Centro de Enseñanza Técnica y Superior, CETYS Universidad

Maestría en ingeniería e innovación con orientación en Sistemas y Tecnologías de la Información

Desarrollo de una plataforma digital para el diagnóstico del nivel de seguridad de la información basado en la norma ISO/IEC 27001.

Tesis
para cubrir parcialmente los requisitos necesarios para obtener el grado de Maestro en ingeniería

Presenta:

Christopher Alan Kanter Ramirez

Ensenada, Baja California, México
2020

Tesis defendida por

Christopher Alan Kanter Ramirez

y aprobada por el siguiente Comité

_____

M.B.A Lucia Beltrán Rocha
Co directora

_____

Dr. Josué Aarón López Leyva
Co director

Miembros del comité

_____

Dr. Carlos Antonio González Campos
Sinodal

_____

Dr. Amanda Nieto
Coordinador del Posgrado

_____

Dra. Dalia Holanda Chávez García
Director de Escuela de Ingeniería

Resumen de la tesis que presenta **Christopher Alan Kanter Ramirez** como requisito parcial para la obtención del grado de Maestro en Ciencias en Ingeniería e Innovación con orientación en Sistemas y Tecnologías de la Información.

Desarrollo de una plataforma digital para el diagnóstico del nivel de seguridad de la información basado en la norma ISO/IEC 27001.

Esta tesis presenta el desarrollo de una plataforma digital para el diagnóstico del nivel de seguridad de la información basado en la norma ISO/IEC 27001, el cual tiene el objetivo de proporcionar un diagnóstico inicial a una empresa independientemente del rubro o nivel actual de seguridad de la información que tenga. Adicionalmente, la optimización del proceso considera que los resultados del diagnóstico serán claros, esto con el propósito de que se puedan llevar a cabo mejoras y reducir el riesgo que produce el no contar un plan de contingencia y/o mejora respecto a la seguridad de la información. En particular, la optimización del proceso consiste en el análisis de un gestor de información convencional y así lograr la propuesta de una plataforma personalizada para empresas que requieran estar normadas con la ISO/IEC 27001. Por lo tanto, se propone un sistema y proceso optimizado el cual será la base para el desarrollo de la plataforma digital. Como resultados preliminares, la reducción de elementos necesarios para un diagnóstico inicial del nivel de seguridad de la información promueve la simplicidad de la aplicación y por tanto, incrementa la posibilidad de aplicar la ISO/IEC 27001 a una mayor cantidad de usuarios, lo que significa que sus niveles de seguridad de la información ha incrementado.

Resumen aprobado por:

_____

MBA Lucia Beltrán Rocha
Co director de tesis

_____

Dr. Josué Aarón López Leyva
Co director de tesis

Palabras clave: desarrollo, software, diseño, ISO/IEC 27001, controles, norma, objetivos, análisis, requerimientos, calidad, seguridad, información, JavaFX, Java.

Abstract of the thesis presented **by Christopher Alan Kanter Ramirez** as a partial requirement to obtain the Master of Science degree in Engineering and Innovation with orientation in Systems and Technologies of information.

Desarrollo de una plataforma digital para el diagnóstico del nivel de seguridad de la información basado en la norma ISO/IEC 27001.

This thesis presents the development of a digital platform to diagnose the level of information security based on ISO/IEC 27001, which has the objective of providing an initial diagnosis to a company regarding their area or current level of information security. In addition, the optimization of the process considers that the results of the diagnosis will be clear, this with the objective that risk mitigation and upgrades can be performed in order to better the level of information security. In particular, the optimization of the process consists of an analysis to a conventional management information system, and with this develop the proposal of a customized platform for companies that desire to be complied with the ISO/IEC 27001. Thus, an optimized process and system are proposed which will be the base for the development of a digital platform. As preliminary results, the reduction of elements needed in order to obtain an initial diagnosis regarding information security promotes the simplicity of the application and by this, increases the possibility of applying the ISO/IEC 27001 to a greater amount of users, which means that their levels of information security have grown.

Abstract approved by:

_____

MBA Lucia Beltrán Rocha
Thesis Co director

_____

Dr. Josué Aarón López Leyva
Thesis Co director

Keywords: development, software, design, ISO/IEC 27001, controls, norm, objectives, analysis, requirements, quality, security, information, JavaFX, Java

Dedicatoria

A mi hijo, que siempre fue, es y será mi motivador más grande ante cualquier adversidad, a mis padres que dieron más de lo que un hijo puede desear con tal que apoyarme a realizar mis sueños.

Agradecimientos

A mis directores de tesis por nunca perder la fe en mí, a mis compañeros de trabajo, por guiarme y orientarme cuando más lo necesite y a mi familia y novia que ante todo y sobre todo siempre me motivaron a seguir adelante.

Tabla de contenido

Lista de figuras

Capítulo 1. Introducción

1.1 Antecedentes

1.1.1 Primer ataque cibernético

El primer ataque cibernético sucedió hace más de 200 años y fue a través de mensajería por telégrafo óptico (Standage, 2017). A finales del siglo XVII, Francia inauguro la primera red de datos de la historia gracias al telégrafo óptico. Estas consistían en un sistema de torres las cuales a través de una codificación alfanumérica transmitían letras y números de torre a torre. Cada torre recibía lo enviado por la anterior y reenviaba el mensaje a la siguiente, creando así una línea de comunicación. Las torres consistían en un mecanismo el cual se ubicaba en la parte superior de brazos movibles, la configuración de ellos indicaba una letra o número distinto como puede observarse en la figura 1. Los operadores ajustaban los brazos para imitar las configuraciones de la torre vecina para después transmitir el símbolo a la siguiente torre hasta finalizar.

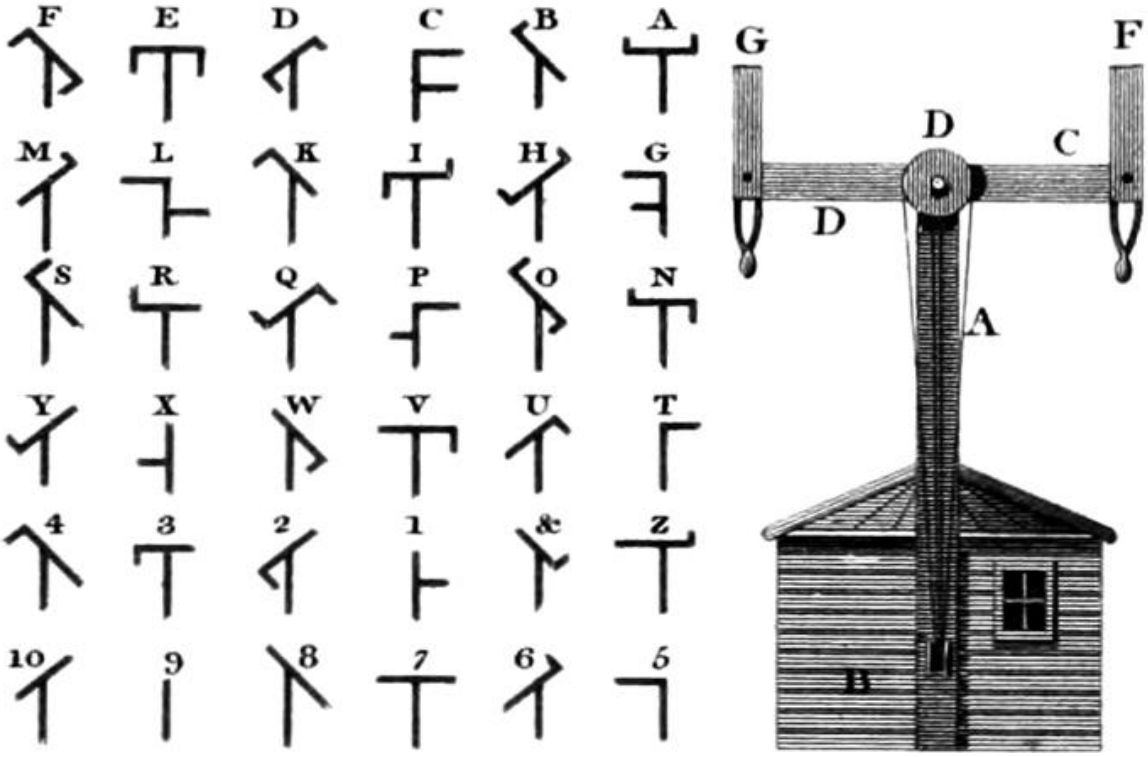

Figura 1. Sistema de telegrafía óptica creado por Claude Chappe.

Los hermanos Blanc descubrieron la manera de utilizar las líneas telegráficas para lograr enviar información sobre oscilaciones del mercado, para ello sobornaron al operador de telégrafos de la ciudad de Tours logrando añadir errores intencionados en los mensajes. Los errores eran vistos por un cómplice a las afueras de Burdeos con un telescopio y luego pasaba la información a los Blanc (Standage, 2017). Los ciberataques surgen con los hermanos Blanc, sin embargo, este no sería el único ataque que se presentaría a lo largo de la historia. A medida que la tecnología evolucionó, los primeros virus informáticos fueron creados trayendo consigo nuevas oportunidades para que los programadores pudieran realizar ataques maliciosos.

1.1.2 Virus informático

Un virus informático es un programa o fragmento de código diseñado para provocar daños en un equipo corrompiendo archivos del sistema, despilfarrando recursos, destruyendo datos o alterando el funcionamiento normal de algún recurso informático (Torres, 2017).

Cuando una persona sale de casa sin abrigarse, se sube a un camión con pasajeros que se encuentran tosiendo, o saludan de beso a alguien con gripe, es probable que sean contagiados, los virus informáticos funcionan de la misma manera. Si se navega en un sitio web, conecta un dispositivo desconocido en una computadora entre otros, se corre el riesgo de ser infectado. Estos son altamente contagiosos debido a que se replican automáticamente y son capaces de copiarse de un archivo o computadora a otra sin consentimiento alguno del usuario. Los virus informáticos a diferencia de los biológicos no se generan espontáneamente, estos son creados con diferentes finalidades como diversión, para hacer el mal y para hacer el bien. En un inicio, algunos programadores únicamente buscaban reírse un rato mientras se burlaban utilizando software, tal fue el caso de Creeper, el primer virus de la historia creado en el año 1971, el cual fue creado con la intención de atacar al sistema operativo Tenex. Cuando Creeper llegaba a una computadora se auto ejecutaba y comenzaba a mostrar el mensaje “I’m the Creeper, ¡catch me if you can!” (Torres, 2017).

Por otra parte, en el año 2000 el virus ILOVEYOU destruyó archivos de más de cincuenta millones de internautas de todo el planeta, impidió el encendido de computadoras y copio las contraseñas de los usuarios para enviarlas a sus creadores, se estima que el valor de los daños ocasionados es de alrededor de nueve mil millones de dólares. Así mismo, el virus Sobig.F provocó treinta y siete mil millones de dólares en pérdidas, esto mediante la detención del tráfico informático en Washington DC y a través del impedimento de partida de la aerolínea Air Canada durante un tiempo (Torres, 2017).

Por último, existen virus que se encargan de infectar un dispositivo sin el consentimiento del usuario, como lo es Linux.Wifatch el cual coordina sus acciones mediante una red entre pares y sirve como una guarda de seguridad impidiendo que otros virus logren llegar al router.

1.1.3 Los ataques informáticos más grandes de la historia

Cada año, las amenazas de un ataque informático generan mayor preocupación en empresas, los virus informáticos son cada vez más sofisticados y frecuentes. McAfee reveló que el crimen cibernético tiene un impacto global en la economía de quinientos mil millones de dólares por año. La complejidad de los asaltos informáticos es medida con base al nivel de importancia que tienen los datos que se miran involucrados y la cantidad de dinero requerida para enmendar los problemas ocasionados (Jiménez, 2017).

Entre los ataques más grandes de la historia se encuentran los siguientes casos:

- PlayStation Network 2011: durante 23 días, el servicio online de PlayStation permaneció sin funcionar, 77 millones de usuarios se vieron afectados sin la posibilidad de generar transacciones generando perdidas de aproximadamente 180 millones de dólares (Milian, 2011).
- LinkedIn 2012: la red social de contactos profesionales fue acreedora de un ataque informático en el cual 117 millones de cuentas fueron afectadas, desde robo de datos confidenciales hasta eliminación de cuentas y contraseñas. Días después al ataque, la información obtenida fue puesta a la venta en la web obscura a cambio de cinco bitcoins (Gunaratna, 2016).
- Yahoo 2013: sufrió el robo de información personal (fechas de nacimiento, direcciones de correo electrónico, números de teléfono y contraseñas) de mil millones de cuentas (Perlroth, 2017).
- eBay 2014: en el mes de mayo, la empresa de compra y venta por internet fue víctima de un ataque a 145 millones de cuentas (Kelion, 2014).

1.2 Hipótesis

El diseño de una plataforma digital para el diagnóstico inicial de la seguridad informática sirve como referencia inicial para una empresa en la modalidad de early-adopter. La presentación de la información básica del estándar permite al usuario percibir el nivel de seguridad de los recursos informáticos.

1.3 Objetivos

1.3.1 Objetivo general

Desarrollar una plataforma digital que permita el diagnóstico del nivel de seguridad de la información basado en la norma ISO/IEC 27001 mediante una innovación de proceso.

1.3.2 Objetivos específicos

1. Revisar los requerimientos generales de la ISO/IEC 27001.
2. Definir los requerimientos generales de la ISO/IEC 27001 a utilizar.
3. Diseñar el flujo, funcionalidad y tecnología a utilizar dentro del sistema.
4. Desarrollar instrumento de diagnóstico a utilizar.
5. Desarrollar interfaces de usuario.
6. Desarrollar base de datos.
7. Capturar información dentro del repositorio.
8. Desarrollar la funcionalidad del sistema e integrar con las interfaces.
9. Realizar pruebas de los desarrollos realizados (pruebas de carga, funcionalidad y usuario).
10. Ejecutar prueba beta.

Capítulo 2. Marco teórico

2.1 Antecedentes de la seguridad de la información

Así como un niño cuida de sus estampitas favoritas para que no se extravíen, maltraten o sean robadas, una empresa cuida de la información que posee. El termino Seguridad de la Información se define como la protección de la información y de los accesos a los sistemas de información, control de su uso, divulgación, alteración, modificación, lectura, registro o destrucción (Maldonado & Cano, 2014).

La información de una empresa no se encuentra expuesta solamente a hackers o delincuentes que busquen robar datos confidenciales, también puede verse afectada por catástrofes naturales, negligencias humanas entre otros. Por ello, el contar con una dinámica o proceso de seguridad de la información es importante, ya que el costo de perdida puede ser inclusive mayor al de protección. El primer índice de protección de datos de DELL EMC indico que, para las empresas mexicanas, la perdida de datos era tres veces más costosa que la inactividad en sus operaciones (Riquelme, 2019).

Según Riquelme (2019), la pérdida de 2.13 terabytes de información representa un costo promedio para las empresas e instituciones gubernamentales y académicas mexicanas de un millón cincuenta y siete mil quinientos noventa y tres dólares. Esto representa tres veces el costo que suponen 20 horas de inactividad en sus operaciones, el cual alcanza solo 335, 935 dólares en promedio.

La primera forma de almacenamiento puede encontrarse en el órgano de barril, el concepto se originó en los países bajos en el siglo 15, en 1972, 3M introdujo la cinta de cartucho de un cuarto de pulgada y en 1967 IBM lanzo el disquete de 8 pulgadas (Haff, 2017). Como se observa, la información era almacenada en diferentes tipos de almacenamiento a lo largo de la historia. Si bien esto era algo confiable en su momento, el avance de la tecnología, así como el de la información manejada requirió el uso de nuevos métodos de seguridad.

Dichos avances trajeron consigo ventajas como la facilidad de disponer de la información en cualquier lugar en cualquier momento, la confiabilidad de contar con respaldos periódicos (servicios que ofrecen algunos de los proveedores de almacenamiento), seguridad ante ataques de intrusión entre otros. Sin embargo, los servidores que hospedan dichas bases de datos no se encuentran exentos de ser víctimas de ciberataques o bien sufrir algún fallo mecánico el cual ocasione perdidas. No cabe duda de que la seguridad ha evolucionado con el paso del tiempo, a medida que las vulnerabilidades y riesgos aumentaron, se tuvieron que implementar nuevos protocolos y medidas de seguridad.

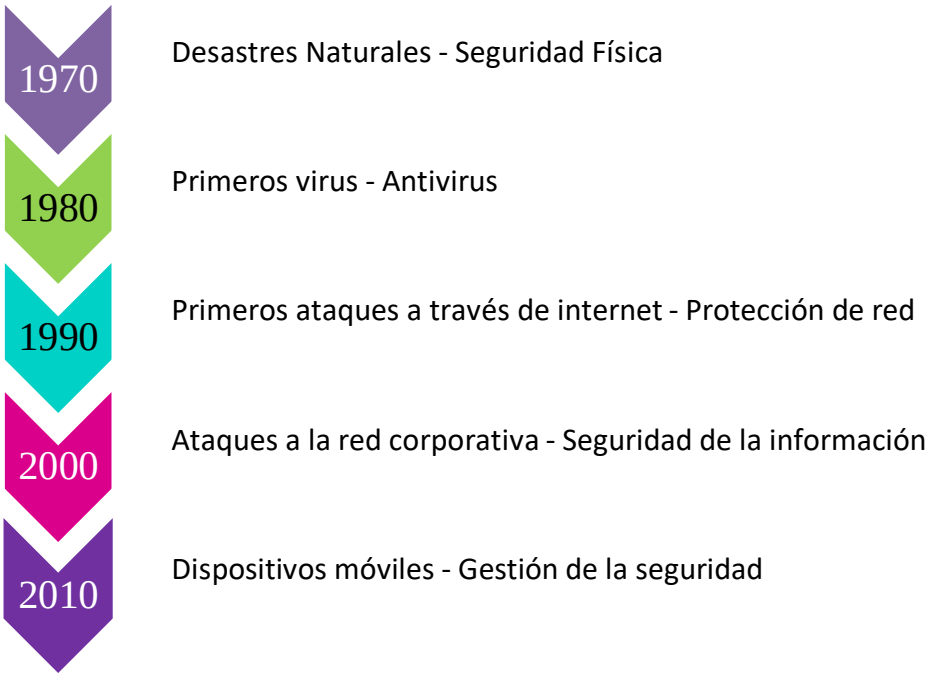

Figura 2. Evolución de la seguridad en las empresas.

Como se puede observar en la figura 2, durante los años setenta, los empleados conocían poco sobre los riesgos relacionados con la información dentro de una empresa, no contaban con copias de seguridad y no se tomaban medidas de seguridad físicas. Por lo tanto, se corría el riesgo de perder los datos y no tener manera de recuperarlos. Con este primer encuentro, las empresas comenzaban a ver la importancia de considerar medidas de seguridad ante desastres naturales o bien errores humanos que pudiesen llevar a perdidas. Sin embargo, ahí no se detendrían los riesgos, durante los años ochenta, nacieron los primeros virus trayendo consigo nuevos retos, las empresas ahora debían asegurar sus servidores para que estuvieran protegidos de ataques físicos como virtuales, con esto en mente, se comenzaron a implementar guardias de seguridad para la protección de datos.

La creación del internet durante los años noventa, trajo consigo un avance en la comunicación, envió y manejo de la información, sin embargo, almacenar información en dispositivos extraíbles con pocas medidas de seguridad era posible permitiendo que esta saliera de entornos seguros. El uso del internet sin concienciación creaba la oportunidad para que un virus fuese implantado en algún computador de la empresa. El nivel de seguridad física seguía sin ser suficiente y el asegurar la integridad de los datos se convertía en una tarea más compleja conforme la tecnología avanzaba.

Entre los años 2000 y 2010, se incrementó el uso de redes sociales, los ataques comenzaron a ser hacia las herramientas que se encargaban de la protección de información y la red corporativa, comenzaban a

ver riesgos de seguridad derivados de empleados insatisfechos y el fraude en línea se convertía en una realidad.

Por último, del año 2010 al 2019 se comenzó a escuchar el termino gestión de la seguridad, en un inicio, las aplicaciones móviles contaban con pocas medidas de seguridad para impedir la fuga de información. Sin embargo, con el paso del tiempo se fue creando un mayor control relacionado con la privacidad de los datos. Debido a la necesidad de proteger información a nivel corporativo y personal, surgen herramientas de cifrado y planes solidos de concientización de los empleados sobre seguridad de la información.
Los avances tecnológicos a lo largo de los últimos 50 años permiten hoy en día compartir información en la nube, interconectar dispositivos electrodomésticos a través de internet y el teletrabajo entre otros, los riesgos amplían su alcance y las amenazas ahora se encuentran en casa. Robo de información, entorpecimiento de sistemas, suplantación de identidad, publicidad de datos personales o confidenciales, robo de dinero o estafas son solo algunos de los problemas con los cuales una empresa puede presentarse de no contar con algún protocolo de seguridad.

Actualmente existen herramientas basadas en la norma ISO/IEC 27001 que guían a las empresas hacia un nivel de seguridad de la información optima a través de la utilización de un sistema de gestión de la seguridad, vsRisk Cloud, Arat, Risk3Sixty, ISO Tools, RM Studio y Abriska son algunas de las más utilizadas.

2.2 Norma ISO/IEC 27001

La norma ISO 27001 es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan. El estándar ISO 27001:2013 para los sistemas de Gestión de la Seguridad de la Información permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos (ISOTools, 2019). La aplicación de la ISO/IEC 27001 significa una diferenciación respecto al resto, que mejora la competitividad y la imagen de una organización, la gestión de la seguridad de la información se complementa con las buenas prácticas o controles establecidos en la norma ISO/IEC 27002 (ISOTools, 2019).

Fue publicado por la International Organization for Standarization y por la comisión Internacional Electrotechnical Commission en octubre del año 2005 y es actualmente el único estándar aceptado a nivel internacional para la gestión de la seguridad de la información. La ISO/IEC 27001 como se conoce hoy en

día, es resultado de la evolución de otros estándares relacionados con la seguridad de la información (Norma BS, BS 7799-1:1995, BS 7799-2:1999, ISO/IEC 17799:2000, BS 7799-2:2002, ISO/IEC 27001:2005, ISO/IEC 17799:2005, ISO 27002:2005, ISO/IEC 27001:2007) (ISOTools Excellence, 2013).

El objetivo de la norma es determinar la manera en la que debe ser administrada la información y en qué momento puede inclinarse por una tendencia. Por ejemplo, la base de datos que almacena las transacciones realizadas en un banco contiene miles de registros por día, sin embargo, cierta información se vuelve obsoleta después de un periodo de tiempo. Con el uso de la norma, se permite conocer que datos son útiles, durante que lapso y en qué momento se pueden desechar. En general, esta norma es una solución de mejora continua para la evaluación de distintos riesgos y establecimiento de estrategias y controles para asegurar la defensa y protección de la información.

La norma ISO/IEC 27001 utiliza el ciclo de Deming tal y como se logra observar en la figura 3, también conocido como mejora continua, el cual consiste en las etapas de planificación, hacer, verificar y actuar o también conocido por sus siglas en ingles PDCA. Además de contar con este ciclo, el modelo contiene diversos indicadores y métricas que permiten medir la eficiencia de los controles.

Actualmente, ha incrementado el número de empresas certificadas con la norma, esto fomenta a que las actividades de protección de la información sean aplicadas constantemente, aumentando la seguridad de la información, imagen y confianza del consumidor (ISOTools Excellence, 2013).

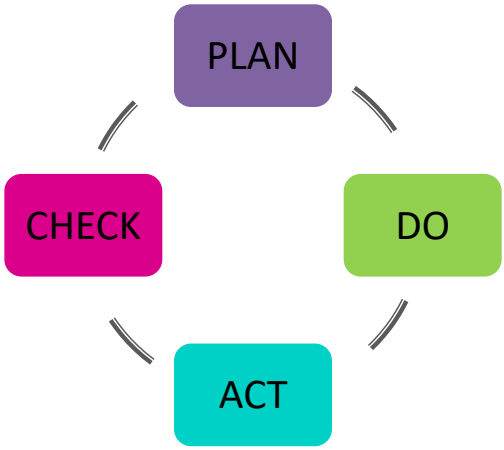

Figura 3. Ciclo de deming, planear, hacer, revisar y actuar por sus siglas en inglés (PDCA). Elaboración propia.

La norma está compuesta por 114 controles de seguridad los cuales se distribuyen a través de 14 secciones mencionadas a continuación:

- Políticas de seguridad de la información: A. 5.
- Organización de la seguridad de la información: A.6.
- Seguridad de los recursos humanos: A. 7.
- Gestión de Activos: A.8.
- Controles de acceso: A.9.
- Criptografía - Cifrado y gestión de claves: A.10.
- Seguridad física y ambiental: A.11.
- Seguridad operacional: A.12.
- Seguridad de las comunicaciones: A.13.
- Adquisición, desarrollo y mantenimiento del sistema: A.14.
- Relación con proveedores: A.15
- Gestión de incidentes de seguridad de la información A.16.
- Aspectos de seguridad de la información para la gestión de la continuidad de negocio: A.17
- Cumplimiento: A.18.

Estos controles se eligen en base a las áreas que conforman a la empresa y sus necesidades de seguridad de la información. Es aquí donde un experto en seguridad de la información debe elegir que controles aplicar utilizando los resultados de la gestión de riesgos, los cuales son explicados en las cláusulas 6 y 8 de la norma.

2.3 Problemática y solución

La norma ISO 27001 es uno de los principales estándares internacionales para la gestión de la seguridad de la información, lo que permite asegurar de un modo eficaz todos los datos importantes de la empresa, tanto financieros como confidenciales, eliminando o minimizando el riesgo de accesos ilegales o sin permiso de terceros que podrían realizar un mal uso de dicha información (ISOTools, 2019). La ISO 27001 es una norma certificable, lo que permite a las organizaciones demostrar su compromiso y conformidad con los mejores estándares y prácticas en materia de seguridad de la información, generando confianza en clientes y proveedores. Esto implica un buen número de beneficios adicionales, tales como (ISOTools, 2019):

- Comunicar a clientes, proveedores y grupos de interés que la seguridad es una de las prioridades de la empresa.

- Identificar los principales riesgos en materia de seguridad informática y establecer controles para gestionarlos o eliminarlos.
- Clasificar los riesgos en función de su gravedad y posibilidades reales de que se lleguen a producir.
- Adaptar y alinear los controles a todas las áreas de la empresa.
- Crear confianza en los clientes y partes interesadas de que sus datos están debidamente protegidos.
- Cumplir con los requisitos y demostrar conformidad y compromiso con los mismos.
- Cumplimiento de las leyes y reglamentos pertinentes reduciendo asV≠ la posibilidad enfrentarse a multas y sanciones.
- Proporcionar el marco más adecuado para la gestión de la seguridad de la información.
- Proteger la reputación de la empresa.
- Ahorrar costes por la reducción de incidentes.
- Implementar procedimientos para permitir la detección oportuna y a tiempo de brechas de seguridad.
- Asegurar que los usuarios que sí están autorizados tengan acceso a la información en el momento en que lo necesitan.
- Conseguir ventaja competitiva.
- Se fortalece la organización interna y los procesos de mejora continua.

Las herramientas existentes que proveen al usuario con un sistema de gestión de la seguridad se ven ligados a altos costos de operación por lo que no son opciones factibles para pequeñas y medianas empresas. Debido a la complejidad y costos de la norma, se analizaron las áreas de oportunidad y se propuso la creación de una plataforma digital la cual apoyará con el diagnóstico del nivel de seguridad de la información de una empresa basado en la norma ISO/IEC 27001. La plataforma permitirá al usuario de manera sencilla, eficiente y optima elegir entre las 13 secciones de la norma e ingresar información que le será solicitada para los respectivos controles, produciendo así una vez ingresados los datos un diagnóstico inicial que proporcionará sugerencias de mejora, así como los datos de los controles contestados. Para brindar comodidad de uso, la plataforma será desarrollada con un diseño de interfaces amigables, también, se implementará el uso de servidores sustentables, los cuales tendrán horarios en donde serán apagados (durante horas de poco uso) para disminuir el uso de recursos, y el diseño e implementación de código será altamente desacoplado y con un alto nivel de calidad, evitando retrabajos, bajos tiempos de vida y con ellos el uso de recursos naturales.

Capítulo 3. Metodología

3.1 Desarrollo de la metodología

Una de las primeras acciones antes de iniciar con el desarrollo de la plataforma digital, consistió en realizar una revisión de los controles que conforman la ISO/IEC 27001. Los controles de la norma son acciones que deben estar contempladas dentro de las empresas y con ellas asegurar la seguridad de la información. Ya que una empresa puede estar compuesta por múltiples áreas, la norma provee 114 controles los cuales permiten definir acciones de control para mitigar posibles riesgos de seguridad de la información. Cada uno de los 114 controles indican acciones que la empresa debe tener realizados y se encuentran redactados a manera de afirmación (Ej. Un conjunto de políticas para la seguridad de la información debe ser definido, aprobado por la dirección, publicado y comunicado a los empleados y partes externas (ISOTools, 2019)).

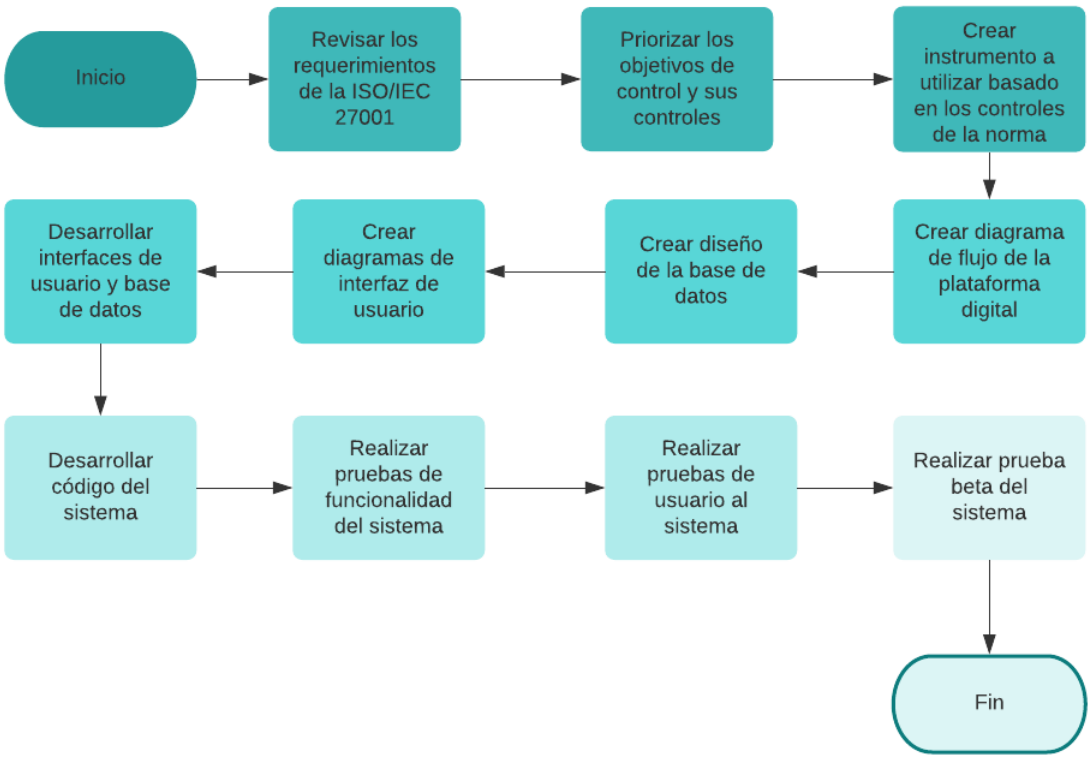

Figura 4. Diagrama de flujo del desarrollo de la metodología. Elaboración propia.

Como se muestra en la figura 4, una vez revisados los requerimientos de la ISO/IEC 27001 se priorizarían los objetivos de control que fuesen pertinentes a utilizar. Con la finalidad de brindar una manera sencilla de interactuar con la herramienta de diagnóstico, los controles se redactaron a manera de pregunta, de modo que el usuario tendrá la opción de responder entre una de las 3 respuestas establecidas (si, no,

n/a), con ello creando el instrumento de diagnóstico que sería utilizado a lo largo del ciclo de vida de la aplicación.

Una vez que el cuestionario fue creado, se verifico que la complejidad de la redacción del cuestionario fuese clara, para ello se les presento a 3 usuarios distintos y se obtuvo retroalimentación, con base a los comentarios arrojados, se realizaron modificaciones al instrumento cumpliendo con el objetivo de asegurar el claro entendimiento de las preguntas realizadas y con ello la veracidad de los resultados de dicha encuesta.

Debido a que el instrumento está conformado por más de 100 preguntas, se procedió al análisis y diseño de la plataforma digital buscando asegurar que la experiencia del usuario no se viera afectada, sobre todo que el usuario no terminara agobiado a raíz de una encuesta extensa, incitándolo a responder aleatoriamente para finalizar rápidamente. Una vez creado el instrumento a utilizar, se procedió con el bosquejo del diagrama de flujo del sistema:

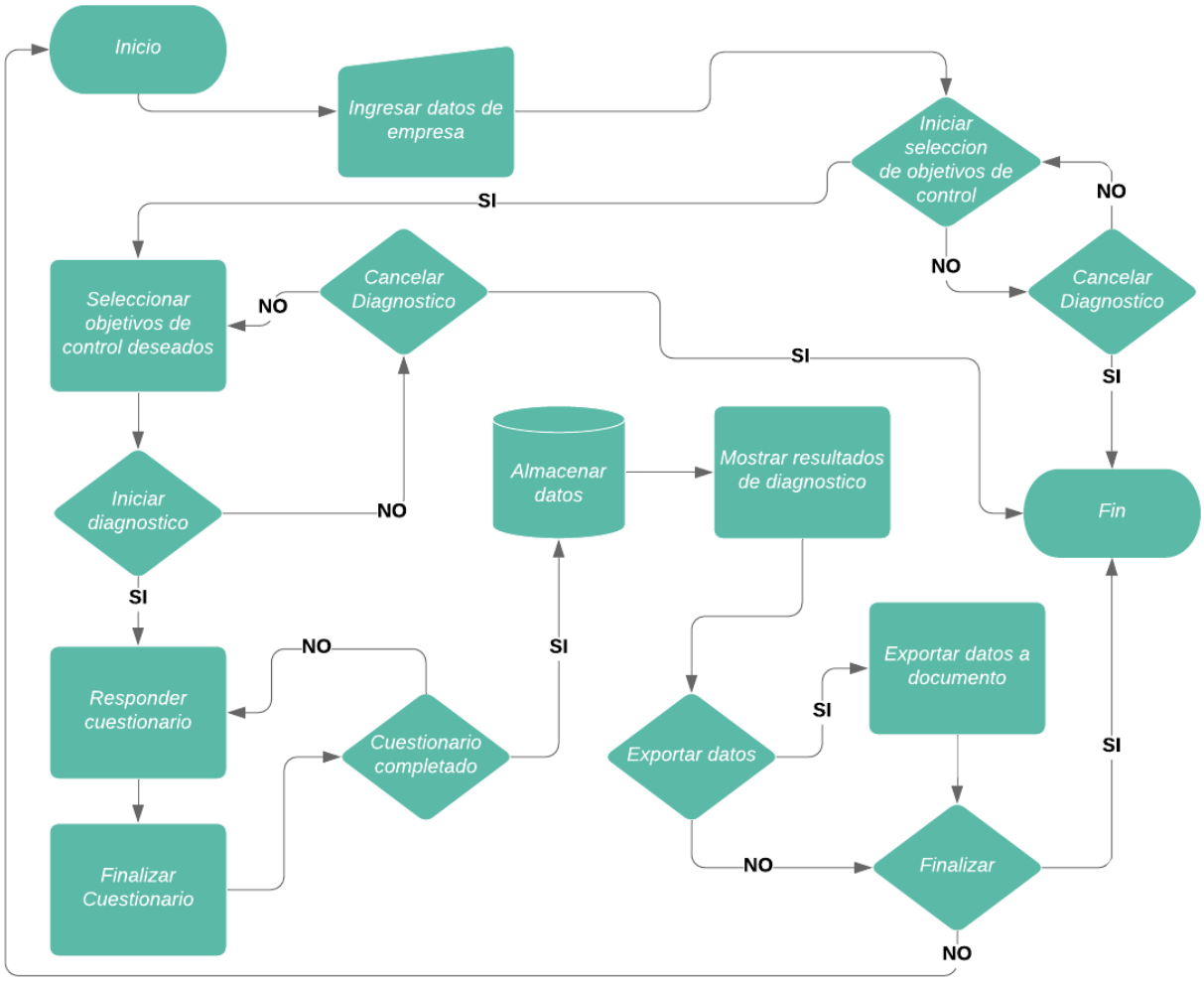

Figura 5. Diagrama de flujo de la herramienta de diagnóstico. Elaboración propia.

Primeramente, el usuario iniciará ingresando el nombre de la compañía, el nombre de la persona realizando la encuesta de diagnóstico y se obtendrá la fecha actual a través de las librerías del lenguaje de programación orientado a objetos Java. Una vez capturada la información, el usuario pulsará el botón de iniciar el cual lo direccionará a la selección de objetivos de control. Además, a manera de ayuda se presentará un texto con instrucciones que indicarán la dinámica de selección de los mencionados.

Para la selección de objetivos de control, se mostrarán los 13 objetivos que se encuentran establecidos en la norma. Siguiente, se contará con una caja de selección lo cual permitirá la selección de las que sean competentes para la empresa y se quieran evaluar. A su vez, cada objetivo tendrá una descripción la cual el usuario podrá visualizar para un mejor entendimiento de este.

Una vez que los objetivos de control deseados a evaluar hayan sido seleccionados, se pulsará el botón de iniciar diagnóstico, esto llevará al usuario a dar inicio con las preguntas relacionadas a los objetivos que fueron seleccionados.

Las preguntas del cuestionario de diagnóstico serán presentadas a manera de lista, si todas las preguntas de un objetivo de control no son respondidas, el usuario no podrá finalizar el diagnostico, tendrá la opción de salir de la aplicación o bien regresar a la selección de objetivos de control en caso de necesitar realizar un cambio. Una vez que se haya finalizado con el proceso de evaluación, se mostrarán los objetivos de control diagnosticados, sus resultados y la recomendación que se le brindará a la empresa con el fin de que pueda llevar a cabo mejoras e incrementar su nivel de seguridad de la información. Los resultados serán almacenados dentro de la base de datos permitiendo contar con puntos de referencia del nivel de seguridad de la empresa. Además, el instrumento, así como las sugerencias de cada control se encontrarán almacenadas de igual manera en la base de datos permitiendo la fácil modificación de los mencionados, finalmente el diagnostico podrá ser exportado a un documento para almacenamiento previo.

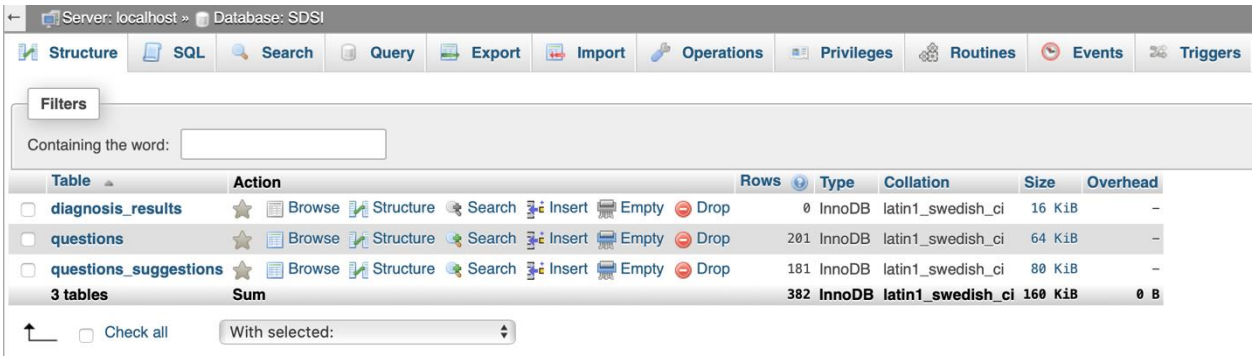

Figura 6. Pantalla de administración de base de datos local XAMPP. Elaboración propia.

La base de datos fue creada utilizando el sistema de gestión de base de datos MariaDB, mediante un servidor local. La administración de dicha fue gestionada a través de la herramienta XAMPP debido a la facilidad de uso e interfaces amigables que contiene para el manejo de esta. Como se puede observar en la figura 6, la interfaz del administrador de la base de datos generada por phpMyAdmin (XAMPP) contiene opciones en la parte superior que facilitan la captura de datos, la visualización de los datos ingresados, exportar e importar datos de la base de datos y definir las características de las tablas y sus columnas. Por otra parte, la interfaz de administración de los servidores locales es de fácil uso como se puede observar en la figura 7.

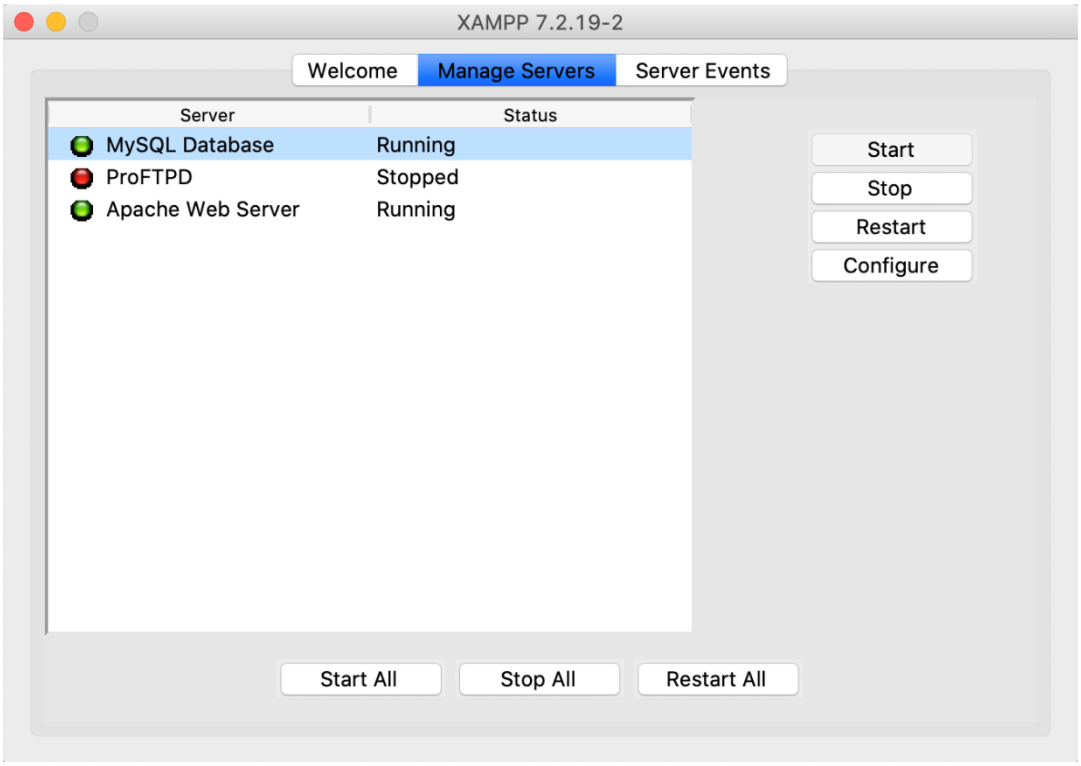

Figura 7. Pantalla de administración de servidores locales XAMPP. Elaboración propia.

Como se puede observar en la figura 8, se contará con una tabla en la cual se almacenarán los datos de la empresa, la fecha del diagnóstico, los resultados obtenidos en los objetivos de control que se hayan seleccionado (en el caso de los objetivos que no hayan sido utilizados, se les asignará un valor de -1) y un identificador de archivo el cual será utilizado para indicar la diferencia entre la versión actual y la pasada. De igual forma en la figura 8 se puede observar la tabla de questions_suggestions, en ella es donde se encontrarán las preguntas del instrumento utilizado y las sugerencias a los controles clasificados por su objetivo de control y en orden ascendiente.

diagnosis_results	
company_name	varchar(200)
user_name	varchar(150)
date	date
archive_id	numeric
objective_control1	numeric
objective_control2	numeric
objective_control3	numeric
objective_control4	numeric
objective_control5	numeric
objective_control6	numeric
objective_control7	numeric
objective_control8	numeric
objective_control9	numeric
objective_control10	numeric
objective_control11	numeric
objective_control12	numeric
objective_control13	numeric

questions_suggestions	
objective_control_id	int(11)
question	varchar(500)
suggestions	varchar(500)

Figura 8. Tabla de resultados de diagnóstico. Elaboración propia.

Con respecto a las interfaces de usuario, estas fueron diseñadas utilizando Adobe XD, se crearon cuatro pantallas para cada una de las vistas. Primeramente, la vista de inicio de sesión contiene el nombre del sistema acompañados de su versión centrado en la parte superior de la pantalla. En la parte inferior se encuentra el logo de la aplicación seguido de dos campos de texto para ingresar el nombre de la empresa y el nombre del usuario contestando la encuesta como se logra percibir en la figura 9. Por último, está situado el botón de iniciar el cual lleva a la selección de objetivos de control, en donde se podrán visualizar los 13 objetivos con su descripción y un objeto de selección. Después, una vez situados dentro de la pantalla de selección de objetivos de control, el usuario contara con la opción de seleccionar que objetivos de control desea evaluar cómo se puede ver en la figura 10. Los objetivos de control estarán acompañados de su descripción, de igual forma, en la parte inferior de la pantalla se encontrará un botón de iniciar diagnostico el cual permitirá proceder con la ejecución del proceso.

En cuanto a la vista de diagnóstico, se mostrarán los objetivos de control que fueron seleccionados junto con los controles a responder, estos se mostraran en orden ascendiente en base a los identificadores de los objetivos de control. Asimismo, cada pregunta tendrá su selección de respuesta situado del lado

derecho de la pantalla como se logra percibir en la figura 11. Debajo del área que contendrá las preguntas, un botón de obtener resultados permitirá la navegación a la última pantalla del sistema.

Por último, una vez situados en la sección de resultados del diagnóstico, se encontrarán en orden ascendiente basado en sus identificadores los objetivos que fueron evaluados como se muestra en la figura 12. El total de preguntas del objetivo de control, el total de preguntas que fueron contestadas con una opción de no, si o n/a y las sugerencias de los controles serán mostradas al usuario.

Figura 9. Vista de inicio de sesión. Elaboración propia.

Asimismo, en la parte inferior de la pantalla, estarán dos botones, uno que permitirá exportar los resultados obtenidos del diagnóstico y otro para salir de sistema. Cabe observar que, a la hora de presionar el botón de salir del sistema, este almacenara los datos automáticamente en la base de datos antes de finalizar la ejecución del sistema.

Con respecto a la codificación de las interfaces de usuario, se utilizó JavaFX ya que cuenta con librerías de Java que pueden ser utilizadas para crear aplicaciones eficientes de internet. Así mismo, las aplicaciones codificadas que utilizan estas librerías pueden ser ejecutadas consistentemente a través de múltiples

plataformas. Por otra parte, la lógica detrás de dichas interfaces fue creada utilizando prácticas de programación orientada a objetos basado en el lenguaje Java, utilizando la herramienta de desarrollo IntelliJ IDEA. La elección de las antes mencionadas fue con base a la experiencia previa del lenguaje y debido a que presentaron la mejor opción para lograr el desarrollo deseado en los tiempos estipulados y sin comprometer calidad.

Figura 10. Vista de selección de objetivos de control. Elaboración propia.

El objetivo principal de las pruebas de funcionalidad es el de someter la aplicación a escenarios predefinidos y evaluar las salidas producidas. Para ello, se definen casos de prueba los cuales están basados en los casos de uso creados a raíz de los requerimientos del sistema. Los casos de prueba proveen indicaciones ampliamente detalladas respecto a la manera en que será revisada una funcionalidad, se indican parámetros de entrada y su salida esperada. Para que una funcionalidad se pueda considerar como válida e indicar que cumple con los requerimientos, esta debe haber pasado exitosamente sus casos de prueba. En cuanto a las pruebas de funcionalidad de este sistema, se evaluaron las acciones que podían

realizarse dentro de la aplicación, la navegación de esta y que los datos fueran correctamente mostrados al usuario. A continuación, se muestran las pruebas de funcionalidad que fueron realizadas a un nivel más detallado:

- Revisar que la navegación entre pantallas sea correcta.
- Obtener datos de la empresa a diagnosticar.
- Enviar datos de la empresa entre pantallas.
- Obtener objetivos de control seleccionados.
- Mostrar preguntas de los objetivos de control seleccionados.
- Obtener respuestas de preguntas mostradas.
- Generar diagnóstico.
- Exportar diagnóstico.
- Almacenar datos en la base de datos.

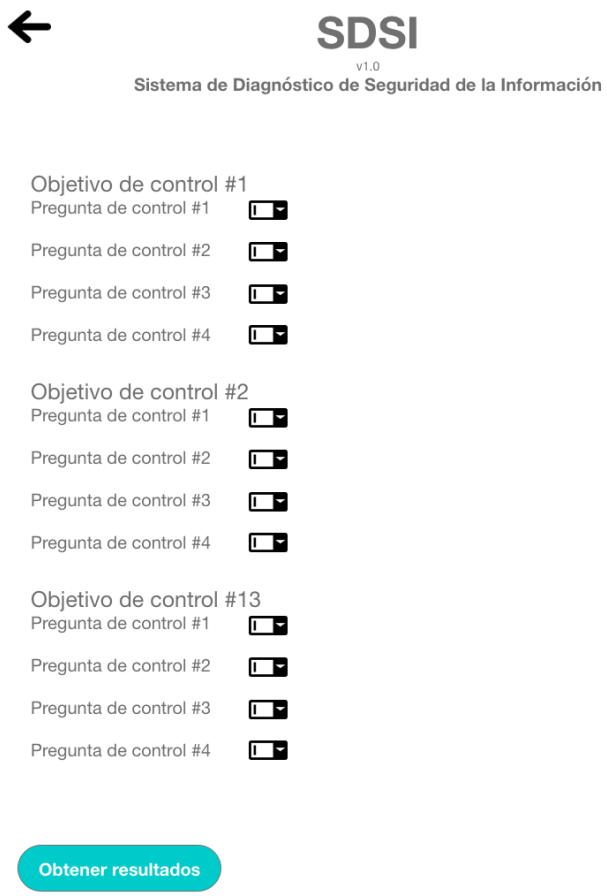

Figura 11. Vista del cuestionario. Elaboración propia.

Las pruebas de usuario permiten evaluar el sistema con usuarios que no están familiarizados con su funcionalidad, con ello se busca la obtención de retroalimentación con la cual se puedan realizar mejoras a la aplicación en desarrollo. Para la etapa de pruebas de usuario, cuatro personas diferentes entre las edades de 20 y 70 años utilizaron la aplicación, después se recopilaron los comentarios y sugerencias y por último se realizaron los cambios que se consideraron pertinentes sin perjudicar los tiempos de entrega del sistema. Entre algunas de las recomendaciones sugeridas se encontraron las siguientes:

- Tamaños de letra más grandes para facilitar la visualización de los textos.
- Poder seleccionar la ubicación de almacenamiento del archivo de diagnóstico a la hora de exportar.
- Contar con una pantalla más interactiva en la sección de resultados del diagnóstico, proporcionando gráficas y porcentajes de los resultados.

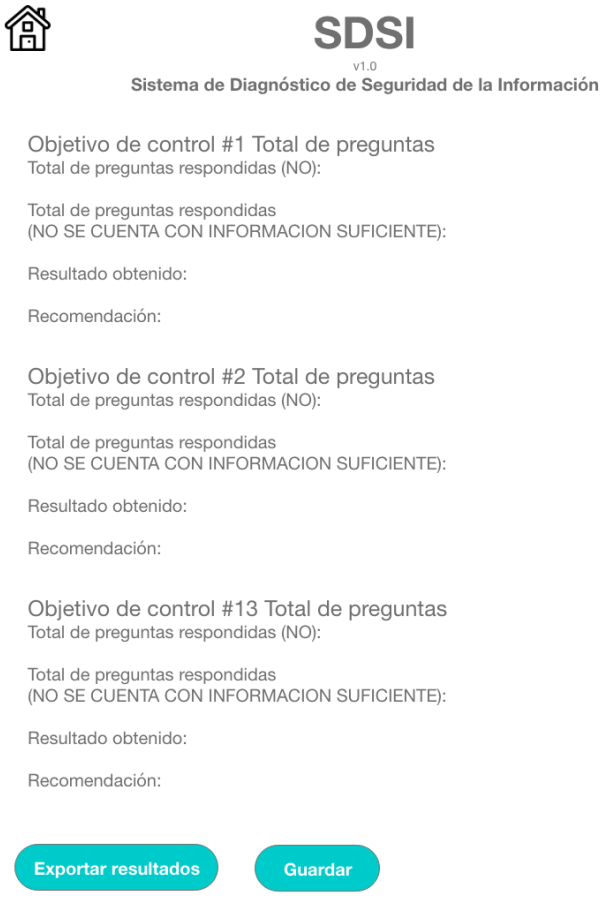

Figura 12. Vista de los resultados del diagnóstico. Elaboración propia.

Por último, el sistema de diagnóstico del nivel de seguridad de la información fue sometido a una prueba beta, en ellas el usuario fue presentado por primera vez con el software y se le guio durante el uso de este. El usuario contesto las preguntas que se le presentaron basados en los objetivos de control seleccionados y se generó el resultado del diagnóstico. Una vez obtenidos los resultados, el usuario proporciono comentarios, retroalimentación y su perspectiva general del diagnóstico que se le presento, por último, se le pregunto si el uso de la herramienta proporcionaba información de valor con el fin de mejorar su nivel de seguridad de la información.

3.2 Obtención y análisis de datos

Mediante la realización de pruebas de usuario, se recopilará información sobre el funcionamiento, diseño y presentación de los datos. Seguidamente, se realizará un análisis sobre lo obtenido y se decidirá cuales cambios son pertinentes para la funcionalidad del sistema y a su vez cuales podrán ser realizados dentro de los tiempos de desarrollo definidos. Así mismo, mediante el uso de la plataforma digital a través de una prueba beta, los usuarios capturaran sus respuestas a las preguntas de los objetivos de control presentados. Una vez contestadas las preguntas y que se genere el resultado de diagnóstico, se procederá a evaluar las sugerencias generadas con el usuario obteniendo retroalimentación sobre lo que se presenta en la aplicación y lo que se requiera implementar dentro de la empresa.

Capítulo 4. Resultados y Discusión

Mediante la realización de la metodología planteada se logró el desarrollo de la aplicación, la indagación de requerimientos, diseño de interfaces y flujo general del sistema, los cuales fueron elementos clave para obtener el resultado esperado. Ya que se utilizó JavaFX como lenguaje principal de programación, el ambiente de desarrollo IntelliJ IDEA creo un proyecto con la estructura mostrada en la figura 13. Dentro de la carpeta de src, se encuentra la carpeta de images, en ella se almacenaron las imágenes que fueron utilizadas dentro de la aplicación para los botones de ir a la pantalla de inicio, regresar a la pantalla inicial y el logotipo de la aplicación. También, se puede visualizar la carpeta de sdsi la cual contiene los archivos fxml (utilizados para las vistas) y java (para los controladores y lógica de las vistas y aplicación), esta carpeta es la más importante de la aplicación ya que contiene todo lo necesario para ser ejecutada.

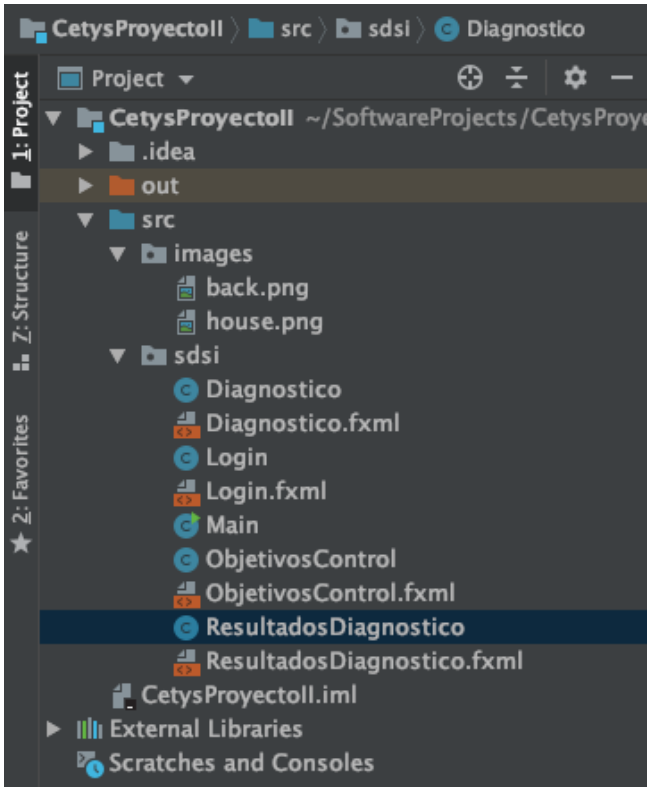

Figura 13. Estructura del proyecto SDSI. Elaboración propia.

Por otra parte, la aplicación consto de cuatro pantallas principales (Login, ObjetivosControl, Diagnostico, ResultadosDiagnostico), aunado a las vistas y sus respectivos controles, el proyecto contiene una clase Main de la cual parte toda ejecución del software. El utilizar JavaFX facilito de gran manera la creación y manejo de las vistas, permitió definir como se visualizaría la interfaz, desarrollarla fácilmente sin utilizar tiempo excesivo y poder continuar con el desarrollo de la lógica principal de la aplicación.

```
<Pane maxHeight="-Infinity" maxWidth="-Infinity" minHeight="-Infinity" minWidth="-Infinity" prefHeight="900.0" prefWidth="700.0" style="-fx-background-color: FFFFFF;" xmlns="http:/
  <children>
    <Label layoutX="308.0" layoutY="22.0" text="SDSI" textFill="#727272">
      <font>
        <Font name="Avenir Black" size="36.0" />
      </font>
    </Label>
    <Label layoutX="338.0" layoutY="69.0" text="v1.0">
      <font>
        <Font name="Avenir Roman" size="13.0" />
      </font>
    </Label>
    <Label layoutX="168.0" layoutY="86.0" text="Sistema de Diagnóstico de Seguridad de la Información" textFill="#727272">
      <font>
        <Font name="Avenir Heavy" size="14.0" />
      </font>
    </Label>
    <TextField fx:id="nombre_empresa" layoutX="26.0" layoutY="505.0" prefHeight="27.0" prefWidth="355.0" />
    <TextField fx:id="nombre_usuario" layoutX="26.0" layoutY="567.0" prefHeight="27.0" prefWidth="355.0" />
    <Label layoutX="432.0" layoutY="505.0" text="Nombre de la empresa" textFill="#727272">
      <font>
        <Font name="Avenir Roman" size="18.0" />
      </font>
    </Label>
    <Label layoutX="444.0" layoutY="567.0" text="Nombre del usuario" textFill="#727272">
      <font>
        <Font name="Avenir Roman" size="18.0" />
      </font>
    </Label>
    <Button fx:id="boton_iniciar" layoutX="26.0" layoutY="656.0" mnemonicParsing="false" onAction="#iniciar" prefHeight="30.0" prefWidth="117.0" style="-fx-background-color: #51C
      <font>
        <Font name="Avenir Black" size="14.0" />
      </font>
    </Button>
    <Label layoutX="254.0" layoutY="867.0" text="&lt;/developed by blacKCat Solutions&gt;" textFill="#727272">
      <font>
        <Font name="Avenir Roman" size="13.0" />
      </font>
    </Label>
  </children>
</Pane>
```

Figura 14. Archivo FXML correspondiente a la vista de Login. Elaboración propia.

Como se puede visualizar en la figura 14, en los archivos fxml únicamente se almacenan los datos de los elementos que conforman la vista, así como los indicadores de los métodos y controlador al que hacen referencia. Para una administración más amigable y sencilla, se utilizó la herramienta Scene Builder desarrollado por Gluon como se puede observar en la figura 15. Esta herramienta permite al usuario visualizar su archivo fxml de manera gráfica, proporcionándole todos los elementos que este necesita para la modificación y creación de este.

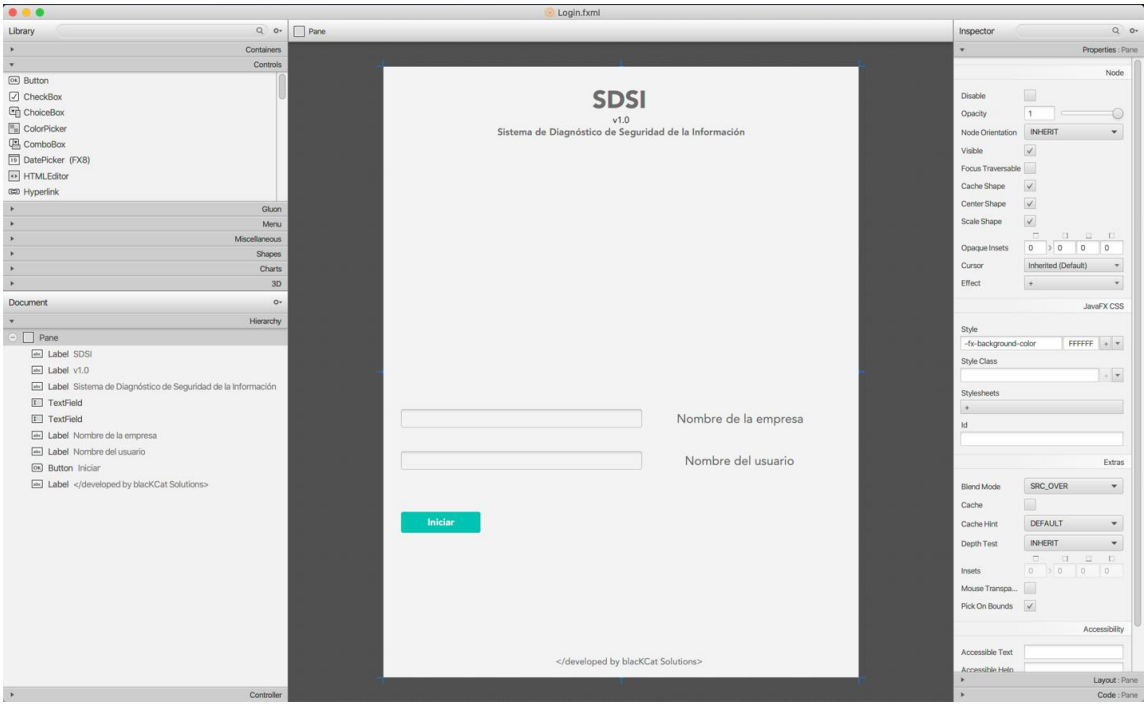

Figura 15. Pantalla de Login vista desde Scene Builder. Elaboración propia.

Respecto a la comunicación entre la vista y su controlador, el archivo fxml tiene un atributo que referencia a la clase Java que contendrá el código que manipulará la funcionalidad de la interfaz. Como podemos observar en la figura 16, se encuentra un fxml tag en la línea 11 de código, en ella se define que el controlador de esa vista será la clase Login dentro del paquete llamado sdsi. Con ello, todas las acciones estipuladas dentro del archivo fxml, harán referencia a los métodos que contengan el mismo nombre que hayan sido codificados en la clase Java.

```
9   <Pane maxHeight="-Infinity" maxWidth="-Infinity" minHeight="-Infinity" minWidth="-Infinity" prefHeight="900.0" prefWidth="700.0"
10          style="-fx-background-color: FFFFFF;" xmlns="http://javafx.com/javafx/8.0.171" xmlns:fx="http://javafx.com/fxml/1"
11          fx:controller="sdsi.Login">
```

Figura 16. Atributos del archivo FXML de la vista de Login. Elaboración propia.

Figura 17. Pantalla de Login del sistema SDSI. Elaboración propia.

Una vez definida la comunicación entre las pantallas y la lógica detrás de ellas, se crearon las funcionalidades correspondientes a cada pantalla, a continuación, se presentarán la funcionalidad y

código correspondiente a las cuatro vistas principales. Primeramente, el usuario será presentado con la interfaz de registro (Login), en ella debe capturar tanto el nombre de la empresa, así como el nombre de la persona que estará contestando las preguntas relevantes al diagnóstico, así como se puede observar en la figura 17. Después, Una vez que el usuario haya capturado la información podrá seleccionar el botón de “Iniciar”, si alguno de los campos no se encuentra capturado, un mensaje de alerta se le presentara indicándole que debe ingresar todos los datos solicitados, esto puede observarse en la figura 18.

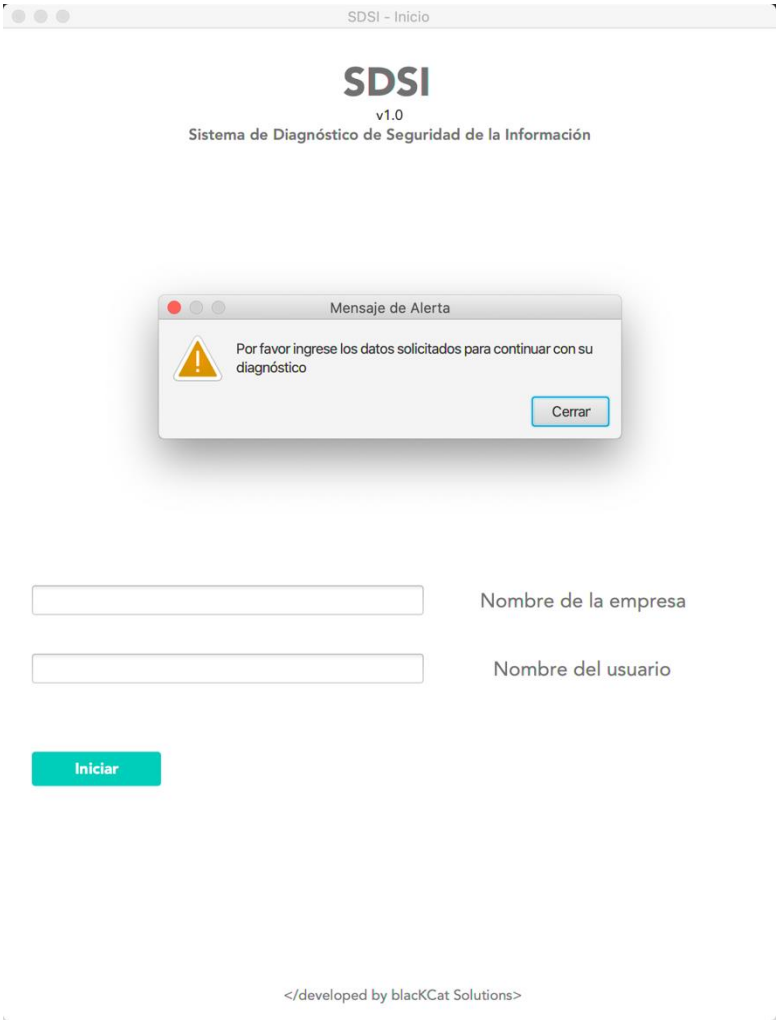

Figura 18. Mensaje de alerta de la pantalla de Login del sistema SDSI. Elaboración propia.

Una vez cumplidos los criterios de inicio, el código del controlador de la vista de Login, cargará la siguiente vista llamada “ObjetivosControl”, esto se realizará a través del código mencionado en la figura 19. Iniciando por la línea 51 de la figura 19, se crea un FXMLLoader con la información de la vista que será cargada (ObjetivosControl.fxml), se crea un objeto Parent llamado root con la información del loader que fue creado lo cual posteriormente es utilizado para obtener el controlador que está asignado a la vista

que se cargará. Una vez obtenido el controlador de la siguiente vista, se le envían los datos que fueron ingresados por el usuario en la vista de Login, estos datos se enviarán a las vistas siguientes ya que serán utilizados como parte del diagnóstico final. Después, un objeto Scene será creado utilizando el objeto Parent que contiene la información del archivo fxml a cargar, este objeto scene será cargado dentro de un objeto Stage el cual será mostrado de manera gráfica utilizando el método show de la librería de javafx como se puede observar en la línea 61 de la figura 19. Por último, de ser exitosa la carga de la vista siguiente, el usuario será presentado con ella, de no serlo, el código cuenta con un manejo de excepciones para asegurar que la experiencia del usuario no se vea afectada.

```
26      @FXML
27      public void iniciar(ActionEvent event)
28      {
29          //Get datetime from God
30          DateTimeFormatter dtf = DateTimeFormatter.ofPattern("dd/MM/yyyy HH:mm:ss");
31          LocalDateTime now = LocalDateTime.now();
32          String dt = "'" + dtf.format(now) + "'";
33
34          if(nombre_empresa.getText().equals("") || nombre_usuario.getText().equals(""))
35          {
36              Alert alert = new Alert(Alert.AlertType.NONE);
37              alert.setAlertType(Alert.AlertType.WARNING);
38              alert.setTitle("Mensaje de Alerta");
39              alert.setHeaderText(null);
40              alert.setContentText("Por favor ingrese los datos solicitados para continuar con su diagnóstico");
41              ButtonType ok = new ButtonType( text: "Cerrar", ButtonBar.ButtonData.CANCEL_CLOSE);
42              alert.getButtonTypes().setAll(ok);
43              alert.show();
44          }
45          else
46          {
47              try
48              {
49                  //This is for the new window to be shown
50                  //We get the controller from the fxml file so we can pass data to it
51                  FXMLLoader loader = new FXMLLoader(getClass().getResource( name: "ObjetivosControl.fxml"));
52                  Parent root = loader.load();
53                  ObjetivosControl controller = loader.<~>getController();
54                  controller.set_login_data(nombre_empresa.getText(), nombre_usuario.getText(), dt);
55                  Scene objetivos_control_scene = new Scene(root);
56
57                  //This is to close up the current window
58                  Stage current_stage = (Stage) ((Node) event.getSource()).getScene().getWindow();
59                  current_stage.hide();
60                  current_stage.setScene(objetivos_control_scene);
61                  current_stage.show();
62              }
63              catch (Exception e)
64              {
65                  System.out.println("Loading of Seleccion de Objetivos de control did not load: \n" + e);
66              }
67          }
68      }
69  }
```

Figura 19. Código del controlador de la pantalla de Login. Elaboración propia.

En cuanto a la pantalla de selección de objetivos de control, esta contiene los trece objetivos de control de la norma ISO/IEC 27001. Cada una de ellas puede ser seleccionada a través de un recuadro de selección que se encuentra de su lado derecho al finalizar el texto como se muestra en la figura 21. Al igual que en la ventana de Login, si el usuario no ha seleccionado por lo menos un objetivo de control, este no podrá proceder a la siguiente sección del diagnóstico arrojando una alerta la cual indicará que debe seleccionar por lo menos un objetivo de control a evaluar, así como se muestra en la figura 20.

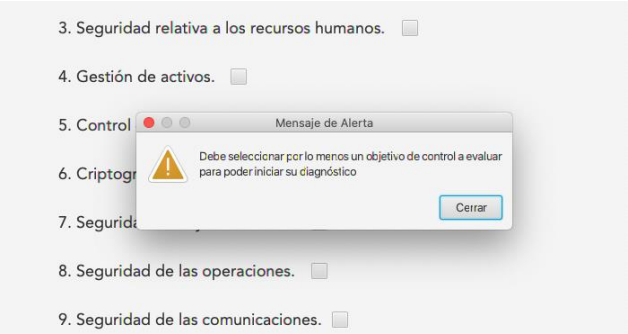

Figura 20. Mensaje de alerta de la pantalla de selección de objetivos de control. Elaboración propia.

Cuando el usuario haya seleccionado por lo menos un objetivo de control podrá proceder a la siguiente fase del diagnóstico, de igual manera en la vista de selección de objetivos de control podrá regresar a la pantalla de inicio si así lo desea, esto por medio del botón que se encuentra en la esquina superior izquierda de la ventana. Así mismo, de la misma manera en que se enviaron los datos de la empresa y usuario utilizando la aplicación, de la pantalla de selección de objetivos de control se envían los objetivos que fueron seleccionados. Los números de los objetivos son almacenados en una variable de texto, esta será utilizada como parámetro para obtener de la base de datos las preguntas correspondientes a esos objetivos de control.

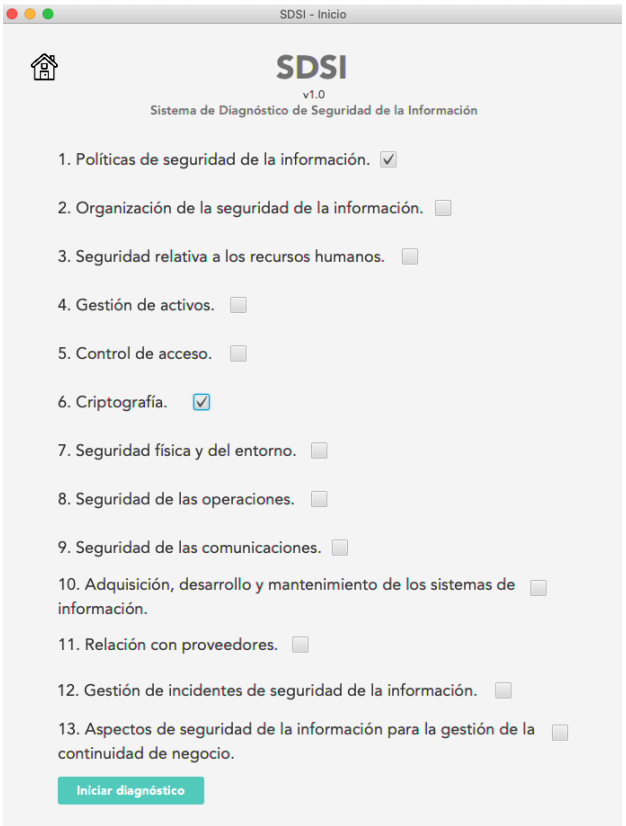

Figura 21. Pantalla de selección de objetivos de control. Elaboración propia.

Una vez situados en la pantalla de diagnóstico, el usuario tendrá dos botones en la parte inferior de la pantalla, estas corresponden a iniciar el diagnóstico y finalizar el diagnóstico. El botón de iniciar diagnóstico estará habilitado de primera instancia, una vez que haya sido seleccionado, pasará a un estado deshabilitado y el botón de finalizar diagnóstico será habilitado. Si el usuario no ha contestado todas las preguntas que se le muestren en pantalla, no podrá finalizar el diagnóstico, se le presentara un mensaje el cual le indicara que todas las preguntas deben ser contestadas. Si bien, el usuario desea regresar a la selección de objetivos de control para modificar la selección realizada, esta opción estará disponible mediante un botón en la esquina superior izquierda de la ventana.

Al iniciar con el diagnóstico, las preguntas de los controles a diagnosticar serán presentadas en el orden que se encuentran dentro de la norma y se mostrará el nombre del objetivo de control al que pertenecen junto con su descripción. Al lado de la pregunta correspondiente al control, estará una caja de selección con la cual el usuario podrá indicar si cumple, no cumple o no aplica dicho control dentro de su empresa. Para la obtención de la información mencionada en el párrafo anterior, se realiza una llamada de selección a la base de datos llamada “questions_suggestions” como se puede ver en la figura 22.

```
132     /**
133      * Get questions from DB given the Objective Controls selected
134      */
135     public void get_questions_from_db()
136     {
137         System.out.println(objective_controls);
138         try
139         {
140             Connection conn =
141                     DriverManager.getConnection( url: "jdbc:mysql://localhost/SDSI?" +
142                             "user=root&password=");
143
144             // Do something with the Connection
145             PreparedStatement pst = (PreparedStatement) conn.prepareStatement(
146                     sql: "select * from questions_suggestions where objective_control_id in ("+objective_controls+");");
147             ResultSet rs = (ResultSet) pst.executeQuery();
148             while(rs.next())
149             {
150                 resultset_data.add(rs.getString( columnLabel: "question"));
151                 resultset_data_objective_ids.add(rs.getString( columnLabel: "objective_control_id"));
152                 resultset_suggestions.add(rs.getString( columnLabel: "suggestions"));
153             }
154             System.out.println("Si se logro la conexion");
155             conn.close();
156         }
157         catch (SQLException ex)
158         {
159             // handle any errors
160             System.out.println("SQLException: " + ex.getMessage());
161             System.out.println("SQLState: " + ex.getSQLState());
162             System.out.println("VendorError: " + ex.getErrorCode());
163         }
164     }
```

Figura 22. Selección de información de la base de datos. Elaboración propia.

En las líneas 150, 151 y 152 se almacena la información obtenida en diferentes listas para facilitar la manipulación de esta. Estas listas son posteriormente utilizadas para crear los objetos que serán cargados en la vista y lograr dar el formato deseado, para ello se utilizó la siguiente lógica mostrada en la figura 23.

```
Inicio;
for(int i=0; i<list.size(); i++)
{
  if(lista.get(i) inicia con ¿)
  {
    Crear combobox con opciones;
    Crear label con texto de lista;
    Agregar label y combobox a contenedor;
  }
  else
  {
    Crear label con informacion de lista;
    Agregar label a contenedor;
  }
}
Definir contenedor dentro de la vista;
Fin;
```

Figura 23. Pseudocódigo para la creación de elementos de la vista de diagnóstico. Elaboración propia.

Esta lógica produciría la vista mostrada en la figura 24, una vez que el usuario haya contestado todas las preguntas presentadas con una respuesta de Si, No o N/A y el botón de finalizar diagnóstico sea seleccionado, se recopilarán todas las respuestas ingresadas por el usuario y serán almacenadas dentro de una nueva lista dentro del controlador.

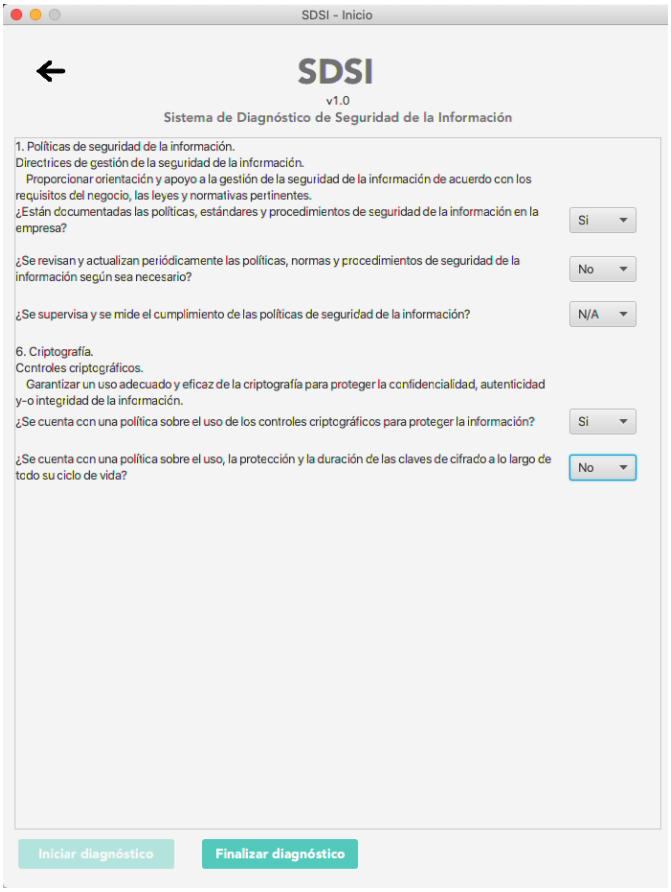

Figura 24. Pantalla de diagnóstico completa. Elaboración propia.

Una vez que se hayan recopilado las respuestas, el controlador generará mediante su código el texto correspondiente al diagnóstico, este formato puede visualizarse en la figura 25. La generación de dicho formato se logra a partir de la manipulación de las listas que resguardan la información capturada, así como de la interacción con la base de datos.

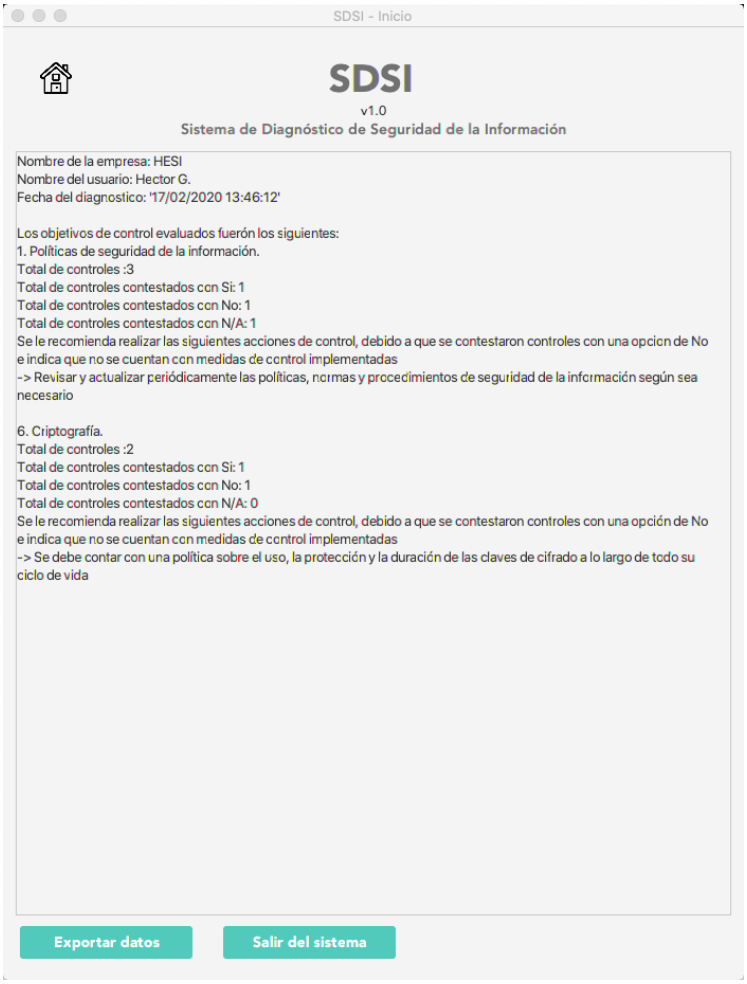

Figura 25. Vista de la pantalla de resultados del diagnóstico. Elaboración propia.

El pseudocodigo utilizado para crear el código de dicha lógica se muestra a continuación:

```
sugerencias = “”
diagnostico = “”
PARA a = 1 HASTA a < longitud(resultset_data)
        SI elemento de resultset_date inicia con "¿"
                ENTONCES
                        SI respuesta seleccionada por el usuario es Si
                                ENTONCES contador_si++
```

SI respuesta seleccionada por el usuario es No

ENTONCES contador_no++

sugerencias = sugerencias + sugerencia del control

SI respuesta seleccionada por el usuario es N/A

ENTONCES contador_na++

SI elemento de resultset_data inicia con un digito

ENTONCES

Agregar texto con totales del objetivo de control a diagnostico

Agregar a diagnostico texto de variable sugerencias

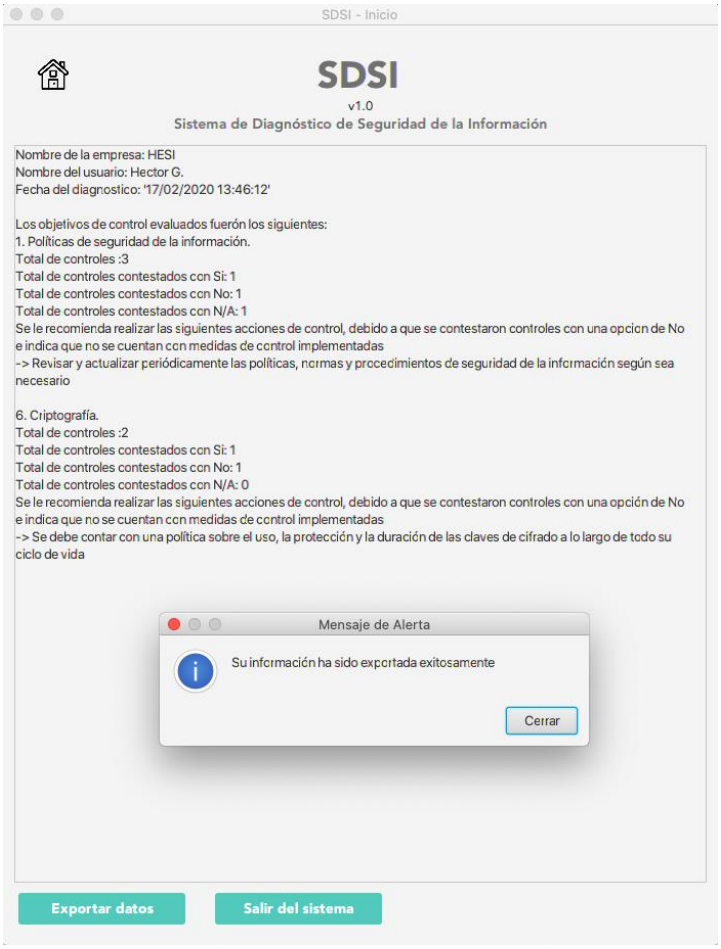

Figura 26. Mensaje de confirmación de exportación de resultados de diagnóstico. Elaboración propia.

Esto llevará al usuario a la última pantalla de la aplicación de diagnóstico, como se mencionó anteriormente, la información de la evaluación será mostrada con el formato especificado brindándole al usuario las recomendaciones que se le sugieren realizar para lograr mejorar su nivel de seguridad de la información como puede observarse en la figura 25. Los resultados podrán ser exportados mediante el

botón de “Exportar datos” que se encuentra en la esquina inferior izquierda. Al seleccionar la opción de almacenar, los datos mostrados en pantalla serán escritos en un archivo de texto plano en el escritorio de la computadora utilizada con el nombre “ResultadosDiagnostico”. En la figura 26 se puede observar el mensaje de confirmación de la exportación del diagnóstico y en la figura 27 se muestra el archivo que fue generado.

Por último, el usuario una vez finalizado su diagnóstico, podrá regresar a la pantalla de inicio o bien finalizar la ejecución del sistema a través del botón de salir del sistema o con el botón de finalizar ventana encontrado en la esquina superior izquierda para sistemas operativos Mac y en la esquina superior derecha para Windows.

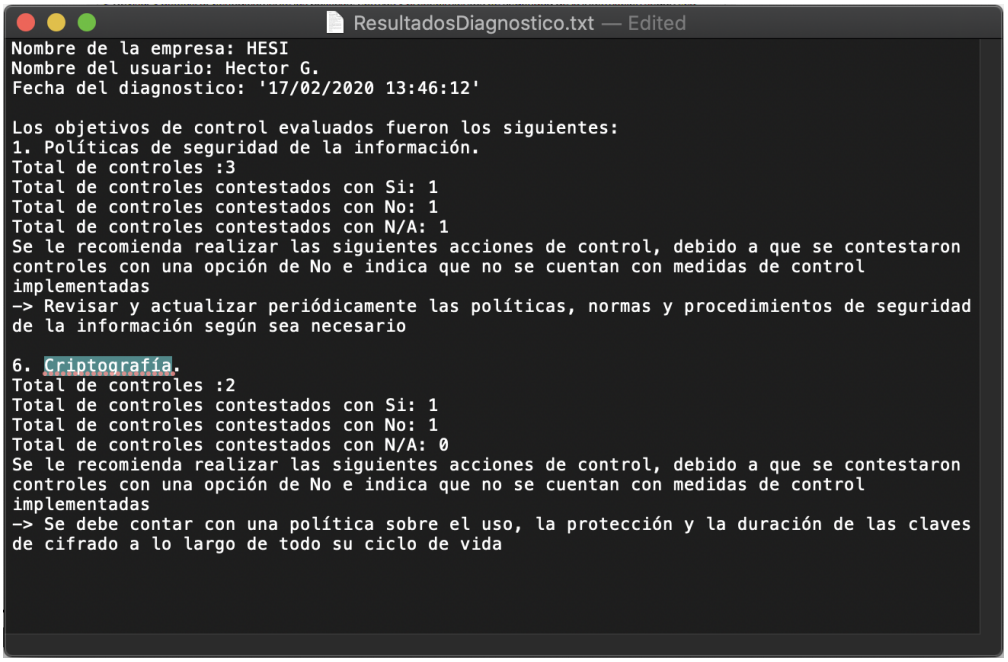

Figura 27. Archivo de texto plano con resultados del diagnóstico realizado. Elaboración propia.

Capítulo 5. Conclusiones

El diseño de una plataforma digital para el diagnóstico inicial de la seguridad de la información sirve como referencia inicial para una empresa en la modalidad de early-adopter. Esto se logró mediante la creación de un instrumento de diagnóstico basado en los 114 controles de la norma ISO/IEC 27001 y el diseño de un flujo de sistema concreto y de calidad. Hay que destacar que el flujo del sistema fue desarrollado con la finalidad de crear una secuencia de pasos directa en donde el usuario obtuviera su resultado esperado de manera rápida y que esta fuera fácil de entender. El uso del lenguaje de programación JavaFX permitió crear interfaces de usuario amigables tanto en funcionalidad como en diseño, así como facilitar el manejo de información entre vistas y la base de datos. Así mismo, produjo la facilidad de crear código altamente desacoplado y capaz de ser ejecutado en múltiples plataformas lo cual es una cualidad que podrá ser utilizada en futuras versiones de la plataforma.

Cabe observar que la redacción de los controles a manera de cuestionario facilito el auto diagnóstico del usuario respecto a su nivel de seguridad de la información. Si bien, el entender la norma sería una tarea exhaustiva, el ser presentado con una serie de preguntas con una opción de respuestas básicas y directas como lo fueron Si, No y N/A brindo al usuario una dinámica sencilla de realizar. Por otra parte, las interfaces de usuario al no contener muchos distractores u opciones que el usuario no requeriría crearon una experiencia amigable, permitiéndole enfocarse en la contestación de las preguntas presentadas.
Respecto a la base de datos, si bien no se crearon tablas relacionales durante la primera fase de este desarrollo, la facilidad de expandir el catálogo de tablas resulta favorable para futuras versiones de este sistema. De igual manera, la manipulación de información fue sencilla ya que la iteración de registros era rápida, de haberse elegido una estructura alrededor de una base de datos no-sql se hubiera puesto es juego la rapidez con la que se mostraran los datos. También el uso de la aplicación XAMPP facilito el manejo de la base de datos, así como la creación de tablas e inserción de datos a estas, tal y como se pensó, la herramienta phpmyadmin proporcionada por XAMPP fue el administrador correcto para dicho desarrollo.

Por último, las pruebas de carga y funcionalidad permitieron identificar posibles errores dentro del código fuente del sistema, así como en el flujo principal del mismo. Aunado a las pruebas mencionadas, las pruebas de usuario ayudaron a mejorar las actuales interfaces para lograr brindarle al usuario una mejor experiencia. Las pruebas de usuario permitieron conocer los comentarios de los usuarios de primera instancia y obtener recomendaciones como, por ejemplo: “El uso de elementos gráficos para la

presentación de los resultados del diagnóstico seria de ayuda para el usuario, ya que le permitiría analizar la información desde un enfoque estadístico". En resumen, los datos presentados, le proporcionan al usuario un punto de referencia respecto a su actual nivel de seguridad de la información, que tan alejado se encuentra del nivel deseado y que acciones puede realizar para alcanzarlo. Con base a las sugerencias que son realizadas, la empresa podrá realizar las acciones recomendadas y de esta manera alcanzar un mejor estado de seguridad de la información. Finalmente, el desarrollo de una plataforma digital para el diagnóstico del nivel de seguridad de la información resulto ser un desarrollo que proporciona a las empresas una herramienta para mejorar su nivel de seguridad de la información, y con ello mejorar su nivel de calidad como empresa en general lo cual le genera un valor agregado a la misma.

Literatura citada

Barafort, B., Mesquida, A.-L., & Mas, A. (2017). Integrating risk management in IT settings from ISO standards and management systems perspectives. *Computer Standards & Interfaces*, *54*, 176–185. https://doi.org/10.1016/j.csi.2016.11.010

Calder, A. (2013). *ISO27001 / ISO27002: A Pocket Guide*. IT Governance Publishing.

Fajar, A. N., Christian, H., & Girsang, A. S. (2018). Evaluation of ISO 27001 implementation towards information security of cloud service customer in PT. IndoDev Niaga Internet. *Journal of Physics: Conference Series*, *1090*, 012060. https://doi.org/10.1088/1742-6596/1090/1/012060

Gunaratna, S. (2016). *LinkedIn: 2012 data breach much worse than we thought*. https://www.cbsnews.com/news/linkedin-2012-data-breach-hack-much-worse-than-we-thought-passwords-emails/

Haff, G., Henry, W. (2017). From Pots and Vats To Programs and Apps. How software learned to package itself. 2–20.

ISOTools. (2019). *ISO 27001—Software ISO 27001 de Sistemas de Gestión*. https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

ISOTools Excellence. (2013). *La importancia de la norma ISO 27001*. PMG SSI - ISO 27001. https://www.pmg-ssi.com/2015/04/la-importancia-de-la-norma-iso-27001/

Jiménez, J. (2017). *Los ataques informáticos más importantes de la historia.* redes zone. https://www.redeszone.net/2017/11/18/los-ataques-informaticos-mas-importantes-la-historia/

Kelion, L. (2014, mayo 21). EBay makes users change passwords. *BBC News*. https://www.bbc.com/news/technology-27503290

LLC, P. I. (2012). *2011 Cost of Data Breach Study: United States*. https://www.ponemon.org/local/upload/file/2011_US_CODB_FINAL_5.pdf

Maldonado, G. B., & Cano, J. A. O. (2014). Metodología de la seguridad de la información como medida de protección en pequeñas empresas. *Cuaderno Activa*, *6*, 71–77.

Mendoza, M. A. (2015, julio 2). *¿Cuál es la idea central de aplicar ISO 27001?* WeLiveSecurity. https://www.welivesecurity.com/la-es/2015/07/02/idea-central-aplicar-iso-27001/

Milian, M. (2011). *Sony: Hacker stole PlayStation users' personal info*. CNN. http://www.cnn.com/2011/TECH/gaming.gadgets/04/26/playstation.network.hack/index.html

Perlroth, N. (2017, octubre 3). All 3 Billion Yahoo Accounts Were Affected by 2013 Attack. *The New York Times*. https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html

Riquelme, R. (2019). *Pérdida de datos le cuesta a una empresa en México más de 1 millón de dólares: DELL EMC*. El Economista. https://www.eleconomista.com.mx/tecnologia/Perdida-de-datos-le-cuesta-a-una-empresa-en-Mexico-mas-de-1-millon-de-dolares-DELL-EMC-20190410-0079.html

Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, *36*(2), 215–225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

Standage, T. (2017, octubre 5). *The crooked timber of humanity*. The Economist 1843. https://www.1843magazine.com/technology/rewind/the-crooked-timber-of-humanity

Torres, G. (2017). *¿Qué es un virus informático? | La guía definitiva sobre virus informáticos*. https://www.avg.com/es/signal/what-is-a-computer-virus

Trilnick, C. (1792). Claude Chappe, Sistema de telegrafía óptica (internet mecánica). [Figura]. Recuperado de https://proyectoidis.org/claude-chappe/

Anexos

A.1 Cuestionario de los objetivos de control y sus controles

Preguntas del cuestionario utilizado dentro de la plataforma digital para la medición del nivel de seguridad de la información.

1. Políticas de seguridad de la información. Directrices de gestión de la seguridad de la información. Proporcionar orientación y apoyo a la gestión de la seguridad de la información de acuerdo con los requisitos del negocio, las leyes y normativas pertinentes.

1.1 ¿Están documentadas las políticas, estándares y procedimientos de seguridad de la información en la empresa?

1.2 ¿Se revisan y actualizan periódicamente las políticas, normas y procedimientos de seguridad de la información según sea necesario?

1.3 ¿Se supervisa y se mide el cumplimiento de las políticas de seguridad de la información?

2. Organización de la seguridad de la información. Organización interna.

   Establecer un marco de gestión para iniciar y controlar la implementación de la seguridad de la información dentro de la organización.

2.1 ¿Se encuentran definidas y asignadas todas las responsabilidades en seguridad de la información dentro de la empresa?

2.2 ¿Se realiza una coordinación de gerentes, usuarios administradores y toda persona involucrada en la organización con el fin de asegurar que estén cumpliendo con las políticas de seguridad de la información establecidas por la empresa?

2.3 ¿Se capacita, entrena o educa a los empleados de la empresa sobre las políticas de seguridad de la información establecidas?

2.4 ¿Se atienden rápidamente (dentro de un lapso de 2 días) los incidentes de seguridad de la información que se presentan dentro de la empresa?

2.5 ¿Se encuentran establecidas de manera clara todas las responsabilidades de la seguridad de la información? (Existen personas encargadas de tareas específicas y encargados de supervisar que se estén cumpliendo dichas tareas)

2.6 ¿Existe un proceso definido e implementado para la autorización de facilidades nuevas de procesamiento de información?

2.7 ¿Se revisa regularmente que los requerimientos de confidencialidad o acuerdos de no divulgación reflejen las necesidades de la organización para proteger la información?

2.8 ¿Se tiene definido el termino información confidencial?

2.9 ¿Se tiene definido el tiempo para mantener la información confidencialmente?

2.10 ¿Se tiene definido el uso permitido?

2.11 ¿Se tiene definidas las acciones a llevar por desacuerdo?

2.12 ¿Se tiene establecido con que autoridad supervisora (policía, bomberos, auditores, etc.) se deben reportar y de qué manera se deben reportar los incidentes?

2.13 ¿Se cuenta con asesoría para un mejor conocimiento sobre seguridad de la información a través de grupos especializados en la materia?

2.14 ¿Se reciben asesorías especializadas cuando existe un incidente de seguridad de la información?

Los dispositivos móviles y el teletrabajo

Garantizar la seguridad en el teletrabajo y en el uso de dispositivos móviles.

2.15 ¿Se tiene adoptada una política y medidas de seguridad adecuadas para la protección contra los riesgos de la utilización de dispositivos móviles?

2.16 ¿Se tiene bien expresado cuando es permitido el uso de dispositivos móviles?

2.17 ¿Se tiene implementado una política y medidas de seguridad adecuadas para proteger la información accedida, tratada o almacenada en emplazamientos de teletrabajo?

3. Seguridad relativa a los recursos humanos. (Antes del empleo)

Para asegurarse que los empleados y contratistas entiendan sus responsabilidades y son adecuados para las funciones para las que se consideran.

3.1 ¿Se lleva a cabo una comprobación de los antecedentes de todos los candidatos al puesto de trabajo?

3.2 ¿Se le deja saber al empleado a la hora de su entrevista que se le hará una investigación de sus antecedentes y hasta qué punto llegará dicha investigación?

3.3 ¿Se establecen los términos y condiciones en el contrato de trabajo sobre lo que respecta a la seguridad de la información, tanto hacia el empleado como la organización?

(Durante el empleo)

Asegurar que los empleados y contratistas conozcan y cumplan con sus responsabilidades en seguridad de la información.

3.4 ¿Se le deja claro a los contratistas las normas de seguridad de la información?

3.5 ¿Se exige a los contratistas que cumplan con las reglas de seguridad de la información?

3.6 ¿Se les proporciona a los empleados de la empresa con educación adecuada, conciencias y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según su puesto de trabajo?

3.7 ¿Se les proporciona a los contratistas con educación adecuada, conciencias y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según su puesto de trabajo?

3.8 ¿Existe un proceso (formalmente comunicado) a seguir en caso de que una de las contrapartes del contrato no cumpla con las normas de seguridad de la información y provoque una brecha de seguridad?

Finalización del empleo o cambio en el puesto de trabajo.

Proteger los intereses de la organización como parte del proceso de cambio o finalización del empleo

3.9 ¿Se encuentran definidas las responsabilidades en seguridad de la información y obligaciones que se deben seguir después del cambio o finalización del empleo?

3.10 ¿Se les notifica a los empleados o contratistas las responsabilidades en seguridad de la información y obligaciones que se deben seguir después del cambio o finalización del empleo?

4. Gestión de activos.

Responsabilidad sobre los activos

Identificar los activos de la organización y definir las responsabilidades de protección adecuadas.

4.1 ¿La información y otros activos asociados a la información y a los recursos para el tratamiento de la información se encuentran claramente identificados?

4.2 ¿La información y otros activos asociados a la información y a los recursos para el tratamiento de la información se encuentran en algún inventario y se actualiza periódicamente?

4.3 ¿Se encuentra claramente identificado el hardware y software utilizado en el tratamiento de la información?

4.4 ¿Se lleva un control de las herramientas utilizadas en el tratamiento de la información?

4.5 ¿Se encuentran identificadas, documentadas e implementadas las reglas de uso aceptable de la información y de los activos asociados con los recursos para el tratamiento de la información?

4.6 ¿Los empleados y terceras partes deben devolver (y/o devuelven) los activos de la organización que están en su poder al finalizar su empleo, contrato o acuerdo?

Clasificación de la información.

Asegurar que la información reciba un nivel adecuado de protección de acuerdo con su importancia para la organización.

4.7 ¿La información se encuentra clasificada en términos de la importancia de su revelación frente a requisitos legales, valor, sensibilidad y criticidad ante revelación o modificación no autorizadas?

4.8 ¿Se encuentra implementado un conjunto adecuado de procedimientos para etiquetar la información, de acuerdo con el esquema de clasificación adoptado por la organización?

4.9 ¿Se tiene desarrollado e implementado un conjunto adecuado de procedimientos para la manipulación de la información, de acuerdo con el esquema de clasificación adoptado por la organización?

Manipulación de los soportes.

Evitar la revelación, modificación, eliminación o destrucción no autorizadas de la información almacenada en soportes.

4.10 ¿Se tienen implementados procedimientos para la gestión de los soportes extraíbles, de acuerdo con el esquema de clasificación adoptado por la organización?

4.11 ¿Se cuentan con métodos establecidos para la correcta disposición de soportes de información, para prevenir incidentes de seguridad de la información?

4.12 ¿Los transportes que realicen trayectos fuera de los límites físicos de la organización y que contengan información, se encuentran protegidos contra accesos no autorizados, usos indebidos o deterioro?

5. Control de acceso.

Requisitos de negocio para el control de acceso.

Limitar el acceso a los recursos de tratamiento de la información y a la información.

5.1 ¿Se cuenta con una política de control de acceso, movimientos de entrada y salida para los visitantes a la organización?

5.2 ¿Se encuentra restringida la red para los usuarios dependiendo el uso y puesto para el cual hayan sido autorizados?

Gestión de acceso de usuario.

Garantizar el acceso de usuarios autorizados y evitar el acceso no autorizado a los sistemas y servicios.

5.3 ¿Se tiene un procedimiento formal de registro y retirada de usuarios que hagan posible la asignación de los derechos de acceso?

5.4 ¿Se cuenta con un procedimiento formal para asignar o revocar los derechos de acceso para todos los tipos de usuarios de todos los sistemas y servicios?

5.5 ¿La asignación y el uso de privilegios de acceso se encuentra restringida y controlada?

5.6 ¿La asignación de la información secreta de autenticación está controlada a través de un proceso formal de gestión?

5.7 ¿Los propietarios de los activos realizan revisiones de derechos de acceso de usuario a intervalos regulares?

5.8 ¿Una vez que un empleado o tercera parte finalizan su empleo, contrato o acuerdo se retiran los derechos de acceso a la información o ajustan en caso de cambio?

Responsabilidades del usuario

Para que los usuarios se hagan responsables de salvaguardar su información de autenticación.

5.9 ¿Se les pide a los usuarios que sigan las prácticas de la organización en el uso de la información secreta de autenticación?

Control de acceso a sistema y aplicaciones.

Prevenir el acceso no autorizado a los sistemas y aplicaciones.

5.10 ¿Se encuentra restringido el acceso a la información y a las funciones de la aplicación, de acuerdo con la política de control de acceso definida?

5.11 ¿Los sistemas y aplicaciones se encuentran controladas por medio de un procedimiento seguro de inicio de sesión?

5.12 ¿Los sistemas para la gestión de contraseñas son interactivas y establecen contraseñas seguras y robustas?

5.13 ¿Se tiene restringido y controlado rigurosamente el uso de utilidades que pueden ser capaces de invalidar los controles del sistema y de la aplicación?

5.14 ¿Se tiene restringido el acceso al código fuente de los programas?

6. Criptografía.

Controles criptográficos.

Garantizar un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y-o integridad de la información.

6.1 ¿Se cuenta con una política sobre el uso de los controles criptográficos para proteger la información?

6.2 ¿Se cuenta con una política sobre el uso, la protección y la duración de las claves de cifrado a lo largo de todo su ciclo de vida?

7. Seguridad física y del entorno.

Áreas seguras.

Prevenir el acceso físico no autorizado, los daños e interferencia a la información de la organización y a los recursos de tratamiento de la información.

7.1 ¿Se tienen establecidos perímetros de seguridad para proteger las áreas que contienen información sensible, así como los recursos de tratamiento de la información?

7.2 ¿Las áreas seguras se encuentran protegidas mediante controles de entrada adecuados, permitiendo de esta manera que únicamente se permita el acceso al personal autorizado?

7.3 ¿Se cuenta con seguridad física diseñada y aplicada para oficinas, despachos y recursos dentro de la empresa?

7.4 ¿Se cuenta con una seguridad física contra desastres naturales, ataques provocados por el hombre o accidentes, que permitan salvaguardar la seguridad de la información?

7.5 ¿Se cuenta con procedimientos diseñados e implementados para trabajar en las áreas seguras?

7.6 ¿Las áreas de carga y descarga y otros puntos donde pueda acceder personal no autorizado a las instalaciones, se encuentran controlados para evitar accesos no autorizados?

Seguridad de los equipos.

Evitar la pérdida, daño, robo o el compromiso de los activos y la interrupción de las operaciones de la organización.

7.7 ¿Los equipos se encuentran situados o protegidos de manera que reduzcan los riesgos de las amenazas y los riesgos ambientales, así como las oportunidades de que se produzcan accesos no autorizados?

7.8 ¿Los equipos se encuentran protegidos contra fallos de alimentación y otras alteraciones causadas por fallo en las instalaciones?

7.9 ¿El cableado eléctrico y de telecomunicaciones que transmite datos o que sirve de soporte a los servicios de información está protegido frente a interceptaciones, interferencias o daños?

7.10 ¿Los equipos reciben un mantenimiento correcto que asegure su disponibilidad y su integridad?

7.11 ¿Se requiere de autorización previa para la extracción de equipos, información o software?

7.12 ¿Los equipos situados fuera de las instalaciones de la organización cuentan con medidas de seguridad?

7.13 ¿Antes de deshacerse de cualquier equipo, se verifica que todo software bajo licencia y dato sensible sea eliminado?

7.14 ¿Se revisan los equipos desatendidos para asegurar que tengan la protección adecuada?

7.15 ¿Las áreas de trabajo se encuentran despejadas de papeles, medios de almacenamiento desmontables y una política de pantalla limpia?

8. Seguridad de las operaciones.

   Procedimiento y responsabilidad operacionales.

   Asegurar el funcionamiento correcto y seguro de las instalaciones de tratamiento de la información.

8.1 ¿Todos los procedimientos operacionales se encuentran documentados y a disposición de todos los usuarios que los necesiten?

8.2 ¿Los cambios en la organización, los procesos de negocio, instalaciones de tratamiento de la información y los sistemas que afectan a la seguridad de la información se encuentran controlados?

8.3 ¿La utilización de los recursos, se encuentra supervisada?

8.4 ¿Se encuentran separados los recursos de desarrollo, pruebas y operación para de esta manera reducir los riesgos de acceso no autorizado o los cambios del sistema en producción?

   Procedimientos y responsabilidades operacionales.

   Asegurar que los recursos de tratamiento de información y la información están protegidos contra malware.

8.5 ¿Existen controles de detección, prevención y recuperación implementados que sirvan como protección contra el código malicioso y procedimientos adecuados de concienciación al usuario?

   Copias de seguridad.

   Evitar la pérdida de datos.

8.6 ¿Se realizan copias de seguridad de la información del software y del sistema?

8.7 ¿Se revisan periódicamente de acuerdo con la política de copias de seguridad acordada?

Registros y supervisión.

Registrar eventos y generar evidencia.

8.8 ¿Se registran, protegen y revisan periódicamente las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información?

8.9 ¿Se encuentran protegidos los dispositivos de registro y la información del registro contra manipulaciones indebidas y acceso no autorizados?

8.10 ¿Se registran, protegen y revisan regularmente las actividades del administrador del sistema y del operador del sistema?

8.11 ¿Los relojes de todos los sistemas de tratamiento de la información dentro de la organización se encuentran sincronizados con una única fuente de tiempo precisa y acordada?

Control de software en explotación.

Asegurar la integridad del software en explotación.

8.12 ¿Se tienen implementados los procedimientos para controlar la instalación del software en explotación?

Gestión de la vulnerabilidad técnica.

Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas.

8.13 ¿Se cuenta con información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información utilizados y se realizan evaluaciones a la exposición que tiene la empresa a dichas vulnerabilidades para poder tomar medidas sobre el riesgo asociado?

8.14 ¿Se tienen establecidos y se aplican reglas que rijan la instalación de software por parte de los usuarios?

Consideraciones sobre la auditoria de sistemas de información.

Minimizar el impacto de las actividades de auditoria en los sistemas operativos.

8.15 ¿Los requisitos y actividades de auditoria que implican comprobaciones en los sistemas operativos son planificados y acordados para minimizar el riesgo de interrupciones en los procesos de negocio?

9. Seguridad de las comunicaciones.

Gestión de la seguridad de las redes.

Asegurar la protección de la información en las redes y los recursos de tratamiento de la información.

9.1 ¿Las redes se encuentran gestionadas y controladas para proteger la información en los sistemas y aplicaciones?

9.2 ¿Se tienen identificados los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red?

9.3 ¿Se tienen segregados en redes distintas los grupos de servicios de información, los usuarios y los sistemas de información?

Intercambio de información.

Mantener la seguridad de la información que se transfiere dentro de una organización y con cualquier entidad externa.

9.4 ¿Se tienen establecidas políticas, procedimientos y controles formales que protegen el intercambio de información mediante el uso de todo tipo de recursos de comunicación?

9.5 ¿Existen acuerdos establecidos para el intercambio seguro de información del negocio y software entre la organización y terceros?

9.6 ¿La información que sea objeto de mensajería se encuentra adecuadamente protegida?

9.7 ¿Los requisitos de los acuerdos de confidencialidad o no revelación están identificados, documentados y son revisados regularmente?

10. Adquisición, desarrollo y mantenimiento de los sistemas de información.

Requisitos de seguridad en los sistemas de información.

Garantizar que la seguridad de la información sea parte integral de los sistemas de información a través de todo el ciclo de vida. Esto también incluye los requisitos para los sistemas de información que proporcionan los servicios a través de redes públicas.

10.1 ¿Los requisitos relacionados con la seguridad de la información se encuentran incluidos en los requisitos para los nuevos sistemas de información o mejoras a los sistemas de información existentes?

10.2 ¿La información involucrada en aplicaciones que pasan a través de redes públicas se encuentra protegida de cualquier actividad fraudulenta, disputa de contrato, revelación y modificaciones no autorizadas?

10.3 ¿La información involucrada en las transacciones de servicios de aplicaciones está protegida para prevenir la transmisión incompleta, errores de enrutamiento, alteración no autorizada del mensaje, revelación, duplicación o reproducción de mensaje no autorizadas?

Seguridad en el desarrollo y en los procesos de soporte.

Garantizar la seguridad de la información que se ha diseñado e implementado en el ciclo de vida de desarrollo de los sistemas de información.

10.4 ¿Se tienen establecidas y se aplican reglas dentro de la empresa para el desarrollo de aplicaciones y sistemas?

10.5 ¿La implantación de cambios a lo largo del ciclo de vida del desarrollo se encuentra controlado mediante el uso de procedimientos formales de control de cambios?

10.6 ¿Las aplicaciones de negocio críticas son revisadas y probadas para garantizar que no existen efectos adversos en las operaciones o la seguridad de la organización cuando se modifican los sistemas operativos?

10.7 ¿Las modificaciones en los paquetes de software son desaconsejadas limitándose a los cambios necesarios y son objetos de un control riguroso?

10.8 ¿Se encuentran establecidos, documentados, mantenidos y aplicados principios de ingeniería de sistemas seguros a todos los esfuerzos de implementación de sistemas de información?

10.9 ¿Está establecido y protegido adecuadamente un entorno de desarrollo seguro para el desarrollo de sistemas y los esfuerzos de integración que cubren todo el ciclo de vida de desarrollo de este?

10.10 ¿Los desarrollos externos de software son supervisados y controlados por la empresa?

10.11 ¿Se realizan pruebas de la seguridad funcional durante el desarrollo de un sistema?

10.12 ¿Se tienen establecidos programas de pruebas de aceptación y criterios relacionados para nuevos sistemas de información, actualizaciones y nuevas versiones?

Datos de prueba.

Asegurar la protección de los datos de prueba.

10.13 ¿Los datos de prueba son seleccionados con cuidado y son protegidos y controlados?

11. Relación con proveedores.

Seguridad en las relaciones con proveedores.

Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.

11.1 ¿Los requisitos de seguridad de la información para la mitigación de los riesgos asociados con el acceso del proveedor a los activos de la organización están acordados con el proveedor y se encuentran documentados?

11.2 ¿Todos los requisitos relacionados con la seguridad de la información están establecidos y acordados con cada proveedor que puede acceder, tratar, almacenar, comunicar o proporcionar componentes de la infraestructura de tecnología de la información?

11.3 ¿Los acuerdos con proveedores incluyen requisitos para hacer frente a los riesgos de seguridad de la información relacionados con las tecnologías de la información y comunicaciones y con la cadena de suministro de productos?

Gestión de la provisión de servicios del proveedor.

Mantener un nivel acordado de seguridad y de provisión de servicios en línea con acuerdos con proveedores.

11.4 ¿La provisión de servicios del proveedor se encuentran controladas, revisadas y auditadas regularmente por la empresa?

11.5 ¿Existe una política y procedimiento implementado para que en caso de que no se otorgue el servicio respecto a lo establecido se pueda minimizar o mitigar el riesgo en los procesos afectados?

12. Gestión de incidentes de seguridad de la información.

Gestión de incidentes de seguridad de la información y mejoras.

Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.

12.1 ¿Se encuentran establecidas las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información?

12.2 ¿Los eventos de seguridad de la información se notifican por los canales de gestión adecuados lo antes posible?

12.3 ¿Los empleados, contratistas, terceras partes, usuarios de los sistemas y servicios de información están obligados a anotar y notificar cualquier punto débil que observen o sospechen que exista en los sistemas o servicios?

12.4 ¿Los eventos de seguridad de la información son evaluados y posteriormente clasificados si son considerados como incidentes de seguridad de la información?

12.5 ¿Los incidentes de seguridad son respondidos de acuerdo con los procedimientos documentados?

12.6 ¿El conocimiento obtenido a partir del análisis y la resolución de incidentes de seguridad de la información es utilizado para reducir la probabilidad de los incidentes en el futuro?

12.7 ¿La organización tiene definidos y aplicados procedimientos para la identificación, recogida, adquisición y preservación de la información que puede servir de evidencia?

13. Aspectos de seguridad de la información para la gestión de la continuidad de negocio.

Continuidad de la seguridad de la información.

La continuidad de la seguridad de la información debe formar parte de los sistemas de gestión de la continuidad de negocio de la organización.

13.1 ¿La empresa tiene determinadas sus necesidades de seguridad de la información y de continuidad para la gestión de la seguridad de la información en situaciones adversas (por ejemplo, durante una crisis o desastre)?

13.2 ¿La empresa tiene establecidos, documentados, implementados y mantenidos procesos, procedimientos y controles para asegurar el nivel requerido de continuidad de la seguridad de la información durante una situación adversa?

13.3 ¿La empresa comprueba los controles establecidos e implementados a intervalos regulares para asegurar que son válidos y eficaces durante situaciones adversas?

Redundancias.

Asegurar la disponibilidad de los recursos de tratamiento de la información.

13.4 ¿Los recursos de tratamiento de la información son implementados con la redundancia suficiente para satisfacer los requisitos de disponibilidad?

Cumplimiento.

Cumplimiento de los requisitos legales contractuales.

Evitar incumplimiento de las obligaciones legales, estatutarias, reglamentarias o contractuales relativas a la seguridad de la información o de los requisitos de seguridad.

13.5 ¿Todos los requisitos pertinentes, tanto legales como regulatorios, estatutarios o contractuales, y el enfoque de la empresa para cumplirlos se encuentran definidos de forma explícita, documentados y se mantienen actualizados para cada sistema de información de la empresa?

13.6 ¿Existen procedimientos adecuados para garantizar el cumplimiento de los requisitos legales regulatorios y contractuales sobre el uso de materiales, con respecto a los cuales puedan existir derechos de propiedad intelectual y sobre el uso de productos de software patentados?

13.7 ¿Los registros están protegidos contra la perdida, destrucción, revelación o acceso no autorizados de acuerdo con los requisitos legales, regulatorios, contractuales y de negocio?

13.8 ¿La protección y privacidad de los datos se encuentra garantizada?

13.9 ¿Los controles criptográficos son utilizados de acuerdo con todos los contratos, leyes y regulaciones pertinentes?

Revisiones de la seguridad de la información.

Garantizar que la seguridad de la información se implementa y opera de acuerdo con las políticas y procedimientos de la organización.

13.10 ¿El enfoque de la organización para la gestión de la información y su implantación, es decir objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información son sometidos a una revisión independiente a intervalos planificados o siempre que se produzcan cambios significativos en la implantación de la seguridad?

13.11 ¿Los directivos aseguran de que todos los procedimientos de seguridad dentro de su área de responsabilidad se realicen correctamente con el fin de cumplir las políticas y normas de seguridad y cualquier otro requisito de seguridad aplicable?

13.12 ¿Los sistemas de información son comprobados periódicamente para asegurar que cumplan con las políticas y normas de seguridad de la información de la empresa?

A.2 Sugerencias a los controles del instrumento de diagnostico

Acciones para realizar para cada pregunta utilizada dentro del instrumento de diagnóstico, el cual está basado en los 114 controles de la norma ISO/IEC 27001.

1. Políticas de seguridad de la información. Directrices de gestión de la seguridad de la información. Proporcionar orientación y apoyo a la gestión de la seguridad de la información de acuerdo con los requisitos del negocio, las leyes y normativas pertinentes.

1.1 Documentar las políticas, estándares y procedimientos de seguridad de la información en la empresa.

1.2 Revisar y actualizar periódicamente las políticas, normas y procedimientos de seguridad de la información según sea necesario.

1.3 Supervisar y medir el cumplimiento de las políticas de seguridad de la información.

2. Organización de la seguridad de la información. Organización interna.

   Establecer un marco de gestión para iniciar y controlar la implementación de la seguridad de la información dentro de la organización.

2.1 Definir y asignar todas las responsabilidades en seguridad de la información dentro de la empresa.

2.2 Realizar una coordinación de gerentes, usuarios administradores y toda persona involucrada en la organización con el fin de asegurar que estén cumpliendo con las políticas de seguridad de la información establecidas por la empresa.

2.3 Capacitar, entrenar o educar a los empleados de la empresa sobre las políticas de seguridad de la información establecidas.

2.4 Atender rápidamente (dentro de un lapso de 2 días) los incidentes de seguridad de la información que se presentan dentro de la empresa.

2.5 Establecer de manera clara todas las responsabilidades de la seguridad de la información y que existan personas encargadas de tareas específicas y encargados de supervisar que se estén cumpliendo dichas tareas.

2.6 Definir un proceso e implementarlo para la autorización de facilidades nuevas de procesamiento de información.

2.7 Revisar regularmente que los requerimientos de confidencialidad o acuerdos de no divulgación reflejen las necesidades de la organización para proteger la información.

2.8 Definir el termino información confidencial.

2.9 Definir el tiempo para mantener la información confidencialmente.

2.10 Definir el uso permitido de la información confidencial.

2.11 Definir las acciones a llevar por desacuerdo de los acuerdos de confidencialidad.

2.12 Establecer con que autoridad supervisora (policía, bomberos, auditores, etc.) se deben reportar y de qué manera se deben reportar los incidentes.

2.13 Contar con asesoría para un mejor conocimiento sobre seguridad de la información a través de grupos especializados en la materia.

2.14 Recibir asesorías especializadas cuando exista un incidente de seguridad de la información.

2.15 Adoptar una política y medidas de seguridad adecuadas para la protección contra los riesgos de la utilización de dispositivos móviles.

2.16 Tener bien expresado cuando es permitido el uso de dispositivos móviles.

2.17 Tener implementada una política y medidas de seguridad adecuadas para proteger la información accedida, tratada o almacenada en emplazamientos de teletrabajo.

3. Seguridad relativa a los recursos humanos. (Antes del empleo)

Para asegurarse que los empleados y contratistas entiendan sus responsabilidades y son adecuados para las funciones para las que se consideran.

3.1 Llevar a cabo una comprobación de los antecedentes de todos los candidatos al puesto de trabajo.

3.2 Dejarle saber al empleado a la hora de su entrevista que se le hará una investigación de sus antecedentes y hasta qué punto llegará dicha investigación.

3.3 Establecer los términos y condiciones en el contrato de trabajo sobre lo que respecta a la seguridad de la información, tanto hacia el empleado como la organización.

3.4 Dejar claro a los contratistas las normas de seguridad de la información.

3.5 Exigir a los contratistas que cumplan con las reglas de seguridad de la información.

3.6 Proporcionar a los empleados de la empresa con educación adecuada, conciencias y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según su puesto de trabajo.

3.7 Proporcionar a los contratistas con educación adecuada, conciencias y capacitación con actualizaciones periódicas sobre las políticas y procedimientos de la organización, según su puesto de trabajo.

3.8 Contar con un proceso (formalmente comunicado) a seguir en caso de que una de las contrapartes del contrato no cumpla con las normas de seguridad de la información y provoque una brecha de seguridad.

3.9 Definir las responsabilidades en seguridad de la información y obligaciones que se deben seguir después del cambio o finalización del empleo.

3.10 Notificar a los empleados o contratistas las responsabilidades en seguridad de la información y obligaciones que se deben seguir después del cambio o finalización del empleo.

4. Gestión de activos.

Responsabilidad sobre los activos

Identificar los activos de la organización y definir las responsabilidades de protección adecuadas.

4.1 Tener claramente identificados los activos asociados a la información y a los recursos para el tratamiento de la información.

4.2 Tener en algún inventario y actualizar periódicamente la información y otros activos asociados a la información y a los recursos para el tratamiento de la información.

4.3 Tener claramente identificado el hardware y software utilizado en el tratamiento de la información.

4.4 Llevar un control de las herramientas utilizadas en el tratamiento de la información.

4.5 Tener identificadas, documentadas e implementadas las reglas de uso aceptable de la información y de los activos asociados con los recursos para el tratamiento de la información.

4.6 Los empleados y terceras partes deben devolver (y/o devuelven) los activos de la organización que están en su poder al finalizar su empleo, contrato o acuerdo.

4.7 La información se debe encontrar clasificada en términos de la importancia de su revelación frente a requisitos legales, valor, sensibilidad y criticidad ante revelación o modificación no autorizadas.

4.8 Tener implementado un conjunto adecuado de procedimientos para etiquetar la información, de acuerdo con el esquema de clasificación adoptado por la organización.

4.9 Tener desarrollado e implementado un conjunto adecuado de procedimientos para la manipulación de la información, de acuerdo con el esquema de clasificación adoptado por la organización.

4.10 Tener implementados procedimientos para la gestión de los soportes extraíbles, de acuerdo con el esquema de clasificación adoptado por la organización.

4.11 Contar con métodos establecidos para la correcta disposición de soportes de información, para prevenir incidentes de seguridad de la información.

4.12 Los transportes que realicen trayectos fuera de los límites físicos de la organización y que contengan información, deberán estar protegidos contra accesos no autorizados, usos indebidos o deterioro.

5. Control de acceso.

Requisitos de negocio para el control de acceso.

Limitar el acceso a los recursos de tratamiento de la información y a la información.

5.1 Contar con una política de control de acceso, movimientos de entrada y salida para los visitantes a la organización.

5.2 Tener restringida la red para los usuarios dependiendo el uso y puesto para el cual hayan sido autorizados.

5.3 Tener un procedimiento formal de registro y retirada de usuarios que hagan posible la asignación de los derechos de acceso.

5.4 Contar con un procedimiento formal para asignar o revocar los derechos de acceso para todos los tipos de usuarios de todos los sistemas y servicios.

5.5 La asignación y el uso de privilegios de acceso deberá encontrarse restringida y controlada.

5.6 La asignación de la información secreta de autenticación deberá estar controlada a través de un proceso formal de gestión.

5.7 Los propietarios de los activos deberán realizar revisiones de derechos de acceso de usuario a intervalos regulares.

5.8 Una vez que un empleado o tercera parte finalizan su empleo, contrato o acuerdo se deberán retirar los derechos de acceso a la información o ajustar en caso de cambio.

5.9 Pedir a los usuarios que sigan las prácticas de la organización en el uso de la información secreta de autenticación.

5.10 Se debe tener restringido el acceso a la información y a las funciones de la aplicación, de acuerdo con la política de control de acceso definida.

5.11 Los sistemas y aplicaciones se deben encontrar controlados por medio de un procedimiento seguro de inicio de sesión.

5.12 Los sistemas para la gestión de contraseñas deben ser interactivas y deben establecer contraseñas seguras y robustas.

5.13 Tener restringidos y controlados rigurosamente el uso de utilidades que pueden ser capaces de invalidar los controles del sistema y de la aplicación.

5.14 Tener restringido el acceso al código fuente de los programas.

6. Criptografía.

   Controles criptográficos.

   Garantizar un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y-o integridad de la información.

6.1 Se debe contar con una política sobre el uso de los controles criptográficos para proteger la información.

6.2 Se debe contar con una política sobre el uso, la protección y la duración de las claves de cifrado a lo largo de todo su ciclo de vida.

7. Seguridad física y del entorno.

   Áreas seguras.

   Prevenir el acceso físico no autorizado, los daños e interferencia a la información de la organización y a los recursos de tratamiento de la información.

7.1 Se deben tener establecidos perímetros de seguridad para proteger las áreas que contienen información sensible, así como los recursos de tratamiento de la información.

7.2 Las áreas seguras se deberán encontrar protegidas mediante controles de entrada adecuados, permitiendo de esta manera que únicamente se permita el acceso al personal autorizado.

7.3 Se debe contar con seguridad física diseñada y aplicada para oficinas, despachos y recursos dentro de la empresa.

7.4 Se debe contar con una seguridad física contra desastres naturales, ataques provocados por el hombre o accidentes, que permitan salvaguardar la seguridad de la información.

7.5 Se debe contar con procedimientos diseñados e implementados para trabajar en las áreas seguras.

7.6 Las áreas de carga y descarga y otros puntos donde pueda acceder personal no autorizado a las instalaciones, se deberán encontrar controlados para evitar accesos no autorizados.

7.7 Los equipos deberán encontrarse situados o protegidos de manera que reduzcan los riesgos de las amenazas y los riesgos ambientales, así como las oportunidades de que se produzcan accesos no autorizados.

7.8 Los equipos se deberán encontrar protegidos contra fallos de alimentación y otras alteraciones causadas por fallo en las instalaciones.

7.9 El cableado eléctrico y de telecomunicaciones que transmite datos o que sirve de soporte a los servicios de información deberá estar protegido frente a interceptaciones, interferencias o daños.

7.10 Los equipos deberán recibir un mantenimiento correcto que asegure su disponibilidad y su integridad.

7.11 Se deberá requerir de autorización previa para la extracción de equipos, información o software.

7.12 Los equipos situados fuera de las instalaciones de la organización deberán contar con medidas de seguridad.

7.13 Antes de deshacerse de cualquier equipo, se deberá verificar que todo software bajo licencia y dato sensible sea eliminado.

7.14 Se deben revisar los equipos desatendidos para asegurar que tengan la protección adecuada.

7.15 Las áreas de trabajo se deben encontrar despejadas de papeles, medios de almacenamiento desmontables y una política de pantalla limpia.

8. Seguridad de las operaciones.

Procedimiento y responsabilidad operacionales.

Asegurar el funcionamiento correcto y seguro de las instalaciones de tratamiento de la información.

8.1 Todos los procedimientos operacionales deben estar documentados y a disposición de todos los usuarios que los necesiten.

8.2 Los cambios en la organización, los procesos de negocio, instalaciones de tratamiento de la información y los sistemas que afectan a la seguridad de la información deben encontrarse controlados.

8.3 La utilización de los recursos debe estar supervisada.

8.4 Deben estar separados los recursos de desarrollo, pruebas y operación para de esta manera reducir los riesgos de acceso no autorizado o los cambios del sistema en producción.

8.5 Deben existir controles de detección, prevención y recuperación implementados que sirvan como protección contra el código malicioso y procedimientos adecuados de concienciación al usuario.

8.6 Se deben realizar copias de seguridad de la información del software y del sistema.

8.7 Se deben revisar periódicamente de acuerdo con la política de copias de seguridad acordada.

8.8 Se deben registrar, proteger y revisar periódicamente las actividades de los usuarios, excepciones, fallos y eventos de seguridad de la información.

8.9 Deberán estar protegidos los dispositivos de registro y la información del registro contra manipulaciones indebidas y acceso no autorizados.

8.10 Se deben registrar, proteger y revisar regularmente las actividades del administrador del sistema y del operador del sistema.

8.11 Los relojes de todos los sistemas de tratamiento de la información dentro de la organización deben estar sincronizados con una única fuente de tiempo precisa y acordada.

8.12 Se deben tener implementados los procedimientos para controlar la instalación del software en explotación.

8.13 Se debe contar con información oportuna acerca de las vulnerabilidades técnicas de los sistemas de información utilizados y se realizan evaluaciones a la exposición que tiene la empresa a dichas vulnerabilidades para poder tomar medidas sobre el riesgo asociado.

8.14 Se deben tener establecidos y se deben aplicar reglas que rijan la instalación de software por parte de los usuarios.

8.15 Los requisitos y actividades de auditoria que implican comprobaciones en los sistemas operativos deben ser planificados y acordados para minimizar el riesgo de interrupciones en los procesos de negocio.

9. Seguridad de las comunicaciones.

   Gestión de la seguridad de las redes.

   Asegurar la protección de la información en las redes y los recursos de tratamiento de la información.

9.1 Las redes deben estar gestionadas y controladas para proteger la información en los sistemas y aplicaciones.

9.2 Se deben tener identificados los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red.

9.3 Se deben tener segregados en redes distintas los grupos de servicios de información, los usuarios y los sistemas de información.

9.4 Se deberán tener establecidas políticas, procedimientos y controles formales que protegen el intercambio de información mediante el uso de todo tipo de recursos de comunicación.

9.5 Deben existir acuerdos establecidos para el intercambio seguro de información del negocio y software entre la organización y terceros.

9.6 La información que sea objeto de mensajería debe estar adecuadamente protegida.

9.7 Los requisitos de los acuerdos de confidencialidad o no revelación deberán estar identificados, documentados y son revisados regularmente.

10. Adquisición, desarrollo y mantenimiento de los sistemas de información.

    Requisitos de seguridad en los sistemas de información.

    Garantizar que la seguridad de la información sea parte integral de los sistemas de información a través de todo el ciclo de vida. Esto también incluye los requisitos para los sistemas de información que proporcionan los servicios a través de redes públicas.

10.1 Los requisitos relacionados con la seguridad de la información se deberán encontrar incluidos en los requisitos para los nuevos sistemas de información o mejoras a los sistemas de información existentes.

10.2 La información involucrada en aplicaciones que pasan a través de redes públicas se debe encontrar protegidas de cualquier actividad fraudulenta, disputa de contrato, revelación y modificaciones no autorizadas.

10.3 La información involucrada en las transacciones de servicios de aplicaciones debe estar protegida para prevenir la transmisión incompleta, errores de enrutamiento, alteración no autorizada del mensaje, revelación, duplicación o reproducción de mensaje no autorizadas.

10.4 Se deben tener establecidas y se deben aplicar reglas dentro de la empresa para el desarrollo de aplicaciones y sistemas.

10.5 La implantación de cambios a lo largo del ciclo de vida del desarrollo debe estar controlada mediante el uso de procedimientos formales de control de cambios.

10.6 Las aplicaciones de negocio criticas deber ser revisadas y probadas para garantizar que no existen efectos adversos en las operaciones o la seguridad de la organización cuando se modifican los sistemas operativos.

10.7 Las modificaciones en los paquetes de software deben ser desaconsejadas limitándose a los cambios necesarios y deben ser objetos de un control riguroso.

10.8 Deberán estar establecidos, documentados, mantenidos y aplicados principios de ingeniería de sistemas seguros a todos los esfuerzos de implementación de sistemas de información.

10.9 Deberá estar establecidos y protegidos adecuadamente el entorno de desarrollo seguro para el desarrollo de sistemas y los esfuerzos de integración que cubren todo el ciclo de vida de desarrollo de este.

10.10 Los desarrollos externos de software deben ser supervisados y controlados por la empresa.

10.11 Se deben realizar pruebas de la seguridad funcional durante el desarrollo de un sistema.

10.12 Se deben establecer programas de pruebas de aceptación y criterios relacionados para nuevos sistemas de información, actualizaciones y nuevas versiones.

10.13 Los datos de prueba deben ser seleccionados con cuidado y ser protegidos y controlados.

11. Relación con proveedores.

Seguridad en las relaciones con proveedores.

Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.

11.1 Los requisitos de seguridad de la información para la mitigación de los riesgos asociados con el acceso del proveedor a los activos de la organización deben estar acordados con el proveedor y se deben tener documentados.

11.2 Todos los requisitos relacionados con la seguridad de la información deben estar establecidos y acordados con cada proveedor que puede acceder, tratar, almacenar, comunicar o proporcionar componentes de la infraestructura de tecnología de la información.

11.3 Los acuerdos con proveedores deben incluir requisitos para hacer frente a los riesgos de seguridad de la información relacionados con las tecnologías de la información y comunicaciones y con la cadena de suministro de productos.

11.4 La provisión de servicios del proveedor deben estar controlados, revisados y auditados regularmente por la empresa.

11.5 Debe existir una política y procedimiento implementado para que en caso de que no se otorgue el servicio respecto a lo establecido se pueda minimizar o mitigar el riesgo en los procesos afectados.

12. Gestión de incidentes de seguridad de la información.

Gestión de incidentes de seguridad de la información y mejoras.

Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación de eventos de seguridad y debilidades.

12.1 Se deben tener establecidas las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información.

12.2 Los eventos de seguridad de la información se deben notificar por los canales de gestión adecuados lo antes posible.

12.3 Los empleados, contratistas, terceras partes, usuarios de los sistemas y servicios de información deben estar obligados a anotar y notificar cualquier punto débil que observen o sospechen que exista en los sistemas o servicios.

12.4 Los eventos de seguridad de la información deben ser evaluados y posteriormente clasificados si son considerados como incidentes de seguridad de la información.

12.5 Los incidentes de seguridad deben ser respondidos de acuerdo con los procedimientos documentados.

12.6 El conocimiento obtenido a partir del análisis y la resolución de incidentes de seguridad de la información debe ser utilizado para reducir la probabilidad de los incidentes en el futuro.

12.7 La organización debe tener definidos y aplicados procedimientos para la identificación, recogida, adquisición y preservación de la información que puede servir de evidencia.

13. Aspectos de seguridad de la información para la gestión de la continuidad de negocio.

Continuidad de la seguridad de la información.

La continuidad de la seguridad de la información debe formar parte de los sistemas de gestión de la continuidad de negocio de la organización.

13.1 La empresa debe tener determinados sus necesidades de seguridad de la información y de continuidad para la gestión de la seguridad de la información en situaciones adversas (por ejemplo, durante una crisis o desastre).

13.2 La empresa debe tener establecidos, documentados, implementados y mantenidos procesos, procedimientos y controles para asegurar el nivel requerido de continuidad de la seguridad de la información durante una situación adversa.

13.3 La empresa debe comprobar los controles establecidos e implementados a intervalos regulares para asegurar que son válidos y eficaces durante situaciones adversas.

13.4 Los recursos de tratamiento de la información deben ser implementados con la redundancia suficiente para satisfacer los requisitos de disponibilidad.

13.5 Todos los requisitos pertinentes, tanto legales como regulatorios, estatutarios o contractuales, y el enfoque de la empresa para cumplirlos deben estar definidos de forma explícita, documentados y se deben mantener actualizados para cada sistema de información de la empresa.

13.6 Deben existir procedimientos adecuados para garantizar el cumplimiento de los requisitos legales regulatorios y contractuales sobre el uso de materiales, con respecto a los cuales puedan existir derechos de propiedad intelectual y sobre el uso de productos de software patentados.

13.7 Los registros deben estar protegidos contra la perdida, destrucción, revelación o acceso no autorizados de acuerdo con los requisitos legales, regulatorios, contractuales y de negocio.

13.8 La protección y privacidad de los datos debe encontrarse garantizada.

13.9 Los controles criptográficos deben ser utilizados de acuerdo a todos los contratos, leyes y regulaciones pertinentes.

13.10 El enfoque de la organización para la gestión de la información y su implantación, es decir objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información deben ser sometidos a una revisión independiente a intervalos planificados o siempre que se produzcan cambios significativos en la implantación de la seguridad.

13.11 Los directivos deben asegurarse de que todos los procedimientos de seguridad dentro de su área de responsabilidad se realicen correctamente con el fin de cumplir las políticas y normas de seguridad y cualquier otro requisito de seguridad aplicable.

13.12 Los sistemas de información deben ser comprobados periódicamente para asegurar que cumplan con las políticas y normas de seguridad de la información de la empresa.

A.3 Claridad del problema que resuelve

El objetivo principal del desarrollo de esta plataforma digital es el de brindar un diagnóstico inicial en lo que respecta al nivel de seguridad de la información de una empresa. La información que se proporciona permite al usuario realizar acciones que mejoren la seguridad de la información y con ello incrementar la calidad general de la empresa. Actualmente las herramientas existentes en el mercado proporcionan al usuario un sistema de gestión basado en la norma ISO/IEC 27001, sin embargo, dichas plataformas tienen un alto costo de anualidad, convirtiéndose en una opción costosa para pequeñas y medianas empresas. Este software permite identificar de manera sencilla y clara las acciones de mejora que pueden ser realizadas, determinar la viabilidad de contratar un sistema de gestión de seguridad de la información e identificar su nivel de seguridad de la información a un bajo costo, haciéndolo accesible a todo tipo de empresas.

A.4 Integración de un paquete tecnológico

Con lo que respecta a un paquete tecnológico transferible a las empresas interesadas en hacer uso de esta plataforma, se propone la integración de diferentes elementos los cuales serán de utilidad en el uso correcto y eficiente de dicha tecnología. A continuación, se muestran a manera de lista los elementos de dicho paquete:

- Manual de usuario.
- Manual técnico.
- Programa computacional.

El usuario recibirá lo mencionado en los puntos anteriores de manera digital, esto con el fin de contribuir al cuidado del medio ambiente reduciendo el uso y deshecho de papel, plástico y otros desechables. Las actualizaciones a dicha plataforma serian realizadas directamente en el servidor, con ello, reduciendo las emisiones relacionadas con empaquetamiento y distribución. De igual manera, todos los manuales y así mismo las actualizaciones a los mismos junto con adiciones al paquete propuesto, serán almacenadas dentro del repositorio de la aplicación, al cual el usuario tendrá acceso durante el plazo de su membresía.

A.5 Análisis de pertinencia

Para poder hacer uso de la plataforma digital desarrollada, una empresa o bien el usuario que se encontrará utilizando dicho software, debe contar con un conocimiento detallado de lo que respecta y relaciona a la seguridad de la información dentro de la institución. Se debe tener en cuenta que, de no contar con el conocimiento necesario, las preguntas no podrán ser contestadas de manera certera, a lo que el diagnostico no será del todo correcto. Así mismo, se requiere de una computadora con un sistema operativo actualizado, un navegador de internet y una versión de Java instalada. También, se debe contar con una conexión a internet confiable ya que el sistema se encontrará alojado en un servidor y el almacenamiento de los datos requiere de una conexión a la base de datos.

A.6 Análisis de viabilidad de éxito

El lienzo de modelo de negocio o Business Model Canvas por su nombre en inglés, es una plantilla de gestión estratégica para el desarrollo de nuevos modelos de negocio o documentar los ya existentes.
A continuación, se presenta el modelo de negocios para el desarrollo propuesto:

- Infraestructura
    - Actividades clave: crear una plataforma digital que permita a un usuario obtener su nivel de seguridad de la información y con ello, una serie de acciones de mejora en las áreas que fue evaluado.
    - Recursos clave: acciones de mejora propuestas en base a las áreas en las que la empresa puede implementar controles de seguridad de la información.
- Oferta
    - Oferta de valor: el producto ofrece una interfaz amigable, a un bajo costo que ayuda a reducir riesgos respecto a la seguridad de la información.
- Clientes
    - Nicho de mercado: PyMes.
- Canales
    - El canal de entrega será a través de canales propios.
- Relaciones con los clientes
    - El tipo de relación con los clientes será en forma de interacción empleado-cliente. Esta asistencia se llevará a cabo durante y/o después de las ventas.

Así mismo, se presenta un análisis FODA, el cual es una herramienta de estudio de la situación de una empresa, institución, proyecto o persona, analizando sus características internas y su situación externa en una matriz cuadrada.

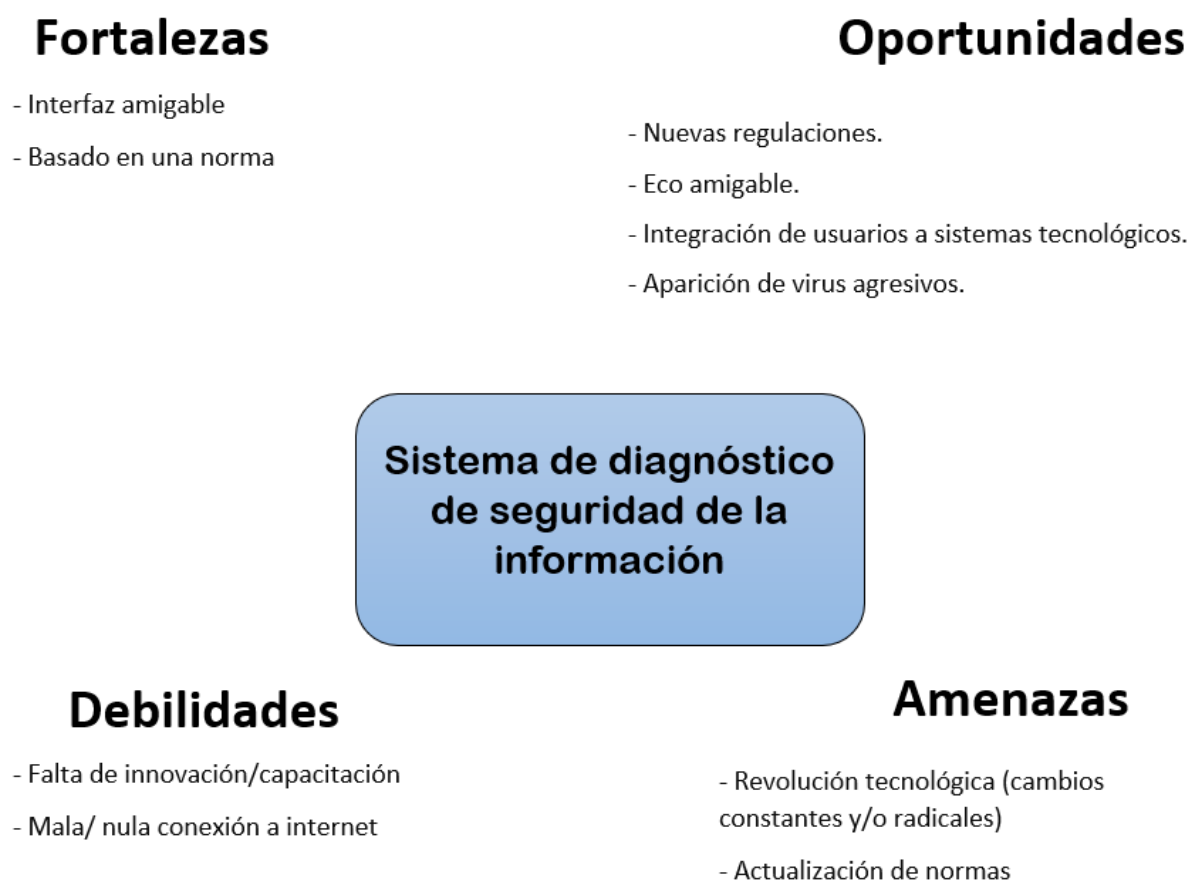

Figura 28. Análisis FODA. Elaboración propia.

Como se observa en la figura 28, las fortalezas son una interfaz amigable que permite el fácil uso de la herramienta y que dicho desarrollo esta basado en una norma. En lo que respecta a las oportunidades, los países solicitan que las empresas se encuentren reguladas sobre una norma de seguridad. De igual manera, la plataforma será ecológica mediante la reducción de papeles, cartones, plásticos y otros desechables. También, la aparición de virus más complejos creara presión para que las empresas tomen acciones sobre sus medidas de seguridad de la información. Por otra parte, las debilidades identificadas son la falta de innovación y/o capacitación de los desarrolladores, así como la falta o mala conectividad de internet, debido que el software requiere de una conexión estable para el uso de la plataforma.

Por último, las amenazas presentadas son la revolución tecnológica y la actualización de normas, ya que si la norma ISO/IEC 27001 sufre una actualización a sus controles establecidos el instrumento no tendrá validez y se deberá crear nuevamente para asegurar la correcta emisión de los diagnósticos.

A.6.1 Estudio de mercado

Los clientes potenciales del desarrollo realizado son pequeñas y medianas empresas, esto debido a el bajo costo que tendrá el uso de dicha plataforma. La necesidad de las empresas de contar con políticas de seguridad de la información incrementa con el avance de las tecnologías y surgimiento de nuevos riesgos. El alto costo de las actuales herramientas representa un impedimento para las pequeñas y medianas empresas que no cuentan con el sustento económico para solventar dicha necesidad. La cantidad de clientes potenciales abarca todas las pequeñas y medianas empresas que deseen obtener un diagnostico inicial sobre su nivel de seguridad de la información, así como conocer las posibles acciones de mejora que puedan realizar con el fin de mejorar su calidad de seguridad de la información.

A.7 Impactos potenciales y esperados para el beneficiario

Dicho proyecto le proveerá al usuario acciones de mejora sobre la seguridad de la información de su empresa, con ello el 100% de los empleados de la empresa se verán beneficiados mediante la implementación de políticas y acciones de control contra riesgos potenciales. Hay que destacar que el aumento de las políticas y controles de seguridad de la información traerán consigo un aumento alrededor del 10% de la calidad general de la empresa, esto considerando que las acciones sean llevadas a cabo.