

Universidad CENFOTEC

Dirección Académica de Posgrados

Maestría Profesional en Ciberseguridad

Análisis y detección de vulnerabilidades en el sistema de gestión y operación de una asociación solidarista.

Proyecto final de graduación presentado como requisito

para optar por la Maestría Profesional en Ciberseguridad

Elaborado por:

Aissen Rodolfo Contreras Castro

2 de Julio del 2021

I. Declaratoria de derecho de autor

Se declara que el presente proyecto de investigación fue realizado por el autor, Aissen Rodolfo Contreras Castro, fundamentado en los diferentes capítulos del trabajo en fuentes bibliográficas, literatura citada, las cuales tienen su respectiva referencia, respetando los derechos de autor de dichos trabajos. De igual manera se tomó como referencia los datos recopilados, a través de las entrevistas realizadas, en las cuales se reflejan los comentarios de los profesionales entrevistados.

Se autoriza la reproducción total o parcial de este trabajo, para ser usados como referencia de trabajos futuros de tipo académico y científico. En este caso, se solicita incorporar la referencia de este trabajo respetando los derechos de los autores.

II. Dedicatoria

A Dios, por haberme permitido llegar hasta este punto, haberme dado salud y coherencia para lograr mis objetivos.

A mi madre, Adriana Castro, por darme la vida y prepararme para las adversidades de la vida. A mi hermana, Heyddri Contreras, por ser mi soporte tácito en todo momento. A mi padre, Alejandro Contreras, por cuidarme desde el cielo y haberme dado una lección de vida que nunca esperé recibir. A Andrea Vargas, por ser mi apoyo incondicional en los momentos más difíciles y mi copiloto oficial.

III. Agradecimientos

Agradezco, asimismo, a L. L. Bean Costa Rica, por haberme patrocinado para cursar la carrera de Maestría Profesional en Ciberseguridad. Sin ellos, esto no hubiera sido posible.

Al profesor Dennis Durán, por guiarme durante esta carrera, tanto como profesor de varios cursos, así como el tutor de mi tesis.

IV. Epígrafe

”La muerte no nos roba los seres amados. Al contrario, nos los guarda y nos los inmortaliza en el recuerdo. La vida sí que nos los roba muchas veces y definitivamente.”

François Mauriac.

universidad cenfotec
tecnologías digitales

Universidad Cenfotec
Carrera de Postgrado
Maestría en Ciberseguridad

Acta N° 110

En conformidad con la reglamentación de la Universidad Cenfotec, se inscribe al estudiante, ***Aissen Rodolfo Contreras Castro***, número de identificación ***112960785***, de la carrera: Maestría en Ciberseguridad, quien presentó y defendió su Proyecto de Investigación Aplicada 2, titulado: ***"Análisis y detección de vulnerabilidades en el sistema de gestión y operación de una Asociación Solidarista".***

Para optar por el grado de: **Maestría en Ciberseguridad**.

Una vez concluida la exposición, el periodo de preguntas y efectuada la deliberación se otorga la calificación de:

[X] Aprobado

[ ] Reprobado. Razones por las que reprobó: _____

_____

Documento escrito:	66,33	*70%
Defensa:	29,66	*30%
Nota obtenida:	96	

*Promedio simple de los miembros del tribunal examinador

Por sus méritos, el Tribunal recomienda la distinción:

[X] Sin distinción

[ ] Cum Laude

[ ] Magna Cum Laude

[ ] Summa Cum Laude

universidad cenfotec

Firmamos conforme, el **02 de julio de 2021**, a las **19:10** horas.

DENNIS ALONSO DURAN CESPEDES (FIRMA) — Firmado digitalmente por DENNIS ALONSO DURAN CESPEDES (FIRMA) Fecha: 2021.07.08 14:24:50 -06'00'

M. Sc. Dennis Durán Céspedes
Tutor

M. Seg. Carlos Raúl Cambronero Sánchez

IGNACIO TREJOS ZELAYA (FIRMA) — Firmado digitalmente por IGNACIO TREJOS ZELAYA (FIRMA) Fecha: 2021.07.08 18:10:33 -06'00'

M. Sc. Ignacio Trejos Zelaya
Lector 2

Firmado digitalmente, de conformidad con la Ley de Certificados, Firmas Digitales y Documentos Electrónicos N° 8454, destacando el artículo 9°.

Tabla de Contenido.

Abstract..... 1

Capítulo 1..... 2

Introducción 2

1.2 Antecedentes del Problema..... 3

1.3 Definición y Descripción del Problema..... 3

1.4 Justificación..... 4

1.5 Viabilidad..... 5

1.5.1 Punto de Vista Técnico...... 5

1.5.2 Punto de Vista Operativo. 5

1.5.3 Punto de Vista Económico...... 6

1.6 Objetivos..... 6

1.6.1 Objetivo General. 6

1.6.2 Objetivos Específicos...... 6

1.7 Alcances y Limitaciones 7

1.7.1 Alcances. 7

1.7.2 Limitaciones. 7

1.8 Marco de Referencia Organizacional y Socioeconómico..... 8

1.9 Estado de la Cuestión..... 13

Capítulo 2..... 24

Marco Teórico o Conceptual. 24

2.1 Introducción. 25

2.2 Concepto de Contenidos. 26

2.2.1 Asociación Solidarista. 26

2.2.2 Junta Administrativa. 27

2.2.3 Dividendos. 27

2.2.4 Asociados. 27

2.2.5 Software. 27

2.2.6 Empleados. 28

2.2.7 Gestión de Crédito. 28

2.2.8 Gestión de Ahorro 28

Capítulo 3. ..... **29**

Marco Metodológico **29**

3.1 Tipo de Investigación 30

3.2 Alcance Investigativo 30

3.3 Enfoque 31

3.4 Diseño 33

Capítulo 4. ..... **35**

Análisis del Diagnóstico **35**

4.1 Software. 37

4.1.1 Microsoft Windows. 37

4.1.2 Microsoft Office. 37

4.1.3.1 Ventana de inicio. 38

4.1.3.2 Ventana de versión del sistema. 39

4.1.3.3 Ventana de ingreso de usuarios. 39

4.1.3.4 Ventana de cambio de contraseñas. 40

4.1.3.5 Ventana de Información de Soporte del Software. 41

4.1.3.6 Ventana de Configuración del Software. 42

4.1.3.7 Ventana de Inicio del Software. 43

4.1.4 Antivirus. 44

4.2.2 Equipo de TI. 44

4.2.3 Conexiones de red. 44

4.3 Mantenimiento. 44

4.3.1 Mantenimiento equipo de TI. 44

4.3.2 Mantenimiento bases de datos. 45

4.4 Respaldos. 45

4.4.1 Respaldo de Información. 45

4.4.2 Respaldo de Electricidad. 45

4.4.3 Respaldo de conexión a Internet. 46

4.5 Seguridad física. 46

4.5.1 Vigilancia y Monitoreo. 46

4.5.2 Perímetros físicos. 47

4.6 Políticas. 47

4.6.1 Política de gestión de contraseñas. 47

4.6.2 Política de gestión de datos. 47

4.6.3 Política de Seguridad y Continuidad del Negocio. 48

Capítulo 5. ..... **49**

Propuesta de Solución **49**

5.1 Solución de Gama Alta. 50

5.2 Solución de Gama Media. 53

5.3 Solución de Gama Entrada. 56

Capítulo 6. ..... **59**

Conclusiones y Recomendaciones **59**

6.2 Recomendaciones 61

Capítulo 7. ..... **62**

Reflexiones Finales **62**

Referencias **66**

Tablas

Tabla 1: Listado de palabras. 15

Tabla 2: Estudios encontrados en Google Scholar. Fuente Propia 21

Tabla 3 Resultados de búsqueda en ACM Digital Library. 22

Tabla 4: Análisis de Resultados de las búsquedas. 23

Tabla 5: Propuesta Gama Alta. Elaboración Propia 52

Tabla 6: Propuesta Gama Media. Elaboración Propia 55

Tabla 7: Propuesta Gama de Entrada. Elaboración Propia. 58

Tabla de Ilustraciones

Ilustración 1 Ejecución de la búsqueda en Google Scholar 19

Ilustración 2: Resultado de búsqueda en ACM Digital Library. 21

Ilustración 3: Nube de Conceptos. 25

Ilustración 4 Composición de una Asociación Solidarista. 26

Ilustración 5: Servicios ASOMIRAVALLE. (Guadamuz Vargas, 2021)..... 36

Ilustración 6: Ventana de inicio de Quarzo. (Guadamuz Vargas, 2021)..... 38

Ilustración 7: Versión del Sistema. (Guadamuz Vargas, 2021) 39

Ilustración 8: Ingreso de Usuarios..... 40

Ilustración 9: Cambio de Contraseña. 40

Ilustración 10: Información de Soporte. (Guadamuz Vargas, 2021)..... 41

Ilustración 11. Configuración del Software. (Guadamuz Vargas, 2021)..... 42

Ilustración 12. Ventana de Inicio del Software. (Guadamuz Vargas, 2021) 43

Ilustración 15: Pilares de la Información. (Forero, 2020)..... 64

Abstract

El uso seguro de sistemas informáticos se convierte a diario en una obligación más por parte del usuario que del desarrollador. Desde el manejo personal de contraseñas hasta la información de los usuarios almacenada en el sistema y cómo esté almacenada. Esta información es parte de las vulnerabilidades que puede llegar a enfrentar las empresas cuando manejan software de este tipo. El objetivo del presente trabajo consiste en identificar y analizar las vulnerabilidades, para proponer una lista de recomendaciones y correcciones que se puedan aplicar en la asociación solidarista, con el fin de mitigarlas y mejorar a diario la gestión de la operación.

Palabras claves: vulnerabilidades, gestión software, gestión acceso, detección, mitigar, ataques, alcances, limitaciones, asociación solidarista, investigación, objetivos, estado de la cuestión, aporte, innovación, viabilidad, alcances, limitaciones.

Capítulo 1.

Introducción

1.1 Generalidades

La propuesta de la presente investigación consiste en analizar las prácticas y estrategias desde la óptica de la ciberseguridad de la operación de la asociación solidarista del centro educativo Miravalle (por las siglas ASOMIRAVALLE), considerando las fortalezas y debilidades así mismo de una reflexión profunda sobre las mejoras que pueden ser implementadas para asegurar la validez de las transacciones y el buen manejo de la información relevante.

1.2 Antecedentes del Problema

Ante las modificaciones de la legislación y los requerimientos de las instituciones reguladoras del sistema financiero nacional y el giro de negocios en la administración, colocación y captación de recursos de sus asociados, se identifican y analizan diversos factores que impactan la práctica diaria, los potenciales riesgos, en lo posible, robustecer los sistemas y acortar las brechas de seguridad.

1.3 Definición y descripción del Problema

Adicionalmente, el proyecto plantea la estructura que se desea emplear para desarrollar un plan remedial que mitigue el impacto que genera la falta de estrategias de administración y control de la información en especial respecto al manejo de históricos, respaldos de bases de datos, accesos y contraseñas. Donde se fomenten procedimientos claros y saludables para lograr una estabilidad económica, incluyendo el ahorro como parte de una cultura para descubrir la libertad financiera. Dicha investigación consta de la siguiente estructura:

Para lograr un mejor entendimiento de las operaciones, se realiza una breve descripción de las generalidades del solidarismo desde su creación hasta el marco

legal en el que actualmente se desempeña esta forma de organización. Seguidamente, se hace referencia a los enfoques teóricos de la cartera de inversiones para obtener un mejor entendimiento del ámbito donde se desarrolla este trabajo.

En la siguiente sección se hace referencia al proceso de edificación del conocimiento compuesto por el marco contextual, que comprende el tema investigado, el marco histórico y, finalmente, el marco conceptual necesario para constituir las partes del problema en investigación.

Esta sección se enfoca en el análisis de la situación diagnosticada, donde se presenta el resultado de la investigación de una forma gráfica, así como su correspondiente análisis e interpretación del resultado, abriendo camino a las conclusiones y recomendaciones, así como la presentación de la propuesta.

De acuerdo con los resultados obtenidos, se sustentan una serie de conclusiones y recomendaciones derivadas del producto de los objetivos de la investigación inicialmente planteados para solventar la problemática expuesta en el primer capítulo.

1.4 Justificación

La fragilidad de la información de más de veinte años de antigüedad deja expuesto a cualquier negocio de pequeña o gran escala, ante las habilidades desarrolladas por los ciber delincuentes. Esto reviste de suma importancia para el patrono, que deposita en la Asociación Solidarista los aportes equivalentes a la cesantía y que ante la finalización repentina del contrato laboral salvaguarda su responsabilidad. Asimismo, para el empleado que, aunado al aporte patronal, realiza sus aportes personales en espera de ser recompensado con beneficios en especie y

la retribución a través de los excedentes determinado por la capacidad de la administración y la junta directiva de maximizar los resultados financieros en respuesta a una buena administración, seguridad y control.

La Asociación recibirá un diagnóstico de la capacidad actual, así como la recomendación práctica de las pautas desde un mensaje coloquial y de potencial ejecución, equivalente al valor agregado, por la oportunidad de desarrollar una investigación de esta índole.

1.5 Viabilidad

La viabilidad de este proyecto se puede enfocar en las facetas que van a determinar si el proyecto es factible o no.

1.5.1 Punto de vista técnico.

La guía que se tiene pensado crear es un manual de buenas prácticas y procedimientos según diversas fuentes académicas e investigativas, con el fin de proveer un instrumento de ayuda a la Asociación para mejorar sus operaciones diarias y evitar cualquier tipo de inconveniente en el futuro, que se hubiese podido solventar de manera eficiente y eficaz en el pasado.

1.5.2 Punto de vista operativo.

La parte operacional de esta guía recae en los investigadores, que desarrollaron este componente dentro del marco práctico que se pretendía. Una vez que este sea distribuido dentro de la Asociación y junta directiva, la ejecución y uso del manual deberá recaer en el personal de los departamentos administrativos y la misma junta para aplicarlo.

1.5.3 Punto de vista económico.

Al ser un proyecto de investigación y creación de un manual, realmente no se requiere una inversión mayor a las horas-hombre destinadas para la investigación y creación del manual. A un promedio de $100 la hora por esfuerzo de recurso, este proyecto se estima preliminarmente a tardar unas 8 horas semanales (esfuerzo parcial de trabajo). En 4 meses sumaría un total de 137 horas, que resultarían en un costo preliminar de $13760,00 (sin estimar otros gastos e imprevistos).

1.6 Objetivos

Para la redacción de estos objetivos se utilizó la taxonomía de Bloom de 1956, debido a que la estructura jerárquica facilita la definición de los objetivos desde los niveles básicos hasta los más complejos. Además de ser las más utilizada a nivel nacional en diferentes áreas como lo son las académicas.

1.6.1 Objetivo general.

Crear una guía de análisis y detección de las vulnerabilidades en el sistema de gestión y operación en la asociación solidarista.

1.6.2 Objetivos específicos.

A. Analizar el proceso actual del sistema de gestión y operación que se usa en la asociación solidarista para su análisis.
B. Formular una lista de posibles vulnerabilidades en el sistema de gestión y operación de la asociación solidarista que se van a utilizar en el siguiente proceso.

C. Elaborar una lista de recomendaciones y soluciones para mitigar los riesgos que se hayan detectado en el proceso anterior.
D. Desglosar todas y cada uno de las posibles vulnerabilidades y sus respectivas soluciones ante la junta de la asociación solidarista.

1.7 Alcances y limitaciones.

Este proyecto contempla la elaboración de una guía con un análisis de vulnerabilidades y sus recomendaciones para mitigarlas.

1.7.1 Alcances.

A continuación, se describe el alcance del proyecto.

Los entregables están compuestos por:

- Un documento escrito con el análisis y la detección de todas las vulnerabilidades encontradas en el sistema de gestión y operación en la asociación solidarista.
- Una reunión con los miembros de la junta para exponer el trabajo de análisis y detección de vulnerabilidades con sus recomendaciones para mitigarlas.

1.7.2 Limitaciones.

Este proyecto no contempla la realización de lo siguiente:

- Desarrollo de software, alguno que pudiese ser necesario para mitigar alguna de las vulnerabilidades previamente detectadas.
- Instalación y configuración de hardware, alguno que pudiese ser necesario para mitigar alguna vulnerabilidad detectada.

Debido a la situación de la pandemia mundial del COVID-19, resultó imposible visitar las instalaciones y reunirse con el personal administrativo y de TI de la Asociación.

1.8 Marco de Referencia Organizacional y Socioeconómico

Existen 1472 asociaciones solidaristas (Quarzo, 2020) que se encargan de promover la economía nacional mediante productos financieros de colocación y captación. Al amparo de la regulación nacional y bajo la supervisión del Banco Central y la Superintendencia General de Entidades Financieras (SUGEF). De manera directa y por el capital administrado solamente 5 asociaciones solidaristas a nivel Nacional son directamente reguladas e intervenidas. Para las asociaciones con capitales inferiores a 100000 colones, el cumplimiento se limita a la presentación de la reserva de capital semestral equivalente al 15% del patrimonio (buscar en BCCR).

Aproximadamente realizan colocaciones por más de 500.000 microcréditos semanales. Algunas asociaciones han sufrido procesos de quiebra por manejos inapropiados de los recursos y por robos, en virtud de una incapacidad operativa y pocas habilidades en el manejo de una operación a escala (o gota a gota). Se requiere de información específica y software o sistemas informáticos competentes. Parte de la responsabilidad de ineficientes controles recaerá en el patrono, quien está expuesto a sanciones por parte del Ministerio de Trabajo.

1.8.1 Historia.

Dado el crecimiento del negocio educativo privado, llamado centro educativo Miravalle, ubicado en la provincia de Cartago, los empleados, de la mano de la junta directiva, se proponen la misión de “Procurar la justicia y la paz social, armonía obrero-patronal y el desarrollo integral de sus asociados” (Ley No. 7960, 1984) el 29 de junio de 1999, tomo 1, folio 153, asiento 134, se inscribe la Asociación Solidarista de Empleados del Centro Docente Miravalle, por sus siglas ASOMIRAVALLE (personería jurídica, 2020), superando por mínimo el número requerido de empleados. La operación continúa en marcha y actualmente la institución cuenta con más de 100 empleados directos, de los cuales el 60% aproximadamente forman parte de la Asociación Solidarista.

A través de los años, las utilidades denominadas “excedentes” fueron creciendo y ASOMIRAVALLE trasladó beneficios monetarios a sus asociados. Adicionalmente, incursionó en negocios relacionados con la operación del centro educativo como la venta de uniformes, la participación en ferias y la apertura de una librería. Lamentablemente, en el año 2012, producto de una administración desacertada y decisiones financieras poco claras, fue necesario, por instrucción de la junta directiva del centro docente Miravalle, realizar una intervención que significó la absorción significativa de una pérdida proporcional de los aportes personales por parte de todos los involucrados (patrono y empleados).

La situación que se presentó el año 2012 implicó decisiones extremas, como la adquisición de un software financiero contable Oftisol de la compañía Oftisoft (SIBU ERP), que se implementó y puso en marcha ese mismo año, la salida de

asociados y una creciente desconfianza en la capacidad de administración de fondos, ante la problemática de la insolvencia de flujo de efectivo.

Desde el 2013 y hasta el 2014, los cambios constantes en la administración general y la contabilidad arrastraron errores significativos en pérdidas de datos, desorden y desconocimiento de la utilidad real. Por lo tanto, en el 2015 se inicia la reingeniería operativa, que implicó la contratación de un nuevo equipo de trabajo y el enfrentamiento a ajustados resultados, razón por la cual se obtuvo durante ese año, únicamente una utilidad de menos de un 0,01% del patrimonio. (Guadamuz Vargas, 2021)

Desde una perspectiva favorable, el crecimiento de las “Distribuciones periódicas de efectivo” (Gitman, 2016) ha sobrepasado el 200% y, para el 2020, se espera que el crecimiento sea cercano al 60% (Junta Directiva, 2020). Durante el 2019 realizaron un reemplazo de software al sistema CODEAS Fácil de la compañía Quarzo tras considerar costo (se cubrió con provisiones del 2016 al 2019), soporte y recursos informáticos limitados.

El reto para la asociación es demostrar capacidad de generar beneficios a todos los empleados del centro educativo, ofrecer servicios rentables y trascender a través del tiempo.

1.8.2 Tipo de negocio y mercado meta.

Corresponde a los empleados de una organización que potencialmente pueden optar por realizar un aporte mensual que oscila entre el 2% y el 5%. El patrono o dueño del negocio que deposita y el que traslada a la asociación solidarista los capitales correspondientes a la cesantía.

1.8.3 Misión, visión y valores.

A continuación, se detalla la información facilitada por la Administración General elaborada y aprobada en el 2015 que corresponde a:

Misión

Utilizar los principios solidaristas, para ofrecer a nuestros asociados y a sus familias alternativas que mejoren su calidad de vida.

Visión

Propiciar un equilibrio entre los beneficios sociales y económicos, mediante servicios que satisfagan las necesidades de los asociados.

Valores

Mejora continua: fortalecer el trabajo diario en búsqueda de un crecimiento permanente.

Solidaridad: buscar beneficios colectivos.

Lealtad: realizar las labores con constancia y un alto sentido de compromiso.

Compromiso: cumplir con nuestros objetivos apegadas a las leyes y reglamentos que nos rigen.

Prudencia: tomar decisiones financieras sin perjudicar los recursos de los asociados.

1.8.4 Políticas Institucionales.

En la Asociación Solidarista del centro docente Miravalle la máxima autoridad es la Asamblea general de Asociados que se celebra anualmente, quienes en votación pública eligen la junta directiva compuesta por siete miembros, en la cual se incluye el representante legal. Las decisiones de mayor relevancia son tomadas en sesiones de la junta directiva aunadas a la realimentación de la administración general respecto de los resultados en la operación y gobierno corporativo “reglas, procesos que se aplican, el control y la regulación” (Gitman, 2016), para las cuales el secretario prepara un informe con un consecutivo anual que se comparte por correo y se almacena digitalmente. Durante el 2020 las sesiones virtuales se han grabado.

Actualmente, cuentan con un reglamento de crédito que ha estado en discusión por parte de la junta directiva desde el 2019 y no se encuentra aprobado la última versión. Responden a las siguientes legislaciones:

- Ley 7960. Asociaciones Solidaristas.
- Directrices del Banco Central de Costa Rica.
- Contraloría General de la República.
- SUGEF (Superintendencia General de Entidades Financieras)
- Ministerio de Trabajo.
- Movimiento Solidarista Costarricense.
- Escuela Social Juan XXIII.
- Ley 9635. Ley de Fortalecimiento de las Finanzas Públicas.
- Ley 9859. Ley de Promoción de la Competencia y Defensa Efectiva del Consumidor

1.9 Estado de la cuestión

La presente propuesta de análisis tiene como finalidad brindar un listado con las mejoras y buenas prácticas para la operación diaria de una asociación solidarista. El estado de la cuestión será basado en la plantilla de Biolchini para una revisión sistemática.

La herramienta utilizada en esta investigación ha sido el de revisión bibliográfica, la cual consiste en búsquedas intensivas del tema tratado mediante múltiples fuentes de información. En este caso solo fueron consultadas fuentes digitales.

1.9.1 Planificación de la revisión.

Se formula en esta etapa una pregunta clara y bien definida del tema de investigación. Se hace una búsqueda de documentación existente en el tema con el objetivo de conocer el desarrollo académico que existe en este, posibles áreas débiles que se puedan ampliar y verificar que no se estén duplicando los estudios realizados en otras investigaciones.

1.9.1.1 Formulación de la pregunta

La formulación de la pregunta contribuye a precisar y a enfocar el tema y los subtemas de investigación, para una mejor y efectiva búsqueda de las publicaciones.

1.9.1.1.1 Foco de la pregunta.

Se requiere realizar búsquedas de publicaciones enfocadas en el área del análisis y detección de vulnerabilidades, las cuales deben aportar mejoras y buenas

prácticas para el manejo de una asociación solidarista, específicamente en la función de esta.

1.9.1.1.2 Amplitud y calidad de la pregunta

Se establece en este apartado la pregunta de investigación que se desea responder de forma clara y concisa, basados en el problema planteado para el desarrollo de este proyecto educativo. Se hace un listado de términos claves relevantes para la búsqueda de información y se consideran componentes clave como son la población específica, exposición y eventos de interés. Se definieron medidas utilizadas para medir el efecto con base en la pregunta planteada y el diseño del presente estudio.

Problema: En muchas instituciones se empiezan a desarrollar formas de trabajo que no han sido previamente analizadas ni aprobadas para evitar cualquier tipo de vulnerabilidad en estos procesos, arriesgando tanto a la institución como tal, a los empleados y en este caso específico a los afiliados de la asociación solidarista.

Pregunta: Con base en la descripción de la problemática anterior, la pregunta de investigación es: ¿Qué análisis de vulnerabilidades y buenas prácticas existen para gestión segura de una asociación solidarista?

Palabras clave y sinónimos: A continuación, se listan todas las posibles palabras claves para encontrar artículos y publicaciones entorno a la temática de investigación.

Palabra en inglés	Palabra en español
vulnerability	vulnerabilidades
analysis	análisis
detection	detecciones
system	sistema

Tabla 1: Listado de palabras

Intervención: En el contexto de la revisión sistemática, se planea extraer los artículos y publicaciones de mayor relevancia acerca de métodos de análisis y evaluación de vulnerabilidades en diferentes instituciones.

Control: En la presente propuesta de investigación no se cuenta con material bibliográfico inicial.

Efectos: Se espera obtener bibliografía de investigaciones previas de propuestas de mejora y de gestión de entidades financieras para posteriormente analizarlas, compararlas e identificar necesidades de investigación u oportunidades de mejora junto con buenas prácticas y manuales.

Medidas de salida: Como medida de resultado, se espera encontrar múltiples investigaciones de propuestas existentes para la correcta gestión de entidades financieras.

Población: Cualquier publicación sobre análisis y mejoras en instituciones específicamente si son de índole financiero.

Aplicación: Este tipo de investigación puede resultar de utilidad para personas en el área administrativa, donde se necesite aplicar mecanismos y mejoras de buenas prácticas para la gestión de empresas de índole financiero.

Diseño experimental: En el diseño experimental se utilizan los conocimientos previos de publicaciones encontradas como base, para una evaluación del estado actual, para detectar deficiencias y posteriormente proponer posibles áreas de mejora e innovación.

1.9.1.2 Selección de fuentes

Se especifican en este apartado las fuentes para la identificación de estudios primarios que se utilizaron para el desarrollo de esta investigación.

1.9.1.2.1 Definición del criterio de selección de fuentes.

La selección de las fuentes está basada principalmente en dos factores:

1- Experiencia del autor de la presente investigación

2- Popularidad de la fuente, adicionalmente deben ser fuentes donde el acceso a las bibliotecas de publicaciones web sea libre y que se puedan realizar búsquedas avanzadas.

1.9.1.2.2 Lenguaje de estudio.

Se utiliza para el estudio tanto el idioma español como el inglés en lo que respecta a las búsquedas. De esta manera se puede incrementar el rango de posibles resultados.

1.9.1.2.3 Identificación de fuentes.

1. Métodos de búsqueda:

El método de selección de fuentes se basa principalmente en el respaldo con el que cuenta la fuente en el área de tecnología, respecto de la publicación de estudios y documentos investigativos. Además, se considera la facilidad de acceso al sitio y para hacer las búsquedas.

2. Lista de fuentes:

La selección de las fuentes más relevantes y utilizadas para la ejecución de la revisión sistemática están:

- Scholar Google
- Research Gate
- IEEE Xplores DIGITAL LIBRARY
- Springer
- Academia

3. Cadena de búsqueda:

Para la selección de los datos se utilizaron los siguientes criterios de búsqueda:

intitle:"vulnerability" intitle:"analysis" intitle:"detection"

intitle:"vulnerabilities" intitle:"analysis" intitle:"detection"

intile:”detection” intile:”system” intile”software”

intile:”asociacion” intile:”solidarista”

management of good business practices

1.9.1.2.4 Selección de fuentes después de la evaluación:

Las variables para seleccionar las fuentes utilizadas fueron: amigable para realizar cadenas de búsqueda y que los resultados sean documentos confiables.

1.9.1.2.5 Comprobación de las fuentes:

Las fuentes utilizadas fueron seleccionadas con base en recomendaciones de expertos en el área de investigación académica.

1.9.1.3 Selección de los estudios.

En este apartado se describe el criterio final de inclusión y exclusión de las publicaciones previamente identificadas y seleccionar las publicaciones relevantes para análisis final.

1.9.1.3.1 Definición del criterio de inclusión y exclusión de estudios:

Se tomaron en cuenta los estudios que aplican algoritmos de mejora en la gestión de empresas o instituciones enfocadas en el tema financiero.

1.9.1.3.2 Definición de tipos de estudio:

La definición de los tipos de estudios está relacionada con la pregunta de investigación.

1.9.1.3.3 Procedimiento para selección de estudios:

Una vez definidos los criterios de inclusión y exclusión, la selección de los estudios se realizó de la siguiente manera:

Paso número uno: se realiza la lectura del abstract.

Paso número dos: se continua con la Introducción.

Paso número tres: lectura de las conclusiones.

Si estas tres lecturas breves proporcionan el resultado esperado se continúa con la lectura completa del artículo. De lo contrario el artículo se descarta.

1.9.2 Ejecución de la revisión.

Se presenta, a continuación, el proceso de selección llevado a cabo para las diferentes fuentes.

1.9.2.1 Ejecución de la selección en la fuente Google Scholar.

1.9.2.1.1 Selección de estudios iniciales.

Siguiendo las recomendaciones provistas por Blanco, et al. (2007), se realiza la búsqueda de estudios iniciales de la siguiente manera:

Búsqueda basada en los siguientes parámetros:

- Analisys.
- Vulnerabilities.
- Detection.



Ilustración 1 Ejecución de la búsqueda en Google Scholar

Tras realizar la búsqueda utilizando los parámetros mencionados, se encontraron cuatro resultados, de los cuales fueron seleccionados cuatro artículos tras aplicar el método de exclusión propuesto (principalmente, se excluye de la lista artículos que no se enfoquen propiamente en las formas de detección de noticias falsas, aplicando técnicas de “machine learning” o minería de datos). A continuación, se presenta el detalle de estos.

#	Título	Autores	Año	URL
1	A Survey of Security Vulnerability Analysis, Discovery, Detection, and Mitigation on IoT Devices	Yu, M.; Zhuge, J.; Cao, M.; Shi, Z.; Jiang, L.	2020	https://www.mdpi.com/1999-5903/12/2/27
2	Analysis of web application security mechanism and Attack Detection using Vulnerability injection technique	R. V. Bhor; H. K. Khanuja	2016	https://ieeexplore.ieee.org/abstract/document/7860004/authors#authors
3	Web Application Vulnerability Detection Using Taint Analysis and Black-box Testing	Heribertus Yulianton1,2, Agung Trisetyarso1, Wayan Suparta1,3,	2020	https://iopscience.iop.org/article/10.1088/1757-899X/879/1/012031/meta

		Bahtiar Saleh Abbas1 and Chul Ho Kang1		
4	Improving vulnerability detection using program analysis.	Rasmus Hagberg	2020	https://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=9030175&fileOId=9030176

Tabla 2: Estudios encontrados en Google Scholar. Fuente propia

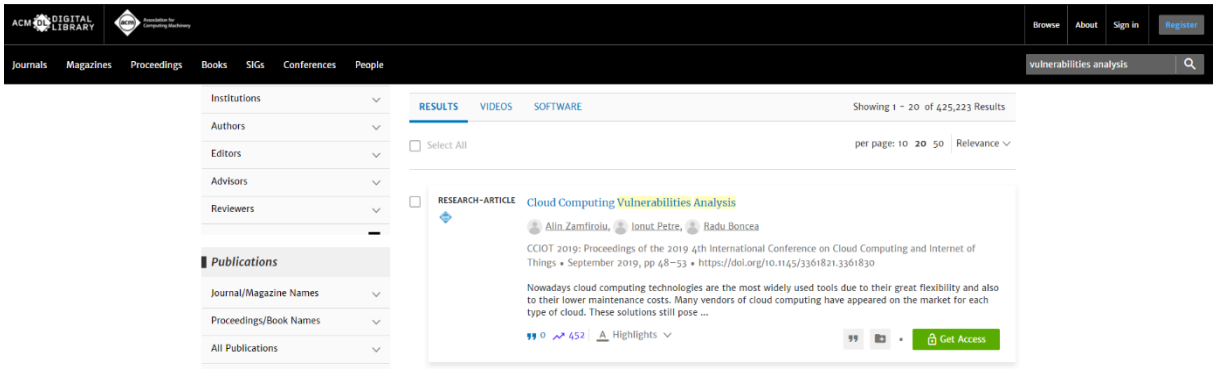


Ilustración 2: Resultado de búsqueda en ACM Digital Library.

#	Título	Autores	Año	URL
1	Cloud Computing Vulnerabilities Analysis	Alin Zamfiroiu, Ionut Petre, Radu Boncea	2019	https://dl.acm.org/doi/10.1145/3361821.3361830

	Analyzing Web Application Vulnerabilities: An Empirical Study on E-Commerce Sector in Bangladesh	Md. Abdur Rahman, Mahfida Amjad profile imageMahfida Amjad, Byezid Ahmed profile imageByezid Ahmed, Md Saeed Siddik profile imageMd. Saeed Siddik	2020	https://dl.acm.org/doi/10.1145/3377049.3377107

Tabla 3 Resultados de búsqueda en ACM Digital Library.

1.9.3 Resumen de los Resultados.

Como parte del proceso de selección de resultados, como se muestra en la tabla X, se analizaron 25 estudios, de los mismos 10 fueron identificados como relevantes, basados en su contenido, número de referencias, año de publicación y calidad. Posterior a esto luego de un proceso de refinamiento se seleccionaron 6 artículos, para los cuales se siguió el proceso de ejecución de la selección detallado en la sección anterior.

Fuente	Estudios	Relevantes	Primarios	Refinados
Google Scholar	17	7	4	0
ACM	8	3	2	0
TOTAL	25	10	6	0

Tabla 4: Análisis de Resultados de las búsquedas.

Capítulo 2.

Marco Teórico o Conceptual.

2.1 Introducción.

Se generó la siguiente nube de conceptos con el objetivo de identificar los conceptos más relevantes mencionados en los diversos artículos incluidos como parte del estado de la cuestión. Es importante mencionar que para la generación de la figura X, se usó el contenido como parte de los resúmenes creados en el estado de la cuestión.

Figura X: Nube de palabras generado utilizando el sitio. Fuente: Elaboración propia.



Ilustración 3: Nube de Conceptos

Elaborado usando el sitio https://www.nubedepalabras.es

2.2 Concepto de contenidos.

Se presenta, a continuación, la definición de los conceptos mayoritariamente mencionados y de mayor relevancia para la investigación. Se debe destacar que, con el fin de brindar un mejor contexto del tema en cuestión, el orden en el que se presentan los conceptos va desde un ámbito general hacía aspectos más específicos necesarios para comprender los diversos elementos asociados al tema.

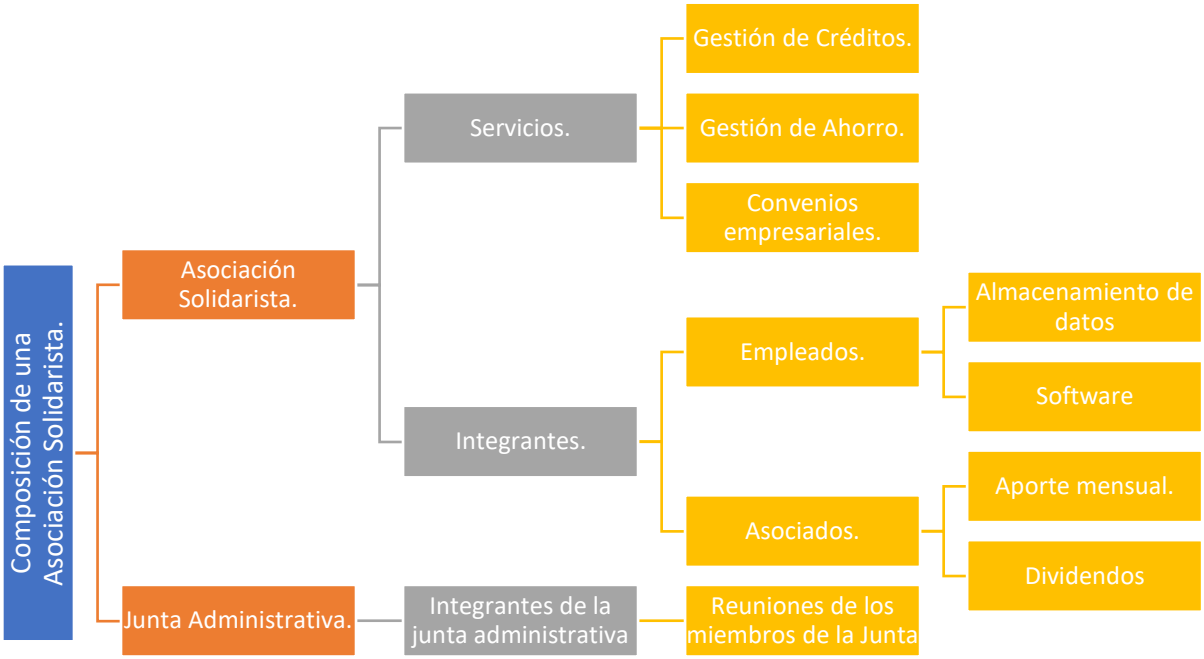


Ilustración 4 Composición de una Asociación Solidarista

2.2.1 Asociación Solidarista.

Las asociaciones solidaristas son organizaciones sociales que se inspiran en una actitud humana, por medio de la cual el hombre se identifica con las necesidades y aspiraciones de sus semejantes, comprometiendo el aporte de sus recursos y esfuerzos para satisfacer esas necesidades y aspiraciones de manera

justa y pacífica. Su gobierno y su administración competen exclusivamente a los trabajadores afiliados a ellas.

2.2.2 Junta Administrativa.

La junta administrativa es el órgano rector, el cual deberá velar por el fiel cumplimiento de las políticas institucionales, para un mejor aprovechamiento de los recursos de que dispone la organización.

2.2.3 Dividendos.

El dividendo es la cuota de dinero de una empresa que se reparte entre los accionistas de una sociedad. Constituye la principal vía de remuneración de los accionistas como propietarios de una sociedad.

2.2.4 Asociados.

Un asociado es una persona o empresa que se junta con otra persona o empresa para un negocio específico. Un asociado "no es dueño de la empresa", tan solo participa en ciertos procesos de esta. No tiene responsabilidades civiles, únicamente en lo que respecta al negocio en particular en que participa.

2.2.5 Software.

Se conoce como software o “logicial” al soporte lógico de un sistema informático, que comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas, en contraposición a los componentes físicos que son llamados hardware.

2.2.6 Empleados.

El empleado es aquella persona que brinda sus servicios a cambio de un salario por parte de un empleador. Así, los detalles de este vínculo son definidos en un contrato (verbal o escrito). Un empleado, en otras palabras, es aquel que realiza una tarea por la cual se le reconoce una remuneración.

Cabe señalar que un empleado puede estar trabajando tanto para una institución privada como para una pública, la que además puede o no tener ánimo de lucro. Por ejemplo, los ministerios y las organizaciones no gubernamentales tienen empleados que reciben un sueldo.

2.2.7 Gestión de crédito.

Sistema que permite a una entidad desde cualquier punto de vista, ya sea como cliente o proveedora del crédito en cuestión, gestionar el proceso general y los pasos de un préstamo, desde el momento que lo solicita hasta que termina de amortizarlo.

2.2.8 Gestión de ahorro

El ahorro es la porción de las rentas que el individuo decide no destinar hoy a su consumo. Entonces, reserva ese capital, fuera cualquier riesgo, para cubrir una necesidad o contingencia futura. Incluso, puede dejarse como herencia. Es decir, el ahorro es el porcentaje de los ingresos que la persona no gasta ni invierte. Así, busca contar con un fondo para un desembolso que deberá efectuar más adelante, por ejemplo.

Capítulo 3.

Marco Metodológico

Este capítulo desarrolla la metodología empleada durante el desarrollo de la investigación, en la cual se destaca de manera principal que este trabajo es teórico, debido a que la información se obtiene a través de entrevistas, cuestionarios, programas de cómputo, observación directa, indirecta e instrumentos que ayudaron a obtener y constituir al final el producto que consta en una serie de buenas prácticas para ser entregado de manera digital a la junta directiva de la asociación donde se va a realizar el trabajo en cuestión.

3.1 Tipo de Investigación

Debido a que el objetivo general de este proyecto consiste en analizar y detectar vulnerabilidades en la gestión de una asociación solidarista, se considera que la siguiente investigación corresponde al tipo investigación evaluativa. Se quiere analizar toda la gestión de la asociación para determinar las posibles vulnerabilidades y la mejor manera de corregirlas por medio de un manual de mejores prácticas. Esto nunca ha sido analizado en esta asociación solidarista, pero en este caso se está realizando no solo un análisis completo de la gestión como tal, sino brindando una serie de lineamientos, si se desea mejorar toda la gestión como tal.

3.2 Alcance Investigativo

Dado el contexto de la presente investigación se consideran los siguientes tipos de investigación.

- Exploratoria

Tomando como referencia la definición de Vargas (2004) sobre investigación exploratoria, la cual indica que este tipo de investigación “tiene por objetivo esencial familiarizar al investigador con un tema no abordado antes, novedoso o escasamente estudiado”. En este caso, si bien hasta la fecha se han realizado distintos esfuerzos en el área de la detección de noticias falsas, lo cierto es que se identificaron pocos estudios de esta clase, en Costa Rica.

- Descriptiva

A fin de justificar este apartado se toma como referencia nuevamente el concepto brindado por Vargas (2004), donde se definen las investigaciones descriptivas de la siguiente manera: “Este tipo de estudio busca especificar las propiedades, las características y los perfiles importantes de personas, grupos, comunidades o cualquier otro fenómeno que se someta a análisis". En el caso del presente trabajo se considera el estudio y análisis del contexto de las noticias verdaderas o falsas, sus características, usuarios que las comparten, contenido, entre otros aspectos.

3.3 Enfoque

Esta investigación utiliza un abordaje alternativo a la hora de definir el enfoque. Se apoya en la referencia de autores como Chavarría (2011), que insisten en la necesidad de reconocer que los enfoques cualitativos y cuantitativos pueden coexistir y que, más aún, carece de sentido hablar de enfoques mixtos pues estos intentan mezclar de manera artificiosa cosas que nunca han estado desligadas. A

continuación, se definen cada una de las dimensiones epistemológica, ontológica y axiológica de la investigación, sin aludir explícitamente a un enfoque, en particular.

La dimensión epistemológica, al tratarse del estudio de algoritmos existentes y contrastar resultados contra una solución nueva, implicó que los investigadores asumieran una posición de observadores. Los investigadores prestaron atención a los detalles de eficacia, eficiencia, escalabilidad y facilidad de implementación. Por ello, las mediciones realizadas debieron efectuarse en condiciones similares, para comprobar y documentar los resultados de los experimentos.

La dimensión ontológica, según algunos conceptos como el expresado por Gruber (1993): "lo que existe es exactamente aquello que puede ser representado". Borst (1997), citado por Arano (2005), lo define como “una especificación formal de una conceptualización compartida”. Studer y su grupo, en 1998, se encargaron de fusionar las 34 definiciones de Gruber y Borst: “Una ontología es una especificación formal y explícita de una conceptualización compartida” (Studer, Benjamins V., & Fensel, 1998). Esta conceptualización se refiere a un modelo abstracto de algún fenómeno en el mundo a través de la identificación de los conceptos relevantes de dicho fenómeno. “Explícita” significa que los conceptos usados se definen claramente. “Formal” se refiere al hecho de que la ontología debería ser entendible por las máquinas. “Compartida” alude a la noción de que una ontología captura conocimiento consensual, esto es, que no es de un individuo, sino que es aceptado por el grupo.

El diccionario de la Real Academia de la Lengua Española define ontología como “Parte de la metafísica que trata del ser en general y de sus propiedades trascendentales”. El primer campo en que se utilizó el término fue en la filosofía. A partir de la década de los años noventa, el concepto de ontología comienza a tener

mayor importancia en las ciencias de la computación, entendida como un conjunto de términos básicos y relaciones entre sí. La representación del conocimiento requiere de mecanismos formales, para expresar con precisión la idea que se desea comunicar.

Este tipo de algoritmos ha sido ampliamente estudiado y es práctica común en las carreras de informática recurrir a ellos para mostrar técnicas de programación. Por ello, se considera que el estudio propuesto tiene una posibilidad clara de representación del conocimiento que se desea producir.

3.4 Diseño

El diseño de una investigación es el plan o estrategia definido para responder a las preguntas de investigación. En otras palabras, es lo que se debe realizar para alcanzar lo que se desea. El diseño de investigación puede ser experimental o no experimental. El término experimento, de forma general, refiere a “elegir o realizar una acción” y después observar las consecuencias. De forma particular un experimento se desarrolla para analizar si una o más variables independientes afectan a una o más variables dependientes y por qué lo hacen (Hernández, Fernández, & Baptista, 2006). En el caso de esta investigación, se aplica el diseño experimental, ya que se requiere, por medio de experimentos, comprobar y comparar los resultados tomando como medida las variables expuestas en la dimensión axiológica que son: eficiencia, eficacia y facilidad de implementación, entre el algoritmo desarrollado y los algoritmos investigados.

El diseño experimental debe cumplir con 3 requisitos. Primero: se debe manipular de forma intencional alguna(s) de las variables independientes. Segundo:

el efecto de una variable independiente sobre una dependiente, debe ser medible; y, por último: debe cumplir con control de validez internos del experimento.

El diseño transeccional se aplica en investigaciones en las que los datos requeridos para desarrollar el experimento se recopilan una única vez, en un solo momento. Dado que los diferentes conjuntos de datos utilizados para los experimentos de este proyecto investigativo fueron recolectados una única vez, los cuales se analizan para comparar y medir las variables definidas, se determina que esta investigación cumple con un diseño transeccional experimental.

El diseño muestra la concepción o configuración del trabajo final de graduación y va de la mano del enfoque seleccionado. Los diseños en estudios cuantitativos enfatizan en hallar relaciones entre variables, en tanto que los diseños en estudios cualitativos se concentran en dar en sentido y valor a categorías de análisis.

Capítulo 4.

Análisis del Diagnóstico

Actualmente, ASOMIRAVALLE les ofrece a todos los socios diferentes servicios, de los cuales algunos son llevados a cabo de manera automática y otros deben ser requeridos específicamente por los asociados. Los siguientes son los servicios que se ofrece en la actualidad:

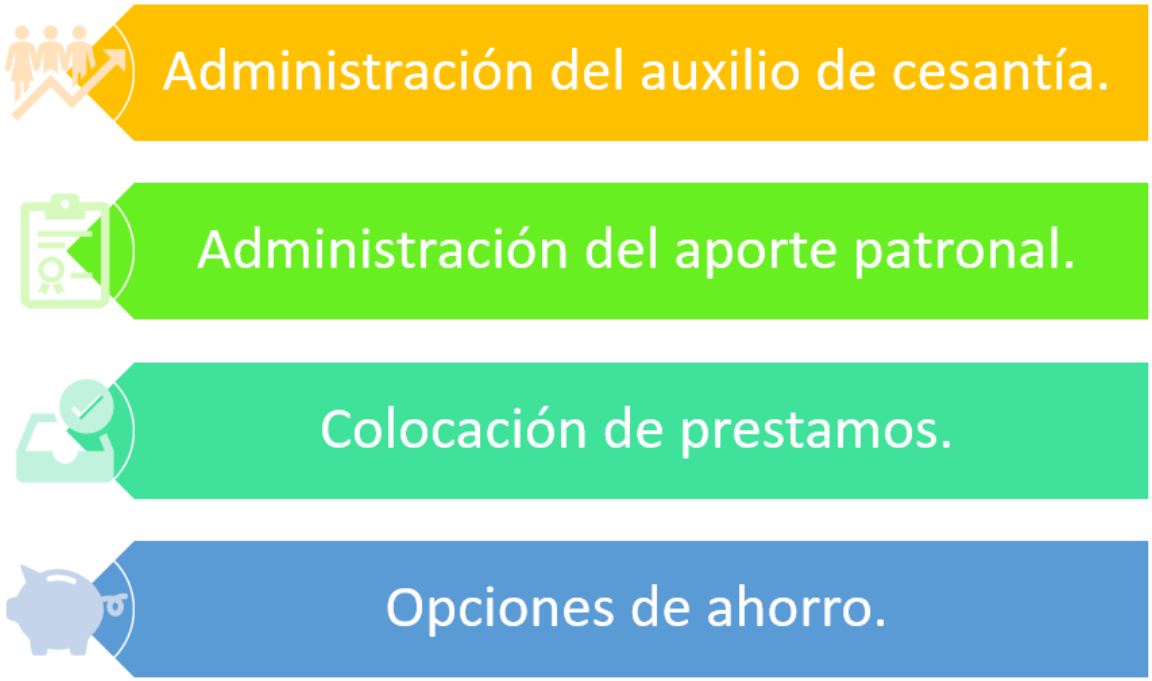


Ilustración 5: Servicios ASOMIRAVALLE (Guadamuz Vargas, 2021)

Para brindarle estos servicios a los asociados y generar cuentas claras de una manera más eficaz y eficiente, ASOMIRAVALLE hace uso de una serie de elementos de TI, los cuales vamos a detallar a continuación.

4.1 Software.

Actualmente, la asociación utiliza, para sus labores diarias, básicamente el siguiente software:

4.1.1 Microsoft Windows.

La versión de Windows que se utiliza para la operación de las computadoras es el que venía configurado en los dispositivos:

- Versión del Windows: 10 de 64 Bits.
- No cuenta con políticas previamente aplicadas.
- No se le hacen mantenimientos programados, solamente las actualizaciones obligatorias de Microsoft como tal.

4.1.2 Microsoft Office.

La versión de Windows que se utiliza en los dispositivos es una licencia que se paga anualmente a la empresa Microsoft.

- Versión del Office: Office 365 Desktop.
- Se usa la licencia de la institución educativa Miravalle.
- No cuenta con políticas de uso.
- No se le hacen mantenimientos programados, solamente las actualizaciones obligatorias de Microsoft como tal.

4.1.3 CODEAS, Quarzo.

Para las labores específicamente de la Asociación, se utiliza un software desarrollado por la empresa CODEAS el cual se llama Quarzo.

- El software actualmente se encuentra almacenado en la computadora portátil de la Asociación.
- Los respaldos de la base de datos del software se hacían en el servidor de la institución educativa Miravalle, pero el servidor se quedó sin espacio en disco duro y ahora se realizan en un disco duro externo propiedad de la misma institución. (Guadamuz Vargas, 2021)

4.1.3.1 Ventana de inicio.

Esta es la ventana de inicio del software Quarzo de CODEAS, el cual en este momento se encuentra instalado únicamente en una computadora portátil en la cual se ingresa por todos los usuarios.



Ilustración 6: Ventana de inicio de Quarzo. (Guadamuz Vargas, 2021)

4.1.3.2 Ventana de versión del sistema.

El software tiene la versión 2005.9008.6175 como se puede ver en la imagen.

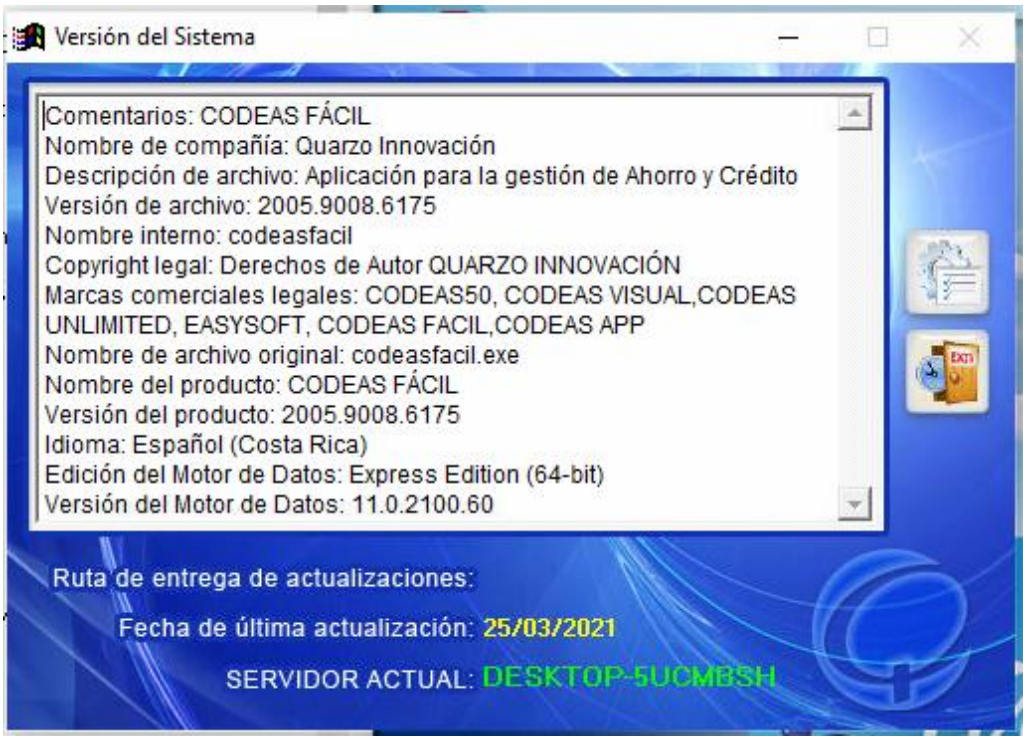


Ilustración 7: Versión del sistema. (Guadamuz Vargas, 2021)

4.1.3.3 Ventana de ingreso de usuarios.

Aquí se puede observar el acceso de los usuarios al software, así como la posibilidad de que la fecha con la que se ingresa sea modificada de manera muy fácil. Esto se necesita de esta manera para ingresar datos en el sistema de otras fechas, sin perjudicar la contabilidad.

Actualmente existen los siguientes usuarios:

- Administradora
- Contabilidad
- Superusuario (para consultores del software)



Ilustración 8: Ingreso de usuarios

4.1.3.4 Ventana de cambio de contraseñas.

En esta ventana es donde los usuarios pueden realizar los cambios de contraseña de manera muy fácil y sin necesidad de contar con el personal de TI. Los usuarios actuales del sistema manejan las mismas claves en caso de que alguno necesite entrar en el perfil del otro. (Guadamuz Vargas, 2021)



Ilustración 9: Cambio de contraseña.

4.1.3.5 Ventana de información de soporte del software.

En esta ventana se puede observar la información de la empresa que le da soporte al software Quarzo, empresa que es la misma que desarrolló el software, por lo que se le paga un soporte anual para contar con lo siguiente:

- Actualizaciones anuales.
- Informes
- Solución a cualquier problema que se llegue a presentar con el software.
- Restauraciones de la base de datos respaldada.
- Reinstalación del software por problemas con el sistema operativo.

(Guadamuz Vargas, 2021)

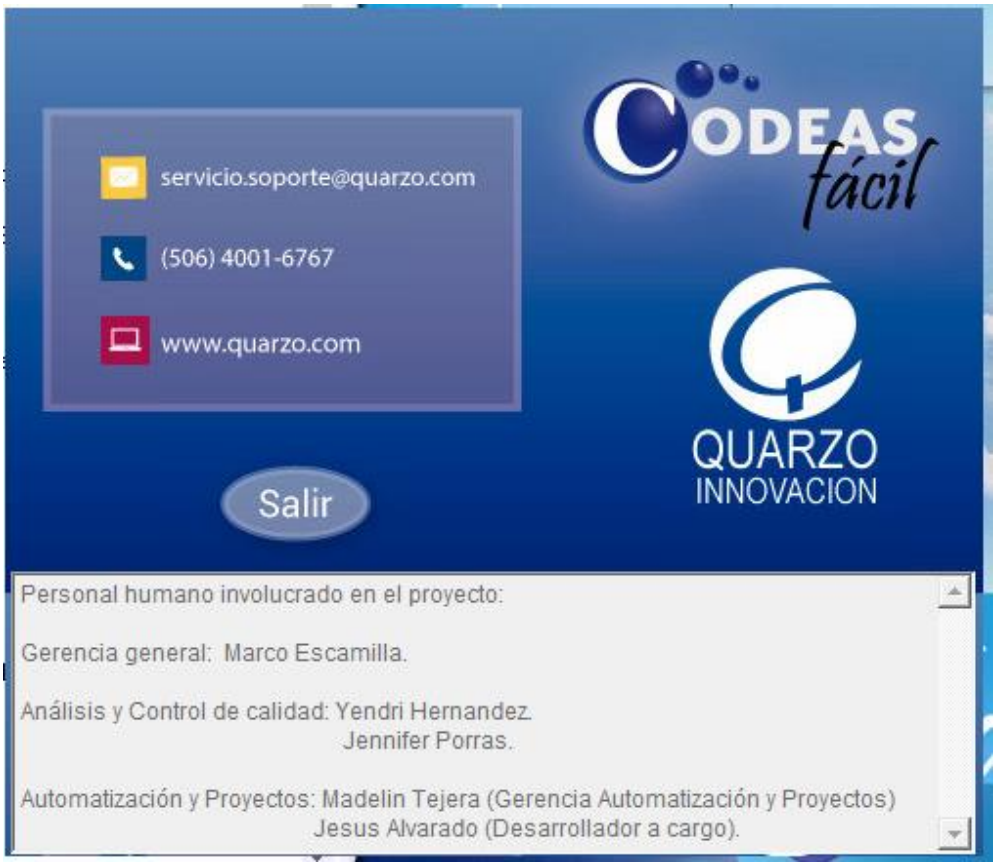


Ilustración 10: Información de Soporte (Guadamuz Vargas, 2021)

4.1.3.6 Ventana de Configuración del Software.

En esta ventana se puede ver todas las opciones que ofrece el software para su configuración:

- Búsquedas
- Impresión
- Notificaciones y mensajes emergentes
- Información general del usuario

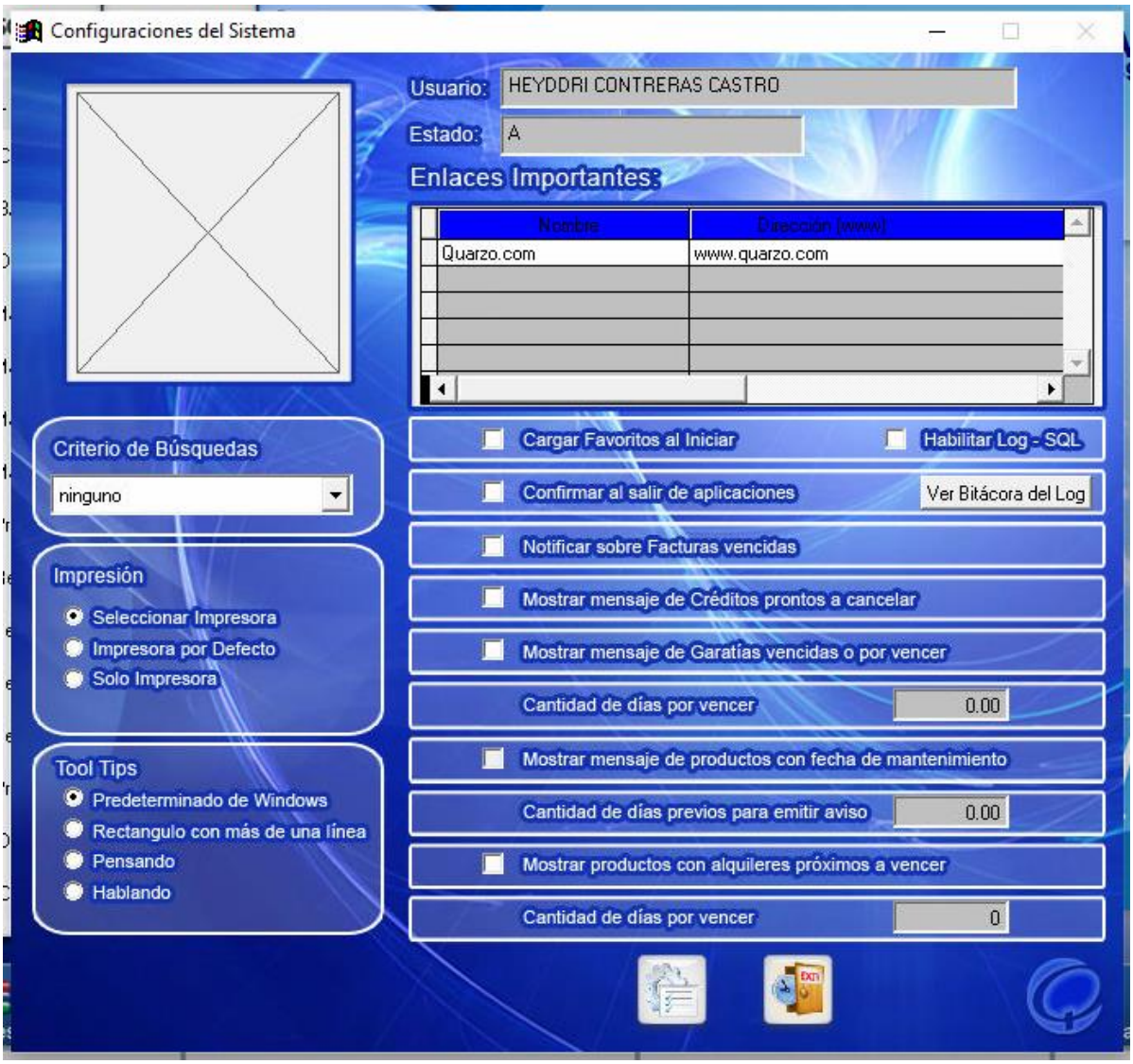


Ilustración 11. Configuración del Software (Guadamuz Vargas, 2021)

4.1.3.7 Ventana de inicio del software.

Esta es la ventana principal del software donde se realizan todos los movimientos de Asociación. Aquí se realizan las siguientes funciones:

- Ingreso y salida de asociados.
- Solicitud de préstamos y ahorros.
- Cálculo de excedentes.
- Estados de cuenta mensuales para los asociados.
- Informes para la Junta Directiva.

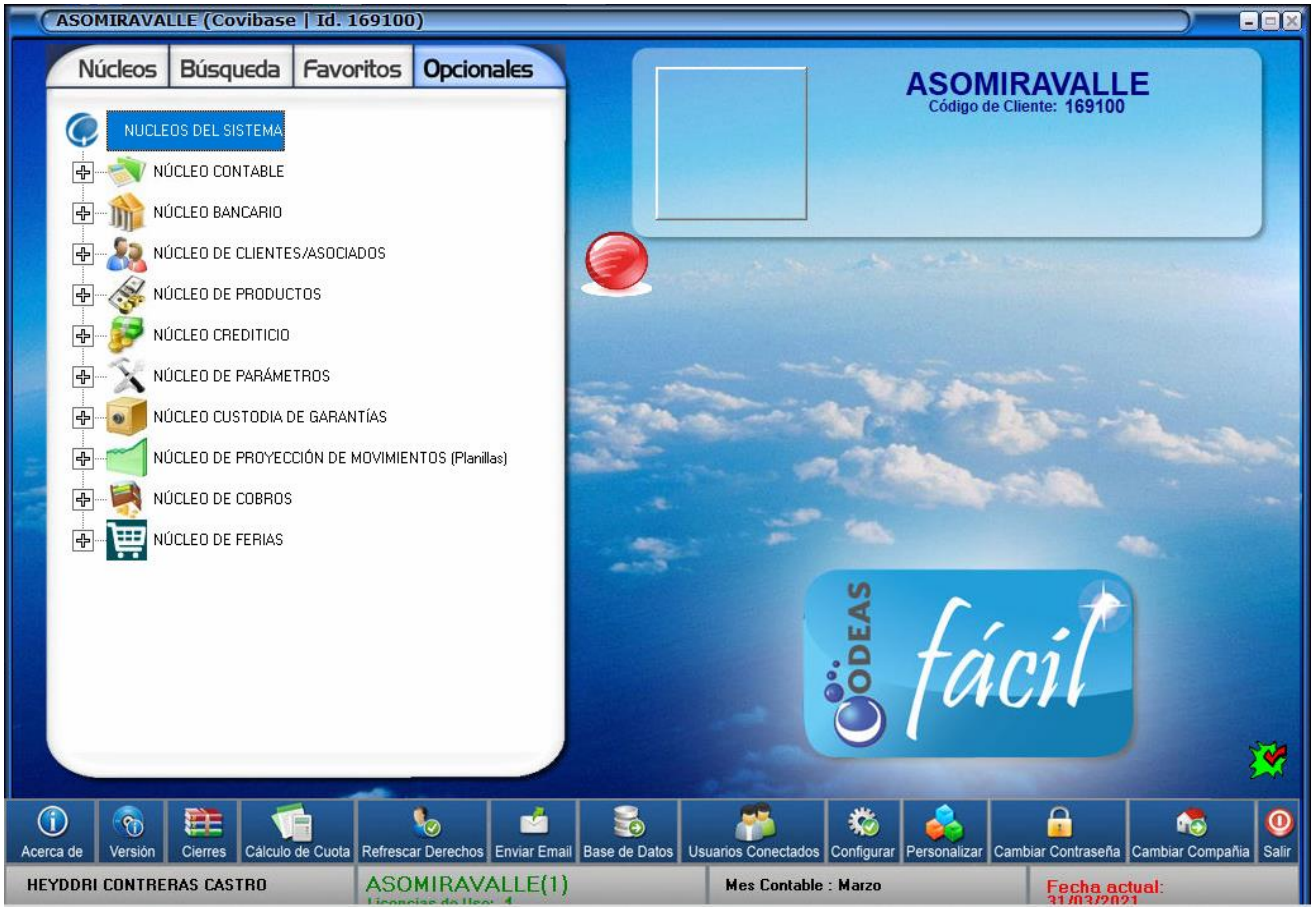


Ilustración 12. Ventana de inicio del software (Guadamuz Vargas, 2021)

4.1.4 Antivirus.

Actualmente, la Asociación utiliza el antivirus que está instalado en el Windows por defecto. No se tiene planeado ningún tipo de mejora en este aspecto, en particular.

4.2 Hardware.

4.2.2 Equipo de TI.

Por tratarse de una empresa pequeña, la Asociación cuenta solamente con dos activos para sus labores diarias, los cuales son:

- Una *laptop*
- Una impresora.

(Guadamuz Vargas, 2021)

4.2.3 Conexiones de red.

Actualmente, la Asociación se encuentra dentro de las instalaciones educativas donde se encuentra el colegio y la escuela. Por este motivo la *laptop* se conecta directamente a la red de la institución educativa Miravalle por medio de un cable de ethernet RJ45. (Guadamuz Vargas, 2021)

4.3 Mantenimiento.

4.3.1 Mantenimiento equipo de TI.

Para el mantenimiento de todo el equipo de TI en la asociación se requiere del personal de TI de la institución educativa Miravalle, por lo que de momento no se

cuenta con personal especializado para estas labores dentro de ASOMIRAVALLE. (Guadamuz Vargas, 2021)

4.3.2 Mantenimiento de bases de datos.

De momento no existe mantenimiento programado para las bases de datos del software de ASOMIRAVALLE. (Guadamuz Vargas, 2021)

4.4 Respaldos.

4.4.1 Respaldo de información.

Actualmente, los respaldos de información de los datos de ASOMIRAVALLE se encuentran a cargo del personal de TI de la institución educativa Miravalle. Los respaldos se realizan en el servidor de la Institución, pero últimamente han tenido problemas de espacio en disco y han realizado los últimos respaldos en discos duros externos, propiedad del departamento de TI del centro educativo.

Por lo general, los respaldos se realizan cada tres meses, pero por el impacto de la pandemia ha sido muy complicado efectuar labores periódicas de mantenimiento, ya que las instalaciones se encuentran cerradas y se está evitando el contacto físico entre los colaboradores. (Guadamuz Vargas, 2021)

4.4.2 Respaldo de electricidad.

En condiciones normales, se cuenta con un generador eléctrico a base de diésel, que abastece a todo el complejo, porque la asociación se encuentra dentro de las instalaciones de la institución educativa Miravalle. Pero de momento, por la pandemia, los funcionarios de la asociación están laborando desde las casas y no cuentan con este recurso.

Actualmente, el único respaldo electico con el que se cuenta es con la batería de la *laptop*, en caso de una falla eléctrica la batería da el tiempo necesario para salvar los trabajos que se estén haciendo y apagar debidamente el equipo. (Guadamuz Vargas, 2021)

4.4.3 Respaldo de conexión a Internet.

En condiciones normales, como la asociación se encuentra dentro de las instalaciones de la institución educativa Miravalle, usa la conexión a internet que le es prevista y no se cuenta con ningún otro tipo de conexión de momento. A raíz de la pandemia, los colaboradores de la asociación se encuentran en las casas y están haciendo uso del internet doméstico de cada uno, sin contar con ningún tipo de respaldo. (Guadamuz Vargas, 2021)

4.5 Seguridad física.

4.5.1 Vigilancia y Monitoreo.

Las oficinas de la asociación se encuentran dentro del complejo de la institución educativa Miravalle, por lo cual se benefician de lo siguiente:

- Oficial de seguridad 24/7/365.
- Monitoreo con circuito cerrado 24/7/365.
- Rondas por parte de los oficiales de seguridad 24/7/365

  . (Guadamuz Vargas, 2021)

4.5.2 Perímetros físicos.

La asociación cuenta con 3 perímetros físicos muy bien delineados, por lo que le da una seguridad bastante alta. Los perímetros se dividirían de la siguiente manera:

1. Acceso al parqueo del complejo de la institución educativa Miravalle por medio de aguja electrónica ubicada en la caseta de seguridad en el borde de la calle.
2. Acceso al Colegio de la institución educativa Miravalle por medio de un portón peatonal.
3. Acceso a las instalaciones de ASOMIRAVALLE por medio de una puerta peatonal con contrapuerta de metal, reforzada.

(Guadamuz Vargas, 2021)

4.6 Políticas.

4.6.1 Política de gestión de contraseñas.

No existe una política de gestión del manejo de las contraseñas en este momento. En este momento, los usuarios que se encuentran configurados en el software cuentan con la misma contraseña. (Guadamuz Vargas, 2021)

4.6.2 Política de gestión de datos.

No existe una política de gestión del manejo de los datos en este momento. Actualmente, se cuenta con una política de manejo de perfiles para los usuarios que ingresan al software Quarzo de CODEAS, los cuales serían de la siguiente manera:

<u>Perfil Administradora:</u>

- Registro de movimientos.
- Actualización de datos
- Generación de créditos.
- Generación de ahorros.
- Consultas en general.

Contadora:

- Módulo contable.
- Mayorización de asientos
- Ajustes varios
- Generación de estados financieros

4.6.3 Política de seguridad y continuidad del negocio.

No existe una política de seguridad o de continuidad del negocio en este momento.

No existe ningún tipo de BIA (Plan de Continuidad del Negocio, por sus siglas en inglés).

Capítulo 5.

Propuesta de Solución

Para la solución de la mejora de sistema de gestión de la Asociación, se han diseñado tres propuestas para que la Junta Administrativa de la Asociación tenga la posibilidad de valorar cuál solución se ajusta más a su presupuesto anual. También se diseñaron de manera tal que puedan ser escalables y no necesariamente elegir una solución signifique no poder elegir las otras, en un futuro cercano.

5.1 Solución de gama alta.

La siguiente solución ha sido diseñada especialmente para la Asociación, contemplando un escenario ideal para la gestión de todas sus actividades diarias sin comprometer la disponibilidad e integridad de los datos de los asociados innecesariamente. Esta solución es el *top* de las otras tres, pero no significa que no tenga sus puntos de mejora continua. Estos son, sin lugar a duda, los cambios necesarios que le va a dar una solidez mayor a la Asociación, se deberían implementar para robustecer y proteger las gestiones diarias.

Propuesta Gama Alta		
Elemento de TI	**Actual**	**Propuesta**
Software	Microsoft Windows 10 licencia comercial	Sin cambio
	Microsoft Office 365	Adquirir una licencia propia de Asomiravalle.
	CODEAS, Quarzo	Contratar el Servicio de CODEAS Quarzo Cloud que cuenta con respaldo en la nube y acceso vía web.
	Antivirus	Adquirir un antivirus profesional que incluya protección contra *Malware* y *phishing*.

Hardware	Equipo de TI.	Adquirir otra computadora para evitar que los usuarios compartan el mismo dispositivo.
		Agendar los respaldos del software en los servidores de CODEAS.
	Conexiones de Red.	Adquirir una tarjeta de datos inalámbricos para contar con respaldo en caso de que llegue a fallar la conexión a internet.
Mantenimiento	Mantenimiento equipo de TI.	Elaborar un plan de mantenimiento anual para asegurar siempre el buen funcionamiento de los equipos de TI.
		Apoyarse con el personal de TI de la institución educativa Miravalle.
	Mantenimiento de Base de Datos.	Elaborar un plan de mantenimiento anual para asegurar siempre la disponibilidad de los datos y su integridad.
		Realizar campañas para actualización de datos.
Respaldos.	Respaldo de información.	Realizar respaldos semanales en el disco duro que se planea comprar. Y trabajar con CODEAS en respaldos preprogramados semanales de la base de datos, incremental.
	Respaldo energético	Compra de una UPS para conectar la computadora y que así no se pierda la información.
	Respaldo de conexión a internet	Adquirir una tarjeta de datos inalámbricos para contar con respaldo, en caso de que llegue a fallar la conexión a internet.
Seguridad física	Vigilancia y monitoreo	Sin cambio
	Perímetros físicos	Sin cambio
Políticas	Política gestión de contraseñas	Elaborar una política de gestión de contraseñas, donde se detalle desde el nivel de complejidad de las contraseñas y el periodo de vencimiento que estas deben tener, idealmente cada tres meses. Los usuarios no deben compartir contraseñas para mantener los logs libres de corrupción.

	Política de gestión de datos	Elaborar una política de gestión de datos donde se detalle donde se va a almacenar la información, cada cuánto serán los respaldos y actualizaciones de la base de datos. Desarrollar un ambiente de Producción y un ambiente de pruebas para no manipular la base de datos global innecesariamente. No permitir que la fecha de ingreso al software sea manipulable.
	Política de Seguridad y Continuidad del Negocio.	Contratar a un experto que pueda realizar un Plan de Continuidad del Negocio (BIA) y que se realicen campañas de concientización para optimizar su uso. Elaborar un plan para seguir funcionando con papelería en caso de que el software no esté disponible.

Tabla 5: Propuesta Gama Alta. Elaboración propia

5.2 Solución de gama media.

La siguiente solución ha sido diseñada para que sea escalable junto con las otras dos. Estos son, sin lugar a duda, los principales cambios, junto con otros más que le darían una solidez mayor a la Asociación, los que se deberían implementar para robustecer y proteger las gestiones diarias, asegurándole así la disponibilidad e integridad de los datos.

Propuesta Gama Media		
Elemento de TI	**Actual**	**Propuesta**
Software	Microsoft Windows 10 licencia comercial	Sin cambio
	Microsoft Office 365	Adquirir una licencia propia de ASOMIRAVALLE.
	CODEAS, Quarzo	Sin cambio
	Antivirus	Adquirir un antivirus profesional que incluya protección contra *Malware* (programas malignos) y *phishing* (técnicas de substracción de datos).
Hardware	Equipo de TI.	Adquirir otra computadora para evitar que los usuarios compartan el mismo dispositivo.

		Adquirir un disco duro para que se puedan hacer los respaldos ahí y que esté en dominio de la Asociación, preferiblemente en un lugar seguro, bajo llave.
	Conexiones de red.	Adquirir una tarjeta de datos inalámbricos para contar con respaldo, en caso de que llegue a fallar la conexión a internet.
Mantenimiento	Mantenimiento equipo de TI.	Elaborar un plan de mantenimiento anual para asegurar siempre el buen funcionamiento de los equipos de TI.
		Apoyarse con el personal de TI de la institución educativa Miravalle.
	Mantenimiento de base de datos.	Elaborar un plan de mantenimiento anual para asegurar siempre la disponibilidad de los datos y su integridad.
		Realizar campañas para actualización de datos.
Respaldos.	Respaldo de información	Realizar respaldos semanales en el disco duro que se planea comprar.
	Respaldo energético	Compra de una UPS para conectar la computadora y que así no se pierda la

		información.
	Respaldo de conexión a internet	Adquirir una tarjeta de datos inalámbricos para contar con respaldo en caso de que llegue a fallar la conexión a internet.
Seguridad física	Vigilancia y Monitoreo	Sin cambio
	Perímetros físicos	Sin cambio
Políticas	Política gestión de contraseñas	Elaborar una política de gestión de contraseñas, donde se detalle desde el nivel de complejidad de las contraseñas y el periodo de vencimiento que estas deben tener. Asimismo, que los usuarios no compartan contraseñas para mantener los *logs* libres de corrupción.
	Política de gestión de datos	Elaborar una política de gestión de datos, en la que se detalle dónde se va a almacenar la información, cada cuándo serán los respaldos y actualizaciones de la base de datos
	Política de seguridad y continuidad del negocio.	Sin cambio

Tabla 6: Propuesta Gama Media. Elaboración propia

5.3 Solución de gama de entrada.

La siguiente solución ha sido diseñada para que sea escalable junto con las otras dos. Estos son, sin lugar a duda, los principales cambios que la Asociación debería implementar para robustecer y proteger más sus gestiones diarias, asegurándole así la disponibilidad e integridad de los datos.

Propuesta Gama de Entrada		
Elemento de TI	**Actual**	**Propuesta**
Software	Microsoft Windows 10 licencia comercial	Sin cambio
	Microsoft Office 365	Sin cambio
	CODEAS, Quarzo	Sin cambio
	Antivirus	Adquirir una versión anual de algún antivirus profesional.
Hardware	Equipo de TI	Mantener la computadora actual sin cambio.
		Adquirir un disco duro para que se puedan hacer los respaldo ahí y que esté en dominio de la Asociación, preferiblemente en un lugar seguro, bajo llave.
	Conexiones de red	Sin cambio
Mantenimiento	Mantenimiento equipo de	Elaborar un plan de mantenimiento

	TI.	anual para asegurar siempre el buen funcionamiento de los equipos de TI.
		Apoyarse con el personal de TI de la institución educativa Miravalle.
	Mantenimiento de base de datos	Elaborar un plan de mantenimiento anual para asegurar siempre la disponibilidad de los datos y su integridad.
		Realizar campañas para actualización de datos.
Respaldos.	Respaldo de información	Realizar respaldos semanales en el disco duro que se planea comprar.
	Respaldo energético	Compra de una UPS para conectar la computadora y que así no se pierda la información.
	Respaldo de conexión a internet	Sin cambio
Seguridad física	Vigilancia y monitoreo	Sin cambio
	Perímetros físicos	Sin cambio
Políticas	Política gestión de contraseñas	Elaborar una política de gestión de contraseñas, donde se detalle desde el nivel de complejidad de las contraseñas y el periodo de vencimiento que estas deben tener. Asimismo, que los

		usuarios no compartan contraseñas para mantener los *logs* libres de corrupción.
	Política de gestión de datos	Elaborar una Política de gestión de datos, en el que se detalle dónde se va a almacenar la información, cada cuánto serán los respaldos y actualizaciones de la base de datos
	Política de Seguridad y Continuidad del Negocio.	Sin cambio

Tabla 7: Propuesta Gama de Entrada. Elaboración propia.

Capítulo 6.

Conclusiones y Recomendaciones

6.1 Conclusiones

A. Actualmente el sistema de gestión y operación es de poca complejidad e intuitivo de parte de los usuarios, con deficiencias significativas de control y riesgos potenciales en la pérdida de información por la ausencia de procedimientos

B. Mediante una serie de entrevistas al personal que trabaja en la asociación se lograron identificar las principales vulnerabilidades, que van desde el uso compartido de una única computadora por ambos usuarios, la inexistencia de políticas de control y cambio de claves, la nula inversión en soporte de parte de un experto, la limitada disponibilidad y el pobre soporte informático hasta el nulo control de la carencia de una política clara de respaldos de la información, el uso de la computadora de trabajo diario como servidor, la inexistencia de documentación detallada y la ausencia de un manual de consulta.

C. Como se logra apreciar, en las soluciones propuestas en este documento, se logra contemplar, para su mitigación, todas las posibles recomendaciones. Estas recomendaciones son producto del análisis que se pudo obtener mediante las entrevistas que se realizaron al personal de la asociación.

D. Las posibles vulnerabilidades identificadas van desde pérdida de información, ataques cibernéticos, alteraciones o daños significativos en la base de datos, lo que afecta la integridad de los datos e imposibilita una futura recuperación de información en el sistema de gestión de la asociación.

6.2 Recomendaciones.

A. Realizar auditorías internas anuales para determinar si todo se encuentra de la manera que debería y que no se hayan realizado cambios que estén afectando la integridad de los datos.

B. Elaborar campañas de concientización para los empleados de la Asociación para que puedan acatar las directrices necesarias en su gestión del buen funcionamiento de la empresa.

C. Dejar de pensar en pequeño. El hecho de ser una empresa pequeña no significa que no tengan activos de valor. En el caso de la información, por ejemplo, si se llegase a perder, sería irrecuperable.

D. Valorar siempre puntos de mejora, ya sea que no se hayan tomado en las recomendaciones y aplicarlas paulatinamente en un futuro cercano o seguir buscando constantemente la mejora operativa, apoyándose en el área de tecnologías de información.

Capítulo 7.

Reflexiones Finales

El tema de la ciberseguridad no debe creerse que es desarrollado solo para empresas de alto nivel, ni tampoco se debe dar por sentado la importancia que los datos de una empresa tengan sin considerar el tamaño de esta. En el caso de esta asociación, es de un tamaño relativamente pequeño en cuanto a personal administrativo, asociados, volumen de gestiones y datos se refiere. Los datos se convierten en el activo más grande que tiene la asociación y, por ende, deberían ser la prioridad en cuanto almacenamiento, integridad y seguridad se refiere.

La constante evolución y avance de las tecnologías de información genera un impacto directo en cómo se transmiten, procesan y se almacenan datos en el mundo. Las organizaciones enfrentan estos retos como oportunidades innovadoras, para ofrecer sus productos y servicios a través de internet, lo cual genera que entren en una carrera de innovación e implementación de nuevas tecnologías. Por esta razón algunas organizaciones adoptan metodologías, técnicas y herramientas para reducir riesgos que generan el uso de estas tecnologías de información hasta un nivel aceptable. (Forero, 2020)

Para hablar de riesgos de seguridad de la información, primero se debe tener claro el significado de todos los conceptos relacionados con el tema. Ese es el primer paso para concientizar al personal de las organizaciones. No se pueden fortalecer los procesos sin tener claro cuáles son y cómo se relacionan.

El objetivo general de esta disciplina es garantizar que la información está “segura”, y para llegar a este objetivo se apoya en los siguientes principios, confidencialidad, integridad y disponibilidad de la información:



Ilustración 13: Pilares de la Información. (Forero, 2020)

En términos de seguridad de la información, la definición de cada uno de los principios mencionados anteriormente es bastante simple como se muestra a continuación.

1) **Confidencialidad**: Principio que requiere que la información esté al alcance únicamente del personal de la organización que esté autorizado para acceder a ella. Es decir, su objetivo es prevenir la divulgación no autorizada.

2) **Integridad**: Principio que requiere que la información no se encuentre alterada y, en caso de que requiera una modificación, sea realizada solamente por el personal autorizado. Es decir, su objetivo es prevenir las modificaciones que no fueron autorizadas.

3) **Disponibilidad**: Principio que requiere que la información se pueda acceder en el momento que se requiera, por el personal autorizado. Es decir su objetivo es garantizar el acceso a los sistemas de información.

La seguridad de la información es un concepto muy amplio y, en cuanto a los elementos que hacen parte de las organizaciones, es necesario que este sea uno de los pilates principales y esté alineado con los objetivos y metas de estas. (Forero, 2020).

En la actualidad, la tendencia de los sistemas de la información se está inclinando a conservar la disponibilidad de la información y se está dejando de lado la integridad de los sistemas y bases de datos, al mismo tiempo de la confidencialidad de la información. Crear resiliencia a través del tiempo no debe repercutir en la desatención de factores importantes como los antes mencionados. El personal que trabaja diariamente con este tipo de sistemas son los que más potencial tienen, al ser una fuente de riesgo para las empresas, por no los procesos ni acatar los protocolos establecidos previamente por profesionales. (Forero, 2020)

Referencias

Referencias

Abdur Rahman, M. A. (2020). *Analyzing Web Application Vulnerabilities: An Empirical Study on E-Commerce Sector in Bangladesh.* Obtenido de https://dl.acm.org/doi/10.1145/3377049.3377107

Alin Zamfiroiu, I. P. (2019). *Cloud Computing Vulnerbilities Analysis.* Obtenido de https://dl.acm.org/doi/10.1145/3361821.3361830

Bhor, R. V., & Khanuja, H. K. (2016). *Analysis of web application security mechanism and Attack Detection using Vulnerability injection technique.* Obtenido de https://ieeexplore.ieee.org/abstract/document/7860004/authors

Forero, L. F. (2020). *Ciberseguridad en las organizaciones, el personal potencial fuente de riesgo.* Obtenido de http://repository.unipiloto.edu.co/handle/20.500.12277/9545.

Guadamuz Vargas, C. (marzo de 2021). (A. Contreras Castro, Entrevistador)

Hagberg, R. (2020). *Improving vulnerability detection using program analysis.* Obtenido de https://lup.lub.lu.se/luur/download?func=downloadFile&recordOId=9030175&fileOId=9030176

Heribertus Yulianton1, 2. A. (2020). *Web Application Vulnerability Detection Using Taint Analysis and Black-box Testing.* Obtenido de https://iopscience.iop.org/article/10.1088/1757-899X/879/1/012031/meta

Yu, M., Zhuge, J., Cao, M., Shi, Z., & Jiang, L. (2020). *A Survey of Security Vulnerability Analysis, Discovery, Detection, and Mitigation on IoT Devices.* Obtenido de https://www.mdpi.com/1999-5903/12/2/27

Anexos.



Ilustración 14: Página principal de CODEAS

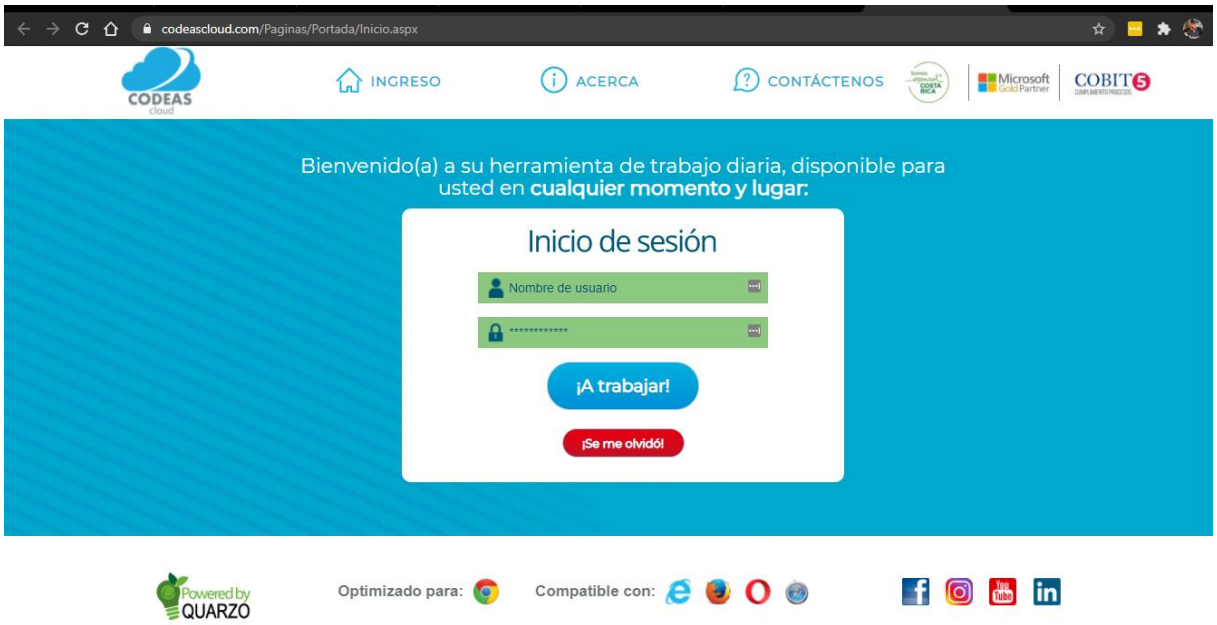


Ilustración 15: Página principal de CODEAS Cloud.

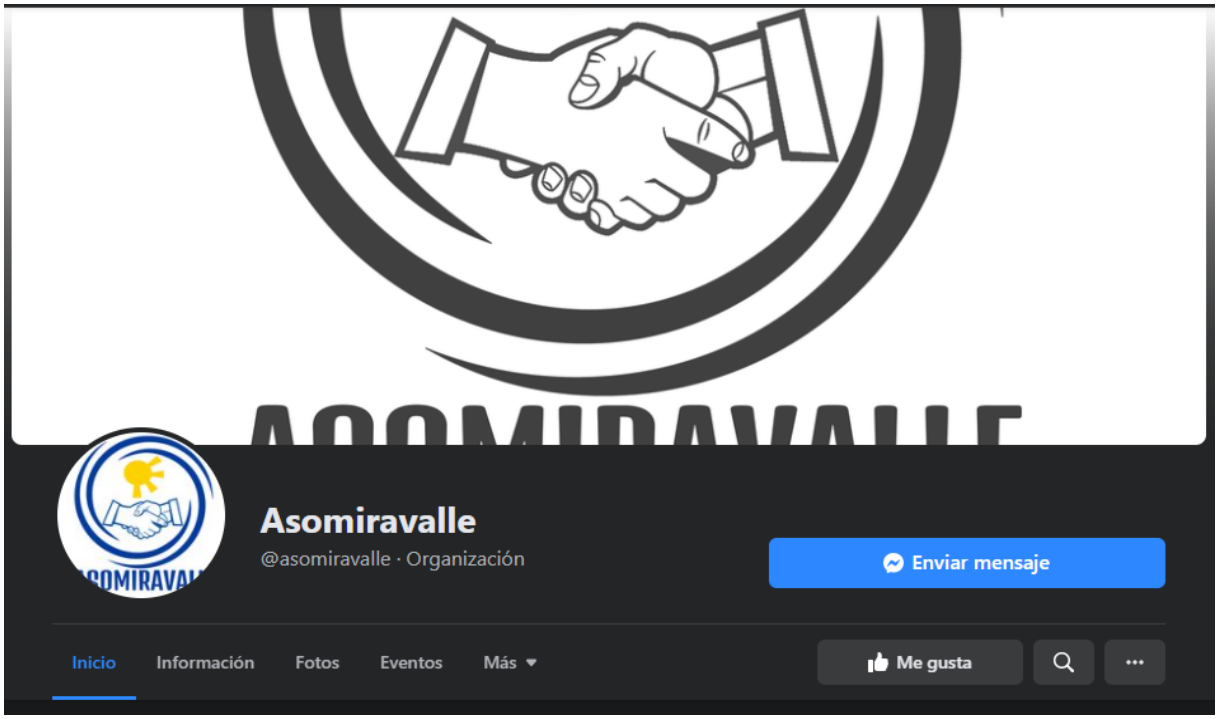


Ilustración 16: Página Facebook de ASOMIRAVALLE.

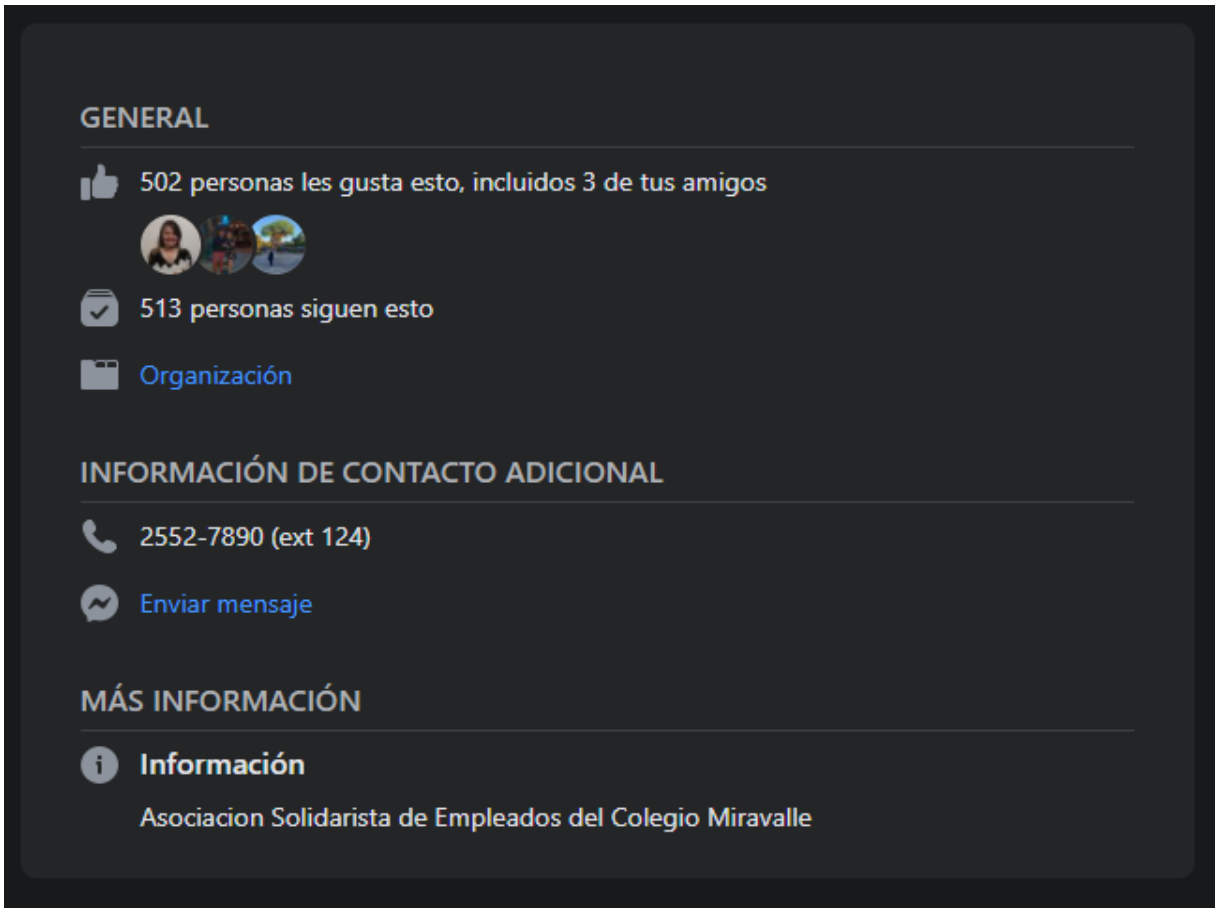


Ilustración 17: Datos de ASOMIRAVALLE de FACEBOOK



Ilustración 18: Logo ASOMIRAVALLE



Ilustración 19 SibuERP



Ilustración 20 Sibu ERP Página Principal