UNIVERSIDAD DON BOSCO
VICERRECTORÍA ACADÉMICA
FACULTAD DE INGENIERÍA

TRABAJO DE GRADUACIÓN PARA OPTAR AL GRADO DE

Maestro(a) en Seguridad y Gestión de Riesgos Informáticos

PROYECTO

Guía de buenas prácticas de seguridad informática para empresas del sector comercio de El Salvador, caso Practico INDOMED.

PRESENTADO POR

OSCAR JOSUE GUARDADO FLORES

ASESOR

IVAN ORLANDO ALVARADO NIÑO

Antiguo Cuscatlán, La Libertad, El Salvador, Centro América

Junio 2023

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

RESUMEN

Desde hace algunos años, muchas empresas han comenzado a implementar un proceso de transformación digital, que entre otras cosas requiere del uso de nuevas tecnologías y almacenamiento de la información en la nube y en diferentes dispositivos electrónicos.

Y aunque esto, sin duda, trae muchas ventajas, también genera más exposición a riesgos cibernéticos, por eso cada vez es más importante contar con un sistema de gestión de seguridad de la información basado en la norma ISO 27001 para proteger los datos y prevenir las consecuencias que traería la materialización de un riesgo de este tipo.

En general, esta norma ofrece herramientas que permiten asegurar, integrar y tener de manera confidencial toda la información de la compañía y los sistemas que la almacenan, evitando así que un ciberataque se materialice y así mismo, hacer más competitiva a la empresa y cuidar su reputación.

En esta investigación, se realizó una guía de buenas prácticas de seguridad informática, analizando e implementando la ISO 27001. Para ello se elabora un documento que contiene los aspectos más importantes al momento de ejecutarla en una empresa.

INTRODUCCIÓN

La empresa INDOMED es una empresa que se dedica a la compra y venta de insumos médicos su nombre surge, de la unión de las primeras letras de las palabras innovaciones médicas. Desde su inicio la empresa a contando con equipo informático y su respectiva área de informática. Sin embargo la mayoría de los empleados solo posee los conocimientos básicos en informática.

Esta investigación se realizó con el fin de brindarle a la empresa una guía de buenas prácticas informáticas, para transmitirles conocimientos a los empleados sobre cómo utilizar y cuidar sus equipos informáticos, y como protegerse ante amenazas informáticas.

El área de informática de la empresa solo cuenta con una persona y está a cargo de cubrir todas las funciones relacionadas con la informática, como soporte técnico, administración de los servidores, configuración de redes, entre otros. Un objetivo de la guía de buenas prácticas informáticas es brindarle apoyo al empleado del área de informática, ya que esta le brindara conocimientos informáticos a los empleados, de esta forma poder disminuir, problemas informáticos, como computadoras lentas, problemas con Office, computadoras sin internet, y olvido de contraseñas.

Se desarrolló la guía de buenas prácticas informáticas, tomando como base los controles de la ISO 27001 Anexo A y los listados de vulnerabilidades y amenazas del hardware, software, red, personal, local y organización, de la ISO 27005 Anexo D.

Se desarrollaron entrevistas con el empleado del área de informática y con el jefe de administración, para conocer cuáles eran los problemas informáticos que con los que cuenta la empresa. De esta forma poder hacer una guía de buenas prácticas más cercana a solucionar la problemática que tiene la empresa.

1. CAPÍTULO 1

1.1. Planteamiento del problema

La empresa INDOMED desde su inicio ha contado con equipo informático de calidad, sin embargo ha descuidado el eslabón más débil de la cadena de seguridad “Las personas que administran los equipos”. Si bien la empresa cuenta con su respectiva área de informática, esta solo tiene a una persona que cubre todas funciones relacionadas con el área.

Durante todos estos años la empresa ha trabajado por ser parte de la solución a las necesidades de los pacientes y los cirujanos de las diferentes especialidades y por crear lazos de amistades con los diferentes usuarios de los productos y hacer de la empresa una gran familia. Es evidente que el equipo informático de la empresa y su información comprende un conjunto de elementos significativamente importantes que los 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.

La norma ISO 27001 permite, regular, gestionar y mitigar al máximo los riesgos a los que está expuesto el departamento de TI tales como incidentes de seguridad, pérdida de información, disponibilidad de servicios entre otros. A la vez se ha encontrado un mecanismo de control que permita al administrador de seguridad establecer una estructura completamente centralizada la cual le permite visualizar y analizar los eventos relevantes que ocurren en una infraestructura de TI.

1.1.1. Formulación del problema

El estudiante de investigación plantea la siguiente interrogante

¿Cómo puede la empresa INDOMED poseer empleados con los conocimientos para utilizar correctamente su equipo informático y proteger su información, a su vez tomando como base la ISO 27001 Anexo A y ISO 27005 Anexo D?

1.2. OBJETIVOS

1.2.1. OBJETIVO GENERAL

Elaborar una guía de buenas prácticas de seguridad informática para empresas del sector comercio de El Salvador, caso práctico INDOMED, tomando como base la ISO 27001 Anexo A y la ISO 27005 Anexo D.

1.2.2. OBJETIVOS ESPECÍFICOS

- Documentar las estrategias en relacionadas con las buenas practicas informáticas.
- Hacer un diagnóstico de vulnerabilidades y brechas de seguridad en la empresa caso de estudio INDOMED.
- Clasificar y proponer buenas prácticas que reduzcan las brechas de seguridad y vulnerabilidades.

1.3. ALCANCE

La empresa INDOMED, pueda realizar buenas prácticas informáticas a sus equipos informáticos y poder proteger su tecnología e información, mediante una guía de buenas prácticas de seguridad informática. La cual cumple con la norma ISO 27001. Así mismo identificar las vulnerabilidades tecnológicas que cuenta la empresa y como mitigarlas con la guía. También para que la empresa reduzcan las brechas de seguridad y vulnerabilidades informáticas.

1.4. LIMITACIONES

- La empresa solo cuenta con una persona en el área de informática.

- La mayoría de los empleados de la empresa solo tienen los conocimientos básicos de informática.

- Escasez de profesionales expertos en informática en la empresa INDOMED.

- No cuentan con un plan de respaldo en caso que se dañe o deteriore los recursos tecnológicos.

1.5. DELIMITACIONES

Evidencias los beneficios de realizar prácticas de seguridad informática, en los distintos ámbitos en los que estas pueden ser aplicadas de manera eficaz.

La presente investigación se delimita a un enfoque cualitativo de tipo descriptivo la cual no abarca el planteamiento de escenarios, ni implementaciones y pruebas de campo por parte del equipo de investigación.

CAPÍTULO 2

2.1. MARCO REFERENCIAL

2.1.1. Antecedentes de seguridad informática

La Seguridad Informática ha experimentado un profundo cambio en los últimos años. Inversiones aisladas llevadas a cabo con el objetivo de fortalecer la seguridad en puntos muy concretos han dado paso a inversiones para asegurar el bien más valioso de la empresa, la información, enfocando la seguridad hacia los procesos de negocio de la empresa.

Durante los años 80 y principios de los 90 la Seguridad Informática se centraba en proteger los equipos de los usuarios, es decir, proporcionar seguridad a los ordenadores y su sistema operativo. Esta seguridad lógica, entendida como la seguridad de los equipos informáticos para evitar que dejasen de funcionar correctamente, se centraba en la protección contra virus informáticos.

Con la aparición de Internet y su uso globalizado a nivel empresarial la Seguridad Informática comenzó a enfocarse hacia la conectividad de redes o networking, protegiendo los equipos servidores de aplicaciones informáticas, y los equipos servidores accesibles públicamente a través de Internet, y controlando la seguridad a nivel periférico a través de dispositivos como Firewalls. Es decir, la posibilidad tecnológica de “estar conectados” llevaba implícita la aparición de nuevas vulnerabilidades que podían ser explotadas, la exposición de información crucial para el negocio que podía ser accesible precisamente gracias a esa conectividad.

El perfil de atacante de un sistema informático ha cambiado radicalmente. Si bien antes los objetivos de un atacante o hacker podían ser más simples (acceder a un sitio donde nadie antes había conseguido llegar, o infectar un sistema mediante algún tipo de virus, pero sin ningún tipo de ánimo de lucro), en la actualidad los atacantes se han percatado de lo importante que es la información y sobre todo de lo valiosa que puede ser. Se trata de grupos organizados que aprovechan las vulnerabilidades de los sistemas informáticos y las redes de telecomunicaciones para acceder a la información crítica y sensible de la

empresa, bien a través de personal especializado en este tipo de ataques, o bien comprando en el mercado negro kits de explotación de vulnerabilidades para obtener información muy específica.

2.1.2. Antecedentes de la ISO 27001

Hace algunos años no existía la tendencia de certificar procesos, o sistemas de gestión, por ello, ISO 9000 vino a redefinir en el año 2000 la certificación de los sistemas de gestión de calidad, mediante la norma ISO 9001:2000.

Pero aún en el 2005, no existía una norma ISO que permitiera certificar, por alguna organización en cuanto a sus prácticas de seguridad informática y las alternativas, en esos momentos se certificaba en normas inglesas (BS) o españolas (UNE).

Hasta 2005, el estándar más conocido en el entorno de seguridad informática era el ISO 17799, pero con la limitación de ser un “código de prácticas” (Information technology Security techniques Code of practice for information security management), en el momento que se publica su última revisión, se anuncia el desarrollo de una serie de estándares ISO 27000, dedicada exclusivamente a la seguridad informática. Con esto se le da un nuevo alcance a la seguridad, porque no sólo es llevar un código de mejores prácticas sino establecer un estándar certificable de forma similar al ISO 9000 (el primero de esa serie en publicarse fue el ISO 27001). (Logisman, 2011)

Las certificaciones han pasado a ser necesidad para demostrar la existencia de sistemas de gestión, con objeto de asegurar procesos consistentes. En el campo de la seguridad informática se tenían certificaciones por parte de estándares británicos y españoles pero, hace pocos años, la ISO emitió los estándares por los sistemas de gestión de seguridad informática con objeto de certificar que las recomendaciones y buenas prácticas brinden una ventaja competitiva a las organizaciones, y no dejar descubiertos todos los sistemas de información que día con día cobran una mayor importancia para sustentar la toma de decisiones y salvaguardar el activo más importante de una organización: la información.

2.1.3. Antecedentes de la empresa INDOMED

La empresa pertenece al rubro de comercio, se dedica a la compra y venta de materiales médicos y hospitalarios.

La sociedad fue constituida el 19 de Noviembre de 1999 con capital 100% salvadoreño y la idea de formar una compañía innovadora, con productos de alta tecnología y enfocada al servicio de sus clientes.

Desde su comienzo la empresa conto con equipo informático y su respectiva área de informática. La empresa solo usa el programa office, para documentar las compras y ventas de los insumos médicos usa Word y para realizar el inventario de los insumos los guarda en Excel.

Inicia sus operaciones en el año 2000 con dos empleados: una vendedora y una Técnico Instrumentista. La oficina estaba ubicada en el Edificio Plaza Médica. Inicialmente se estaba negociando la distribución de Biomet y por cuestiones del destino, se presentan los distribuidores de Zimmer y se decide cambiar.

Rápidamente fuimos adicionando clavos bloqueados, prótesis de hombro, placas y tornillos, placas peri articulares y los productos nuevos que Zimmer va desarrollando.

En al año 2001 la empresa adquirió la distribución exclusiva de la Marca Linvatec de USA, vendiendo productos para cirugías de artroscopia y equipos de artroscopia, sistema de corte para ortopedia y neurocirugía.

En el año 2005 a fin de incrementar ventas e introducir nuevas líneas, la empresa realizo alianza con la empresa 3M y nos convertimos en distribuidores de producto de inmovilización para pacientes: huata, fibra de vidrio, stockinete, vendas, apósitos, etc.

En el año 2006 con el fin de diversificar las líneas, se invirtió en la línea de cateterismo marca Terumo.

Para continuar con la innovación y diversificación, en el año 2009 se decide invertir en la línea de columna, con productos de Marca Zimmer Spine y una línea nueva de productos para cirugía artroscópica más innovadora, la marca Arthrex.

En el año 2010 la empresa compro e instalo dos servidores locales, uno con base de datos del ERP y otro para guardar archivos de office como Word y Excel. Actualmente se siguen usando y funcionando.

A partir del año 2012 inicia con el proceso de innovación en la línea de maxilofacial, incluyendo en el portafolio pines y mallas biodegradables. Amplía la gama de placas y tornillos de titanio para cirugías de maxilofacial, cirugías de mano de la línea de KLS Martín de Alemania.

2.2. BASES TEORICAS

2.2.1. ¿Qué es la ISO 27001?

La ISO 27001:2013 es la norma internacional que proporciona un marco de trabajo para los sistemas de gestión de seguridad de la información (SGSI) con el fin de proporcionar confidencialidad, integridad y disponibilidad continuada de la información, así como cumplimiento legal. La certificación ISO 27001 es esencial para proteger sus activos más importantes, la información de sus clientes y empleados, la imagen corporativa y otra información privada. La norma ISO incluye un enfoque basado en procesos para lanzar, implantar, operar y mantener un SGSI.

La implantación de la ISO 27001 es la respuesta ideal a los requisitos legislativos y de los clientes, y otras amenazas potenciales, incluyendo: Crimen cibernético, violación de los datos personales, vandalismo / terrorismo, fuego / daños, uso malintencionado, robo y ataque de virus.

2.2.2. El alcance de la norma ISO 27001 en esta investigación

El anexo A de la ISO 27001 proporciona un catálogo de 114 controles (medidas de seguridad) distribuidos en 14 secciones, con secciones de A.5 a A.18

También las secciones se dividen en dos grupos

- Los controles vinculados a la organización
- Los controles no vinculados a la organización

Para desarrollar la guía de buenas prácticas informáticas se descartaran los controles no vinculados a la organización, también solo se utilizaran una serie de controles que se adapten a la empresa INDOMED.

A continuación se muestran los controles de la ISO 27001 Anexo A que se utilizaran para desarrollar la guía buenas prácticas informáticas:
A.5.1.1 Políticas para la seguridad de la información
A.5.1.2 Revisión de las políticas para la seguridad de la información
A.8.1.1 Inventario de activos
A.8.2.1 Clasificación de la información
A.12.3.1 Copia de seguridad de la información
A.12.6.1 Gestión de vulnerabilidades técnicas
A.12.6.2 Restricción en la instalación de software
A 12.7.1 Controles de auditoria de los sistemas de información

2.2.3. ¿Qué es la ISO 27005?

La ISO/IEC 27005 proporciona directrices para el establecimiento de un enfoque sistemático de Gestión de Riesgos de Seguridad de la Información el cual es necesario para identificar las necesidades organizacionales con respecto a los requisitos de Seguridad de la Información para crear un sistema eficaz de gestión de la seguridad de la información. Además, esta norma internacional es compatible con los conceptos de la ISO/IEC 27001 y está diseñada para ayudar a una implementación eficaz de la seguridad de la información basados en un enfoque de gestión del riesgo.

2.2.3. Principales características de la ISO 27001

- Un estándar internacional enfocado en mantener la seguridad de la información
- Ofrece un marco completo y bien estructurado para proteger la información
- Establece como identificar la información que debe ser protegida, a cuáles riesgos está expuesta y como tratar dichos riesgos.

- Propone la implementación del Sistema de Gestión de Seguridad de la Información (SGSI).

2.2.4. Controles de la ISO 27001

El anexo A de la ISO 27001 proporciona un catálogo de 114 controles (medidas de seguridad) distribuidos en 14 secciones, con secciones de A.5 a A.18

También las secciones se dividen en dos grupos

Los controles vinculados a la organización
Política de Seguridad de la Información. A5.
Organización de la Seguridad de la Información. A6.
Gestión de activos. A8.
Control de acceso. A9.
Criptografía. A10.
Seguridad de las operaciones. A12.
Seguridad de las comunicaciones. A13.
Adquisición, desarrollo y mantenimiento de sistemas. A14.
Gestión de incidentes de seguridad de la información. A16.
Aspectos de seguridad de la información de la gestión de la continuidad del negocio. A17.

Los controles no vinculados a la organización
Seguridad de los Recursos Humanos. A7**.**
Seguridad física y ambiental. A11.
Relaciones con proveedores. A15.
Cumplimiento. A18.

2.2.5. Listado de las principales vulnerabilidades y amenazas de la ISO 27005

La ISO 27005 del año 2019, Anexo D proporciona vulnerabilidades y amenazas del hardware, software, red, personal, local y organización.

A continuación se muestran seis tablas sobre las vulnerabilidades y amenazas del hardware, software, red, personal, local y organización, de la ISO 27005 Anexo D

Tabla 1 Listado de las vulnerabilidades y amenazas del hardware de la ISO 27005 Anexo D

Vulnerabilidades	Amenazas
Mantenimiento insuficiente/instalación defectuosa de medios de almacenamiento	Brecha en la capacidad de mantenimiento del sistema de información
Falta de esquemas periódicos de reemplazo	Destrucción de equipos o medios
Susceptibilidad a la humedad, polvo, suciedad	Polvo, corrosión, congelamiento
Sensibilidad a la radiación electromagnética	Radiación electromagnética
Controles de cambios de configuración ineficientes	Error en uso
Susceptibilidad a variaciones de voltaje	Perdida de suministro de energía
Susceptibilidad a variaciones de temperatura	Fenómeno meteorológico
Almacenamiento no protegido	Robo de medios o documentos
Falta de cuidado en la eliminación	
Copiado no controlado	

Tabla 2 Listado de las vulnerabilidades y amenazas de red o las comunicaciones

Vulnerabilidades	Amenazas
Falta de prueba de envío o recepción de un mensaje	Negación de acción
Líneas de comunicación desprotegidas	Escucha
Trafico sensible desprotegido	Falla en el equipo de telecomunicaciones
Pobre conjunto de cableado	Falsificación de derechos
Punto único de falla	Espionaje remoto
Falta de identificación y autenticación del remitente y el receptor	Saturación del sistema de información
Arquitectura de la red insegura	Uso no autorizado de equipos

Transferencia de contraseñas en claro	
Inadecuada gestión de red (resiliencia de ruteo)	
Conexiones de red pública sin protección	

Tabla 3 Listado de las vulnerabilidades y amenazas de la aplicación

Vulnerabilidades	Amenazas
Falta o insuficientes pruebas de software	Abuso de derechos
Fallas bien conocidas en el software	Corrupción de datos
No cerrar la sesión cuando se abandona la estación de trabajo	Error en uso
Eliminación o reutilización de medios de almacenamiento sin borrado apropiado	Falsificación de derechos
Carencia de pistas de auditoria	Procesamiento ilegal de datos
Incorrecta asignación de derechos de acceso	Mal funcionamiento del Software
Software ampliamente distribuido	Manipulación con software
Aplicación de programas de aplicación a datos erróneos en términos de tiempo	Robo de medios o documentos
Interface de usuario complicada	Uso no autorizado de equipos
Falta de documentación	
Establecer parámetros incorrectos	
Fechas incorrectas	
Falta de mecanismos de identificación y autenticación como autenticación de usuarios	
Tablas de contraseñas no protegidas	
Manejo pobre de contraseñas	
Habilitación de servicios innecesarios	
Software nuevo o inmaduro	
Especificaciones poco claras o incompletas para desarrolladores	
Control de cambio ineficiente	
Descarga y uso no controlado de software	
Falta de copias de respaldo	
Falta de protección física del edificio, puertas y ventanas	
Falla en la producción de reportes de gestión	

2.2.6. Listado de buenas prácticas de seguridad informática

El estudiante ha diseñado prácticas para protegerse de amenazas informáticas en la empresa, basada en sus conocimientos y experiencia. Prevenir es, sin duda, la mejor forma de evitar los ataques informáticos.

1. Antivirus actualizado

El antivirus es el primer freno frente a los ataques informáticos. Es prioritario tener instalado y actualizado un antivirus que rastree permanentemente en busca de amenazas.

2. Firewall

Un solo equipo desprotegido pone en riesgo la seguridad de toda la empresa. El firewall protege la red privada y cifra la información que se envía desde todos los dispositivos conectados a ella.

3. Protección wifi

La red wifi de la empresa se debe proteger ocultando la SSID y creando una red de invitados que identifiquen su dirección. Cuando se accede desde fuera de la oficina, conviene utilizar redes VPN o datos del móvil.

4. Software actualizado

Las actualizaciones del sistema operativo y del software incorporan parches de seguridad frente a nuevas amenazas.

5. Copias de seguridad al día

Las copias de seguridad pueden evitar más de un disgusto, no solo frente a amenazas informáticas, sino también frente a problemas técnicos.

6. Prevenir errores humanos

La imprudencia y el desconocimiento suelen ser las causas de los fallos de ciberseguridad en las empresas. Es más que recomendable disponer de una guía de buenas prácticas para evitar:

Instalar programas desconocidos.

Seguir enlaces sospechosos.

Desvelar información en redes sociales.
Conectar dispositivos sin analizar.
Permitir accesos no autorizados.
Pérdidas o robos de dispositivos.

7. Cambiar las contraseñas predeterminadas y ajustar la configuración de seguridad para satisfacer las necesidades específicas.

8. Desactivar o deshabilitar cualquier función que no se necesite.

9. Para los dispositivos capaces de utilizar aplicaciones de terceros, utilizar únicamente aplicaciones legítimas de proveedores válidos.

10. Actualizar el firmware y las aplicaciones del dispositivo para que éste esté protegido contra vulnerabilidades de seguridad conocidas.

11. En términos de configuración de aplicaciones en dispositivos, revisar los permisos que requieren y limitar el acceso otorgado a estas apps.

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.

2.3.1. Ley de creación del sistema salvadoreño para la calidad

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.

2.3.2. Ley especial contra delitos informáticos y conexos

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)

2.3.3. Ley de firma electrónica

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.

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.

3. CAPÍTULO 3

3.1. Metodología de la investigación

3.1.1. Tipo de Investigación

Debido al tema y su aplicación, la investigación se clasifica a partir de varios criterios y autores como (Sampieri, 2000) establece dos enfoques: cualitativo y cualitativo, la presente investigación se corresponde con un enfoque cuantitativo, porque presenta un conjunto de procesos. La presente investigación se clasifica como tipo descriptiva por su alcance de evidenciar los aspectos mínimos y condiciones que deben tomarse en cuenta a evaluar, abordando documentación bibliográfica utilizándola para la redacción del mismo.

3.1.2. Procedimiento

El desarrollo de la guía metodológica tendrá como base en documentación técnica y artículos, así como referencias a buenas prácticas de la seguridad de la información y sus propiedades.

Se desarrollarán cuadros exponiendo y explicando las variables, las unidades de análisis y el respectivo instrumento que se implementara para la obtención de la información en la investigación.

Primer objetivo específico: Documentar las estrategias en relacionadas con las buenas practicas informáticas.

Para la recolección de información que dará respuesta a este objetivo se utilizaran los siguientes instrumentos:

Tabla 4 Instrumentos del Análisis primer objetivo específico

No	Unidades de análisis	Técnica de análisis	Instrumento
01	Seguridad informática	Análisis de contenido	Tabla de estrategias de seguridad informática. Ver Anexo 1
02	Buenas prácticas de informáticas	Análisis de contenido	Tabla de buenas prácticas informáticas. Ver Anexo 2

Segundo objetivo específico: Hacer un diagnóstico de vulnerabilidades y brechas de seguridad en la empresa caso de estudio INDOMED.

Para la recolección de información que dará respuesta a este objetivo se utilizaran los siguientes instrumentos:

Tabla 5 Instrumentos de Análisis Segundo objetivo específico

No	Unidades de análisis	Técnica de análisis	Instrumento
01	Jefe de informática de la empresa.	Revisión documental	Tabla de vulnerabilidades informáticas. Ver Anexo 3.
02	Jefe de Administración	Revisión documental	Tabla de brecha de seguridad informática. Ver Anexo 4.

Tercer objetivo específico: Clasificar y proponer buenas prácticas que reduzcan las brechas de seguridad y vulnerabilidades.

Para la recolección de información que dará respuesta a este objetivo se utilizaran los siguientes instrumentos:

Tabla 6 Instrumentos de Análisis Tercer objetivo específico

No	Unidades de análisis	Técnica de análisis	Instrumento
01	Documentación de la ISO 27001.	Análisis de contenido	Tabla de los controles de seguridad informática a implementar. Ver Anexo 5.
02	Documentación de la ISO 27005.	Análisis de contenido	Tabla de las vulnerabilidades y amenazas informática analizadas. Ver Anexo 6

4. CAPÍTULO 4

4.1. ANALISIS E INTERPRETACION DE RESULTADOS

A continuación se presentaran los resultados obtenidos del capítulo tres, utilizando los respectivos instrumentos de los tres objetivos específicos.

Para el primer objetivo específico y el tercer objetivo específico, se utilizaron tablas que muestran los componentes que constituyen los instrumentos, también se brinda su respectivas descripciones y explicaciones de cada uno de los componentes.

Para el objetivo específico número dos, se realizó entrevistas con el fin de recopilar información de cómo esta implementada la informática en la empresa. Se realizaron dos entrevistas, la primera entrevista se realizó al jefe de informática, para detectar como está estructurada la informática en la empresa y que recomienda para disminuir la brecha de seguridad, la segunda entrevista se le realizo al jefe de administración, con el fin conocer los problemas informáticos que enfrentan los empleados que no conocen de informática y como los solucionan. En la entrevista nos comentaba los únicos programas que usan son el Word para realizar toda su documentación como compra y venta, y Excel para gestionar el inventario de los insumos médicos que compran y venden, en sus problemas informáticos más comunes me comentaba, que eran computadoras lentas, que los usuarios olvidan las contraseñas de las computadoras o problemas en Word. A su vez se desarrolló su respectivo análisis.

4.1.1. ESTRATEGIAS EN RELACIÓN A LA BUENAS PRÁCTICAS INFORMATICAS.

Primer objetivo específico: Documentar las estrategias en relacionadas con las buenas practicas informáticas.

Tabla 7 de estrategias de seguridad informática.

Tabla de estrategias de seguridad informática.	
Nombre de la estrategia informática	Descripción
Controles de acceso a los datos más estrictos	Una de las principales medidas de seguridad es limitar el acceso a la información. Cuantas menos personas accedan a una información, menor será el riesgo de comprometerla. Por lo tanto, es necesario implantar en nuestra empresa un sistema que impida dar acceso a datos innecesarios, a un usuario, cliente, etc.
Copias de seguridad del correo electrónico	Poseer un sistema de copias de seguridad periódico permite que la empresa garantice que puede recuperar los datos ante una incidencia de carácter catastrófico, impidiendo la pérdida de los mismos y permitiendo la recuperación de la normalidad en el trabajo en apenas unos minutos.
Contratar un software de contraseñas seguras	El acceso a las distintas plataformas que utiliza la empresa (correo electrónico, servidor de copias de seguridad NAS, etc.) debe realizarse utilizando claves de seguridad (contraseñas) seguras, que impidan que puedan ser fácilmente descubiertas por piratas informáticos. El uso de contraseñas seguras es una de las medidas de seguridad informática más importantes en una empresa.
Proteger el correo electrónico	Hoy en día, la mayoría de comunicaciones de nuestra empresa la realizamos utilizando el correo electrónico. Por lo tanto, otra medida de seguridad es utilizar filtros anti spam y sistemas de encriptado de mensajes, para asegurar la protección y privacidad de toda esa información.
Contratar un software integral de seguridad	La mejor forma es contratando un paquete de seguridad integral que contenga antivirus, anti espías, antimalware, firewall, etc., y que permita proteger la información ante posibles ataques externos a través de internet.
Utilizar software DLP	Existen programas de prevención de pérdidas de datos (DLP) que pueden ser

	implementados como medida de seguridad en nuestra empresa para supervisar que ningún usuario esté copiando o compartiendo información o datos que no deberían.
Trabajar en la nube	Trabajar en la nube permite, entre otras ventajas, contar con los sistemas de seguridad de la información que posee el proveedor de servicios. Además, este proveedor será responsable de esa seguridad.
Involucrar a toda la empresa en la seguridad	Para que las medidas de seguridad informática de una empresa funcione, debemos involucrar en su participación a todos los estamentos que participan en la misma, incluyendo a los agentes externos como puedan ser clientes, proveedores, etc. Muchas veces, nuestra empresa tiene implantados los sistemas correctos de seguridad, y la brecha en la misma, se produce al relacionarnos con un tercero que carece de estas medidas de seguridad.
Monitorización continua y respuesta inmediata	Debemos implantar en nuestra empresa un sistema que permita monitorizar la gestión de los datos y detectar aquellos posibles fallos o actuaciones incorrectas. Este sistema de control permitirá actuar rápidamente para solventar cualquier incidencia y minimizar su repercusión.

Tabla 8 de buenas prácticas informáticas.

Tabla de buenas prácticas informáticas	
Nombre	**Descripción**
Antivirus actualizado	El antivirus es el primer freno frente a los ataques informáticos. Es prioritario tener instalado y actualizado un antivirus que rastree permanentemente en busca de amenazas.
Firewall	Un solo equipo desprotegido pone en riesgo la seguridad de toda la empresa. El firewall protege la red privada y cifra la información que se envía desde todos los dispositivos conectados a ella.
Protección wifi	La red wifi de la empresa se debe proteger ocultando la SSID y creando una red de invitados que identifiquen su dirección. Cuando se accede desde fuera de la oficina, conviene utilizar redes VPN o datos del móvil.

Software actualizado	Las actualizaciones del sistema operativo y del software incorporan parches de seguridad frente a nuevas amenazas.
Copias de seguridad al día	Las copias de seguridad pueden evitar más de un disgusto, no solo frente a amenazas informáticas, sino también frente a problemas técnicos.
Prevenir errores humanos	La imprudencia y el desconocimiento suelen ser las causas de los fallos de ciberseguridad en las empresas. Es más que recomendable disponer de una guía de buenas prácticas para evitar: Instalar programas desconocidos. Seguir enlaces sospechosos. Desvelar información en redes sociales.
Cambiar las contraseñas periódicamente	Cambiar las contraseñas predeterminadas y ajustar la configuración de seguridad para satisfacer las necesidades específicas.
Gestionar las funciones	Desactivar o deshabilitar cualquier función que no se necesite.
Gestionar las aplicaciones	Para los dispositivos capaces de utilizar aplicaciones de terceros, utilizar únicamente aplicaciones legítimas de proveedores válidos.
Realizar actualizaciones del dispositivo	Actualizar el firmware y las aplicaciones del dispositivo para que éste esté protegido contra vulnerabilidades de seguridad conocidas.
Revisar los permisos de los dispositivos	En términos de configuración de aplicaciones en dispositivos, revisar los permisos que requieren y limitar el acceso otorgado a estas apps.

Uno de los mayores riesgos que cuentan las empresas, es mantener los datos, ya sean públicos o privados, de acceso restringido o de acceso libre, seguros. Para ello, las empresas se enfrentan a retos cada día desconocidos, pues el descubrimiento de vulnerabilidades es algo que hay que controlar de manera continua, ya que cada día se descubren nuevas que pueden afectar a nuestros sistemas.

La empresa tiene dos grandes responsabilidades, proteger su información y proteger sus activos informáticos, estos se cubren con la implementación de la seguridad informática, para garantizar la seguridad informática, se ha desarrollado una lista de estrategias de seguridad informática:

- Controles de acceso a los datos más estrictos: es necesario implantar en nuestra empresa un sistema que impida dar acceso a datos innecesarios, a un usuario, cliente, etc.
- Copias de seguridad del correo electrónico: Gestionar los correos recibidos y enviados, de tal forma siempre quede copia de seguridad.
- Contratar un software de contraseñas seguras: El uso de contraseñas seguras es una de las medidas de seguridad informática más importantes en una empresa.
- Proteger el correo electrónico: utilizar filtros anti spam y sistemas de encriptado de mensajes, para asegurar la protección y privacidad de toda esa información.
- Contratar un software integral de seguridad: La mejor forma es contratando un paquete de seguridad integral que contenga antivirus, anti espías, antimalware, firewall, etc.,
- Utilizar software DLP: para supervisar que ningún usuario esté copiando o compartiendo información o datos que no deberían.
- Trabajar en la nube: Trabajar en la nube permite, entre otras ventajas, contar con los sistemas de seguridad de la información que posee el proveedor de servicios.
- Involucrar a toda la empresa en la seguridad: Para que las medidas de seguridad informática de una empresa funcione, debemos involucrar en su participación a todos los estamentos que participan en la misma, incluyendo a los agentes externos como puedan ser clientes, proveedores, etc.
- Monitorización continua y respuesta inmediata: El sistema de control permitirá actuar rápidamente para solventar cualquier incidencia y minimizar su repercusión.

Para reducir el riesgo de exposición a vulnerabilidades, se pueden llevar a cabo buenas prácticas con el fin de evitar que la compañía sufra un ciberataque, o que una vulnerabilidad en nuestro sistema sea explotada.

El factor humano juega un papel decisivo, ya que, si el usuario no tiene una cultura de ciberseguridad al usar un sistema, este puede ser el desencadenante de un ciberataque en toda la compañía, y, por lo tanto, que los datos sean comprometidos. Por dicho motivo se ha desarrollado un listado de buenas prácticas:

- Antivirus actualizado: El antivirus es una importante herramienta a la hora de proteger la computadora y su información, sin embargo las amenazas informáticas van evolucionado, lo que genera la necesidad de actualizar el antivirus, cabe mencionar que es necesario tener el antivirus en su última versión.
- Firewall: El firewall protege la red privada y cifra la información que se envía desde todos los dispositivos conectados a ella.
- Protección wifi: La red wifi de la empresa se debe proteger ocultando la SSID y creando una red de invitados que identifiquen su dirección.
- Software actualizado: Las actualizaciones del sistema operativo y del software incorporan parches de seguridad frente a nuevas amenazas.
- Copias de seguridad al día: Las copias de seguridad pueden evitar más de un disgusto, no solo frente a amenazas informáticas, sino también frente a problemas técnicos.
- Prevenir errores humanos: La imprudencia y el desconocimiento suelen ser las causas de los fallos de ciberseguridad en las empresas. Es más que recomendable disponer de una guía de buenas prácticas para evitar: Instalar programas desconocidos, Seguir enlaces sospechosos, Desvelar información en redes sociales.
- Cambiar las contraseñas periódicamente: Cambiar las contraseñas predeterminadas y ajustar la configuración de seguridad para satisfacer las necesidades específicas.
- Gestionar las funciones: Desactivar o deshabilitar cualquier función que no se necesite.

- Gestionar las aplicaciones: Para los dispositivos capaces de utilizar aplicaciones de terceros, utilizar únicamente aplicaciones legítimas de proveedores válidos.
- Realizar actualizaciones del dispositivo: Se tienen que revisar todos los dispositivos con los que cuenta la empresa, a su vez para una mejor protección y un uso óptimo, es necesario tener los dispositivos actualizados.
- Revisar los permisos de los dispositivos: Cualquier amenaza puede aprovechar cualquier oportunidad para acceder a nuestros dispositivos o información, por eso hay que revisar y gestionar todos los permisos que brindamos y limitar o quitarlos si es necesario.

4.1.2. DIAGNOSTICO DE VULNERABILIDADES Y BRECHAS DE SEGURIDAD

Segundo objetivo específico: Hacer un diagnóstico de vulnerabilidades y brechas de seguridad en la empresa caso de estudio INDOMED.

Tabla 9 de vulnerabilidades informáticas en la empresa caso de estudio INDOMED.

Tabla de vulnerabilidades informáticas en la empresa.	
Nombre de la vulnerabilidad informática	Descripción
Ataques informáticos	Está relacionada con un uso incorrecto o negligente por parte de un usuario. Una mala asignación de privilegios o permisos puede hacer que un usuario tenga acceso a opciones de administración o configuración para las que no está preparado, cometiendo errores que suponen una amenaza para la empresa.
Riesgos en seguridad informática	El usuario siempre tiene el riesgo de cometer un error que pueda generar una vulnerabilidad que suponga una amenaza informática. Por eso en seguridad informática se tiende a automatizar procesos críticos para minimizar o eliminar el factor de riesgo del error humano.
Formación en seguridad informática	También generan vulnerabilidades, como la apertura de ficheros de dudosa procedencia, engaños por publicidad falsa, apertura de correos fraudulentos y similares. Estas acciones son una amenaza a sufrir ataques como el phishing (suplantación de identidad) o similares.
Vulnerabilidades del sistema	Los sistemas y aplicaciones informáticos siempre tienen algún error en su diseño, estructura o código que genera alguna vulnerabilidad. Por muy pequeño que sea ese error, siempre podrá generar una amenaza sobre los sistemas y la información**,** siendo la puerta de entrada para recibir ataques externos o internos.

Tabla 10 de brechas de seguridad informática.

Tabla de brechas de seguridad informática	
Nombre de la brecha de seguridad informática	Descripción
Un exploit	Ataca una vulnerabilidad del sistema, como un sistema operativo obsoleto. Los sistemas anteriores no actualizados, por ejemplo, las empresas en las que se utilizan versiones de Microsoft Windows antiguas o que han dejado de actualizarse, son especialmente vulnerables a este tipo de ataques.
Las contraseñas débiles	Pueden descifrarse o piratearse. Incluso en la actualidad hay quien utiliza como contraseña la palabra «contraseña», y conviene saber que utilizar «contra$eña» no es mucho más seguro.
Los ataques con malware	Como los correos electrónicos de phishing, pueden emplearse para penetrar en sistemas. Basta con que un empleado haga clic en un enlace de un mensaje de phishing para que el software malicioso empiece a propagarse por la red.
Las descargas ocultas	Utilizan virus o malware instalado a través de un sitio web fraudulento o infectado.
La ingeniería social	También puede utilizarse para penetrar en sistemas. Por ejemplo, un intruso puede telefonear a un empleado haciéndose pasar por un compañero del departamento de informática y solicitarle su contraseña para «arreglarle» el ordenador.

La dependencia de las empresas por las tecnologías de la información para realizar sus actividades principales de negocio ha generado una alta preocupación por la seguridad informatica.

Las vulnerabilidades y amenazas informáticas son un riesgo para los sistemas y la información de la empresa, sobre todo en el entorno actual, altamente digitalizado y dependiente de los servicios TI.

Para poder tomar las medidas adecuadas para proteger los recursos tecnológicos y la información de la empresa es necesario conocer cuáles son las principales amenazas y vulnerabilidades que ponen en riesgo la seguridad de la empresa en la red.

Vulnerabilidades informáticas:

- **Ataques informáticos:** Está relacionada con un uso incorrecto o negligente por parte de un usuario. Una mala asignación de privilegios o permisos puede hacer que un usuario tenga acceso a opciones de administración o configuración para las que no está preparado, cometiendo errores que suponen una amenaza para la empresa.

- **Riesgos en seguridad informática:** El usuario siempre tiene el riesgo de cometer un error que pueda generar una vulnerabilidad que suponga una amenaza informática. Por eso en seguridad informática se tiende a automatizar procesos críticos para minimizar o eliminar el factor de riesgo del error humano.

- **Formación en seguridad informática:** También generan vulnerabilidades, como la apertura de ficheros de dudosa procedencia, engaños por publicidad falsa, apertura de correos fraudulentos y similares. Estas acciones son una amenaza a sufrir ataques como el phishing (suplantación de identidad) o similares.

- **Vulnerabilidades del sistema:** Los sistemas y aplicaciones informáticos siempre tienen algún error en su diseño, estructura o código que genera alguna vulnerabilidad. Por muy pequeño que sea ese error, siempre podrá generar una amenaza sobre los sistemas y la información, siendo la puerta de entrada para recibir ataques externos o internos.

Brechas de seguridad informática:

- **Un exploit:** Ataca una vulnerabilidad del sistema, como un sistema operativo obsoleto. Los sistemas anteriores no actualizados, por ejemplo, las empresas en las que se utilizan versiones de Microsoft Windows antiguas o que han dejado de actualizarse, son especialmente vulnerables a este tipo de ataques.

- **Las contraseñas débiles:** Pueden descifrarse o piratearse. Incluso en la actualidad hay quien utiliza como contraseña la palabra «contraseña», y conviene saber que utilizar «contra$eña» no es mucho más seguro.

- **Los ataques con malware:** Como los correos electrónicos de phishing, pueden emplearse para penetrar en sistemas. Basta con que un empleado haga clic en un enlace de un mensaje de phishing para que el software malicioso empiece a propagarse por la red.

- **Las descargas ocultas:** Utilizan virus o malware instalado a través de un sitio web fraudulento o infectado.

- **La ingeniería social:** También puede utilizarse para penetrar en sistemas. Por ejemplo, un intruso puede telefonear a un empleado haciéndose pasar por un compañero del departamento de informática y solicitarle su contraseña para «arreglarle» el ordenador.

4.1.3. BUENAS PRÁCTICAS

Tercer objetivo específico: Clasificar y proponer buenas prácticas que reduzcan las brechas de seguridad y vulnerabilidades.

Tabla 11 de los controles de seguridad informática a implementar.

Tabla de los controles de seguridad informática a implementar.		
Numeración de la norma	**Nombre**	**Control**
A.5.1.1	Políticas para la seguridad de la información	Un conjunto de políticas de seguridad de la información debe ser definido y aprobado por la Dirección, publicarlo y comunicarlo a todos los empleados y entidades externas pertinentes.
A.5.1.2	Revisión de las políticas para la seguridad de la información	Las políticas para la seguridad de la información debe revisarse a períodos planificados o siempre que se produzcan cambios significativos, para asegurar que se mantenga su continuidad, idoneidad, adecuación y efectividad.
A.8.1.1	Inventario de activos	Activos asociados con información e instalaciones de procesamiento de la información deben ser identificados y un inventario de estos activos debe ser levantado y mantenido.
A.8.2.1	Clasificación de la información	La información debe ser clasificada en términos de su valor, requerimientos legales, sensibilidad y criticidad a modificaciones o divulgación no autorizada.
A.12.3.1	Copia de seguridad de la información	Se debe hacer copias de seguridad de la información, software e imágenes del sistema y probarlas periódicamente de acuerdo a la política de respaldo.
A.12.6.1	Gestión de vulnerabilidades técnicas	Se debe obtener información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información usados, evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para abordar el riesgo asociado.
A.12.6.2	Restricción en la instalación de software	Se deben establecer e implementar reglas que rijan la instalación de software por parte de los usuarios.
A 12.7.1	Controles de auditoria de los sistemas de información	Los requerimientos y actividades de auditoria que involucran los sistemas en producción deben ser cuidadosamente planificados y acordados para

		minimizar las interrupciones a los procesos de negocio.

Tabla 12 de las vulnerabilidades y amenazas informática analizadas de la ISO 27005.

Tabla de las vulnerabilidades y amenazas informática analizada ISO 27005.		
Tipo	**Vulnerabilidad**	**Amenaza**
Hardware	Mantenimiento insuficiente/instalación defectuosa de medios de almacenamiento	Brecha en la capacidad de mantenimiento del sistema de información
Hardware	Controles de cambios de configuración ineficientes	Destrucción de equipos o medios
Hardware	Copiado no controlado	Polvo, corrosión, congelamiento
Software	Software nuevo o inmaduro	Corrupción de datos
Software	Control de cambio ineficiente	Error en uso
Software	Falla en la producción de reportes de gestión	Mal funcionamiento del Software
Red	Líneas de comunicación desprotegidas	Negación de acción
Red	Trafico sensible desprotegido	Saturación del sistema de información
Red	Arquitectura de la red insegura	Uso no autorizado de equipos

Basados en la información proporcionada por la empresa, se realizaron listas de controles a implementar de la ISO 27001, también se realizó una tabla con las vulnerabilidades y amenazas, de hardware, software y red de la ISO 27005 relacionados con la empresa.

A continuación, se describe de manera más detallada los controles de la ISO 27001 que se implementaran, también las vulnerabilidades y amenazas de hardware, software y red, relacionados con la empresa.

Controles a implementar:

- A.5.1.1 Políticas para la seguridad de la información: La política de seguridad de información es el documento en el que una empresa define los lineamientos generales para proteger la información y minimizar los riesgos que pudieran afectarla.

- A.5.1.2 Revisión de las políticas para la seguridad de la información: Las políticas de la Seguridad de la información deben adaptarse continuamente a las necesidades y cambios de la organización por lo que no pueden permanecer estáticas. Se trata entonces de mantener actualizada la política de la seguridad de la información. Para ello es interesante tener en cuenta algunas recomendaciones

- A.8.1.1 Inventario de activos: Una parte importante de las empresas, son sus activos, y estos no están exentos de mala manipulación o mal uso, por dicho motivo. Es necesario realizar un inventario de activos.

- A.8.2.1 Clasificación de la información: El objetivo es la clasificación de la Información, e indica que a las organizaciones deben asegurarse de que la información reciba un nivel adecuado de protección.

- A.12.3.1 Copia de seguridad de la información: es un proceso mediante el cual se duplica la información existente de un soporte a otro, con el fin de poder recuperarlos en caso de fallo del primer alojamiento de los datos.

- A.12.6.1 Gestión de vulnerabilidades técnicas: Es la actividad en la que se buscan vulnerabilidades en redes y sistemas, mediante diferentes técnicas y aplicaciones especializadas, con el fin de identificarlas y subsanarlas para evitar que sean utilizadas por los ciberdelincuentes en su beneficio.

- A 12.7.1 Controles de auditoria de los sistemas de información: Es la rama que se encarga de llevar a cabo la evaluación de normas, controles, técnicas y procedimientos que se tienen establecidos en una empresa para lograr confiabilidad, oportunidad, seguridad y confidencialidad de la información que se procesa a través de los sistemas de información.

A continuación se describe las vulnerabilidades y amenazas del hardware, software y la red, de la ISO 27005 relacionados con la empresa:

Vulnerabilidades y amenazas de hardware

Vulnerabilidades de hardware

- Mantenimiento insuficiente/instalación defectuosa de medios de almacenamiento: Se tiene que revisar el hardware y el software de los equipos informáticos, ya sé que cuenten con un buen software pero el hardware no sea el indicado o viceversa.
- Controles de cambios de configuración ineficientes: No se tienen controles adecuados para realizar cambios en la configuración de los programas que cuenta la empresa.
- Copiado no controlado: Las copias de seguridad, son una parte importante para las empresas, sin embargo no solo es su realización, sino también cuando realizarla y que copiar.

Amenazas de hardware

- Brecha en la capacidad de mantenimiento del sistema de información: Se tiene que brindar mantenimiento al sistema de información, porque ningún sistema esta exceptuó de desperfecto, mal uso, o datos corrompidos.
- Destrucción de equipos o medios: Tanto en el hogar como en el trabajo la gran mayoría de las personas poseen más de un dispositivo tecnológico (TIC). Debido a los avances tecnológicos, los ciclos de vida de los teléfonos, ordenadores se han visto reducido por lo que los usuarios reemplazan sus equipos informáticos y dispositivos a un ritmo mucho más rápido. Todo esto hace incrementar la cantidad de residuos electrónicos a nivel mundial.
- Polvo, corrosión, congelamiento: La empresa pueda medir el riesgo de falla del equipo, realizando una revisión de equipo periódicamente.

Vulnerabilidades y amenazas de software

Vulnerabilidades de software:

- Software nuevo o inmaduro: Muchos problemas informáticos, se presentan por software obsoletos, que presentan problemas o no son compatibles con la tecnología actual.

- Control de cambio ineficiente: No se tiene un control eficiente a la hora de evaluar el equipo informático o de comprar, lo que genera que se trabaje con equipos obsoletos o que el equipo no sea el adecuado.
- Falla en la producción de reportes de gestión: Los programas que generan reportes presenten fallas, por culpa del hardware o del software.

Amenazas de software:

- Corrupción de datos: se refiere a los errores en los datos informáticos que se producen durante la transmisión o la recuperación, la introducción de cambios no deseados a los datos originales.
- Error en uso: es un problema en un programa de computador o sistema de software que desencadena un resultado indeseado.
- Mal funcionamiento del Software: es un problema en un programa de computador o sistema de software que desencadena un resultado indeseado.

Vulnerabilidades y amenazas de la red:

Vulnerabilidades de la red:

- Líneas de comunicación desprotegidas: Intervenir una infraestructura de comunicación como redes de telefonía fija, móvil e internet, requiere modificar o alterar físicamente su funcionamiento con el fin de interceptar y/o manipular el contenido que viaja en ella.
- Trafico sensible desprotegido: No contar con una solución de seguridad de endpoint implica tener un eslabón clave de su empresa completamente desprotegido. Por esta razón, es importante que identifique los elementos que hacen de la ciberseguridad un aspecto indispensable.
- Arquitectura de la red insegura: Una red mal configurada es un punto de entrada primario para usuarios no autorizados. Al dejar una red local abierta, confiable, vulnerable a la Internet que es altamente insegura, es casi como que dejar una puerta abierta en un vecindario con alta criminalidad

Amenazas de la red:

- Negación de acción: Los privilegios los usuarios es un punto importante para las empresas, se tienen que revisar los privilegios para evitar personas equivocadas accedan al sistema o en su defecto que no le niegue la acción a un usuario establecido.
- Saturación del sistema de información: Todo tiene un límite, se tiene que estar revisando periódicamente los recursos informáticos, para determinar si tienen espacio disponible.
- Uso no autorizado de equipos: Si no se tiene un correcto control, del lugar, personas sin autorización pueden utilizar los equipos informáticos.

5. CAPÍTULO 5

5.1. PROPUESTA DE USO

La guía de buenas prácticas de seguridad informática para la empresa INDOMED, se constituye de dos normas, La primera norma que se uso es la ISO 27001, para identificar controles de seguridad informática a implementar. La segunda norma que se uso es la ISO 27005, para detectar las vulnerabilidades y amenazas informáticas relacionadas con la empresa.

Las vulnerabilidades y amenazas de ISO 27005, relacionadas con la empresa INDOMED, son los siguientes:

Vulnerabilidades de hardware

- Mantenimiento insuficiente/instalación defectuosa de medios de almacenamiento
- Controles de cambios de configuración ineficientes
- Copiado no controlado

Amenazas de hardware

- Brecha en la capacidad de mantenimiento del sistema de información
- Destrucción de equipos o medios
- Polvo, corrosión, congelamiento

Vulnerabilidades y amenazas de software

Vulnerabilidades de software:

- Software nuevo o inmaduro
- Control de cambio ineficiente
- Falla en la producción de reportes de gestión

Amenazas de software:

- Corrupción de datos
- Error en uso
- Mal funcionamiento del Software

Vulnerabilidades y amenazas de la red:

Vulnerabilidades de la red:

- Líneas de comunicación desprotegidas
- Trafico sensible desprotegido
- Arquitectura de la red insegura

Amenazas de la red:

- Negación de acción
- Saturación del sistema de información
- Uso no autorizado de equipos

Los controles de la ISO 27001 a implementar para mitigar las vulnerabilidades y amenazas, son los siguientes:

A.5.1.1 Políticas para la seguridad de la información

A.5.1.2 Revisión de las políticas para la seguridad de la información

A.8.1.1 Inventario de activos

A.8.2.1 Clasificación de la información

A.12.3.1 Copia de seguridad de la información

A.12.6.1 Gestión de vulnerabilidades técnicas

A.12.6.2 Restricción en la instalación de software

A 12.7.1 Controles de auditoria de los sistemas de información

Guía de buenas prácticas de seguridad informática.

1. Establecer políticas de seguridad.

Deben estar orientadas a proteger la información y los activos de la compañía. Entre las medidas que se pueden tomar se encuentran: política de contraseñas segura y actualizada, protección de datos o limitación de acceso a la información. Este paso se simplifica enormemente si has realizado la Auditoría GAP Análisis que indicábamos en el paso anterior.

2. Firewall

Un solo equipo desprotegido pone en riesgo la seguridad de toda la empresa. El firewall protege la red privada y cifra la información que se envía desde todos los dispositivos conectados a ella.

3. Software actualizado

Las actualizaciones del sistema operativo y del software incorporan parches de seguridad frente a nuevas amenazas.

4. Copias de seguridad al día

Las copias de seguridad pueden evitar más de un disgusto, no solo frente a amenazas informáticas, sino también frente a problemas técnicos.

5. Prevenir errores humanos

La imprudencia y el desconocimiento suelen ser las causas de los fallos de ciberseguridad en las empresas. Es más que recomendable disponer de una guía de buenas prácticas para evitar:

Instalar programas desconocidos.

Seguir enlaces sospechosos.

Desvelar información en redes sociales.

Conectar dispositivos sin analizar.

Permitir accesos no autorizados.

Pérdidas o robos de dispositivos.

6. Cambiar las contraseñas predeterminadas y ajustar la configuración de seguridad para satisfacer las necesidades específicas.

7. Desactivar o deshabilitar cualquier función que no se necesite.

8. Para los dispositivos capaces de utilizar aplicaciones de terceros.
Utilizar únicamente aplicaciones legítimas de proveedores válidos.

9. En términos de configuración de aplicaciones en dispositivos.
Revisar los permisos que requieren y limitar el acceso otorgado a estas apps.

10. No dejar dispositivos desatendidos. La seguridad física de los dispositivos es tan importante como su seguridad técnica. Si se necesita dejar el ordenador portátil, teléfono o tableta por un período de tiempo, es mejor cerrarlo para que nadie más pueda usarlo. Si se guarda información confidencial en una unidad flash o en un disco duro externo, hay que asegurarse de mantenerlos bloqueados también.

Finalidad de la guía de buenas prácticas de seguridad informática.
Se busca que la guía de buenas prácticas de seguridad informática, permite que los empleados que tienen los conocimientos básicos en informática, puedan proteger la información y proteger su equipo informático. Al mismo tiempo ayudando al área de informática, ya que esta solo cuenta con una persona, y no da abasto para toda la empresa.

La guía de buenas prácticas de seguridad informática, para la empresa INDOMED tiene los siguientes objetivos:

- Disminuir riesgos y detectar posibles problemas y amenazas de seguridad.
- Garantizar el uso adecuado de recursos y aplicaciones del sistema.
- Limitar pérdidas y recuperación pertinente del sistema a partir de un incidente de seguridad.
- Proteger la Confidencialidad de los Datos.
- Preservar la Integridad de los Datos.

Otro fin que tiene la guía de buenas prácticas de seguridad informática es explicarle al personal que no conoce sobre informática, como proteger su computadora. Porque el factor humano es el eslabón más débil de la cadena y es el principal responsable de que un ataque se lleve a cabo de forma efectiva. Es por eso que los cibercriminales, que saben esto, constantemente intentan aprovechar la incredulidad o los descuidos de los empleados cuando lanzan sus campañas maliciosas. Pero también podemos ver esta realidad como una oportunidad, ya que con el conocimiento y la capacitación necesaria puede convertir a esos empleados en la primera línea de defensa de una empresa.

6. CAPÍTULO 6

6.1.1. CONCLUSIONES

En base a los criterios que se le dio al proyecto de investigación, se desarrollaron ocho conclusiones, dos conclusiones en relación con el planteamiento del problema y dos en relación a cada uno de los tres objetivos específicos:

A continuación se presentan las dos conclusiones en relación al planteamiento del problema.

- La norma ISO27001:2013 es una herramienta efectiva para manejar un Sistema de Gestión de Seguridad de la Información en cualquier organización, sin importar a que se dedique esta, debido a que es un tema de extrema trascendencia y permanente actualidad. Es de uso global y además es certificable.

- El grado de conciencia que tenga el usuario respecto a la seguridad de la información representa en gran medida el nivel de seguridad de un sistema de seguridad en las empresas, mediante pruebas se logra identificar brechas de seguridad dentro de la empresa, tal como el uso de contraseñas débiles, siendo esto, la puerta de entrada a riesgos mayores.

A continuación se presentan las dos conclusiones en relación al primer objetivo específico.

- Se cumple el objetivo de este proyecto, la guía de buenas prácticas informáticas beneficiara a la empresa y a sus empleados, también los jefes ven con buenos ojos la guía de buenas prácticas informáticas que se le proporciona.

- La empresa no cuenta con un plan de para la recuperación de la tecnología y la información en caso de un desastre natural, sin embargo se espera que con la guía de buenas prácticas se puede gestionar la idea de un plan.

A continuación se presentan las dos conclusiones en relación al segundo objetivo.

- Con el resultado del diagnóstico de vulnerabilidades informáticas, se desarrolló una guía de buenas prácticas informáticas, que beneficie a la empresa y permita ampliar los conocimientos de los empleados con conocimientos básicos en informática.

- La empresa siempre ha tenido equipo informático de calidad, sin embargo la mayoría de los empleados solo tienen conocimientos básicos en informática, y no buscan la forma de aumentar sus conocimientos, y hay que tomar en cuenta que la tecnología va avanzando.

A continuación se presentan las dos conclusiones en relación al tercer objetivo.

- La guía de buenas prácticas informáticas beneficiara a la empresa, explicando a los empleados como utilizar correctamente el equipo informático, a su vez la guía apoyara en su labor, disminuyendo la cantidad de errores.

- Desde su comienzo hasta ahora, la empresa ha podido completar las actividades relacionadas con el área de informática, a pesar de que este solo cuente con un empleado, no obstante esto no quiere decir que la empresa este bien, ya la empresa como todas necesita empleados con amplios conocimientos en informática.

6.1.2. RECOMENDACIONES

- 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.

- 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.

- 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.

- 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.

7. REFERENCIAS BIBLIOGRÁFICAS

1. Empresa INDOMED. https://www.innomed.com.sv/

2. Norma ISO 27001. https://normaiso27001.es/

3. Norma ISO 27001. https://advisera.com/27001academy/es/que-es-iso-27001/

4. Norma ISO 27001. https://advisera.com/27001academy/es/que-es-iso-27001/https://www.normas-iso.com/iso-27001/

5. Norma ISO 27005. https://www.pmg-ssi.com/2017/01/iso-27005-como-identificar-los-riesgos/

6. Antecedentes de la seguridad informática. http://lahistoriadelaseguridad.blogspot.com/p/evolucion-de-la-seguridad-informatica.html

7. Antecedentes de la ISO 27001. https://www.pmg-ssi.com/2013/08/la-nch-iso-27001-origen-y-evolucion/

8. Ley de creación del sistema salvadoreño para la calidad. LA ASAMBLEA LEGISLATIVA DE LA REPUBLICA DE EL SALVADOR, DECRETO Nº 790. [En línea] https://www.defensoria.gob.sv/download/ley-de-creacion-del-sistema-salvadoreno-para-la-calidad/

9. Ley especial contra delitos informáticos y conexos. LA ASAMBLEA LEGISLATIVA DE LA REPUBLICA DE EL SALVADOR, DECRETO No. 236. [En línea]https://www.asamblea.gob.sv/sites/default/files/documents/decretos/D1F13E1E-9860-428F-8703-2B61D5DF1D47.pdf

10. Ley de firma electrónica. LA ASAMBLEA LEGISLATIVA DE LA REPUBLICA DE EL SALVADOR, DECRETO No. 133. [En línea] https://www.asamblea.gob.sv/sites/default/files/documents/dictamenes/CA79C34D-FD9D-429B-87CF-68024E88C822.pdf

11. Tipo de la investigación. **Roberto Hernández Sampieri**. 2018, Metodología de la investigación: las rutas cuantitativa, cualitativa y mixta

8. ANEXOS

ANEXO 1.

Tabla 13 Anexo 1 Estrategias de seguridad informática.

Tabla de estrategias de seguridad informática.	
Nombre	**Descripción**

ANEXO 2.

Tabla 14 Anexo 2 Buenas practicas informáticas.

Tabla de buenas prácticas informáticas	
Nombre	**Descripción**

ANEXO 3.

Tabla 15 Anexo 3 Vulnerabilidades informáticas.

Tabla de vulnerabilidades informáticas	
Nombre de la vulnerabilidad informática	Descripción

ANEXO 4.

Tabla 16 Anexo 4 Brechas de seguridad informática.

Tabla de brechas de seguridad informática	
Nombre de la brecha de seguridad informática	Descripción

ANEXO 5.

Tabla 17 Anexo 5 de los controles de seguridad informática a implementar.

Tabla de los controles de seguridad informática a implementar.		
Numero	**Nombre**	**Control**

ANEXO 6.

Tabla 18 Anexo 6 de las vulnerabilidades y amenazas informática encontradas.

Tabla de las vulnerabilidades y amenazas informática analizada ISO 27005.		
Tipo	**Vulnerabilidad**	**Amenaza**