	44%
Pocas veces	7	44%
Nunca	2	13%
Total	**16**	**100%**



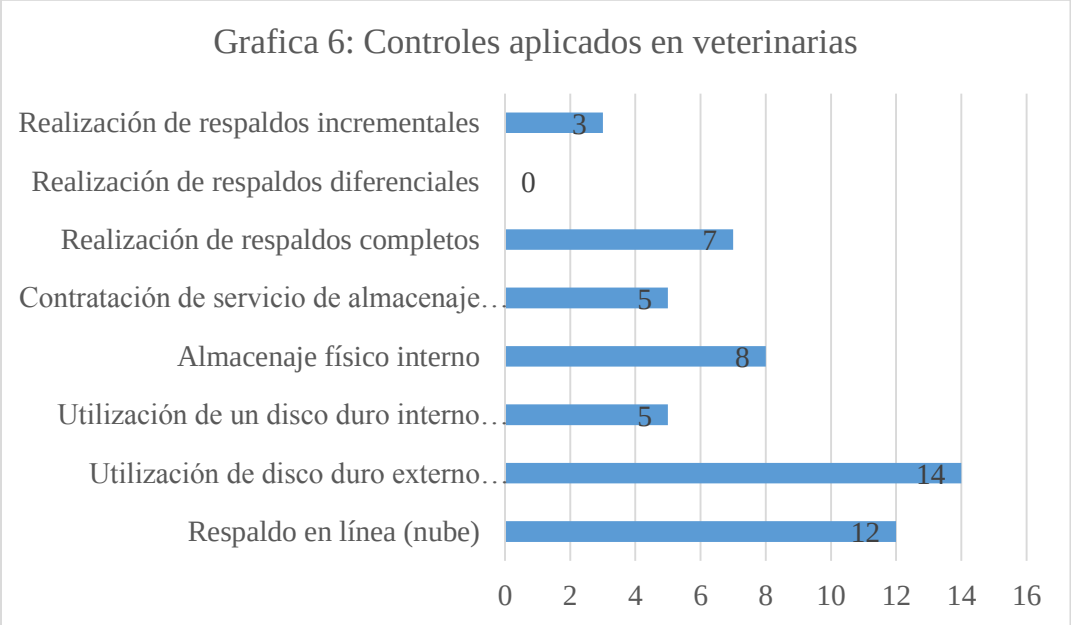
Análisis e Interpretación:
De los 12 contadores que han recibido capacitaciones relacionadas con los SGSI, 5 indican que "Siempre" han aplicado los conocimientos adquiridos (41.67%), 6 mencionan que "Pocas veces" los han aplicado (50%) y 1 persona respondió que "Nunca" ha aplicado dichos conocimientos (8.33%). Los demás se quedan fuera del análisis debido a que respondieron negativamente la pregunta N°3.

Pregunta 6:

De la siguiente lista de controles relacionados al respaldo de la información, señale cuáles son los controles aplicados en la entidad.

Objetivo: Conocer si en la clínica veterinaria se han definido controles para el resguardo de la información, y si estos son adecuados

Opción	Frecuencia absoluta
Respaldo en línea (nube)	12 de 23
Utilización de disco duro externo exclusivo para back-ups	14 de 23
Utilización de un disco duro interno (computadoras con uso múltiple)	5 de 23
Almacenaje físico interno	8 de 23
Contratación de servicio de almacenaje externo	5 de 23
Realización de respaldos completos	7 de 23
Realización de respaldos diferenciales	0 de 23
Realización de respaldos incrementales	3 de 23



Análisis e Interpretación:

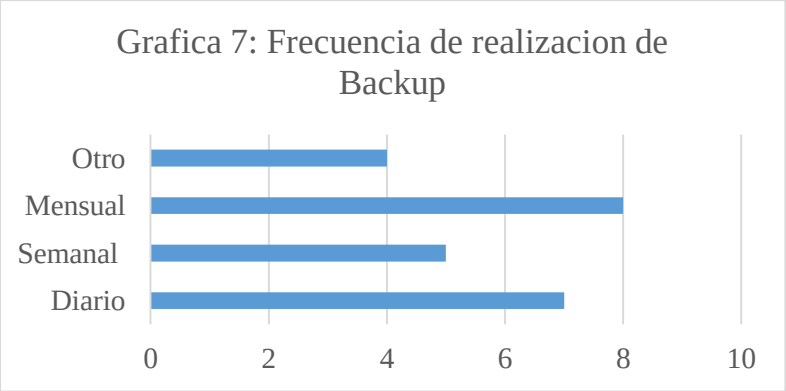
El respaldo en la nube y la utilización de discos duros externos con un 52% y 61% respectivamente son los controles mayormente aplicados por las clínicas veterinarias. Por otra parte, la realización de respaldos diferenciales y respaldos incrementales son lo menos utilizados con un 0% y un 13% correspondientemente.

Pregunta 7:

Con base en los controles seleccionados anteriormente, indique ¿Con qué frecuencia se realiza back-up de la información en disco duro?

Tabla de resultados 7: Frecuencia de realización de Backup

Opción	Frecuencia absoluta	Frecuencia relativa
Diario	7	29%
Semanal	5	21%
Mensual	8	33%
Otro	4	17%
Total	**24**	**100%**



Análisis e Interpretación:

El 33% de los encuestados mencionó que realizan back-up mensualmente, un 29% lo hacen diario, 21% semanalmente y el 17% restante indicó otra periocidad.

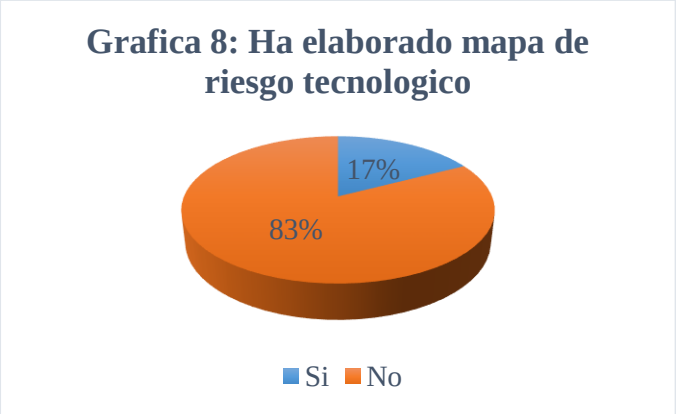
Pregunta 8:

En su empresa ¿Han elaborado un mapa de riesgo tecnológico?

Objetivo: Determinar qué riesgo es el que más afecta el resguardo de la información en las clínicas y hospitales veterinarios.

Tabla de resultados 8: Ha elaborado mapa de riesgo tecnológico

Opción	Frecuencia absoluta	Frecuencia relativa
Si	4	17%
No	19	83%
Total	**23**	**100%**



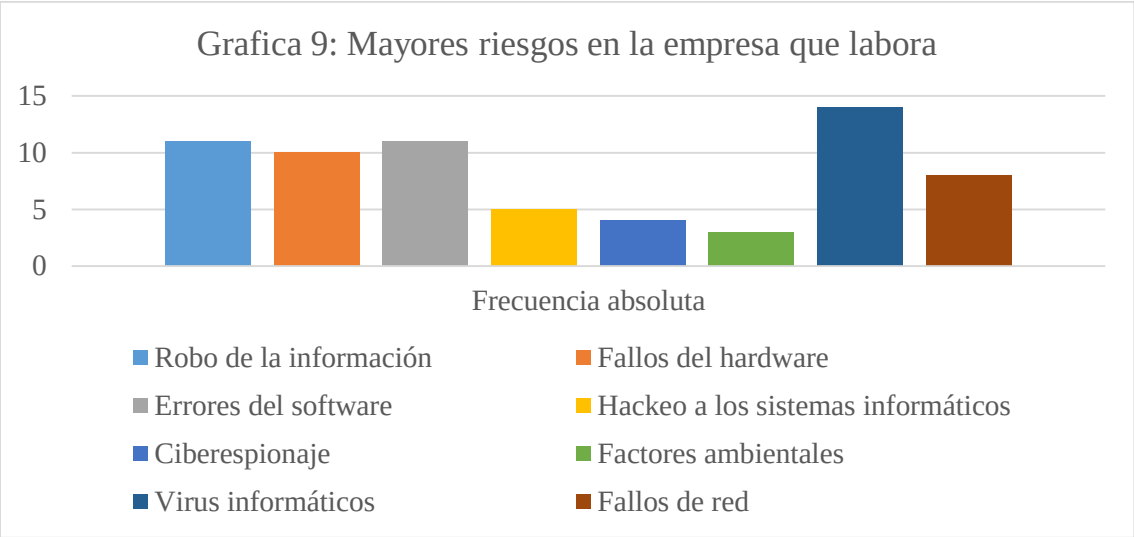
Análisis e Interpretación:

Apenas el 13% de las clínicas veterinarias cuenta con un mapa de riesgo tecnológico, contra un 87% que indica no poner en práctica esa mencionada técnica para la gestión de riesgos.

Pregunta 9:

¿Cuáles cree que son los mayores riesgos a los que se expone la información que resguardan en la entidad en la que usted labora?

Opción	Frecuencia absoluta
Robo de la información	11 de 23
Fallos del hardware	10 de 23
Errores del software	11 de 23
Hackeo a los sistemas informáticos	5 de 23
Ciberespionaje	4 de 23
Factores ambientales	3 de 23
Virus informáticos	14 de 23
Fallos de red	8 de 23
Total	**66**



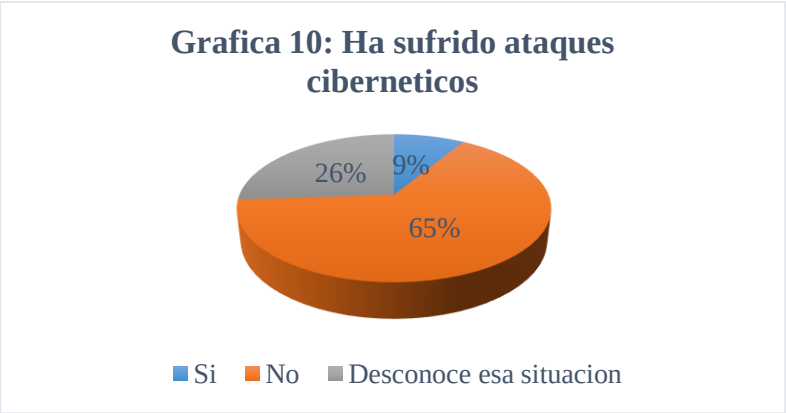
Análisis e interpretación:
De los 23 contadores, 14 (60.87%) de ellos considera que uno de los principales riesgos de la información donde labora son los virus informáticos, y el 47.83% considera que robo de la información y errores de software puede presentarse en la veterinaria donde labora.

Pregunta 10:

¿La empresa dónde usted labora ha sufrido de ataques cibernéticos?

Tabla de resultados 10: Ha sufrido ataques cibernéticos

Opción	Frecuencia absoluta	Frecuencia relativa
Si	2	9%
No	15	65%
Desconoce esa situación	6	26%
Total	**23**	**100%**



Análisis e interpretación:

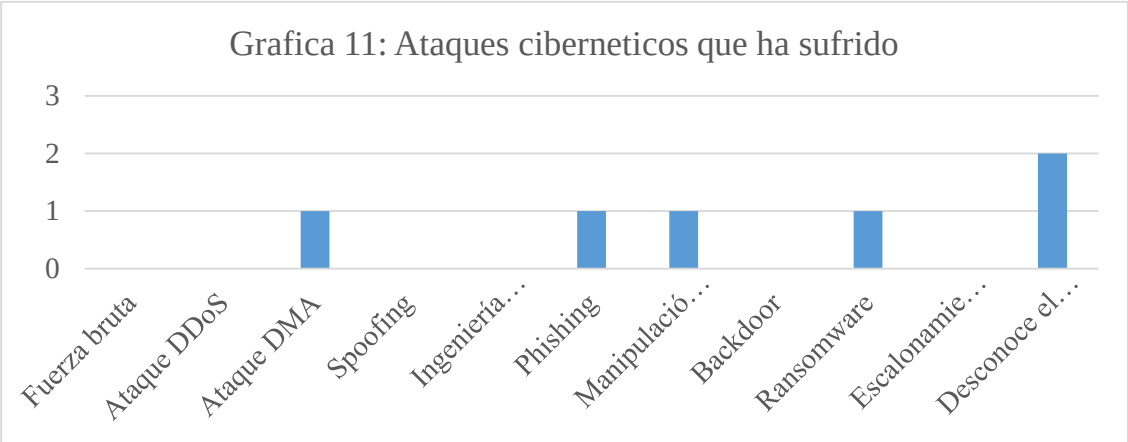
El 65% de los encuestados dice no haber sufrido ataques cibernéticos mientras el 26% desconoce esa situación. Esto indica que las veterinarias no tienden a ser objetivo de este tipo de ataques.

Pregunta 11:

Con respecto a la pregunta anterior, si su respuesta es afirmativa, señale cuál o cuáles de los siguientes ataques cibernéticos ha sufrido su empresa.

Tabla de resultados 11: Ataques cibernéticos que ha sufrido

Opción	Frecuencia absoluta
Fuerza bruta	0 de 23
Ataque DDoS	0 de 23
Ataque DMA	1 de 23
Spoofing	0 de 23
Ingeniería Social	0 de 23
Phishing	1 de 23
Manipulación de URL	1 de 23
Backdoor	0 de 23
Ransomware	1 de 23
Escalonamiento de privilegios	0 de 23
Desconoce el tipo de ataque	2 de 23
Total	**6**



Análisis e interpretación:

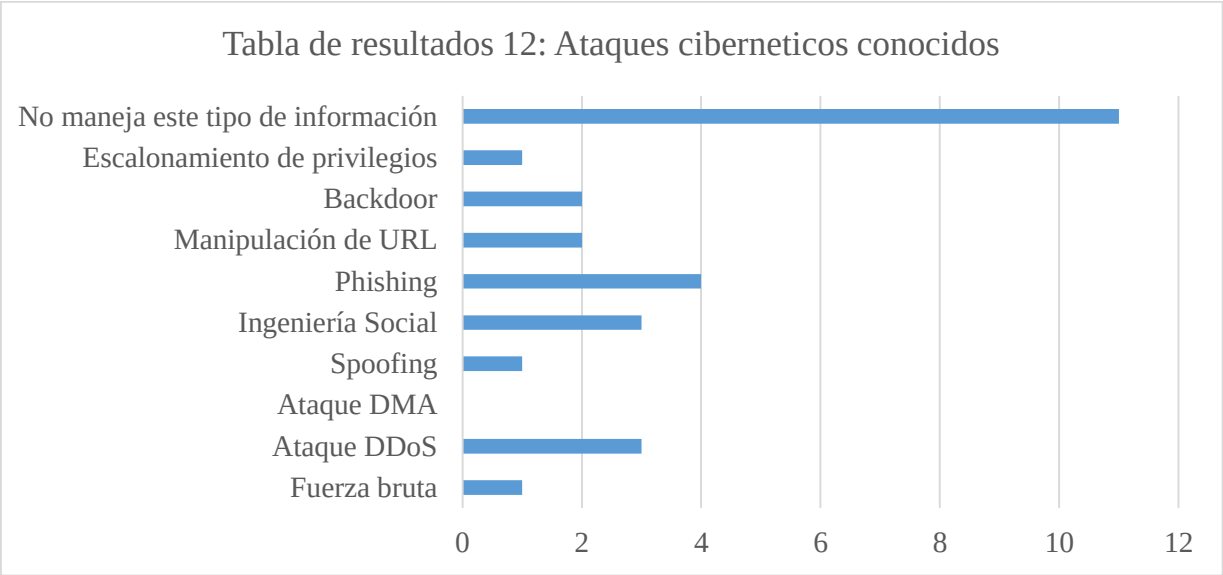
De las veterinarias que han sufrido ataques cibernéticos, 2 de ellas desconoce el tipo de ataque, mientras que otros ataques son el ataque DMA, Phishing, Manipulación de URL y Ransomware que son ataques que se centran en la obtención o secuestro de información para obtener beneficios económicos. Lo que indica que las veterinarias, a pesar de no sufrir ataques constantes, estos van destinados a la información importante (financiera) de la sociedad.

Pregunta 12:

Respecto a la pregunta 10, en caso de que su respuesta sea negativa, señale cuál o cuáles de los siguientes ataques cibernéticos conoce o ha escuchado mencionar.

Tabla de resultados 12: Ataques cibernéticos conocidos

Opción	Frecuencia absoluta
Fuerza bruta	1 de 23
Ataque DDoS	3 de 23
Ataque DMA	0 de 23
Spoofing	1 de 23
Ingeniería Social	3 de 23
Phishing	4 de 23
Manipulación de URL	2 de 23
Backdoor	2 de 23
Escalonamiento de privilegios	1 de 23
No maneja este tipo de información	11 de 23
Total	**28**



Análisis e interpretación:

De los contadores encuestados, 47.86% no conoce los tipos de ataques cibernéticos mencionados, esto indique que casi la mitad de la muestra no está en condiciones de identificar un ataque oportunamente.

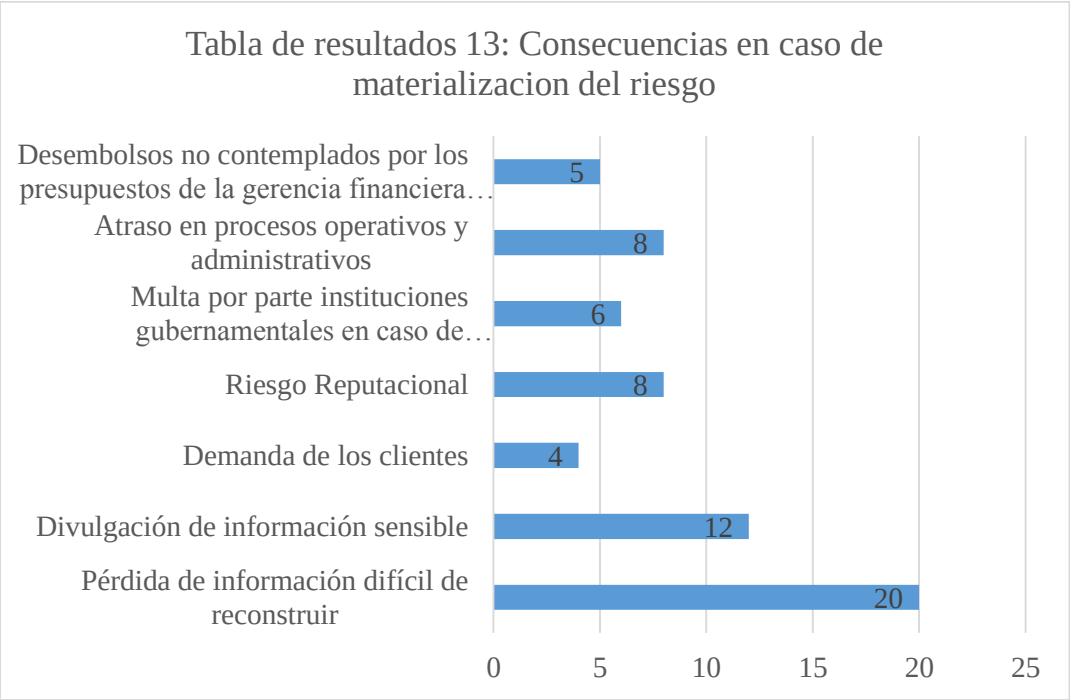
Pregunta 13:

¿Cuáles considera que son las principales consecuencias en caso de materialización de los riesgos de seguridad de la información?

Objetivo: Determinar si la empresa identifica las principales consecuencias ocasionadas al ocurrir alguno de los riesgos mencionados.

Tabla de resultados 13: Consecuencias en caso de materialización del riesgo

Opción	Frecuencia absoluta
Pérdida de información difícil de reconstruir	20 de 23
Divulgación de información sensible	12 de 23
Demanda de los clientes	4 de 23
Riesgo Reputacional	8 de 23
Multa por parte instituciones gubernamentales en caso de requerimientos de información no disponible	6 de 23
Atraso en procesos operativos y administrativos	8 de 23
Desembolsos no contemplados por los presupuestos de la gerencia financiera o el área de contabilidad	5 de 23
Total	**63**



Análisis e interpretación:

De los encuestados 86.96% considera que la consecuencia principal por la materialización de un riesgo es la perdida de información difícil de reconstruir. Esto nos indica que la mayoría de contadores de veterinarias consideran que los ataques que afecten la información (pérdida o secuestro) pueden representar situaciones más complicadas de corregir en la entidad.

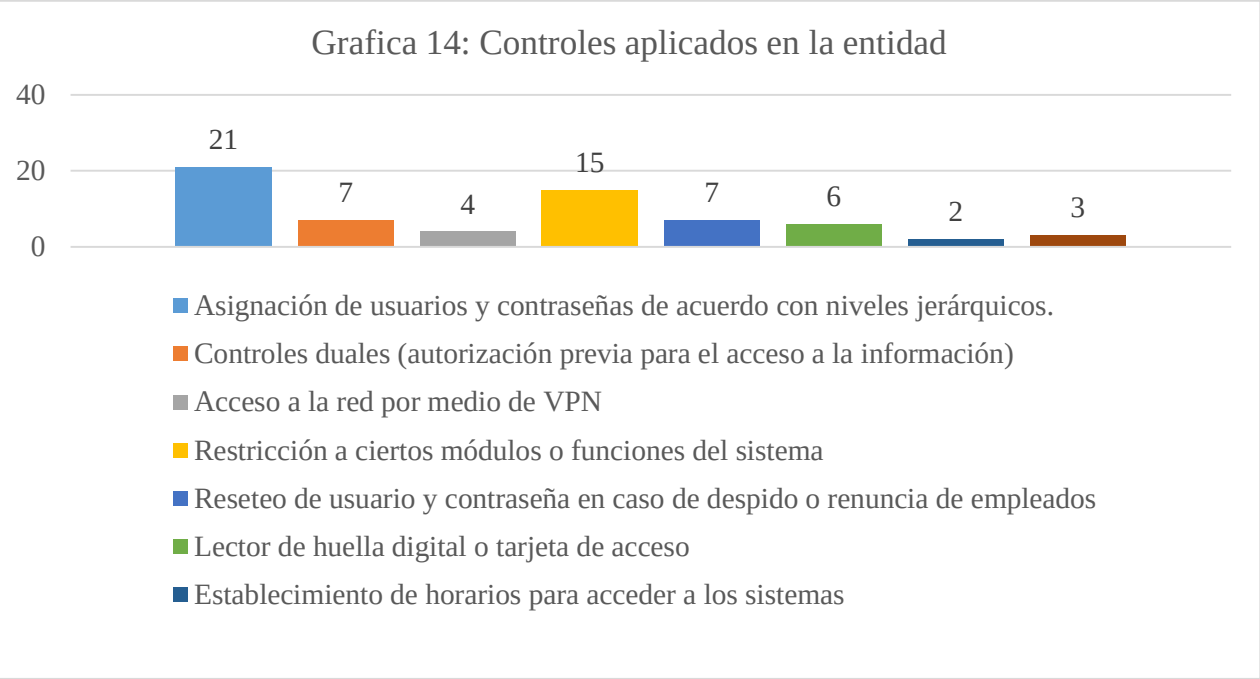
Pregunta 14:

De la siguiente lista de controles relacionados con el acceso no autorizado a la información, señale cuáles son los controles aplicados en la entidad.

Objetivo: Conocer si en las clínicas veterinarias se han definido controles para el acceso a la información, y si estos son adecuados

Tabla de resultados 14: Controles aplicados en la entidad

Opción	Frecuencia absoluta
Asignación de usuarios y contraseñas de acuerdo con niveles jerárquicos.	21 de 23
Controles duales (autorización previa para el acceso a la información)	7 de 23
Acceso a la red por medio de VPN	4 de 23
Restricción a ciertos módulos o funciones del sistema	15 de 23
Reseteo de usuario y contraseña en caso de despido o renuncia de empleados	7 de 23
Lector de huella digital o tarjeta de acceso	6 de 23
Establecimiento de horarios para acceder a los sistemas	2 de 23
Timeout a las sesiones de cada usuario autorizado	3 de 23
Total	**65**



Análisis e interpretación:

Del total de encuestados, 21 aplican los controles de asignación de usuarios y contraseñas de acuerdo a niveles jerárquicos, además, 15 también poseen controles de restricción de acceso a ciertos módulos del sistema. Esto indique que las veterinarias enfocan sus controles al acceso a los sistemas informáticos (software) y a la confidencialidad de la información que en ellos se maneja.

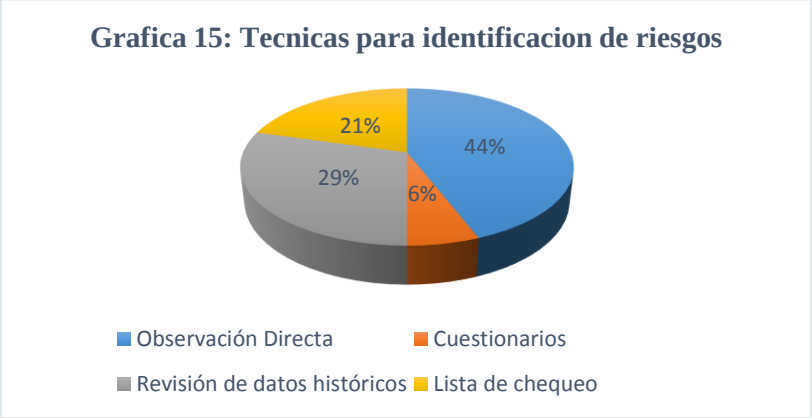
Pregunta 15:

¿Qué técnicas utiliza para la identificación de riesgos en las actividades que realiza la empresa en la cual labora?

Objetivo: Evaluar si las técnicas de identificación de riesgos son las más apropiadas según el tipo de actividades que realizan las clínicas y hospitales veterinarios.

Tabla de resultados 15: Técnicas para identificación de riesgos

Opción	Frecuencia absoluta
Observación Directa	15 de 23
Cuestionarios	2 de 23
Revisión de datos históricos	10 de 23
Lista de chequeo	7 de 23
Total	**34**



Análisis e interpretación:

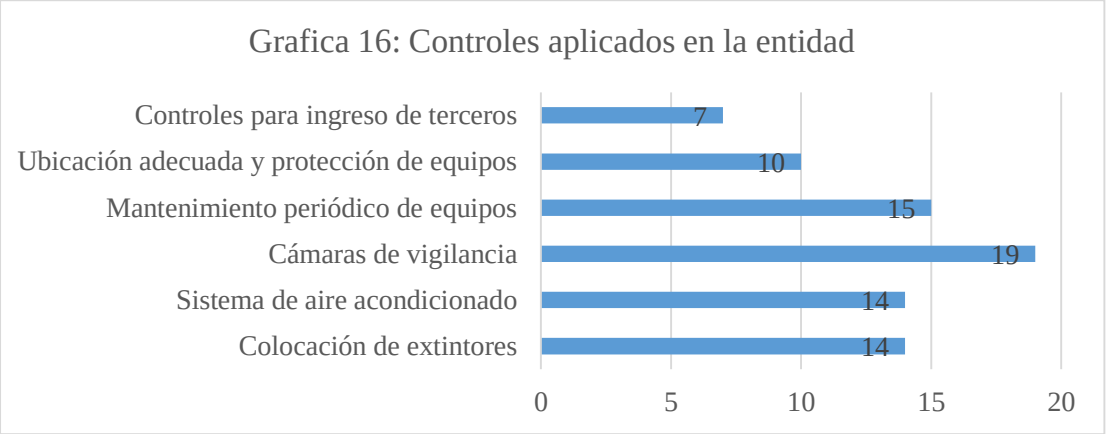
El 44% de los contadores de veterinarias utilizan la técnica de observación directa para la identificación de riesgos que pueden darse dentro de la entidad, mientras que 29% se base en el histórico de riesgos.

Pregunta 16:

De los siguientes controles relacionados a los riesgos de la seguridad física de sistemas informáticos ya sea por desastres naturales, fallas en el sistema o robo, señale cuáles son los controles aplicados en la entidad.

Tabla de resultados 16: Controles aplicados en la entidad

Opción	Frecuencia absoluta
Colocación de extintores	14 de 23
Sistema de aire acondicionado	14 de 23
Cámaras de vigilancia	19 de 23
Mantenimiento periódico de equipos	15 de 23
Ubicación adecuada y protección de equipos	10 de 23
Controles para ingreso de terceros	7 de 23



Análisis e interpretación:

Los datos obtenidos no representan el universo de la investigación debido a que se trata de pregunta de selección múltiple. El 82.61% utiliza las cámaras de video vigilancia como control en la seguridad física de las veterinarias, tratándose de un control correctivo, esto indica que no se establecen controles para la prevención de ataques.

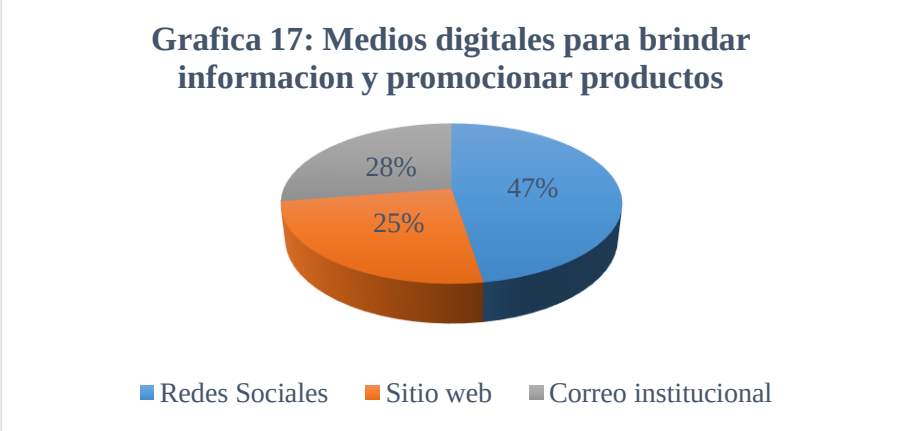
Pregunta 17:

¿Cuáles de los siguientes medios digitales utiliza la entidad para brindar información y promocionar sus productos o servicios?

Objetivo: Determinar si la entidad aplica los controles necesarios y adecuados con los medios digitales que utiliza para brindar información a sus clientes y proveedores y promociona sus productos o servicios.

Tabla de resultados 17: Medios digitales para brindar información y promocionar productos

Opción	Medios digitales para brindar información y promocionar productos
Redes Sociales	19 de 23
Sitio web	10 de 23
Correo institucional	11 de 23



Análisis e interpretación:

De los resultados obtenidos, 47% utiliza las redes sociales para promocionar y brindar información de sus productos y servicios. Las redes sociales deben utilizarse principalmente para promoción y el acercamiento con el cliente, mientras que los sitios web y correos institucionales pueden representar mejor a la veterinaria, pues estos medios añaden mayor confianza al cliente sobre el resguardo de su información.

Pregunta 18:

¿Considera que la implementación de un SGSI será de utilidad para mejorar los procesos de seguridad informática y ciberseguridad de los hospitales y clínicas veterinarias?

Objetivo: Comprobar la utilidad de la implementación de un sistema de gestión de la seguridad de la información en las clínicas veterinarias.

Tabla de resultados 18: Utilidad del SGSI

Opción	Frecuencia absoluta	Frecuencia relativa
Si	22	96%
No	1	4%
Total	**23**	**100%**

Análisis e interpretación:

El 96% de los contadores de las veterinarias consideran que la implementación de un SGSI seria de utilidad para el manejo de la información dentro de la entidad. Esto indica la importancia que las veterinarias le dan al manejo adecuado de la información para evitar la materialización de riesgos.