ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE SISTEMAS

UNIDAD DE TITULACIÓN

APLICACIÓN DE CONTROLES DEL ESTÁNDAR ISO 27002 PARA LA PREVENCIÓN DE VULNERABILIDADES EN LA PRIVACIDAD DE DATOS EN SERVICIOS WEB DEL FRAMEWORK LARAVEL

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL GRADO DE MAGISTER EN SOFTWARE CON MENCIÓN EN SEGURIDAD INFORMÁTICA

PABLO SANTIAGO PÁEZ ORTIZ

pablo.paez01@epn.edu.ec

Director: EDISON LOZA-AGUIRRE, PhD

edison.loza@epn.edu.ec

CO-Director: DANIEL ALEJANDRO MALDONADO, MSc

daniel.maldonado02@epn.edu.ec

Quito, enero 2021

APROBACIÓN DEL DIRECTOR

Como director del trabajo de titulación APLICACIÓN DE CONTROLES DEL ESTÁNDAR ISO 27002 PARA LA PREVENCIÓN DE VULNERABILIDADES EN LA PRIVACIDAD DE DATOS EN SERVICIOS WEB DEL FRAMEWORK LARAVEL desarrollado por Pablo Santiago Páez Ortiz, estudiante de la carrera de Ingeniería en Sistemas, habiendo supervisado la realización de este trabajo y realizado las correcciones correspondientes, doy por aprobada la redacción final del documento escrito para que prosiga con los trámites correspondientes a la sustentación de la Defensa oral.

Edison Loza

DIRECTOR

Daniel Maldonado

CO-DIRECTOR

DECLARACIÓN DE AUTORÍA

Yo, Pablo Santiago Páez Ortiz, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

La Escuela Politécnica Nacional puede hacer uso de los derechos correspondientes a este trabajo, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

PABLO SANTIAGO PÁEZ ORTIZ

DEDICATORIA

Quisiera dedicar este proyecto, primeramente, a mi familia en el cual incluye, mi querida madre Rocío Ortiz Lara, mi hermana Dayana Páez Ortiz y la princesita de mi hogar Alessia Carrera Páez.

A mis tutores Daniel Alejandro Maldonado y Edison Loza quienes han sabido guiarme para poder desarrollar este documento.

A la Doctora Pamela Flores que me ha sabido darme la apertura en el proceso académico para poder ejecutar este proyecto en los tiempos indicados.

Y finalmente a Fausto Naranjo Jefe de Tecnología del Servicio Ecuatoriano de Capacitación Profesional conocido como SECAP, por darme esa facilidad de poder ejecutar la evaluación planteada en el instituto académico.

AGRADECIMIENTO

Quisiera atender a mi mama Rocío Ortiz por su apoyo incondicional en la realización de este proyecto. Como al Servicio Ecuatoriano de Capacitación Profesional SECAP, por haberme brindado las facilidades y accesos a sus sistemas de información para la ejecución de esta evaluación planteada.

ÍNDICE DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

LISTA DE ANEXOS

RESUMEN

El presente trabajo tiene como objetivo aplicar controles de las normas ISO 27002 e ISO 27701 para la prevención de vulnerabilidades en la privacidad de datos en servicios web del Framework Laravel y, a partir de su aplicación, la generación de una guía de mejoras especifica. Para el desarrollo teórico se realizó una revisión de trabajos relacionados a lo que se propone realizar, en los que se aplicó, previa investigación teórica, la metodología Action Research. Con los conceptos conocidos, se procedió a aplicar la metodología tomando en cuenta los puntos base para su ejecución como son: el diagnóstico, planificación de las acciones a tomarse, toma de acciones, evaluación de las acciones implementadas e identificación de los hallazgos de la puesta en marcha de la metodología.

Luego de identificar el estado del SECAP, institución escogida para este estudio, se realizó el análisis de vulnerabilidades en la privacidad de datos y la evaluación de amenazas a nivel de redes, datos y de acceso; dando como resultado un riesgo medido muy alto.

A partir de la realización del análisis y la evaluación de la situación actual de la institución estudiada, se definieron políticas en las que se incluyen medidas específicas para mitigar las amenazas identificadas sobre cada bien informático. Cada una de las medidas está basada en la probabilidad de ocurrencia de un evento malicioso y el peso de riesgo estimado para cada uno de los activos tecnológicos analizados, disminuyendo de esta forma el peso total del riesgo.

Como parte de la de la valoración de los resultados encontrados, se halló una serie de vulnerabilidades en servicios web del módulo de autenticación, parte del aplicativo analizado en este estudio. Basándose en estas vulnerabilidades y las amenazas relacionadas actualmente vigentes para este módulo, se elaboró un plan de mejoras y se puso a disposición del SECAP para poder prevenir las vulnerabilidades encontradas.

Palabras clave: ISO 27002, ISO 27701, vulnerabilidad, privacidad de datos, Action Research

.

ABSTRACT

This research project has as main goal the application of ISO 27002 and ISO 27701 guidelines controls in order to prevent data privacy vulnerabilities among Laravel Framework web services and, through its application, the generation of a specific improvement guidance manual. For the theoretical development it is made a review of related works, in which is applicated the Action Research methodology. With all the basic concepts knowns, the methodology was applied counting on ground basis for its execution like: diagnosis, planning future actions, evaluation of these actions and identification of methodology application findings.

After identifying SECAP initial status, privacy data vulnerabilities analysis was performed. Also, the evaluation of data, access systems and networking threats; obtaining a very high measured risk.

After all the analysis and evaluations, it was defined policies that included specific measures in order to mitigate any identified threats over informatic goods. Every one of the measures is based on the probability of occurrence of a malicious even and the related risk. All of that to reduce the total weight of the measured risk.

As part of the results of the analysis, it was found several vulnerabilities on Authentication module web services, as part of the studied module. Based on those vulnerabilities and the related threats, it was developed an improvement policies plan, in order to SECAP can prevent all found vulnerabilities.

Keywords: ISO 27002, ISO 27701, vulnerability, data privacy, Action Research.

1. INTRODUCCIÓN

En los últimos años los sistemas de información se han generalizado, brindando cada vez más ventajas a las organizaciones, como la interconexión estable y segura con proveedores y clientes. A la par se ha evidenciado el incremento de ataques contra estos sistemas y los servicios relacionados a los mismos. Los ataques y robo de información se han convertido en un gran inconveniente, debido a que la información manejada por toda organización le proporciona los medios para controlar todas sus funciones de una manera adecuada. De allí que es importante aplicar controles para prevenir vulnerabilidades que se pueden reflejar en la seguridad y la privacidad de los datos. La tendencia tecnológica actual demanda aplicativos modernos que puedan manejar la información, especialmente sus datos privados, de tal manera que estén disponibles cada vez que se los requiera y sea sencillo para su administración.

Bajo esta premisa, para muchas organizaciones actuales, la seguridad de la información consiste en un grupo de profesionales que instalan y configuran equipos y software, con el fin de preservar la confidencialidad, disponibilidad e integridad. Es decir, el tener seguridad de la información es la aplicación de diferentes herramientas de protección a sus sistemas informáticos como: firewalls, antivirus, cifrado de datos, sistemas de contraseña entre otros. Sin embargo, como lo demuestra la práctica, la seguridad técnica nunca será suficiente para disuadir a los interesados en obtener activos de la organización. Especialmente cuando son personas ajenas a la compañía o institución, las cuales pueden realizar un hurto de esa información.

Hoy en día el robo de datos es algo tan crítico para una empresa o negocio que es considerado como un delito, ya que se puede usufructuar de los datos sustraídos para realizar muchas actividades ilícitas como: transacciones fraudulentas, daños a la persona dueña de esa información, venta al mercado negro, etc. Sobre todo cuando esa información obtenida es de carácter confidencial o privada.

En países avanzados tecnológicamente se considera a la privacidad de la información como algo fundamental para el funcionamiento de un aplicativo de software implementado en una organización. Los aplicativos modernos a medida están constituidos por un *BackEnd* y *FrontEnd*. El *BackEnd* tiene una estructura en capas, basándose en un patrón de diseño de Modelo-Vista-Controlador (MVC), con el fin de desacoplar funcionalidades y que cada módulo de un aplicativo sea cada vez más independiente, transaccional y escalable. Cumple funciones transaccionales y de negocio, ya que se encarga de realizar

las funcionalidades de manejo de información directamente con la base de datos, mediante modelos. Igualmente, realiza operaciones propias de cada tipo de negocio dando una respuesta al *FrontEnd* a través del uso de controladores y vistas. La misma es desarrollada con varios lenguajes de programación como C#, PHP, Java, entre otros. El *FrontEnd,* finalmente, consume esa información de respuesta arrojada por el *BackEnd* y la muestra al usuario, de una forma dinámica y amigable.

1.1. Preguntas de investigación

Pregunta Principal

¿Qué importancia tiene la aplicación de controles del estándar ISO 27002 e ISO 27701 para la prevención de vulnerabilidades en la privacidad de datos en servicios web del framework Laravel en el módulo de Autenticación del Servicio Ecuatoriano de Capacitación Profesional SECAP?

Preguntas Secundarias

¿Por qué aplicar controles basados en estándares de seguridad para proteger la privacidad de datos?

¿Se pueden hallar vulnerabilidades en la privacidad de datos en servicios web transaccionales?

¿El Framework de desarrollo Laravel presenta vulnerabilidades en el manejo de privacidad de datos?

¿Se puede prevenir vulnerabilidades en la privacidad de datos transaccionales con la aplicación de controles de un estándar de seguridad?

¿Cuáles son los datos privados más importantes a tomar en cuenta en servicios web transaccionales?

1.2. Objetivo general

Aplicar controles del estándar ISO 27002 e ISO 27701 para la prevención de vulnerabilidades en la privacidad de datos en servicios web del framework Laravel y generación de una guía de mejoras.

1.3. Objetivos específicos

- Realizar una selección de los tipos de controles necesarios para nuestra evaluación.
- Definir el aplicativo y sus servicios web con framework Laravel para la realización de estudio.
- Aplicar los controles del estándar ISO 27002 e ISO 27701 acordados en servicios web definidos.
- Presentar de resultados obtenidos de la evaluación ejecutada.
- Proponer una guía de mejoras basándose en la evaluación realizada.

1.4. Marco Teórico

1.4.1. Controles de la Norma ISO 27002

La norma ISO 27002 fue publicada por la Organización Internacional de Estandarización y la Comisión Electrotécnica Internacional (IEC). Originalmente fue nombrada ISO / IEC 1779 y publicada en el año 2000, luego fue actualizada en el 2005 y acompañada con una nueva publicación del ISO 27001. Ambas normas fueron desarrolladas para ser complementarias entre sí. (Imam Riadi, 2018).

Las normas ISO 27001 y 27002 están enfocadas a la protección de la información de un negocio. ISO 27002 proporciona ciento catorce controles potenciales y mecanismos que están diseñados para implementarse con la orientación proporcionada en el ISO 27001. Los controles están destinados a abordar problemas específicos identificados durante una evaluación formal de riesgos. (Imam Riadi, 2018).

La norma también está destinada a proporcionar una guía para el desarrollo de estándares de seguridad y prácticas efectivas de administración de seguridad. *“La ISO 27002 provee guías y principios generales para iniciar, implementar, mantener y mejorar la administración*

de la información en un sistema que consisten en mejores prácticas en la administración de seguridad en el campo de la información" (Sari Widya Sihwi, 2016).

La norma ISO 27002 puede ser aplicada a todo tipo de empresas, su organización es de 14 dominios, 35 objetivos de control y 114 controles. En la ISO/IEC 27002: 2013 se establecen 18 controles para la seguridad de la información, los cuatro primeros detallan los objetivos, referencias normativas, términos y definiciones y estructura de la norma.

Los controles están clasificados en 4 diferentes categorías de servicios: La primera es sobre políticas y regulaciones de la organización, la segunda es la autenticación, el cual incluye identificación de un usuario, la tercera es el control de acceso, que relaciona confidencialidad de datos y regulaciones de privacidad y la cuarta es la integridad de datos, el cual incluye gestión de activos para prevenir divulgación, destrucción, remoción o modificación no autorizada de información. (Josefina Gutiérrez-Martínez, 2015)

Dentro de los dominios, el primero es el objetivo, el segundo son las referencias normativas, el tercero son los términos y definiciones, el cuarto detalla la estructura, es decir los cuatro primeros son puntos introductorios al manejo de la norma. El quinto, es denominado como Política y se basa en el contexto en el que opera una organización se consideran los *"fines y objetivos, las estrategias adoptadas para alcanzar sus objetivos, la estructura y los procesos adoptados, los objetivos generales y específicos relacionados con el tema de la política y requisitos de las políticas procedentes de niveles más superiores relacionadas"* (ISO/IEC 27002, 2013).

Las políticas contienen: resumen, introducción, ámbito de aplicación, objetivos, principios, responsabilidades, descripción de los mecanismos organizativos, resultados clave, políticas relacionadas, sistema de gestión de seguridad de la información.

En la sección sexta se trata sobre la organización de la seguridad de la información en una empresa, esta tiene una organización interna y/o con respecto a terceros. Para que esta funcione adecuadamente es necesario que sea gestionada de una manera adecuada mediante los representantes de la organización, los mismos *"que deben tener responsabilidades bien definidas y proteger las informaciones de carácter confidencial"* (Pandini, 2015, p. 11).

En la sección séptima se considera la seguridad en recursos humanos, aquí se toma en cuenta la contratación de un empleado o proveedores para que se pueda tratar de manera adecuada la información de carácter confidencial. Con eso se pretende *"mitigar el riesgo*

de robo, fraude o mal uso de los recursos" (Pandini, 2015, p. 14). Es decir, concienciar al empleado de las responsabilidades y obligaciones que este tiene y como debe tratar la información de la empresa.

Gestión de activos corresponde a la sección octava y según la norma activo es: Cualquier cosa que tenga valor para la organización y que necesita ser protegido. Pero para ello *"los activos deben ser identificados y clasificados, de modo que un inventario pueda ser estructurado y posteriormente mantenido. Además, deben seguir reglas documentadas, que definen qué tipo de uso se permite hacer con dichos activos"* (ISO/IEC 27002, 2013).

En la norma en la sección novena se considera el control de acceso que son *"los equipos e instalaciones de procesamiento de información crítica o sensible deben mantenerse en áreas seguras, con niveles y controles de acceso apropiados, incluyendo protección contra amenazas físicas y ambientales"* (Pandini, 2015, p. 13).

En la sección décima se establece la Criptografía, es decir se definen los controles criptográficos para *"garantizar un uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad e/o integridad de la información"* (ISO/IEC 27002, 2013).

La sección undécima establece la seguridad Física y del ambiente, aquí se definen procedimientos y responsabilidades para el procesamiento de la información, incluidos todos aquellos servicios tercerizados, con el objetivo de minimizar riesgos. En esta sección se considera la creación de copias de seguridad con un procedimiento adecuado, así como la administración segura de las redes de comunicaciones.

La seguridad de las operaciones se considera en la sección duodécima, esta incluye el procesamiento de la información y los procesos de negocios. Sus controles se basan en los requisitos y en la seguridad de la información. Debe garantizarse el acceso de usuario autorizado y previene el acceso no autorizado a los sistemas de información, a fin de evitar daños a documentos y recursos de procesamiento de la información que estén al alcance de cualquiera.

Para la adquisición, desarrollo y mantenimiento de sistemas se considera la sección décimo tercera, en la cual se establecen los requisitos de seguridad de las comunicaciones que *"deben ser identificados y acordados antes de su desarrollo y/o de su implementación, para que así puedan ser protegidos para el mantenimiento de su confidencialidad, autenticidad o integridad por medios criptográficos"* (ISO/IEC 27002, 2013).

En la sección decimocuarta se establece la adquisición, desarrollo y mantenimiento de los sistemas de información cuyo objetivo principal es *"garantizar que la seguridad de la información es una parte integral de los sistemas en todo su ciclo de vida"* (ISO/IEC 27002, 2013).

Por otro lado, en las secciones quince, dieciséis y diecisiete se establece la relación con los proveedores, la gestión de incidentes de seguridad de la información y la gestión de la continuidad del negocio. Para ello es necesario tener procedimientos establecidos tanto para empleados, proveedores y terceros con el fin de que si hay algún inconveniente se debe corregir en un tiempo prudente para evitar que se interrumpan las actividades.

Por último, en la sección dieciocho se considera el cumplimiento, la misma que tiene el fin de evitar la violación de cualquier ley criminal o civil, *"garantizando estatutos, regulaciones u obligaciones contractuales y de cualesquiera(sic) requisitos de seguridad de la información. En caso necesario, la empresa puede contratar una consultoría especializada, para que se verifique su conformidad y adherencia a los requisitos legales y reglamentarios"* (Pandini, 2015, p. 13).

Es decir, en esta sección se considera todo en cuanto leyes y reglamentos para asegurarse que las actividades que desarrolla la empresa se hagan de acuerdo con lo establecido por las leyes y códigos vigentes.

Por otro lado, en la guía de implementación de la ISO/IEC 27002:2013 se dice que *"la organización debería definir y establecer las funciones y responsabilidades asociadas con la gestión técnica de vulnerabilidades, incluido el monitoreo de vulnerabilidades, la evaluación de riesgos de vulnerabilidad"* (ISO/IEC 27002, 2013).

Esto, combinado con la documentación producida como parte del proceso de modelado de amenazas, proporciona una mejor comprensión del sistema. Permite al revisor ver dónde están los puntos de entrada a la aplicación y las amenazas asociadas con cada punto. El modelo moderno analiza un sistema desde la perspectiva de un atacante potencial, en oposición al punto de vista de un defensor. Es decir, permite obtener los puntos en los cuales hay mayor vulnerabilidad de que ocurran incidentes que afecten la seguridad de la información.

1.4.2. ISO/IEC 27701

ISO / IEC 27701 es un estándar en seguridad de la información y gestión de la privacidad. Su objetivo es llenar el vacío de garantía de seguridad y proporcionar un enfoque basado en los otros estándares internacionales como ISO 27001, para la protección de datos como una extensión de la seguridad de la información.

La ISO/IEC 27701 *"especifica los requisitos y proporciona orientación para establecer, implementar, mantener y mejorar el Sistema de Gestión de Información de Privacidad (PIMS) y en forma de una extensión a ISO / IEC 27001 e ISO / IEC 27002 para la gestión de privacidad dentro del contexto de la organización"* (ISO/IEC 27701, 2019).

El documento es aplicable a todos los tipos y tamaños de organizaciones, incluidas empresas públicas y privadas, entidades gubernamentales y organizaciones sin fines de lucro, que son controladores PII y / o procesadores PII dentro de un Sistema de Gestión de la Seguridad de la Información (SGSI). (ISO/IEC 27701, 2019)

1.4.3. Vulnerabilidad

Según lo expresado por Proag (2014) *"la vulnerabilidad es el grado en que un sistema, o parte de él, puede reaccionar negativamente durante la ocurrencia de un evento peligroso"* (p. 369). La vulnerabilidad considerada desde este punto de vista incluye el riesgo asociado con los aspectos físicos, sociales y económicos, así como la capacidad del sistema para hacer frente al evento resultante.

Por otro lado, Shitangsu (2015) define a la vulnerabilidad como *"la incapacidad de un sistema para resistir las perturbaciones de los factores estresantes externos"* (p. 64). Es decir, una vulnerabilidad es un factor externo que impide que un sistema trabaje eficiente y eficazmente.

Para considerar las vulnerabilidades es necesario considerar diferentes factores como son: desastres, peligro, riesgo y vulnerabilidad.

El desastre es cualquier evento negativo que ocurre de forma repentina, inesperada o extraordinaria, el peligro y riesgo pueden ser natural o inducido por el hombre con el fin de crear pérdidas. La exposición real de algo de valor humano a un peligro es un riesgo y a menudo se considera como la combinación de probabilidad y pérdida. Por lo tanto, un peligro es una amenaza potencial, y el riesgo (o consecuencia) es la probabilidad de que

ocurra un peligro específico (Sahni, Dhameja, & Medury, 2001). La vulnerabilidad implica cierto riesgo combinado con el nivel de responsabilidad social y económica, y la capacidad de hacer frente al evento resultante. La vulnerabilidad se ha definido como el grado en que un sistema, o parte de un sistema, puede reaccionar negativamente durante la ocurrencia de un evento peligroso (Proag, 2014).

Por otra parte, una vulnerabilidad de software según Shahnila (2018) "*Es el problema en la implementación, especificación o configuración de un sistema de software cuya ejecución puede violar una política de seguridad explícita o implícita"* (p. 1). Basándose en la experiencia, este problema en la mayor parte de casos se da debido a que los aplicativos desarrollados utilizan lenguajes de programación inseguros debido a que son gratuitos, más sencillos y son mejor conocidos por el programador en general.

Es importante considerar que "*la complejidad del software a menudo se supone que es el enemigo de la seguridad del software*" (Shin & Williams, 2008, p. 8). Es decir, la mayor parte de la falta de seguridad y la vulnerabilidad surge en el diseño de software. Es por ello que se plantea el uso de buenas prácticas de desarrollo de software, vulnerabilidades y factores de mitigación.

Para la presente investigación se utilizarán datos levantados según las especificaciones de las normas explicadas en un proceso formal, ya que según la ISO/IEC 27002:2013 se establece que "*la información sobre vulnerabilidades técnicas de los sistemas de información que se utilizan debe obtenerse de manera oportuna, evaluar la exposición de la organización a dichas vulnerabilidades y tomar las medidas apropiadas para abordar el riesgo asociado*" (ISO/IEC 27002, 2013).

1.4.4. Gestión de la parte tecnológica

1.4.4.1. Servicios web

En la actualidad, varias aplicaciones y sitios dependen de los servicios web para intercambiar información entre sí, proporcionando una forma de transferir datos diferentes a través de la red, debido a que reutilizan la funcionalidad en todos los servicios. (Moulia & Jevitha, 2016).

Los protocolos de servicios web incluyen:

- El protocolo Simple Object Access Protocol (SOAP), Extensible Markup Language – Remote Procedure Call (XML-RPC) y JavaScript Object Notation - Remote Procedure Call (JSON-RPC) para la comunicación de mensajes
- Como lenguaje de descripción de servicios web se utiliza Web Services Description Language (WSDL) y Universal Directory y Discovery Integration (UDDI) para descripción y descubrimiento de servicios web.
- Los marcos utilizados para crear/desarrollar servicios web incluyen principalmente Apache Axis, .NET, Zend y Hypertext Preprocessor (PHP).

Debido a la variedad de protocolos y marcos involucrados en el desarrollo de un servicio web, se vuelven vulnerables y con frecuencia propensos a ataques. La mayoría de los ataques a servicios web son por inyección XML, inyección XPath, inyección Structured Query Language (SQL), suplantación de identidad, denegación de servicio y ataque del hombre en el medio. Los ataques de Denegación de servicio (Denial of Service o DoS) afectan la disponibilidad del sistema y sus recursos para solicitudes válidas. La carga útil recursiva aprovecha la amplia anidación de etiquetas XML para sobrecargar los analizadores y causar ataques Diagnostic Xentry OpenShell (XDOS). *"La carga útil coercitiva carga un largo mensaje XML en la memoria que utiliza una gran cantidad de recursos de la Central Processing Unit (CPU), lo que hace que el servidor no esté disponible, lo que contribuye a los ataques de DoS*" (Moulia & Jevitha, 2016).

Por otro lado, las plataformas web permiten que las aplicaciones se comuniquen entre sí independientemente de la plataforma o el idioma. Sin embargo, son propensas a ataques en forma de DoS, por ello es importante la implementación de la seguridad del servicio web. Aunque se proponen muchas soluciones para minimizar los ataques, no existe una solución única para mitigarlos.

1.4.4.2. PHP

Trabajos previos realizados por (Salas & Martins, 2014), (Elzar Esen, 2016), (Ahsan, Shahazzat Hossain, Nahar, & Khatun, 2014) y (Moulia & Jevitha, 2016) detallan que PHP es un lenguaje de tipo scripting para sistemas cliente servidor, el cual fue diseñado exclusivamente para páginas web. Este lenguaje de programación tiene varias ventajas como: desempeño, escalabilidad, ser de código abierto, portabilidad, entre otros. Acorde a Yalowitz (2019), PHP es el lenguaje de tipo scripting más común en internet con un 82%

de cobertura. Sin embargo, como puede ser una ventaja también puede presentarse como una vulnerabilidad, porque la mayoría de desarrolladores no están muy familiarizados con la sintaxis de lenguajes de consulta (*query)* como *Sql* y prefieren extraer la información de una base de datos usando la forma tradicional en la que sea fácil de entender, ejecutar las transacciones de CRUD (Create, Read, Update and Delete o Crear, Leer, Actualizar y Eliminar) requeridas (Ummi Khaira Latif, 2017).

Los programadores al momento de realizar scripts directamente con la base de datos pueden generar una gran vulnerabilidad porque otros usuarios con fines maliciosos también pueden manipularlos. Por esta razón se ha llegado al uso de Frameworks, porque tienen una estructura MVC con el propósito de proteger esa vulnerabilidad, como también generar optimización del rendimiento. Estudios de campo realizados por (Salas & Martins, 2014) y (Ahsan, Shahazzat Hossain, Nahar, & Khatun, 2014), afirman que los frameworks de PHP son los mejores en tiempo de respuesta, porque su especialidad son las aplicaciones web comparados con otros frameworks. La figura 1 respalda el estudio mencionado:

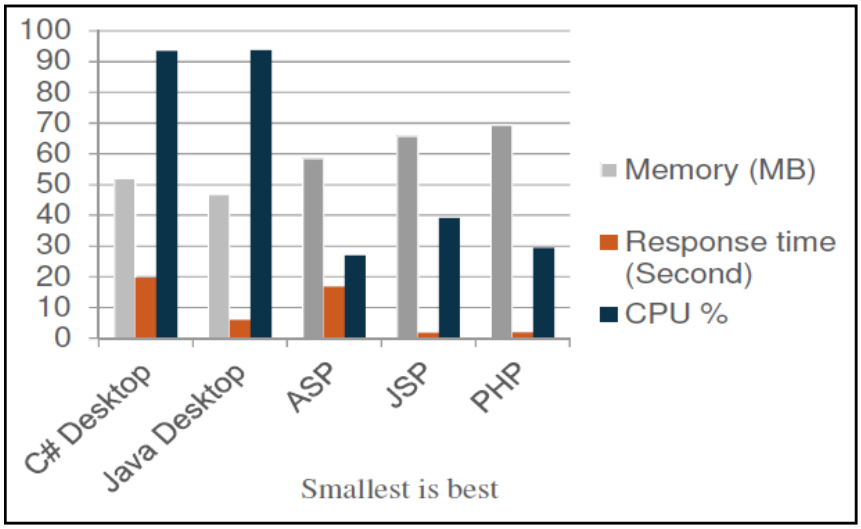


Figura 1: Rendimiento de lenguajes de desarrollo populares

Razón por la cual, Ummi (2017) afirma que de una muestra de más de un millón de sitios en Internet que son distribuidos por frameworks, la mayoría de ellos son desarrollados para el lenguaje PHP. Ocupando una popularidad de casi el 40%, como indica la figura 2 (Ummi Khaira Latif, 2017).

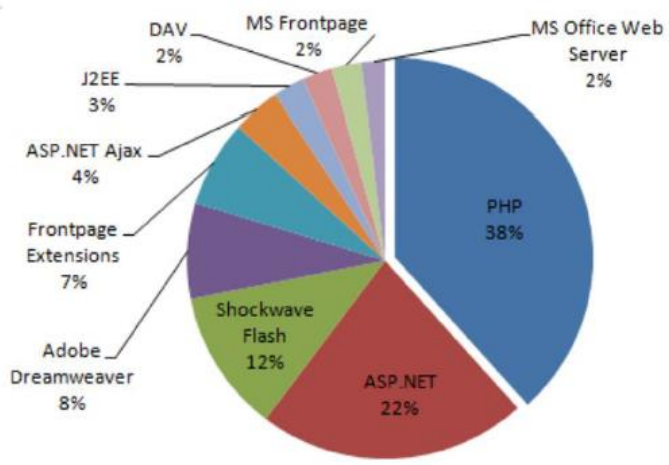


Figura 2: Distribuciones de Frameworks según los sitios mejor rankeados

Laravel es un framework open-source, para desarrollo web en PHP, creado por Taylor Otwell con el propósito de construir aplicaciones web basadas en el patrón de diseño MVC. Una de las mejoras de Laravel es el sistema de empaquetado modular dedicado al manejo de dependencias, diferentes maneras de acceso a bases de datos relacionales, como también utilitarios dedicados al mantenimiento e implementación (Elzar Esen, 2016; Ahsan, Shahazzat Hossain, Nahar, & Khatun, 2014; Moulia & Jevitha, 2016).

2. METODOLOGÍA

La metodología Action Research *"es un enfoque intervencionista para la adquisición de conocimiento científico que tiene bases sólidas en la tradición post-positivista" (Baskerville & Wood-Harper, 1996)*. Se caracteriza porque un grupo de personas identifica un problema, toma acciones para resolverlo, evalúa sus esfuerzos y, si no está satisfecho, vuelve a intentarlo.

2.1. Explicación de la metodología

Para O'Brien (2001) la metodología Action Research (AR) tiene como objetivo contribuir a las preocupaciones prácticas de las personas en una situación problemática inmediata. Por lo tanto, existe un doble compromiso en AR para estudiar un sistema y colaborar simultáneamente con miembros del sistema para cambiarlo en lo que juntos se considera una dirección deseable. Lograr este objetivo doble requiere la colaboración activa del investigador y el cliente, y por lo tanto enfatiza la importancia del aprendizaje conjunto como un aspecto primario del proceso de investigación.

Lo que separa este tipo de metodología de las prácticas profesionales es la consulta o la resolución diaria de problemas mediante el énfasis en el estudio científico, es decir, el investigador estudia el problema sistemáticamente y se asegura que la intervención esté informada por consideraciones teóricas. Gran parte del tiempo del investigador se dedica a perfeccionar las herramientas metodológicas para satisfacer las exigencias de la situación y a recopilar, analizar y presentar datos de manera cíclica y continua.

Para Bryman & Bell (2011) la metodología Action Research se puede definir como *"un enfoque en el que el investigador de acción y un cliente colaboran en el diagnóstico del problema y en el desarrollo de una solución basada en el diagnóstico" (p. 1).* Es decir, una característica importante es la relación que existe entre el investigador y el miembro de la organización para resolver problemas organizacionales.

Varios atributos separan la metodología Action Research de otros tipos de metodología como:

- El enfoque, en el cual se convierte a las personas involucradas en investigadores.
- Tiene una dimensión social en la que la investigación se lleva a cabo en situaciones del mundo real y tiene como objetivo resolver problemas reales.

- Finalmente, la persona que inicio la metodología a diferencia de otras disciplinas no intenta ser objetivo, sino que reconoce abiertamente el trabajo de los otros participantes.

2.1.1. Estructura de la metodología Action Research

Según el modelo planteado por Baskerville & Wood-Harper (1996) la metodología Action Research es cíclica, cada ciclo tiene cuatro pasos: planificar, actuar, observar, reflexionar, como se muestra en la figura 3.

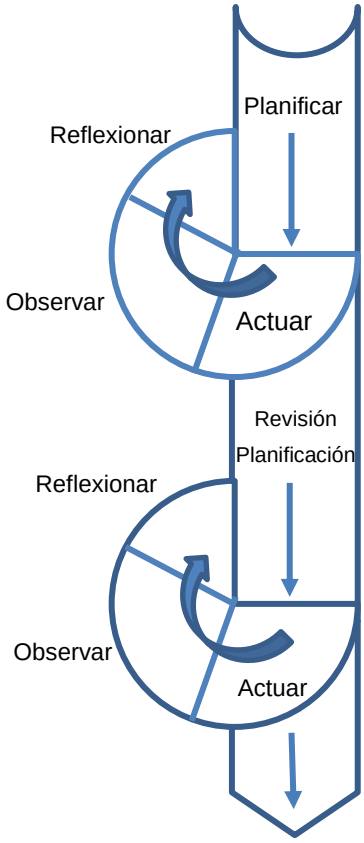


Figura 3: Modelo Action Research

Por otro lado, en el modelo presentado por Gerald Susman (1983) y Avison, Lau, Myers, & Nielsen (1999) se considera una lista más elaborada, formada de cinco fases que se llevarán a cabo dentro de cada ciclo de investigación. Inicialmente, se identifica un problema y se recopilan datos para un diagnóstico más detallado. Esto es seguido por una postulación colectiva de varias soluciones posibles, de las cuales emerge y se implementa un único plan de acción. Los datos sobre los resultados de la intervención se recopilan y analizan, y los resultados se interpretan a la luz del éxito de la acción. En este punto, el

problema se vuelve a evaluar y el proceso comienza otro ciclo. Este proceso continúa hasta que se resuelva el problema.

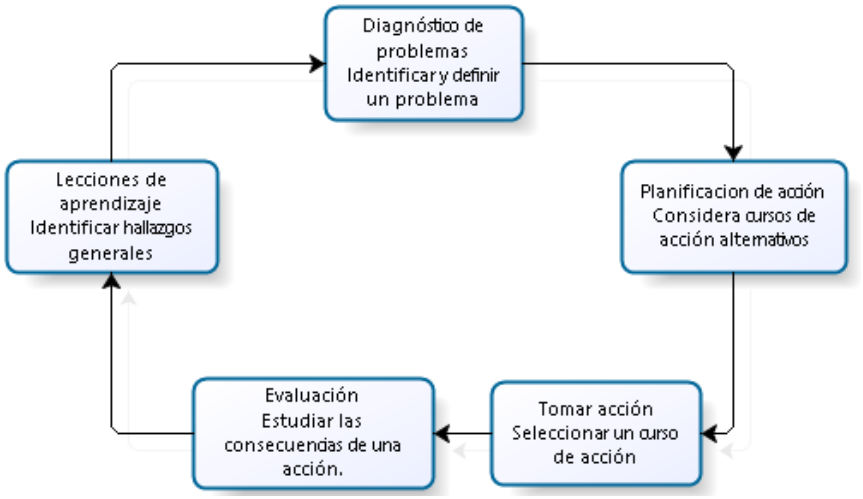


Figura 4: Modelo Action Research según Avison, Lau, Myers, & Nielsen (1999)

Como se muestra en la Figura 4, los pasos para alcanzar AR son:

- El primer paso para la aplicación de esta metodología es el diagnostico, en esta etapa se realiza la identificación de problemas primarios y la recolección de datos e información del lugar de estudio.
- Luego se tiene la etapa de planificación de las acciones a tomarse, aquí se especifican las acciones para mejorar los problemas identificados.
- Toma de acciones en la cual se selecciona y ejecuta la evaluación planificada en la organización.
- Luego se realiza una evaluación de las acciones implementadas, así como de los resultados obtenidos.
- Al final se obtienen las lecciones aprendidas con base a la identificación de hallazgos encontrados, así como el resultado del éxito o fracaso de las acciones implementadas.

Cabe recordar que la metodología es cíclica y por ello permite volver a iniciar las veces que se consideren necesarias.

Para la investigación se considerará los cinco pasos definidos por la metodología propuesta por Avison, Lau, Myers & Nielsen (1999), debido a la facilidad que esta presenta para la identificación de vulnerabilidades en la privacidad de datos en servicios web.

2.2. Metodologías existentes para el análisis de vulnerabilidades

Para el desarrollo se realizó una revisión de trabajos previos realizados por (Baskerville & Wood-Harper, 1996), (Myers, 1997), (Baskerville & Myers, 2004), (Loza Aguirre & Buitrago Hurtado, 2014). En cada estudio realizado por los autores antes mencionados se detalla el modelo Action Research y la aplicación que este tiene en investigaciones en Sistemas de Información. Para el análisis de las vulnerabilidades se considerará lo establecido en la ISO/IEC 27002:2013 inciso 12.6 e ISO/IEC 27701:2019 inciso 6.9.6: Gestión de vulnerabilidades técnicas.

2.3. Aplicación de controles de la Norma ISO 27002 e ISO 27701 para la prevención de vulnerabilidades en la privacidad de datos

Una vez definida Action Research como la metodología a utilizar en el Servicio Ecuatoriano de Capacitación Profesional (SECAP) se implementarán controles para la prevención de vulnerabilidades. Los cuales se detallan en los incisos 12.6 y 6.9.6, que definen la Gestión de vulnerabilidades técnicas.

Para descubrir las vulnerabilidades en las aplicaciones, los atacantes suelen usar herramientas o métodos específicos. Razón por la cual se tomarán revisiones técnicas formales, las cuales son acciones de evaluación de un producto de software, cuya finalidad es descubrir errores en su funcionalidad. Esta revisión se la realizará en el módulo de autenticación utilizando la ISO/IEC 27002:2013 e ISO/IEC 27701:2019.

Para ello se seguirá la guía de implementación de controles dentro del proceso de un Sistema de Gestión de Seguridad de la Información (SGSI) basado en la ISO/IEC 27002:2013 e ISO/IEC 27701:2019. En la ISO/IEC 27002 se considera que como requisito es necesario un inventario actual de activos. Para el caso de estudio se considerará los activos que tiene el SECAP en el módulo de autenticación, ya que el mismo será migrado al Framework Laravel. En el inventario de activos se incluirá al Software, la versión, el estado actual y las personas responsables dentro de la organización del manejo del software.

2.3.1. Pasos para la aplicación de controles

Para la aplicación de controles de la Norma ISO/IEC 27002:2013 e ISO/IEC 27701:2019 sobre los servicios web del Framework Laravel usado para el módulo de autenticación

implementado en el SECAP, es necesario identificar ciertas características para el levantamiento de la información y establecer en qué área es necesario desarrollar un estudio de vulnerabilidades técnicas, es decir establecer un objeto de estudio y por consiguiente realizar el análisis de vulnerabilidades según la guía de la norma escogida.

- **Diagnóstico**

  En esta etapa se realizará la identificación de roles y responsabilidades asociados con la gestión de vulnerabilidades técnicas. En el SECAP se han identificado los siguientes roles:

  - Personas involucradas en la autenticación.
  - Técnicos de TICs.

  Se ha escogido el módulo de Autenticación, debido a que el mismo maneja datos confidenciales de una persona como son: identificaciones, datos básicos, nombre de usuario, contraseñas, entre otros. Adicionalmente, los servicios web del módulo en cuestión están desarrollados en el Framework Laravel como parte del sistema SISECAP (Sistema Integrado del SECAP).

- **Planificación de las acciones a tomarse**

  Antes de ejecutar cualquier plan de mejoras, es necesario hacer un diagnóstico del estado actual de la institución de estudio, que permita una planificación de acciones futuras. Para ello se realizará una matriz de los controles especificados en la ISO/IEC 27002:2013 e ISO/IEC 27701:2019, las cuales se encuentran adaptadas para identificar las vulnerabilidades en la privacidad de datos en servicios web en el módulo de autenticación del Framework Laravel.

  La matriz considera aspectos importantes para conocer los controles implementados para el Sistema de Gestión de Seguridad de la Información (SGSI), que en sus primeras fases de implementación se utiliza para verificar el estado inicial de la organización, es decir si existen controles y que los mismos sean adecuados para evitar incidentes de seguridad, los mismos que se encuentran valorados con la escala de la tabla 1.

Tabla 1: Criterio de implementación

Criterio Implementación	Valor
Totalmente implementado	5
Implementado	4
Medianamente implementado	3
En proceso de implementación	2
Sin implementarse	1

Por otro lado, se utiliza una escala para el cumplimiento para obtener datos que ayuden a proponer una guía de mejoras basándose en la evaluación realizada. La escala utilizada para la evaluación del cumplimiento se encuentra detallada en la tabla 2, en la cual se considera 5 niveles con las siguientes valoraciones: 5 cumple en su totalidad, 4 Cumple significativamente, 3 Cumple Parcialmente, 2 Cumple mínimamente y 1 cuando no cumple.

Tabla 2: Criterio de cumplimiento

Criterio Cumplimiento	Valor
Cumple en su totalidad	5
Cumple significativamente	4
Cumple Parcialmente	3
Cumple mínimamente	2
No cumple	1

La matriz permite valorar dos aspectos, el primero para entender y evaluar el Sistema de Gestión de Seguridad de la Información (SGSI) de la institución de estudio y el segundo que se relaciona directamente con las vulnerabilidades en la privacidad de datos en servicios web del módulo especifico a estudiarse. Los parámetros que se estudiaran, basados en las normas 27001 y 27701 son:

- **Políticas de seguridad:** Permite conocer las políticas, las normas, los procedimientos, los responsables y controles implementados. Los aspectos organizativos de la seguridad de la información permiten establecer un marco de gestión e iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización, es decir ayudan a conocer los roles y las personas implicadas en la seguridad.
- **La seguridad de recursos humanos:** Es utilizada para asegurar que los empleados y contratistas entiendan sus responsabilidades y verificar si son aptos para los roles para los cuales están siendo considerados. Al analizar el control de acceso relacionado a cada perfil se conoce como se limita el acceso a la

información y a las instalaciones de procesamiento de información, para evitar y controlar accesos no autorizados. Es decir, el fin es identificar a los usuarios y la información que maneja cada uno, así como las conexiones de redes existentes.

- **Análisis de medios criptográficos implementados:** Se verifica si los sistemas tecnológicos enfocados a la criptografía protegen la confidencialidad, autenticidad e/o integridad de la información.
- **Análisis de seguridad física:** El análisis de la seguridad física y ambiental permite obtener la información necesaria para evitar accesos físicos no autorizados, daños e interferencias contra las instalaciones que la procesan.
- **El control de adquisición, desarrollo y mantenimiento de los sistemas.** Se verifica si la seguridad de la información es considerada como una parte integral en el desarrollo de los sistemas de información en todo el ciclo de vida del software. Los aspectos de seguridad permiten determinar los esquemas de construcción de software y métodos de continuidad que actualmente se encuentren implementados en el SECAP para situaciones adversas como lo es una crisis o un desastre.
- **Gestión de Activos:** Permite identificar los activos de la organización y definir las responsabilidades de protección adecuadas, y del cual se desprenden los controles siguientes:
    - **Seguridad de operaciones.** Es el control más importante dentro de la presente investigación, ya que se liga directamente a la gestión de vulnerabilidades. Mediante este se verifica si las operaciones relacionadas con el procesamiento de la información se realizan de una manera adecuada y segura, así como evaluar y prevenir vulnerabilidades técnicas.
    - **Seguridad de las telecomunicaciones.** Se evalúa la protección de la información en redes y de la infraestructura de soporte existente en el SECAP.
    - **Gestión de incidentes en la seguridad de la información**. Permite valorar los incidentes de seguridad de la información enfocada en los activos mediante un enfoque consistente y eficaz, estos incluyen la comunicación de eventos de seguridad y debilidades.

- **Toma de acciones**

Identificado el estado de la institución se tomarán las acciones necesarias para el análisis de vulnerabilidades en la privacidad de datos confidenciales del módulo de

autenticación, además de definir un procedimiento para abordar la situación en la que ha sido identificada la vulnerabilidad. Este procedimiento se realizará mediante el inciso 12.6.1. para la Gestión de vulnerabilidades técnicas establecidas en la ISO/IEC 27002:2013 e ISO/IEC 27701:2019 (apartado 2.3.2.4 que corresponde al desarrollo de la toma de acciones) y se aplicará pruebas mediante el aplicativo SISECAP, actuando como un auditor externo al sistema.

- **Evaluación**

  Una vez identificadas las vulnerabilidades asociadas al módulo de autenticación se realizará una evaluación que permita definir la construcción del manual de mejoras para el módulo de autenticación que será aplicado tanto con un enfoque administrativo y técnico.

2.3.2. Implementación de la solución

2.3.2.1. Descripción de la institución de estudio

El SECAP, forma “parte de las Redes de Capacitación y es la instancia encargada de la operativización de la capacitación no profesional, técnica de las instituciones, entidades, empresas y organismos establecidos en el ámbito de la LOSEP, en los temas de su competencia" (Echeverria, 2016, p. 1)

Misión del Servicio Ecuatoriano de Capacitación Profesional - SECAP

“Contribuir al desarrollo del país impulsando la trasformación Productiva y fortaleciendo el servicio público, a través de los servicios de perfeccionamiento, capacitación, y certificación de personas, con excelencia” (Echeverria, 2016, p. 4).

Principios y Valores del SECAP

- Compromiso: Siendo activos y proactivos a favor de la Institución en la cual trabajamos como servidores públicos, dando calidad y calidez a la sociedad. Es importante reconocer la virtud de los compañeros de trabajo, esforzándonos permanentemente por alcanzar un excelente ambiente laboral en todas sus unidades.
- Calidad: Se refiere a los efectos positivamente valorados por la sociedad respecto del servicio de perfeccionamiento, capacitación y certificación laboral que se lleva a cabo en las personas y empresas, con principios de relevancia, eficacia, pertinencia, equidad y eficiencia.

- Transparencia: En todos sus procesos y en todos sus niveles de la Gestión Institucional, con acceso inmediato a la información, que se verá reflejada en la Ley Orgánica de Transparencia y Acceso a la Información LOTAIP.
- Innovación: En la búsqueda permanente de ideas, conceptos, prácticas y metodologías para el cumplimiento eficaz y eficiente de los servicios ofertados, por parte de la Institución.
- Integridad: Siendo responsables en las actividades cotidianas aun cuando nadie las está observando. Considerando el bien personal, sin afectar los intereses de las demás. Con lo cual, se pretende alcanzar la realización de un trabajo honesto, integral y a tiempo. (Echeverria, 2016, p. 4)

Objetivos Institucionales del SECAP

- Alinear la oferta de capacitación a las necesidades del sector productivo y público del País;
- Generar ingresos por venta de servicios en pos de auto sostenimiento financiero;
- Impulsar el desarrollo del Talento Humano institucional; y,
- Mejorar la capacidad de gestión institucional y la eficiencia en el uso de los recursos. (Echeverria, 2016, p. 4)

La estructura organizacional de los puestos directivos se muestra en la figura 5:

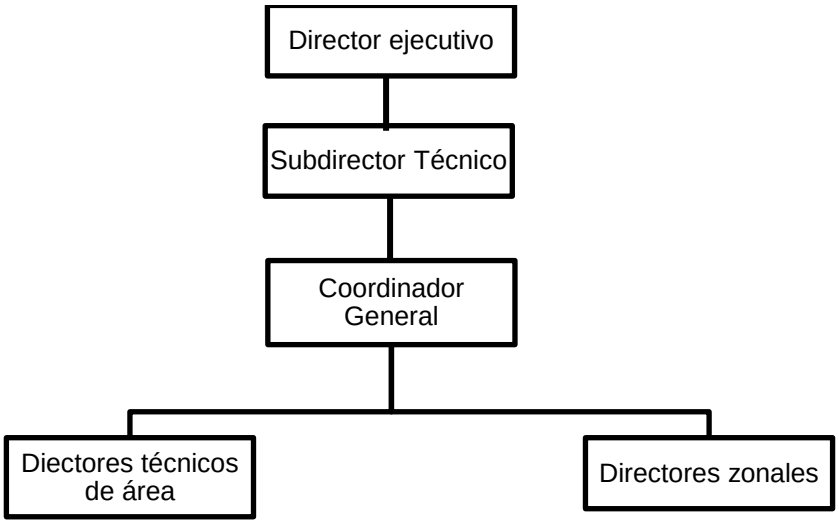


Figura 5: Estructura organizacional del SECAP

La estructura general de la organización se realiza de acuerdo con principios gobernantes definidos en el Estatuto Orgánico vigente y se detallan en la Figura 6:

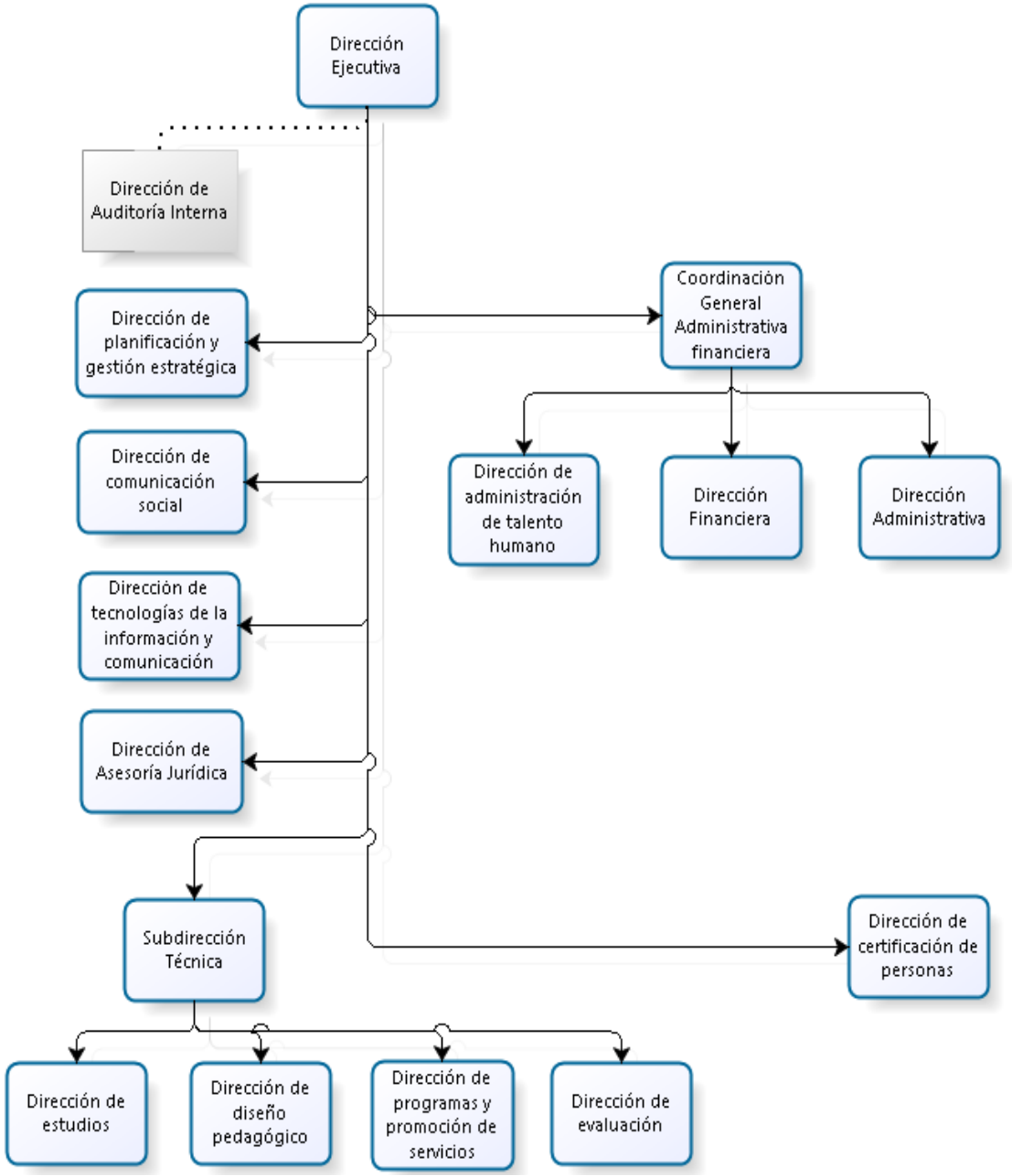


Figura 6: Estructura orgánica por procesos del SECAP

2.3.2.2. Identificación de roles

El módulo de autenticación está bajo la supervisión de Dirección de Tecnologías de la Información y Comunicación, el cual posee una estructura organizacional basada en

procesos internos y se presenta en el anexo 2. En la tabla 3 se hace un detalle de los encargados del área de TICs con sus responsabilidades.

Tabla 3: Roles SECAP (Echeverria, 2016)

Rol	Responsabilidad
Director de TICs	1. Gestionar el esquema gubernamental de seguridad de la información en la institución, así como el ciclo de vida de las aplicaciones y sistemas informáticos para automatizar y mejorar los procesos internos y los servicios al ciudadano; 2. Asegurar la disponibilidad y operatividad de toda la plataforma tecnológica de la Institución;
Analista de TICs	1. Elaborar repositorios e inventarios de códigos fuente versionados, scripts de base de datos versionados, instaladores, archivos de configuración y parametrización, reportes de control de cambio y versiones del desarrollo de los aplicativos y sistemas informáticos desarrollados, adquiridos o adaptados; 2. Servicios web y documentación relacionada para compartir e intercambiar datos e información electrónica por medio de la plataforma gubernamental; dispositivos electrónicos, hardware y software, enfocados a brindar seguridad a la información institucional;
Analista de TICs administración central	1. Informes de gestión, manuales, procedimientos y estándares de operación y monitoreo de equipos, redes, bases de datos, servidores de aplicaciones web, balanceadores de carga, etc.; 2. Diagramas de aplicaciones y arquitecturas de servidores, redes LAN/WAN/WIRELESS, interconexión, almacenamiento, respaldo y recuperación, centralización y virtualización, solicitudes y formatos de cambios en aplicativos sistemas y servicios informáticos de la institución; 3. Inventario de producción, mantenimiento de redes y telecomunicaciones, incidentes, planes de entrenamiento en aplicativos, respaldos y restauraciones; 4. Reportes de análisis estadísticos de los datos obtenidos en las encuestas sobre los servicios de TI; 5. Inventario de soporte tecnológico, respaldos y restauraciones. 6. Políticas de seguridad de la información y procedimientos para su aplicación; 7. Planes de contingencia y prevención de impacto operativo a nivel de seguridad, por cambios, equipamiento y servicios tecnológicos; 8. Pruebas periódicas de copias de resguardo y restauración de la información en base a los perfiles de usuario;

En la supervisión técnica se encuentran el Director de Tecnología, el Coordinador de proyectos de TI y el equipo de desarrollo formado por tres personas.

2.3.2.3. Ejecución de la Metodología

De acuerdo con AR, es necesario definir los pasos que deben seguirse para obtener resultado deseado. En la Figura 7 se describen los pasos que conforman el plan de acción. La recolección de información (1) se realizará mediante un análisis del estado actual del SECAP mediante la aplicación de la matriz del Anexo 1, en base a los controles de la ISO/IEC 27002:2013.

Como parte del análisis del estado actual, se revisa si en la organización existe un inventario actual y completo de activos; esto incluye toda la información del software utilizado en la organización: su versión, estado actual, los responsables, etc. El inventario de activos se utilizará para apoyar la gestión de vulnerabilidades técnicas mediante una valoración de activos en disponibilidad, integridad y confidencialidad.

Como parte del análisis, se verificará también el sistema informático y los controles existentes mediante la aplicación de la matriz de la Tabla 4 para identificar las vulnerabilidades en la privacidad de datos en el módulo de autenticación del SECAP. Esto con el fin de conocer cómo afectan las vulnerabilidades al software basándose en la lista de inventario de activos asociados al desarrollo del módulo de autenticación.

A continuación, se procede a utilizar herramientas para la detección de vulnerabilidades (2) a nivel de implementación del módulo, con el aplicativo SonarQube que será utilizado a nivel de código. Con esta herramienta también se procederá a hacer pruebas de penetración (3) en el funcionamiento del módulo con el fin de encontrar la mayor parte de vulnerabilidades para su respectivo análisis (4).

Luego se procederá a elaborar un plan de seguridad informática (5) en el que se indique cómo reaccionar ante una vulnerabilidad en la privacidad de datos para finalizar con una matriz en la que se detallen las vulnerabilidades encontradas en el módulo de autenticación del SECAP (tabla 26).

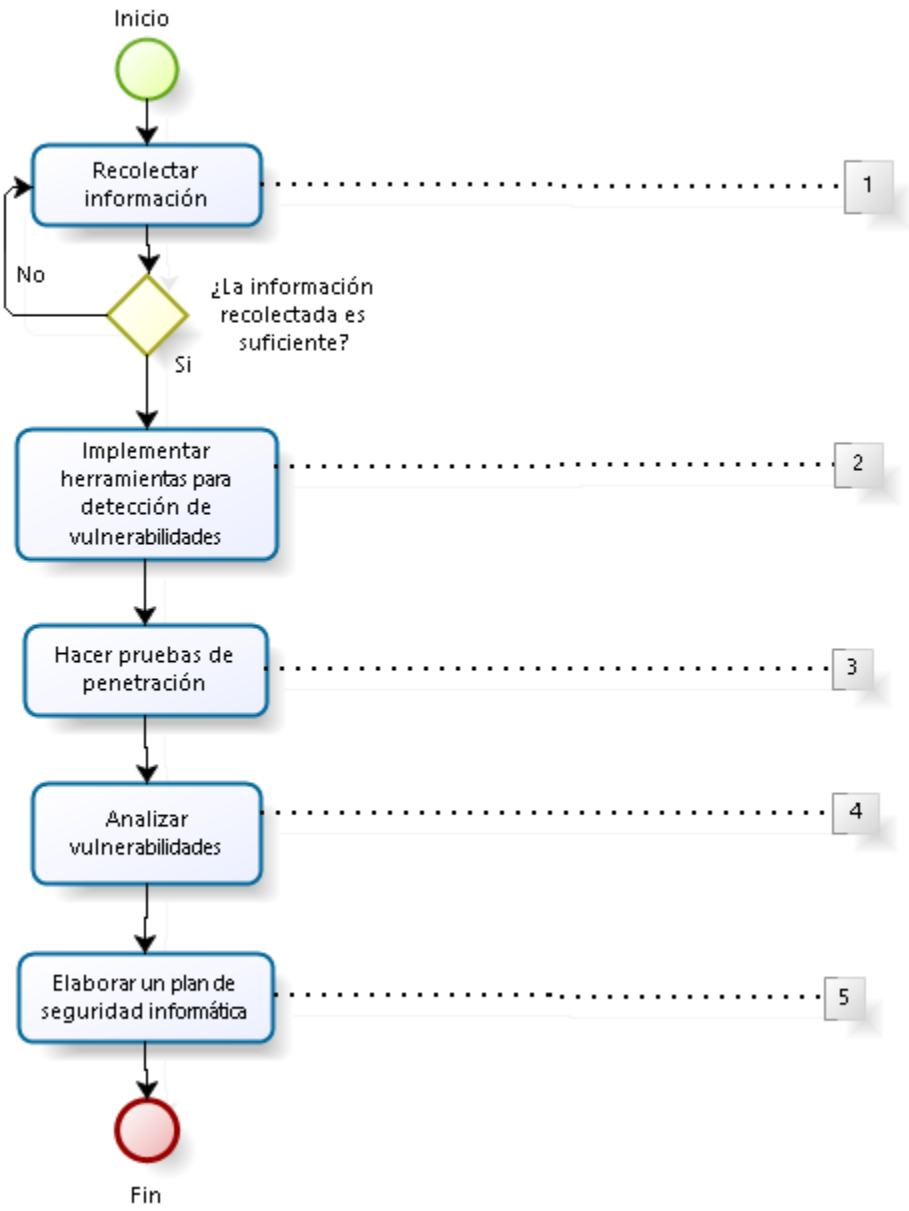


Figura 7: Planificación de acciones a desarrollarse

Para la recolección de la información se utilizó una matriz conforme a los controles indicados en la Norma ISO 27002 y 27701 la misma que fue aplicada a continuación, se desarrolla la matriz con los resultados de la implementación de los controles de la norma ISO/IEC 27002: 2013 en el módulo de autenticación del SECAP, como parte de esta se hace una valoración de implementación y de cumplimiento, como se muestra los resultados se encuentran en el Anexo 3.

Debido a las condiciones sanitarias actuales durante las cuales se desarrolló el proyecto, la valoración la realizó el encargado del área de tecnología en el SECAP bajo la tutoría y asesoramiento del investigador a través de videoconferencia, para así garantizar su fiabilidad.

2.3.2.4. Valoración de los activos de la organización

En la evaluación se evidenció que el módulo de autenticación del SECAP no posee implementado en su totalidad controles para el Sistema de Gestión de Seguridad de la Información (SGSI).

Como parte del análisis de la recopilación de información, en las tablas 4, 5 y 6 se resume los activos físicos con los que cuenta el departamento encargado de la realización del Módulo de autenticación del SECAP en el mismo que se especifica la cantidad, la ubicación y la persona responsable de su manejo, como se detalla en la tabla 4.

Tabla 4: Características de los equipos de computo

Ambiente	Cantidad	Equipo de computo	CPU	RAM	Disco Duro
	4	Desktop	Core i7 3,4 Ghz (3gen)	12 Gb	256 Gb
Servidor Desarrollo	1	Virtual Server	4 Vcpu 3 Ghz	8 Gb	200 Gb
Secure Quality Management (SQM)	1	Laptop	Core i7 3 Ghz (3gen)	8 Gb	512 Gb
Servidor SQM	1	Virtual Server	4 Vcpu 3 Ghz	1 2 Gb	200 Gb

Los programas instalados en los equipos de cómputo se muestran en la tabla 5.

Tabla 5: Programas instalados en equipos de computo

Equipo de Desarrollo	Servidor de Desarrollo	SQM
Windows 10	CentOS 7	Widows 10
Laragon 4.0	Apache 2.4	Laragon 4.0
Apache 2.4	MySql 5.7	Apache 2.4

MySql 5.7	Php 7.2	MySql 5.7
Php 7.2	Avast Antivirus	Php 7.2
Visual Studio Code 1.44		Visual Studio Code 1.44
Postman 7.24		Postman 7.24
Navicat 12.1		Navicat 12.1
Avast Antivirus		Avast Antivirus

Los activos usados en el módulo de Autenticación del SECAP se presentan a continuación:

Tabla 6: Activos módulo de Autenticación del SECAP

Ámbito	**Activo**
Información (I)	Datos de usuarios
	Información de recursos educativos
Aplicaciones informáticas (AI)	Windows 10
	Centos 7
	Laragon 4.0
	Apache 2.4
	MySql 5.7
	Php 7.2
	Visual Studio Code 1.44
	Postman 7.24
	Navicat 12.1
Equipos informáticos (EI)	Impresoras
	Router
	Computadoras personales
	Servidor virtual

Una vez identificados los activos se procede a valorarlos, según la importancia que tienen para la empresa. Se evalúa su disponibilidad integridad y confidencialidad como se muestra en la tabla 7, mientras que en las tablas 8 y 9 se explican los resultados de las valoraciones obtenidas para cada uno de los activos físicos. Se inicia con los activos relacionados al módulo de Autenticación para identificar las vulnerabilidades en la privacidad de datos.

Tabla 7: Valoración de activos

Disponibilidad	
Valor	**Criterio**
0	No aplica/ no es relevante
1	Debe estar disponible al menos el 10% del tiempo
2	Debe estar disponible al menos el 50% del tiempo
3	Debe estar disponible al menos el 90% del tiempo
4	Debe estar disponible al menos el 99% del tiempo

Integridad	
Valor	**Criterio**
0	No aplica/ no es relevante
1	No es relevante los errores que tenga o la información que falte
2	Tiene que estar correcto o completo al menos en un 50%
3	Tiene que estar correcto o completo al menos en un 75%
4	Tiene que estar correcto o completo al menos en un 95%

Confidencialidad	
Valor	**Criterio**
0	No aplica/ no es relevante
1	Daños muy bajos, el incidente solo afecta a esta área
2	Daños relevantes, afectan a otras áreas
3	Daños considerables, afectan a casi todo el funcionamiento de la empresa
4	Daños catastróficos, afectan la imagen y reputación de la empresa

Tabla 8: Valoración de datos de usuario

Dimensión	**Valor**	**Justificación**
Disponibilidad	2	La información de los usuarios debe de estar disponible la mayor parte del tiempo, ya que es necesaria para el correcto funcionamiento de las demás áreas.
Integridad	4	Los datos personales de los usuarios deben ser protegidos para que no puedan ser modificados por personal no autorizado, ya que si se modifican puede ocasionar que afecte el funcionamiento de la organización.
Confidencialidad	2	Los datos personales de los usuarios no deben estar expuestos a personas no autorizadas ya que puede causar daños que afecten otras áreas.

Tabla 9: Valoración de información de recursos educativos

Dimensión	Valor	Justificación
Disponibilidad	4	Los recursos educativos deben estar disponibles la mayor parte del tiempo, ya que estos son usados todo el tiempo ya sea por docentes o estudiantes.
Integridad	4	Debe estar correcto o completo para el funcionamiento adecuado
Confidencialidad	0	No aplica, ya que la información debe ser de libre acceso.

A continuación, se procede a la valoración de aplicaciones informáticas, tal como se detalla en las tablas 10, 11 y 12, según los valores de la tabla 7.

Tabla 10: Valoración de Laragon 4.0

Dimensión	Valor	Justificación
Disponibilidad	4	La aplicación informática debe estar disponible la mayor parte del tiempo ya que permite la integración de varias funcionalidades de Laravel y PHP
Integridad	4	La información que posee el programa tiene que ser resguardada para que no pueda ser alterada sin autorización; además se debe controlar que la información este completa.
Confidencialidad	4	El acceso no autorizado a la información puede ocasionar daños que afecten a la organización.

Tabla 11: Valoración de Apache 2.4

Dimensión	Valor	Justificación
Disponibilidad	4	La aplicación informática debe estar disponible la mayor parte del tiempo ya que permite el correcto funcionamiento del módulo de autenticación
Integridad	4	La información que posee el programa tiene que ser resguardada para no ser alterada sin autorización; además se debe controlar que la información este completa.
Confidencialidad	4	El acceso no autorizado a la información puede ocasionar daños que afecten a la organización.

Tabla 12: Valoración de Php 7.2

Dimensión	Valor	Justificación
Disponibilidad	4	La aplicación informática siempre debe estar disponible ya que permite el correcto funcionamiento del aplicativo del Framework de Laravel y PHP
Integridad	4	La información que posee el programa tiene que ser resguardada ya que estos no pueden ser alterados sin autorización; además se debe controlar que la información este completa.
Confidencialidad	4	El acceso no autorizado a la información puede ocasionar daños catastróficos que afecten a la organización.

Finalmente, en las tablas 13, 14, 15 y 16 se realiza la valoración de los equipos informáticos que forman parte del módulo de autenticación del SECAP. Para ello se utiliza la valoración de la tabla 7.

Tabla 13: Valoración de computadoras equipo de desarrollo

Dimensión	Valor	Justificación
Disponibilidad	4	Las computadoras del equipo de desarrollo tienen que estar disponibles siempre ya que estas proporcionan información indispensable para el funcionamiento de otras áreas.
Integridad	4	La información que poseen los equipos de cómputo tiene que ser resguardada ya que estos no pueden ser alterados sin autorización; además se debe controlar que la información este completa.
Confidencialidad	4	El acceso no autorizado puede ocasionar daños catastróficos que afecten a la organización.

Tabla 14: Valoración de Servidor de desarrollo

Dimensión	Valor	Justificación
Disponibilidad	4	Debe estar disponible ya que este proporciona información para el desarrollo de otras áreas.
Integridad	4	Este debe de funcionar adecuadamente en al menos un 95% ya que la información proporciona datos importantes.
Confidencialidad	4	El servidor de desarrollo es importante ya que si alguien no autorizado accede a la información que este posee puede ocasionar daños catastróficos que afecten la imagen y funcionamiento de la organización.

Tabla 15: Valoración de SQM (Secure Quality Management)

Dimensión	Valor	Justificación
Disponibilidad	4	Debe de estar disponible para asegurar la calidad de la información que este proporciona
Integridad	4	Los datos de este módulo siempre deben de ser correctos para asegurar la calidad y también deben ser protegidos para que no puedan ser modificados por personal no autorizado, ya que si se modifican puede causar un daño grave.
Confidencialidad	3	El SQM es importante ya que si alguien no autorizado accede a este puede ocasionar daños catastróficos que afecten la imagen y funcionamiento de la organización.

Tabla 16: Valoración de servidor SQM

Dimensión	Valor	Justificación
Disponibilidad	4	La información del servidor SQM debe de estar disponible, ya que es necesaria para el correcto funcionamiento de las demás áreas.
Integridad	4	Los datos del servidor SQM deben ser protegidos para que no puedan ser modificados por personal no autorizado, ya que si se modifican puede causar un daño grave.
Confidencialidad	3	El servidor de desarrollo es importante ya que si alguien no autorizado accede a la información que este posee puede ocasionar daños catastróficos que afecten la imagen y funcionamiento de la organización.

A partir de la valoración de los medios físicos se procede con su evaluación en función de su utilización en el desarrollo del módulo de autenticación utilizando los servicios web del Framework Laravel, mediante los siguientes aspectos:

- ÁMBITO (Amb): Información (I), Aplicaciones informáticas (AI), Equipos informáticos (EI)
- FUNCIÓN (Fun): Importancia de la tarea que cumplen los bienes informáticos.
- COSTO (Co): Valor y valor de uso de los bienes informáticos.
- IMAGEN (Im): Repercusión interna y/o externa que ocasionaría la pérdida de los bienes informáticos.
- CONFIDENCIALIDAD (Con): Necesidad de proteger la información que de los bienes informáticos pueda obtener.
- INTEGRIDAD (Int): Necesidad de que la información no se modifique o destruya.

- DISPONIBILIDAD (Disp): Que los bienes informáticos se puedan obtener en todo momento de forma autorizada.
- IMPORTANCIA. (Imp): Importancia de los bienes informáticos. Esta se obtiene de la suma de la función, costo, imagen, confidencialidad, integridad y disponibilidad.

Los activos serán valorados según la tabla 17.

Tabla 17: Valoración de activos

Criterio	**Valor**
Importancia baja	1
Importancia media	2
Importancia alta	3
Importancia muy alta	4

La importancia de los bienes informáticos se calcula mediante el promedio de la función, costo, imagen, confidencialidad, integridad y disponibilidad. Se considera la fórmula del estudio realizado por (Franco, Perea, & Tovar, 2013), mostrada en la Tabla 18.

$$Imp = \frac{Fun + Co + Im + Con + Int + Disp}{6}$$

Tabla 18: Evaluación de activos

Activo	Ámbito	Función	Costo	Imagen	Confidencialidad	Integridad	Disponibilidad	Importancia
Datos de usuario	I	3	4	4	2	4	2	3,17
Recursos educativos	I	1	1	2	0	4	4	2
Laragon 4.0	AI	3	4	4	4	4	4	3,83
Apache 2.4	AI	3	4	4	4	4	4	3,83
MySql 5.7	AI	4	4	4	4	4	4	3,83
Php 7.2	AI	3	4	4	4	4	4	3,83
Computadoras desarrollo	EI	3	3	4	4	4	4	3,67
Servidor de desarrollo	EI	4	4	4	4	4	4	4
SQM	EI	4	4	4	3	4	4	3,83
Servidor SQM	EI	4	4	4	3	4	4	3,83

En la tabla 18 se muestra con color rojo los resultados de los activos que se consideran más importantes en el módulo de autenticación del SECAP.

Los bienes informáticos críticos para la organización según la importancia son las computadoras del equipo de desarrollo, el servidor de desarrollo, SQM y el servidor de SQM. Estos bienes proporcionan todos los recursos necesarios para el desarrollo en el Framework Laravel. Las aplicaciones informáticas críticas son Laragon, Apache, MySql y PHP.

2.3.2.5. Identificación de amenazas y estimación de riesgos

Luego de identificar los bienes informáticos críticos que necesitan ser resguardados se procede a identificar las amenazas que se relacionan a estos ya que su pérdida potencial tiene un alto impacto en el módulo de Autenticación según lo establecido en la norma ISO/IEC 27701:2019.

Para la estimación del riesgo sobre los bienes informáticos de mayor importancia se determina las diferentes amenazas que pueden ocurrir encada uno. La identificación de amenazas se puede agrupar en las categorías de la tabla 19.

Tabla 19: Identificación de amenazas

Criterio	Código	Valor
Origen físico	AF 1	Incendio
	AF 2	Inundaciones
	AF 3	Sismo
	AF 4	Sobrecarga eléctrica
	AF 5	Falla de corriente (apagones)
	AF 6	Falla del sistema / Daño de disco duro
Nivel de usuario	AU1	Falta de inducción, capacitación y sensibilización sobre riesgos
	AU2	Mal manejo de sistemas y herramientas
	AU3	Perdida de datos por error de usuario
Nivel Hardware y Software	AH1	Propagación de virus informático
	AH2	Exposición o extravío de equipo, unidades de almacenamiento
	AH3	Perdida de datos por error hardware
	AH4	Falta de mantenimiento físico
	AS1	Falta de actualización de software (proceso y recursos)
Nivel de datos y redes	AD1	Manejo inadecuado de datos críticos (modificar, borrar, etc.)
	AD2	Transmisión no cifrada de datos críticos
	AR1	Dependencia de servicio técnico externo
	AR2	Red inalámbrica expuesta al acceso no autorizado
	AR3	Acceso electrónico no autorizado a sistemas externos
	AR4	Acceso electrónico no autorizado a sistemas internos
Acceso	AA1	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)
	AA2	Compartir contraseñas o permisos a terceros no autorizados

Con las amenazas identificadas en la Tabla 19 se hace una valoración del riesgo de que cada una de ellas ocurra, utilizando la valoración de la Tabla 20. El peso se obtiene del producto del riesgo total por la importancia según la fórmula del estudio realizado por (Franco, Perea, & Tovar, 2013).

$$Peso = Riesgo\ total * Importancia$$

Para encontrar los activos informáticos que poseen mayor riesgo se considera como datos de entrada la valoración de la tabla 17, y se la compara con los valores expuestos en la tabla 20.

Tabla 20: Valoración de riesgos

Criterio	Valor
Riesgo bajo	0 - 1
Riesgo medio	1,1 - 2
Riesgo alto	2,1 - 3
Riesgo muy alto	3,1 - 4

Tabla 21: Valoración de riesgos con amenazas de origen físico

Ámbito	Activo	Amenazas (Ocurrencia)						Riesgo total	Importancia	Peso
		AF1	AF2	AF3	AF4	AF5	AF6			
Aplicaciones informáticas (AI)	Servidor de desarrollo	1	1	2	2	1	2	1,50	3,67	5,50
	SQM	1	1	2	2	1	3	1,67	4	6,68
	Servidor SQM	1	1	2	2	1	3	1,67	3,83	6.40
	Laragon 4.0	1	1	2	2	2	3	1,83	3,83	7,01
	Apache 2.4	1	1	2	2	2	3	1,83	3,83	7,01
	MySql 5.7	1	1	2	2	2	3	1,83	3,83	7,01
	Php 7.2	1	1	2	2	2	3	1,83	3,83	7,01
Equipos informáticos (EI)	Computadoras de desarrollo	1	1	2	2	1	3	1,67	3,83	6,40
								Total	**30,65**	**53,02**

El peso total se obtiene mediante la fórmula del estudio realizado por (Franco, Perea, & Tovar, 2013), considerando como los valores a utilizarse los obtenidos de las mediciones mostradas en la tabla 21. La fórmula se expresa como:

$$Peso_{total} = \frac{Peso}{Importancia}$$

$$Peso_{total} = \frac{53{,}02}{30{,}65}$$

$$Peso_{total} = 1{,}73$$

Según la valoración de riesgos de la tabla 20 existe un riesgo medio de que ocurran amenazas de origen físico.

Tabla 22: Valoración de riesgos con amenazas de nivel de usuario

Ámbito	Activo	Amenazas (Ocurrencia)			Riesgo	Importancia	Peso
		AU1	AU2	AU3			
Aplicaciones informáticas (AI)	Servidor de desarrollo	3	2	3	2,67	3,67	9,80
	SQM	3	2	4	3	4	12
	Servidor SQM	3	2	4	3	3,83	11,49
	Laragon 4.0	2	2	4	2,67	3,83	10,23
	Apache 2.4	2	2	4	2,67	3,83	10,23
	MySql 5.7	2	2	4	2,67	3,83	10,23
	Php 7.2	2	2	4	2,67	3,83	10,23
Equipos informáticos (EI)	Computadoras de desarrollo	3	2	3	2,67	3,83	10,23
					Total	**30,65**	**84,44**

$$Peso_{total} = \frac{84{,}44}{30{,}65} = 2{,}75$$

La valoración total de los riesgos, mostrada en la tabla 22 permite calcular el peso total de las amenazas a nivel de usuario, teniendo este un valor de 2,75 lo que indica que posee un riesgo alto (ver tabla 20).

Tabla 23: Valoración de riesgos con amenazas a nivel de hardware y software

Ámbito	Activo	Amenazas (Ocurrencia)					Riesgo	Importancia	Peso
		AH1	AH2	AH3	AH4	AS1			
Aplicaciones informáticas (AI)	Servidor de desarrollo	3	2	4	3	3	3	3,67	11,01
	SQM	3	2	3	2	3	2,6	4	10,4
	Servidor SQM	3	2	4	3	3	3	3,83	12
	Laragon 4.0	2	1	4	1	3	2,2	3,83	8,43
	Apache 2.4	2	1	4	1	3	2,2	3,83	8,43
	MySql 5.7	3	3	4	1	3	2,8	3,83	10,72
	Php 7.2	2	3	4	1	3	2,6	3,83	9,96
8Equipos informáticos (EI)	Computadoras de desarrollo	3	2	4	3	3	3	3,83	11,49
							Total	**30,65**	**82,44**

$$Peso_{total} = \frac{82{,}44}{30{,}65}$$

$$Peso_{total} = 2{,}69$$

A nivel de activos físicos, la tabla 23 permite calcular el peso total de sus amenazas intrínsecas. Siguiendo la fórmula de (Franco, Perea, & Tovar, 2013), se obtiene un valor de 2,69 lo que indica que su riesgo es alto (ver tabla 20).

La tabla 24 muestra las mediciones sobre los valores de datos y redes, que es un valor independiente de los valores medidos hasta el momento.

Se muestra en rojo los resultados debido a que son los más relevantes e indican que estas amenazas tienen la mayor probabilidad de ocurrencia

Tabla 24: Valoración de riesgos con amenazas a nivel de datos y redes

Ámbito	Activo	Amenazas (Ocurrencia)						Riesgo	Importancia	Peso
		AD1	AD2	AR1	AR2	AR3	AR4			
Aplicaciones informáticas (AI)	Servidor de desarrollo	4	4	3	4	4	4	3,83	3,67	14,06
	SQM	4	4	3	4	3	4	3,33	4	13,32
	Servidor SQM	4	4	3	4	4	4	3,83	3,83	14,67
	Laragon 4.0	4	4	4	3	3	4	3,67	3,83	14,06
	Apache 2.4	4	4	4	3	3	4	3,67	3,83	14,06
	MySql 5.7	4	4	4	3	3	4	3,67	3,83	14,06
	Php 7.2	4	4	4	3	3	4	3,67	3,83	14,06
Equipos informáticos (EI)	Computadoras de desarrollo	4	3	4	3	4	4	3,33	3,83	12,75
								Total	**29,51**	**111,05**

* Para el código de amenazas de ocurrencia se considera la tabla 19

$$Peso_{total} = \frac{111{,}05}{29{,}51}$$

$$Peso_{total} = 3{,}76$$

El peso total de las amenazas a nivel de datos y redes es de 3,76 lo que indica que su riesgo es muy alto (ver tabla 20).

Tabla 25: Valoración de riesgos con amenazas de acceso

Ámbito	Activo	Amenazas (Ocurrencia)		Riesgo	Importancia	Peso
		AA1	AA2			
Aplicaciones informáticas (AI)	Servidor de desarrollo	4	4	4	3,67	14,68
	SQM	3	4	3,5	4	14
	Servidor SQM	4	3	3,5	3,83	13,40
	Laragon 4.0	3	4	3,5	3,83	13,40
	Apache 2.4	4	4	4	3,83	15,32

	MySql 5.7	4	4	4	3,83	15,32
	Php 7.2	4	4	4	3,83	15,32
Equipos informáticos (EI)	Computadoras de desarrollo	3	4	3,5	3,83	13,40
				Total	**30,65**	**114,84**

* Para el código de amenazas de ocurrencia se considera la tabla 19

$$Peso_{total} = \frac{111{,}05}{29{,}51}$$

$$Peso_{total} = 3{,}76$$

Asimismo, los valores de la tabla 25 muestran que el peso total de las amenazas a nivel de acceso es de 3,76 lo que indica que su riesgo es muy alto (ver tabla 20).

En los resultados obtenidos en las tablas precedentes se encontró que las amenazas a nivel de redes, datos y de acceso tienen un riesgo muy alto. Por ello se deben definir políticas que permitan mitigar o eliminar las vulnerabilidades y amenazas para que no afecten el correcto desarrollo de la institución. A partir de estas políticas se deben establecer medidas específicas que permitan la ejecución de las políticas y así mitigar las amenazas identificadas sobre cada bien informático en particular, considerando su probabilidad de ocurrencia y el peso de riesgo estimado para cada uno de ellos, disminuyendo de esta forma el peso total del riesgo.

2.3.2.6. Calidad de codificación del módulo

Para evaluar la calidad de código, se va a aplicar la herramienta SonarQube scanner versión 6.7.7. SonarQube, en comparación de otros aplicativos evaluados, es de libre uso, no necesita depender de la instalación de otro sistema operativo para su funcionamiento, está especializado en varios lenguajes de desarrollo conocidos incluido PHP, permite realizar análisis de vulnerabilidades y el resultado es expresado como problemas de calidad de software (casos en los que se rompieron las reglas de codificación). El programa realiza un análisis estático del código fuente (archivos Java, programas COBOL, etc.). Se puede realizar un análisis estático del código compilado para ciertos lenguajes (archivos .class en Java, archivos .dll en C #, etc.). Durante el análisis, se solicitan datos del servidor, se analizan los archivos proporcionados durante el análisis y los datos resultantes se

envían al servidor al final en forma de informe, que luego se analiza de forma asíncrona en el lado del servidor.

Los informes de análisis se ponen en cola y se procesan secuencialmente, por lo que es muy posible que durante un breve período después de que su registro de análisis muestre su finalización, los valores actualizados no sean visibles en su proyecto SonarQube. Los resultados obtenidos del análisis del software como activo se presentan en la sección 3.2 del Capítulo 3.

Nivel de implementación de funcionalidades relacionadas con la autenticación

El nivel de implementación se encuentra relacionado con políticas y funcionalidades actualizadas, con el fin de prevenir ataques de personas externas o del mismo personal que trabaja en la institución. El módulo de autenticación se encuentra conformado por un usuario y una contraseña. Lo cual se ha determinado como los datos sensibles de este módulo, ya que son la llave de acceso al sistema principal (SISECAP).

2.3.2.7. Evaluación

Al realizar la evaluación del módulo de autenticación del SECAP se encontró los resultados mostrados en la tabla 26.

Tabla 26: Evaluación de acciones a tomarse

Vulnerabilidad	Acción a tomarse	Evaluación
Nombres de usuarios y perfiles de usuario para acceso al sistema		
No se encuentra definido un perfil de usuario	En el aplicativo SISECAP se debe implementar perfiles de usuario para el ingreso diferenciando estudiante, docente o directivo	Al definir perfiles de usuario se tendrá un acceso controlado al sistema SISECAP y por ende mayor seguridad.
No se encuentra implementado un administrador de dominio	Se debe crear un nombre de usuario con una cuenta genérica de administrador de dominio para un estudiante, o una cuenta propia para un docente o directivo	Si se implementa un administrador de dominio se reduce del costo y el esfuerzo de la administración de una red de dominio. También se facilita la centralización de los recursos y de gestión, así como la autenticación y autorización de usuarios.
Políticas de ingreso de contraseñas		
No se asigna contraseña por defecto al ingreso de usuario	Se le debe asignar una contraseña por defecto al usuario, y el mismo tendrá la obligación de cambiarlo	Al crear una contraseña por defecto se puede gestionar de

	por una nueva clave para poder ingresar al aplicativo	una manera adecuada el ingreso al aplicativo
No tiene un número mínimo de caracteres en contraseña	Establecer una política para ingreso de contraseñas de mínimo 8 caracteres para tener un nivel de seguridad aceptable, ingresar una mayúscula, por lo menos un número y un carácter especial	Al controlar los caracteres de la contraseña se asegura que esta tenga un nivel aceptable de seguridad
El aplicativo no cuenta con un tiempo de caducidad de la contraseña registrada por el usuario	Agregar un tiempo de caducidad de contraseña ingresada de por lo menos tres meses para mitigar esta vulnerabilidad	Si se implementa un tiempo de caducidad de contraseña se puede subir el nivel de seguridad
Segundo factor de autenticación		
El segundo factor de autenticación no implementa el uso de SMS o mail para recibir clave, temporal, tampoco usa aplicaciones como como Authy, Google Authenticator, FreeOTP, etc.	Implementar un segundo factor de autenticación para que el aplicativo SISECAP tenga otro nuevo filtro en caso de posibles usurpaciones.	Si se implementa un segundo factor de autenticación se tiene mayor protección y se evita que se atacantes puedan acceder a la cuenta
No se gestiona adecuadamente en caso de olvido de contraseña	En caso de olvido de contraseña, utilizar algunas de las sugerencias del segundo factor de autenticación, y en el aplicativo solicitar el ingreso de una nueva clave de ingreso.	Si se implementa un segundo factor de autenticación se podrá gestionar adecuadamente la recuperación de contraseña, además de verificar que la nueva clave ingresada cumpla con los parámetros solicitados para mayor seguridad
Caducidad de sesión de usuario		
El aplicativo no cuenta con un tiempo de caducidad de la contraseña registrada por el usuario	El aplicativo deberá tener una caducidad de sesión por inactividad de 10 minutos.	Al implementar un tiempo de caducidad de sesión se ayuda a que los datos de usuario no estén expuestos y por lo tanto se mejora la seguridad del aplicativo
No se controla el acceso a través de varios dispositivos	En caso se ingresar al sistema con el mismo usuario desde otro dispositivo, deberá generar un cierre automático de la sesión iniciada en el dispositivo anterior	Si se controla el ingreso al sistema a través de varios dispositivos se ayuda a manejar adecuadamente la seguridad
Path o URL del aplicativo SISECAP		

El path del sistema SISECAP se encuentra expuesto en la web	Se recomienda aplicar alguna herramienta de enmascaramiento del path del sistema académico como por ejemplo Dynamic Data Masking	Al aplicar una herramienta de enmascaramiento se protege el ingreso de personas no autorizadas al sistema
Codificación en desarrollo de módulo de autenticación		
110 bugs en código fuente de módulo de autenticación de aplicativo	La herramienta recomienda remover código basura, relacionado con: Métodos no utilizados, variables y objetos innecesarios, y valores que quemados en las validaciones lógicas de este módulo.	Si se sigue las recomendaciones se mejora la seguridad en el aplicativo
1,5 k Code Smell lo que significa que existe un problema relacionado con la mantenibilidad en el código, 54% de código duplicado.	Se recomienda seguir las guías de corrección de la herramienta de análisis Sonar Qube para mitigar estas vulnerabilidades presentadas. Sonar Qube sugiere principalmente hacer refactorizaciones de métodos, funciones propias del framework y reducir validaciones redundantes para un mejor mantenimiento del código.	Si se sigue las recomendaciones se mejora la seguridad en el aplicativo
Se encontraron 2 puntos de acceso de seguridad (hotspots)	Aplicar las correcciones propuestas por la herramienta, refactorizar los métodos para que los mismos sean desacoplados, y puedan ser reutilizados, según lo requiera la lógica del módulo analizado	Si se sigue las recomendaciones se mejora la seguridad en el aplicativo
Se encontraron 1074 problemas abiertos.	Aplicar las reglas de codificación que propone la herramienta Sonar Qube para mitigar las vulnerabilidades de código mencionadas.	Si se sigue las recomendaciones se mejora la seguridad en el aplicativo

3. RESULTADOS

En el presente capítulo se muestran los resultados de la aplicación de los controles del SGSI sobre el módulo de autenticación del SECAP para la prevención de vulnerabilidades en la privacidad de datos del Framework Laravel, como paso final de la metodología Action Research (Identificación de los hallazgos de la puesta en marcha de la metodología), además se presentan los resultados de la herramienta aplicada para la detección de vulnerabilidades.

3.1. Gestión de Seguridad de SECAP

En la figura 8 se muestran los resultados relaciónados a la implementación y en cuanto al cumplimiento, la figura 9 muestra los valores relacionados a esta evaluación. Al analizar la implemetación se encuentra que no hay ningun control implementado en su totalidad, la mayoria se encuentran implementados medianamente o en proceso.

Al analizar el cumplimiento se obtuvo que los controles relacionados con Políticas de Seguridad, Aspectos Organizativos de la seguridad de la información, Seguridad de recursos humanos, Gestión de activos y Control de acceso cumplen en su totalidad la mayor parte de controles. Los controles de criptografía, seguridad física y ambiente, Seguridada de operaciones, Seguridad en las telecomunicaciones, Adquisición, desarrollo y mantenimiento de los sistemas, Gestión de incidentes en la seguridad de la información y Aspectos de seguridad de la información en la gestión de la continuidad del negocio se encuentran parcial o medianamente implementados.

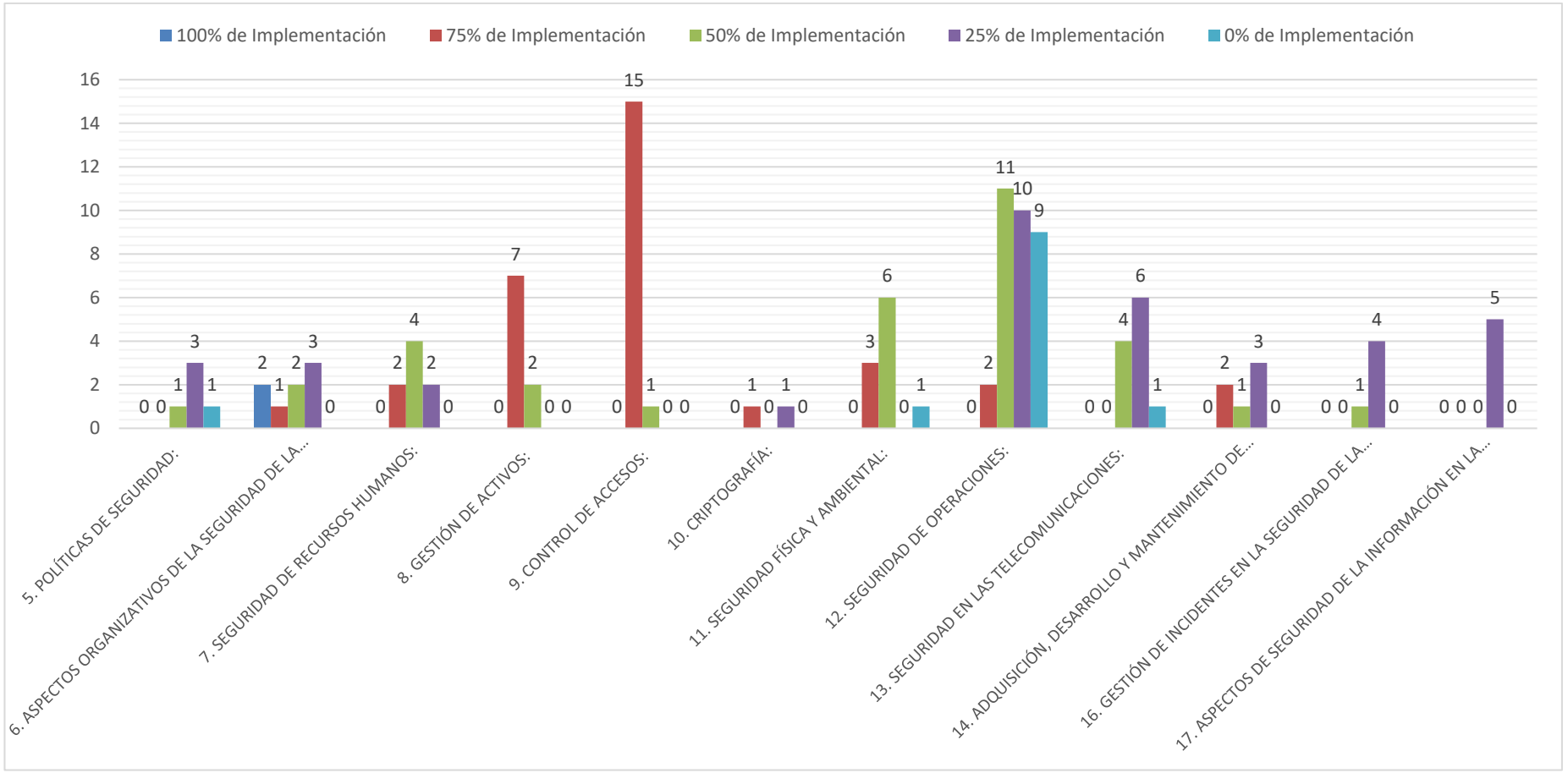


Figura 8: Resultados implementación de controles de la Norma ISO/IEC 27002: 2013

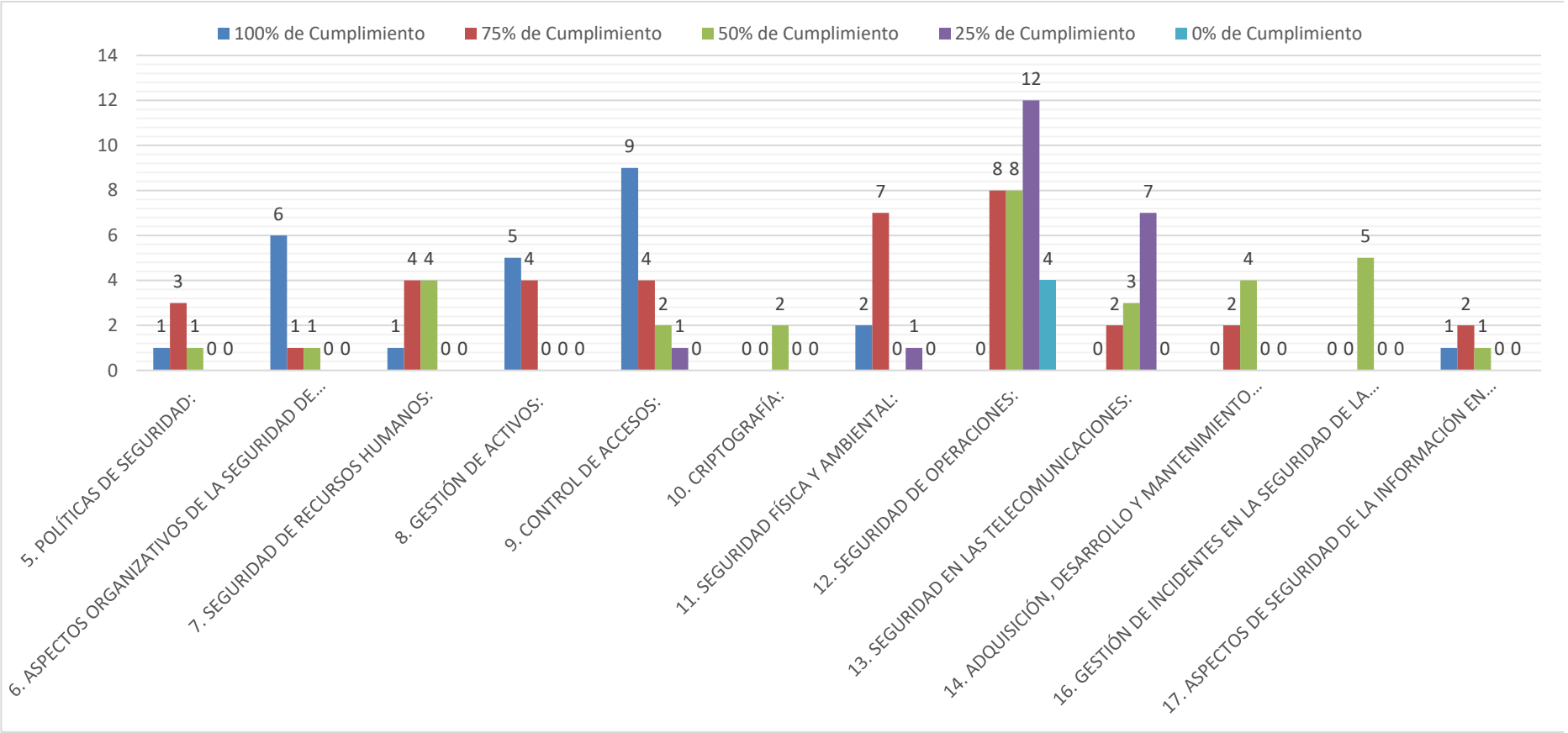


Figura 9: Resultados cumplimiento de controles de la Norma ISO/IEC 27002: 2013

En la evaluación del SGSI en el módulo de autenticación del SECAP se evidenció que no posee implementado todos los controles necesarios de la norma ISO 27002. El 2% de controles (2) tienen un 100% de implementación, el 24% (29 controles) tienen un 75% de implementación. 38 controles o el 32% están implementados al 50%, 38 controles o el 32% tienen solamente un 25% de implementación, y 8 controles o el 10% están con un 0% de implementación como se muestra en la figura 10.

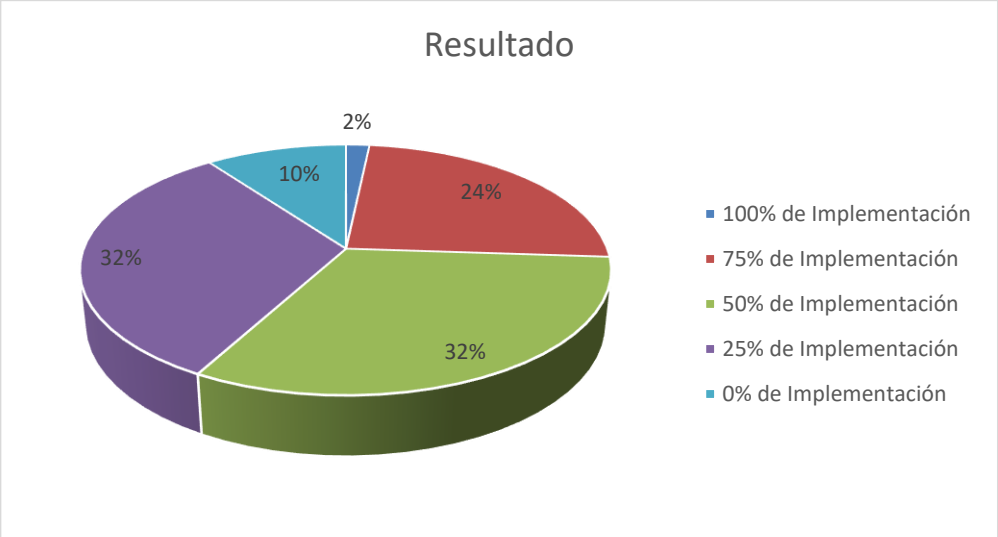
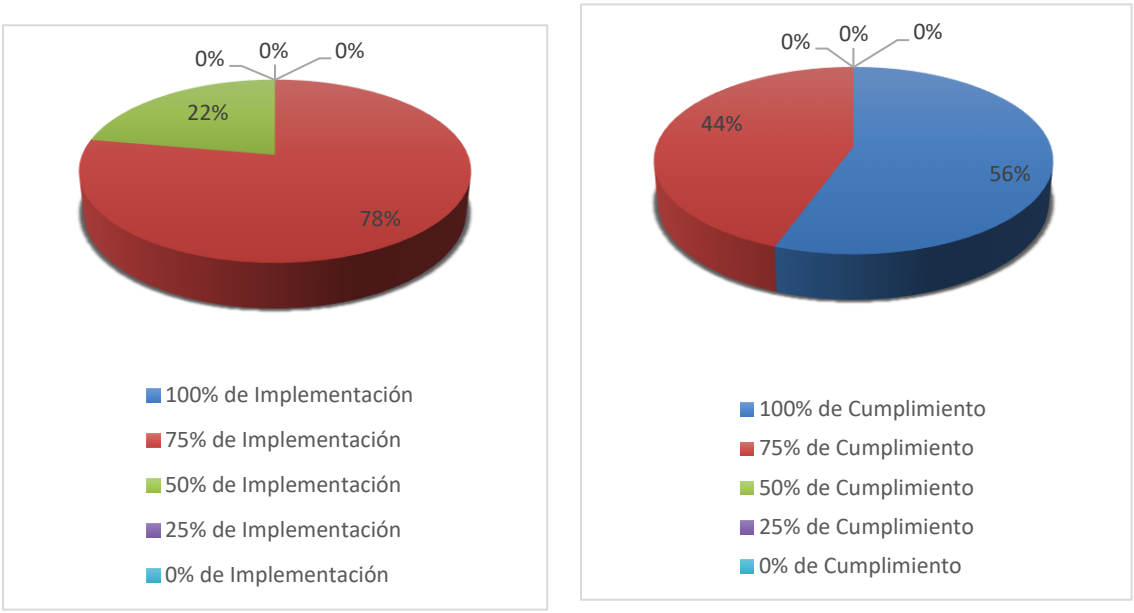


Figura 10: Controles implementados SECAP

En la figura 11(a) se puede evaluar los controles para la seguridad de la información implementados, y en la figura 11(b) se evalúa el cumplimiento. Ámbitos que ayudan a conocer la situación actual del módulo de Autenticación del SECAP y se procede con el plan de acción para la detección de vulnerabilidades en la privacidad de datos.

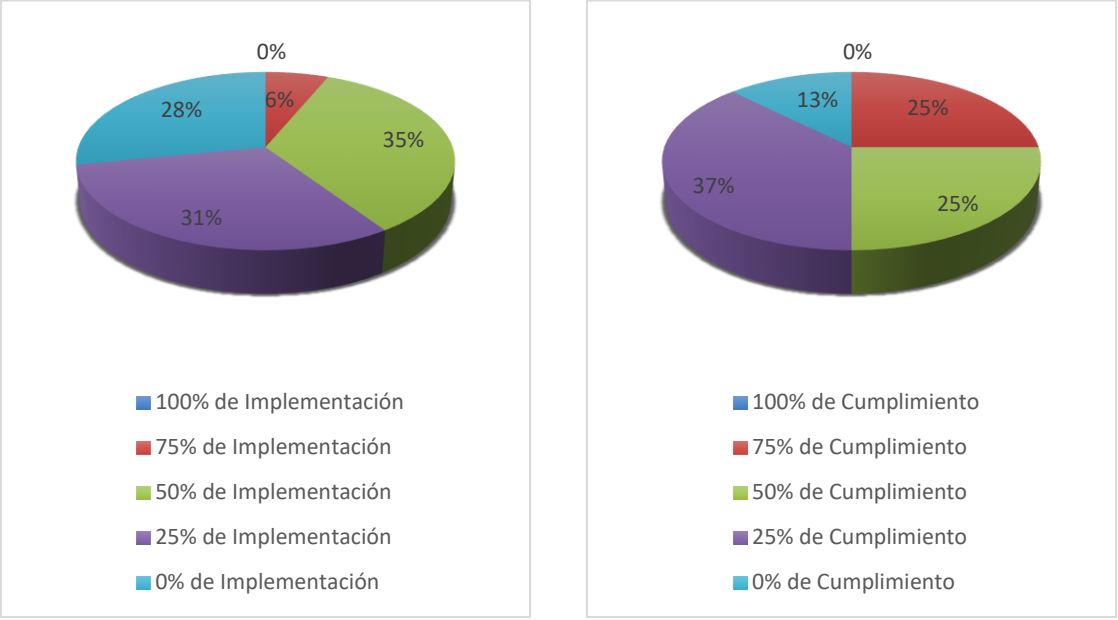


a) Implementación b) Cumplimiento

Figura 11: Gestión de activos SECAP

En la figura 11(a) se puede ver que existe un 22% de controles están implementados a un 50% y un 78% de controles se encuentran implementados a un 75%. No existe ningún control implementado al 100%, debido a que actualmente no hay un inventario actualizado de activos, ni tampoco se conoce exactamente los datos, software, equipos y servicios.

La seguridad de operaciones es uno de los controles más importantes para la presente investigación. La ISO 27002 en el punto correspondiente a la gestión de vulnerabilidad técnica presenta la guía de implementación, cuyo objetivo es prevenir la explotación de vulnerabilidades técnicas y en el módulo de autenticación del SECAP se obtuvieron los resultados mostrados en la figura 12.

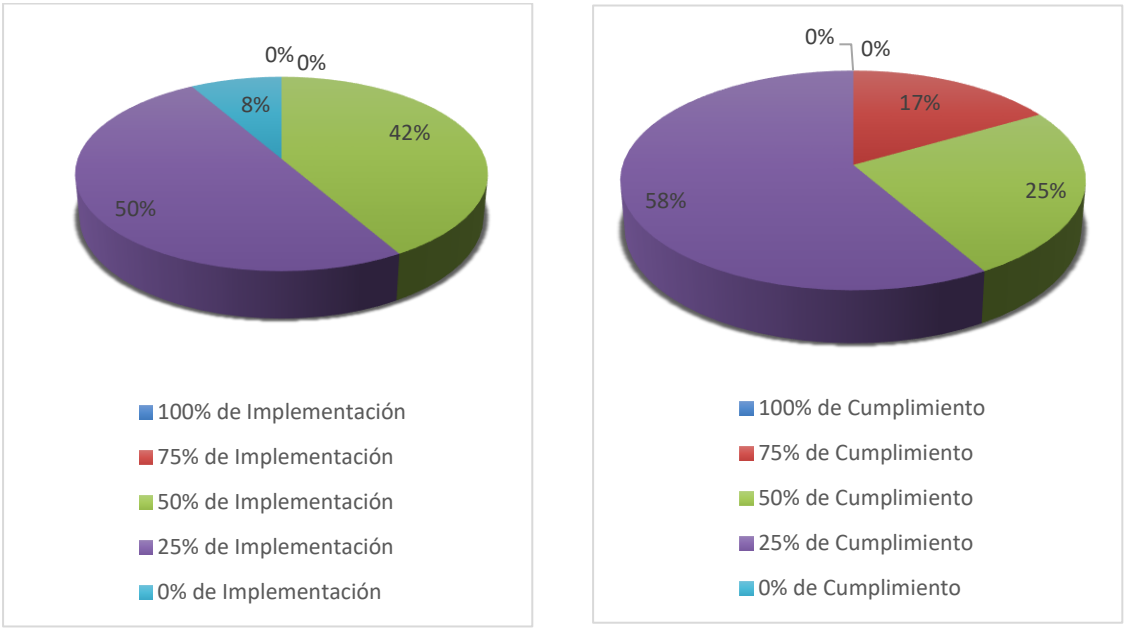


a) Implementación b) Cumplimiento

Figura 12: Seguridad de operaciones SECAP

En la figura 12 (a) se puede observar que tan solo el 6% se encuentra implementado al 100%. En cuanto al cumplimiento figura 12 (b) se tiene que ninguno cumple al 100%.

La seguridad de las telecomunicaciones tiene como objetivo proteger la información en las redes y por ello es una de las más propensas a sufrir cualquier tipo de ataque que afecte su seguridad y las vuelve más vulnerables. En la figura 13 se presentan los resultados de la aplicación de los controles de la ISO 27002 en cuanto a cumplimiento e implementación.

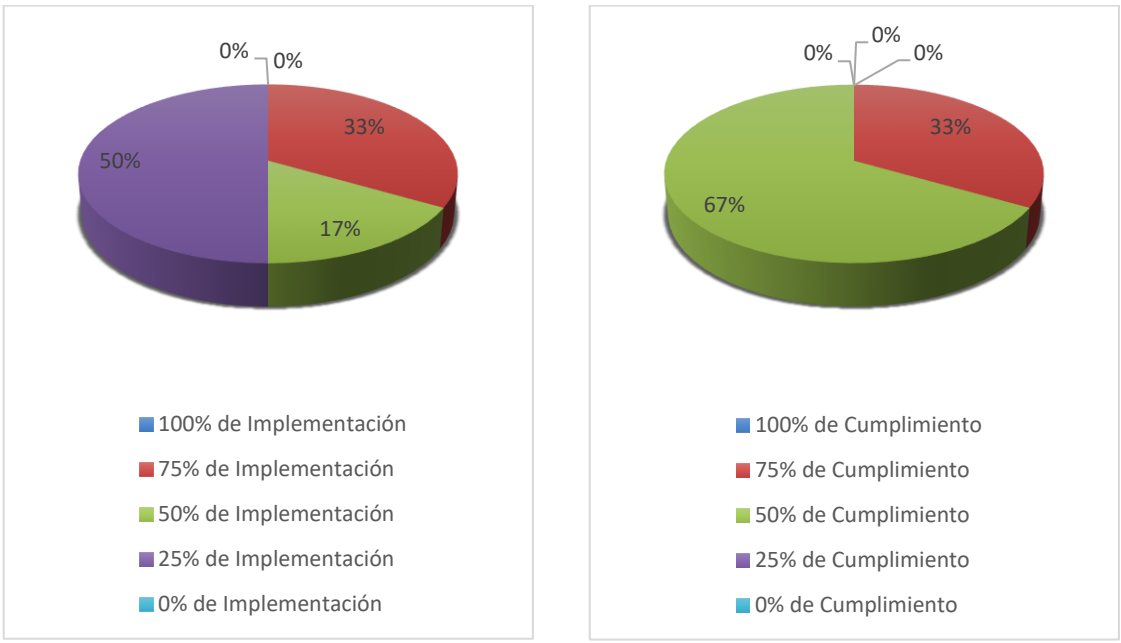


a) Implementación b) Cumplimiento

Figura 13: Seguridad de telecomunicaciones SECAP

Al evaluar la implementación de controles con respecto a la seguridad de telecomunicaciones en el SECAP, la figura 13 (a) muestra que un 50% tiene apenas un 25% de implementación, un 42% se encuentra a un 50% de implementación y un 8% que no está implementado. En la evaluación respecto al cumplimiento figura 13 (b) se tiene que ninguna cumple en su totalidad y un 58% cumplen apenas a un 25%.

La adquisición, desarrollo y mantenimiento de los sistemas (figura 14) es otro de los aspectos importantes en la seguridad de la información ya que en esta se considera el ciclo de vida de la información y los requisitos de los servicios a través de redes públicas.

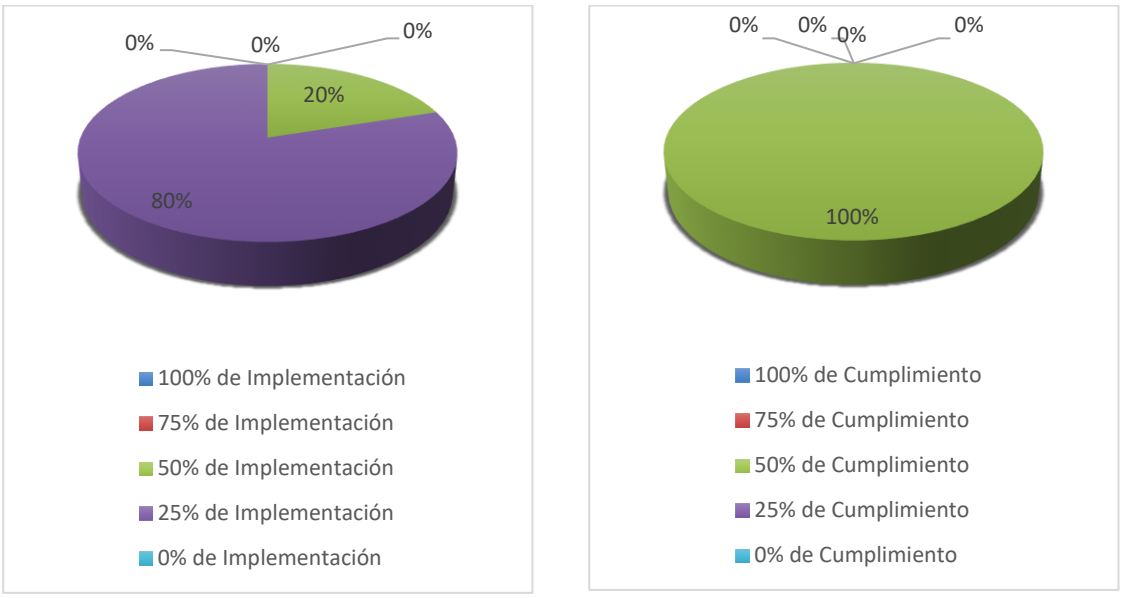


a) Implementación b) Cumplimiento

Figura 14: Adquisición, desarrollo y mantenimiento de los sistemas SECAP

En la figura 14 (a) se puede observar que ningún control de adquisición, desarrollo y mantenimiento de los sistemas en el módulo de autenticación del SECAP se encuentran totalmente implementados y un 50% están en un 25% de implementación. En la figura 14 (b) se observa que ningún control cumple a 100%, un 67% tiene un 50% de cumplimiento y un 33% cumple a un 25%

Los resultados recabados en la gestión de incidentes de seguridad de la información (figura 15) permiten resaltar en la Figura 15(a) que ningún control se encuentra implementado a 100% y un 80% se encuentra implementado a un 25%. En cuanto a la Figura 15 (b) relacionada con el cumplimiento, se encontró que el total de controles cumplen apenas a un 50%.



a) Implementación b) Cumplimiento

Figura 15: Gestión de incidentes SECAP

Finalmente se analiza el control 9 de la ISO/IEC 27002 el cual considera el Control de acceso (figura 16) debido a que la presente investigación es desarrollada en el módulo de autenticación para así determinar las vulnerabilidades en la privacidad de datos en el módulo que utiliza los servicios web del framework Laravel lo cual lleva a la creación de una guía de mejoras.Al analizar los datos referentes al control de acceso con respecto a implementación se encontró que el 75% se encuentran implementados a 75%, el 19% se encuentran implementados a un 50% y el 6% a un 25% de implementación. En cuanto a cumplimiento se encontró que el 56% cumple en su totalidad, el 25% lo hacen a 75%, el 13% lo hace a 50% y el 6% lo hacen a un 25%.

3.2. Análisis de Calidad de Software

De la implementación de SonarQube se obtuvieron los siguientes resultados:

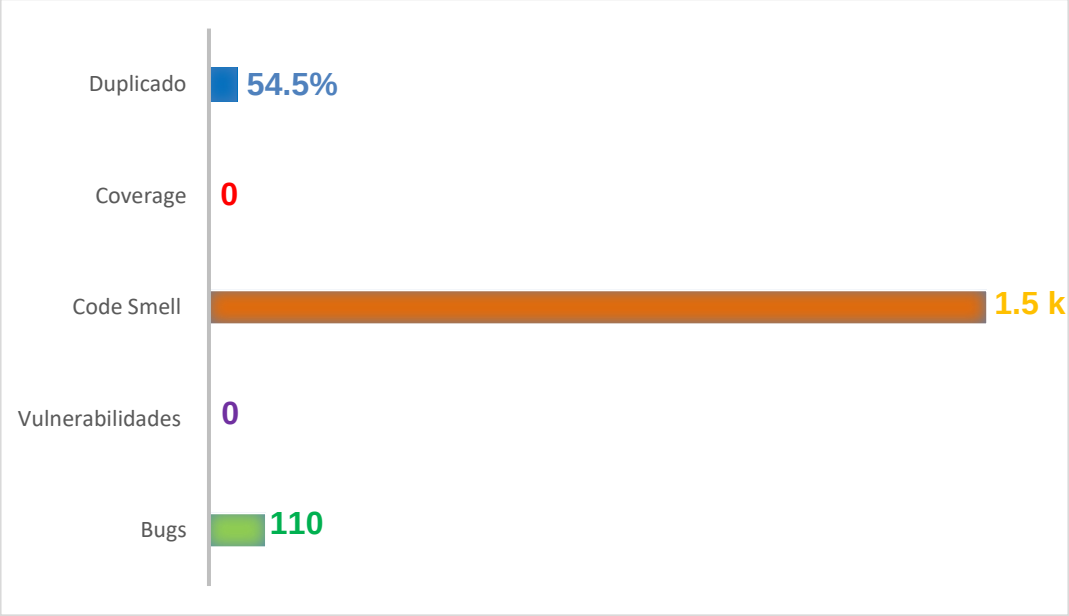


Figura 16: Resultados implementación de SonarQube

- La figura 17 resume que SonarQube encontró:110 bugs: significa que hay un problema que se representa como algo mal implementado dentro del código. Si esto aún no se ha roto (es decir ha presentado alguna función inadecuada o errónea) lo hará en algún momento del futuro.
- 1,5 k code smells: conocido también como hedor en el código (Anexo 4), lo que significa que existe un problema relacionado con la mantenibilidad en el código. Esto implica que los encargados del mantenimiento tendrán un escenario más complejo, cuando se requieran cambios funcionales en el aplicativo desarrollado. Cada uno de estos code smells puede causar confusión para los desarrolladores, especialmente en la lógica del desarrollo del código, lo que puede provocar que aparezcan nuevos errores a medida que se realicen cambios.
- 54,5% duplications: código duplicado dentro de la aplicación.

En la figura 18 se puede observar que se encontraron 2 puntos de acceso de seguridad (security hotspots), es decir piezas de código sensibles a infiltraciones de seguridad medibles y que deben revisarse manualmente. Adicionalmente se descubrió que hay una porción de código completamente vulnerable desde su construcción, la misma que debe

corregirse. En el anexo 5 se encuentran los puntos de acceso encontrados en el código fuente.

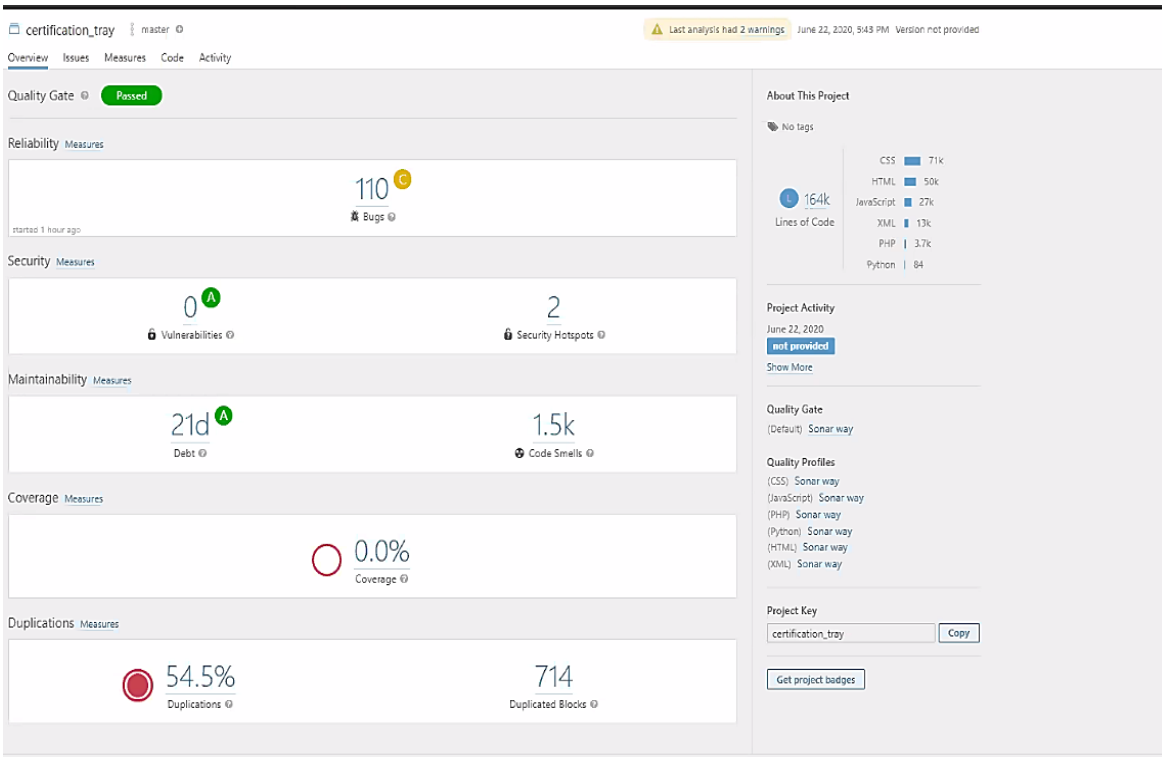


Figura 17: Puntos de acceso de seguridad según SonarQube

En la figura 19 se muestra que existen 1074 problemas abiertos, es decir fragmentos de código no cumple con una regla definida dentro de las mediciones, que se registran como un problema en la instantánea. Se puede registrar un problema en un archivo fuente o en un archivo de prueba unitaria. Estos problemas pueden ser de tres tipos: errores, olores de código (code smells que pueden provocar un riesgo de errores o futuros fallos) y vulnerabilidades.

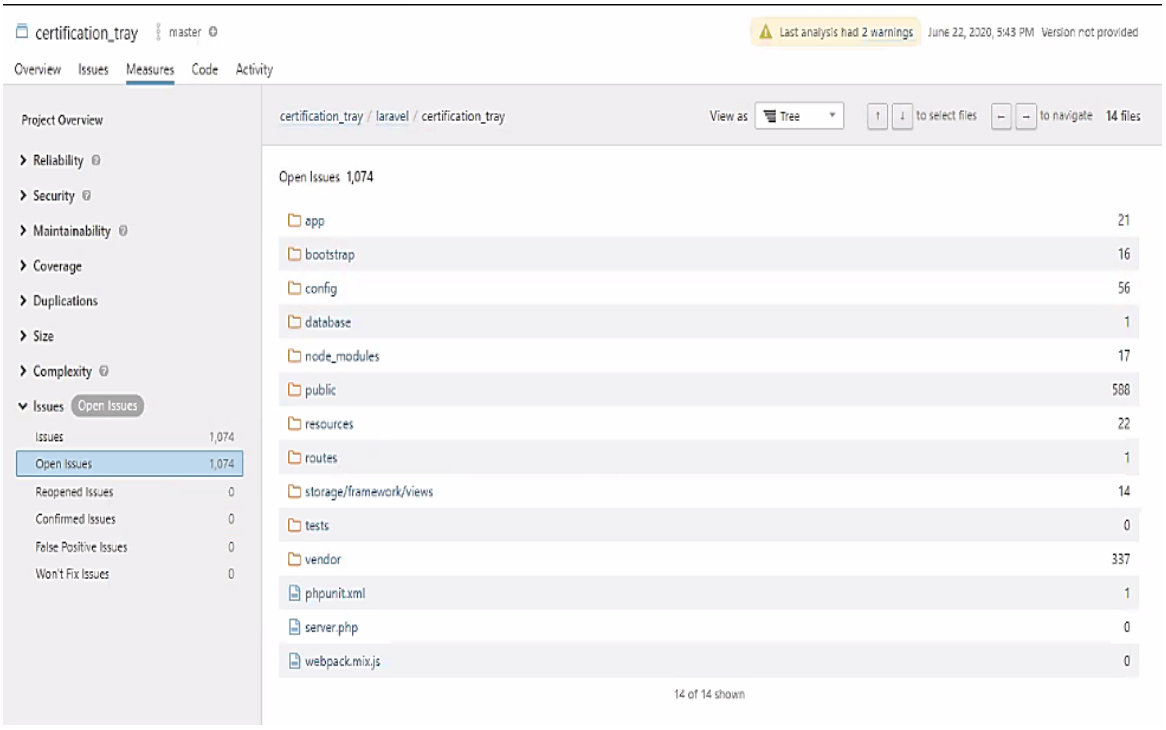


Figura 18: Problemas abiertos según SonarQube

3.3. Discusión y comparación de resultados

Investigaciones realizadas por Montoy (2017), Solarte, Enriquez & Benavides (2015) y Merello & Hidalgo (2019) indican que al menos el 75% de los problemas relacionados a la seguridad se deben principalmente a: a) fallos en la configuración de los equipos o mal uso por parte del personal de la empresa; b) poca cultura organizacional con respecto a la seguridad de la información; c) falta de aplicación de controles de seguridad y; d) no seguimiento de los controles aplicados. Estas investigaciones, sin embargo, se han realizado sobre las organizaciones en su conjunto, sin considerar elementos críticos en específico que pueden aumentar la probabilidad de ataques al explotar las vulnerabilidades inherentes a la falta de controles de seguridad. Esta investigación resuelve estos problemas al enfocarse en el módulo de autenticación del SISECAP. Esta investigación encontró que hay un alto riesgo, por ende amenazas a nivel de datos y redes, sobre el sistema de autenticación tal como estaba funcionando; con un puntaje 3,76. Sin embargo, en la evaluación realizada se obtuvo que adicionalmente, no existían controles adecuados en el acceso, tanto por parte de los usuarios como durante la implementación del módulo, lo que generaba mayor inseguridad, tomando en cuenta que el módulo estudiado es la puerta de acceso al aplicativo SISECAP.

Al analizar el nivel de cumplimiento de los controles sobre el módulo de autenticación del SECAP se encontró que el 20% lo ha realizado totalmente, por otro lado, el 22% simplemente lo ha cumplido a un 25%. Con esto se ratifica el riesgo que existe en la falta de aplicación de controles sobre el módulo estudiado, tomando en cuenta que el mismo maneja datos sensibles durante su ejecución. La falta de controles se traduce en la falta de cultura organizacional de seguridad, que en nuestro caso se demuestra cuando apenas un 2% de controles se han implementado totalmente. Sin embargo, se pudo evidenciar que el SECAP ya tenía un insipiente conocimiento sobre los controles a aplicar, por lo que se pudo constatar que el 32% de los mismos se encontraban en un 25% de implementación sobre el módulo evaluado al inicio de la investigación.

Al aplicar los controles de la norma ISO 27002 e ISO 27701 se encontró que, basados en la implementación general de un SGSI, tan solo el 26% de controles están implementados en un rango del 75% y 100% y un 74% se encuentra entre el 0% y 50% de implementación. Con esto se puede esperar que, previo a la utilización de la guía de mejoras resultado de este trabajo hubieran incidentes que comprometan la seguridad de la información que se maneja en este módulo. Es decir, las amenazas a nivel de redes, datos y de acceso tienen un riesgo muy alto. Entre otras, las políticas de acceso son las más afectadas al no existir controles sobre nombres de usuario o intentos de acceso al sistema; ni siquiera un segundo factor de autenticación de los usuarios. Estas fallas de implementación vuelven vulnerable al módulo de autenticación a ataques de fuerza bruta. La necesidad de la guía de mejoras propuesta en esta investigación cumple la labor no solo de generar la cultura organizacional necesaria sino acelerar la implementación del 74% restante de controles para mitigar los riesgos asociados a la falta de controles.

Con respecto al cumplimiento se encontró que en el módulo de autenticación del SECAP solo el 20% cumple al 100% y que el 80% restante cumple cumplen un rango comprendido del 75% al 0%. Lo que implica que previo a este estudio la información que transaccionaba el módulo de autenticación estaba expuesta y no se gestionaba adecuadamente su seguridad, comprometiendo no solo a los usuarios sino a la organización en general.

Los análisis llevaron a demostrar que, analizando el módulo de autenticación, los datos críticos con los que trabaja se encuentran expuestos a más de un ataque. No solo a nivel de controles sino también a causa de problemas dentro del código fuente del módulo. La valoración realizada mediante la herramienta SonarQube, a pesar de no detectar vulnerabilidades inherentes dentro del código, si mostro que existían problemas como código duplicado y bugs que, bien explotados puedan constituir en riesgos potenciales. A

través del análisis de esos valores contra la matriz de controles ISO 27002, se identifica que con respecto a código no hay vulnerabilidades, pero existen vulnerabilidades a nivel de datos, redes y acceso.

La guía propuesta dentro de esta investigación cumple con dos funciones específicas: a) aumentar la cultura organizacional con respecto a la concienciación sobre la necesidad de la implementación de seguridad dentro de la organización y, b) acelerar la aplicación de los controles requeridos de seguridad a través de indicaciones y sugerencias que aumentan la seguridad, tanto física y lógica como de utilización del módulo. Es decir, la guía de buenas prácticas indica que si se implementan las medidas planteadas en el plan de mejoras propuesto en esta investigación se pueden evitar riesgos que comprometan la seguridad de la información que maneja el módulo de autenticación del SECAP específicamente. Cada una de las medidas añadidas tanto dentro del plan de mejoras como en el manual de buenas prácticas están diseñadas para que el SISECAP específicamente resuelva sus riesgos de seguridad, demostrados durante esta investigación.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

- Este estudio ha permitido demostrar que, mientras más tiempo pase un activo de información sin ser gestionado, los riesgos y las amenazas a nivel de datos, redes y accesos incrementan su probabilidad de ocurrencia. Las brechas de seguridad encontradas responden a la falta de una evaluación adecuada, las cuales no son visibles hasta que ocurra un evento que explota las vulnerabilidades del módulo estudiado.

- Las omisiones en el estudio de la seguridad por parte de la Alta Dirección dentro de una organización, como el SECAP, contribuyen a aumentar las falencias en: errores de código fuente, políticas de seguridad relacionadas a perfiles, contraseñas, factores de autenticación, etc. Esto contribuye a que las vulnerabilidades propias de los sistemas crezcan si no son adecuadamente controlados, medidos y erradicados.

- El estudio de análisis de brecha dentro del módulo estudiado comparado con las normas implementadas para este estudio comprobó que los controles de las normas ISO 27002 inciso 12.6 e ISO 27701 inciso 6.9 son los ideales a utilizarse durante el control y el aseguramiento de las vulnerabilidades en entornos de programación, implementación y mantenimiento para módulos como el estudiado.

- La evaluación del código fuente dentro de este estudio permitió determinar que, a pesar de la experticia del desarrollador, el código también es una fuente de vulnerabilidades dentro de la organización. Estudiar las vulnerabilidades del código como un esquema aparte dentro de los activos informáticos permite analizar, descubrir y reparar sus vulnerabilidades inherentes antes de que se conviertan en vulnerabilidades para todo el componente computacional de una organización. Las herramientas que se utilizan para estos análisis deben ser, como en este estudio, de acceso libre y de código abierto, para no solo mantener el código limpio sino para mantener el código lo más independiente de marcas y sistemas operativos.

- El establecimiento de medidas de seguridad basadas en normas y controles estandarizados permite mantener un control periódico de la evolución de la seguridad en el módulo en los que fue aplicada la normativa, y permite además medir la aplicación de las medidas de seguridad al evaluar y corregir cada una de las vulnerabilidades que han sido descubiertas.

- La guía de mejoras elaborada producto de la investigación realizada permite el establecimiento de directrices y sugerencias diseñadas para mitigar las vulnerabilidades. Esta guía de mejoras, integrada como parte del sistema de control y seguridad de la organización, será utilizada como línea base para la prevención de vulnerabilidades y otros eventos, además de ser el inicio de futuras investigaciones.

Recomendaciones

- La continuación del presente estudio debe ser realizada de manera gradual, con controles que se encuentren en proceso de implementación para el módulo de autenticación con el fin de mejorar el SGSI basado en la guida de buenas prácticas inicial. Es importante apuntar a llegar al 100% de implementación y cumplimiento para garantizar la seguridad en los datos que maneja la organización.

- La metodología *Action Research* debe ser mantenida para los futuros trabajos que se realicen sobre el SECAP, ya que, al permitir la creación de una matriz especifica de la ISO 27002, permite ahorrar tiempo en diseño y planeamiento de la metodología para generar un SGSI eficiente y auditable.

- Para investigaciones futuras se recomienda usar SoapUI y comparar los resultados de esta aplicación con los de Sonar Qube, utilizada en este estudio, para comprobar la eficacia y eficiencia de las herramientas de análisis de código para el Framework Laravel PHP y su facilidad para el análisis de vulnerabilidades a nivel de código fuente de aplicativos.

- Futuras investigaciones, además, tienen el trabajo de completar el manual de mejoras presentado en este trabajo, ya que el diseño solo correspondió al módulo de autenticación del SISECAP. La generación de un SGSI para todo el SECAP tiene

que apuntar por la generación de un manual holístico que abarque transversalmente a todos los aplicativos de la institución académica.

BIBLIOGRAFÍA

Ahsan, A., Shahazzat Hossain, M., Nahar, N., & Khatun, D. (1 de Junio de 2014). An Empirical Analysis of C#, PHP, JAVA, JSP and ASP.Net regarding performance analysis based on CPU utilization. Bangladesh: Bangladesh University of Engineering and Technology.

Avison, D., Lau, F., Myers, M., & Nielsen, P. A. (1999). Action Research to make academic research relevant, researchers should try out their theories with practitioners in real situations and real organizations. *Communications of the ACM, 42*(1), 94-97.

Baskerville, R. L., & Wood-Harper, T. (1996). A critical perspective on action research as a method for information systems research. *Journal of Information Technology, 11*, 235-245.

Baskerville, R., & Myers, M. (2004). Special isuue on Action Research in Information Systems: Making is research relevant to practice- foreword. *MIS Quarterly, 28*(3), 329-335.

Bryman, A., & Bell, E. (2011). *Business Research Methods 3rd edition.* Oxford University Press.

Echeverria, C. (2016). *Estatuto Orgánico de Gestión por procesos del SECAP, Registro Oficial Suplemento 817, 11-ago.* Quito.

Elzar Esen, M. D. (Agosto de 2016). Developing web application for islamic baking module using iterative incremental method and LAravel Framework for distribution ZISWAF fund to sme's. Telkom, Indonesia.

Hofacker, A. (2008). *Rapid lean construction - quality rating model.* Manchester: s.n.

Imam Riadi, E. K. (1 de Enero de 2018). SECURITY LEVEL ANALYSIS OF ACADEMIC INFORMATION SYSTEMS BASED ON STANDARD ISO 27002: 2013 USING SSE-CMM. Yogyakarta, Indonesia: Department of Informatics Engineering Islamic University of Indonesia.

ISO 27002.es. (2015). Obtenido de El portal de ISO 27002 en Español: http://iso27000.es/iso27002_5.html

ISO/IEC 27001. (2013). *Information technology — Security techniques — Information security management systems — Requirements.* International Organization for Standardization, International Electrotechnical Commission.

ISO/IEC 27002. (2013). *Information technology - Security techniques - Code of practice for information security controls.* Switzerland: ISO copyright office. Obtenido de El portal de ISO 27002 en Español: http://iso27000.es/iso27002_5.html

ISO/IEC 27701. (2019). *Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines.* Switzerland: ISO copyright office.

Josefina Gutiérrez-Martínez, M. A.-G.-M. (30 de Enero de 2015). Business Model for the Security of a Large-Scale PACS, Compliance with ISO/27002:2013 Standard. Mexico DF, Mexico, Mexico.

Koskela, L. (1992). *Application of the new production philosophy to construction.* Finland: VTT Building Technology.

Loza Aguirre, E. F., & Buitrago Hurtado, A. F. (2014). Evaluación cualitativa de la aceptación de los usuarios en el marco de la Investigación-Acción y la Investigación Diseño-Acción: dos estudios de caso. *Latin American Journal of Computing, 1*(1).

MacIsaac, D. (1995). *An Introduction to Action Research.* Obtenido de http://www.phy.nau.edu/~danmac/actionrsch.html (22/03/1998)

Montoy, Y. A. (2017). *Desarrollo e implemetación de controles para el dominio de seguridad física y ambiental para la empresa Felmova S.A usando la norma ISO 27002.* Guayaquil: Escuela Superior del Litoral.

Moulia, V., & Jevitha, K. (2016). Web Services Attacks and Security- A Systematic Literature Review. *Elsevier*, 870-877.

Myers, M. D. (1997). Qualitative Research in Information Systems. *MISQ Discovery*.

O'Brien, R. (2001). *An Overview of the Methodological Approach of Action Research.* Obtenido de https://www.web.ca/~robrien/papers/arfinal.html#_Toc26184651

Pandini, W. (30 de diciembre de 2015). *ISO 27002: Buenas prácticas para gestión de la seguridad de la información.* Obtenido de https://ostec.blog/es/generico/iso-27002-buenas-practicas-gsi

Proag, V. (2014). The concept of vulnerability and resilience. *Elsevier, 18*, 369-376. doi:10.1016/S2212-5671(14)00952-6

Sahni, P., Dhameja, A., & Medury, U. (2001). *Disaster Mitigation : Experiences and Reflections.* India: Prentice-Hall.

Salas, M., & Martins, E. (2014). *Security Testing Methodology for Vulnerabilities Detection of XSS in Web Services and WS-Security.* Campinas, Brazil : UNICAMP, State University of Campinas.

Sari Widya Sihwi, F. A. (1 de Enero de 2016). An Expert System for Risk Assessment of Information System Security Based on ISO 27002. Surakarta,, Indonesia.

Shahnila, F. (2018). Software Security Vulnerabilities. *Computer Fraud & Security*, .

Shin, Y., & Williams, L. (2008). Is complexity really the enemy of software security? *Computer Science*.

Shitangsu Kumar, P. (2015). Vulnerability concepts and its application in various fields: A review on geographical perspective. *Life Earth Sci, 8*, 63-81. doi:10.3329/jles.v8i0.20150

Solarte, F. N., Enriquez Rosero, E. R., & Benavides Ruano, M. d. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica ESPOL – RTE*, 492-507.

Ummi Khaira Latif, T. F. (2017). Performance Comparison of Executing Large Data in Yii2 and Laravel Framework. Telkom: Department of Industrial Engineering Telkom University.

Winter, R. (1987). *Action-Research and the Nature of Social Inquiry: Professional Innovation and Educational Work.* Aldershot, England: Gower Publishing Company.

Yalowitz, K. (2 de 1 de 2019). *W3Techs - World Wide Web Technology Surveys*. Obtenido de https://w3techs.com/

ANEXOS

Anexo 1: Matriz controles ISO 27002

5. POLÍTICAS DE SEGURIDAD:
¿Existen documento(s) de políticas de seguridad de Sistema de Información?
¿Existe normativa relativa a la seguridad del Sistema de Información?
¿Existen procedimientos relativos a la seguridad de Sistema de Información?
¿Existe un responsable de las políticas, normas y procedimientos?
¿Existen controles regulares para verificar la efectividad de las políticas?
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN:
¿Existen roles y responsabilidades definidos para las personas implicadas en la seguridad?
¿Existe un responsable encargado de evaluar la adquisición y cambios de Sistema de Información?
¿Participan la Dirección y las áreas de la Organización en temas de seguridad?
¿Existen condiciones contractuales de seguridad con terceros y outsourcing?
¿Existen criterios de seguridad en el manejo de terceras partes?
¿Existen programas de formación en seguridad para los empleados, clientes y terceros?
¿Existe un acuerdo de confidencialidad de la información que se accede?
¿Se revisa la organización de la seguridad de forma periódica por una empresa externa?
7. SEGURIDAD DE RECURSOS HUMANOS:
¿Se tienen definidas responsabilidades y roles de seguridad?
¿Se tiene en cuenta la seguridad en la selección y baja del personal?
¿Se plasman las condiciones de confidencialidad y responsabilidades en los contratos?
¿Se imparte la formación adecuada de seguridad y tratamiento de activos?
¿Existe un canal y procedimientos claros a seguir en caso de incidente de seguridad?
¿Se recogen los datos de los incidentes de forma detallada?
¿Informan los usuarios de las vulnerabilidades observadas o sospechadas?
¿Se informa a los usuarios de que no deben, bajo ninguna circunstancia, probar las vulnerabilidades?
¿Existe un proceso disciplinario de la seguridad de la información?
9. CONTROL DE ACCESOS:
¿Existe una política de control de accesos?
¿Existe una política de uso de los servicios de red?
¿Existe un procedimiento formal de registro y baja de accesos?
¿Se controla y restringe la asignación y uso de privilegios en entornos multi-usuario?
¿Existe una gestión de los privilegios de usuarios?
¿Existe una revisión de los derechos de acceso de los usuarios?
¿Existe el uso del password?
¿Se controla el uso de información secreta de autenticación?
¿Existe restricción de acceso a la información?
¿Se han establecido procedimientos para el inicio de sesión seguros?

¿Existe un control de acceso al código fuente del programa?
¿Existe una autenticación de usuarios en conexiones externas?
¿Existe un control de la conexión de redes?
¿Existen procedimientos de log-on al terminal?
¿Se ha incorporado medidas de seguridad a la computación móvil?
¿Está controlado el teletrabajo por la organización?

10. CRIPTOGRAFÍA:

¿Existen políticas sobre el uso de controles criptográficos?
¿Se realizan procedimientos adecuados para la gestión de claves?

11. SEGURIDAD FÍSICA Y AMBIENTAL:

¿Existe perímetro de seguridad física (una pared, puerta con llave)?
¿Existen controles físicos de entrada?
¿Existe un área segura cerrada, aislada y protegida de eventos naturales?
¿En las áreas seguras existen controles adicionales al personal propio y ajeno?
¿La ubicación de los equipos está de tal manera para minimizar accesos innecesarios?
¿Existen protecciones frente a fallos en la alimentación eléctrica?
¿Existe seguridad en el cableado frente a daños e intercepciones?
¿Se asegura la disponibilidad e integridad de todos los equipos?
¿Existe algún tipo de seguridad para los equipos retirados o ubicados en el exterior?
¿Se incluye la seguridad en equipos móviles?

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS:

¿Se asegura que la seguridad está implantada en los Sistemas de Información?
¿Existe seguridad en las aplicaciones?
¿Existe seguridad en los ficheros de los sistemas?
¿Existe seguridad en los procesos de desarrollo, testing y soporte?
¿Existen controles de seguridad para los resultados de los sistemas?
¿Existe la gestión de los cambios en los Sistemas Operativos?

17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO:

¿Existen procesos para la gestión de la continuidad?
¿Existe un plan de continuidad del negocio y análisis de impacto?
¿Existe un diseño, redacción e implantación de planes de continuidad?
¿Existe un marco de planificación para la continuidad del negocio?
¿Existen prueba, mantenimiento y reevaluación de los planes de continuidad del negocio?

8. GESTIÓN DE ACTIVOS:

¿Existen un inventario de activos actualizado?
¿El Inventario contiene activos de datos, software, equipos y servicios?
¿Se dispone de una clasificación de la información según la criticidad de la misma?
¿Existe un responsable de los activos?
¿Existen procedimientos para clasificar la información?
¿Existen procedimientos de etiquetado de la información?
¿Existen procedimientos para el manejo de activos?
¿Se realiza gestión en medios extraíbles?
¿Existen procedimientos para la transferencia de medios físicos?

12. SEGURIDAD DE OPERACIONES:

¿Existen procedimientos operativos documentados?

¿Se realiza gestión de cambio?

¿Existe Gestión de capacidad?

¿Se han definido separación de los entornos de desarrollo, prueba y operación?

¿Existen controles contra malware?

¿Se han establecido parámetros para realizar copia de seguridad de la información?

¿Existe un registro de eventos?

¿Se realizan procedimientos para la protección de la información de registro?

¿Se realizan controles para la instalación de software en sistemas operativos?

¿Existen restricciones en la instalación de software?

¿Existen controles de auditoría de sistemas de información?

¿Existe Gestión de vulnerabilidades técnicas?

¿Se definen y establecen los roles y responsabilidades asociados con la gestión de vulnerabilidades técnicas?

¿Se supervisan las vulnerabilidades?

¿Se aplican parches?

¿Se han identificado los recursos de información que se utilizaran para vulnerabilidades?

¿Los recursos de información se actualizan basándose en los cambios del inventario?

¿Existe un cronograma para reaccionar a las notificaciones de vulnerabilidades relevantes?

¿Existen procedimientos para riesgos asociados y acciones a ser tomadas?

¿Si está disponible un parche (patch), los riesgos asociados con la instalación del parche (patch) son evaluados?

¿Se prueban y evalúan los parches antes de ser instalados?

Si no está disponible ningún parche:

- ¿Existen procedimientos para bajar servicios o funcionalidades relacionadas con la vulnerabilidad?
- ¿Se adaptan o agregan controles de acceso, por ejemplo: cortafuegos (firewalls) en los bordes de la red?
- ¿Se aumenta el seguimiento para descubrir ataques reales?
- ¿Se fomentar conciencia de la vulnerabilidad?

¿Existe un registro de auditoría para todos los procedimientos emprendidos?

¿Se supervisa y evalúa con regularidad el proceso de gestión de vulnerabilidades técnicas para asegurar su eficacia y eficiencia?

¿Existe una gestión de los sistemas de riesgo alto?

¿La vulnerabilidad técnica está alineada con las actividades de gestión de incidentes?

¿Existen procedimientos técnicos si ocurre un incidente?

¿Existen procedimientos para vulnerabilidades identificadas?

¿Se evalúan los riesgos relacionados con la vulnerabilidad conocida y se definen las acciones de investigación y correctivas adecuadas?

13. SEGURIDAD EN LAS TELECOMUNICACIONES:

¿Todos los procedimientos operativos identificados en la política de seguridad están documentados?

¿Están establecidas responsabilidades para controlar los cambios en equipos?

¿Están establecidas responsabilidades para asegurar una respuesta rápida, ordenada y efectiva frente a incidentes de seguridad?
¿Existe algún método para reducir el mal uso accidental o deliberado de los Sistemas?
¿Existe una segregación en redes?
¿Existen políticas y procedimientos de transferencia de información?
¿Existen controles contra software maligno?
¿Se realizar copias de backup de la información?
¿Existen logs para las actividades realizadas por los operadores y administradores?
¿Se ha establecidos controles para realizar la gestión de los medios informáticos (cintas, discos, removibles, informes impresos)?
¿Existen medidas de seguridad en el comercio electrónico?
¿Se han establecido e implantado medidas para proteger la confidencialidad e integridad de información publicada?
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN:
¿Se comunican los eventos de seguridad?
¿Se comunican las debilidades de seguridad?
¿Existe definidas las responsabilidades antes un incidente?
¿Existe un procedimiento formal de respuesta?
¿Existe la gestión de incidentes?

Anexo 2: Funcionalidades del área de Tecnologías de la Información y Comunicación

PROCESOS	PRODUCTO	ACTIVIDADES
Gestión de Proyectos de TIC	Arquitectura tecnológica de TI con características de escalabilidad y flexibilidad que permitan la reducción de tiempos de atención en las soluciones, procesos, y proyectos de TI;	Solicitar Análisis de arquitectura tecnologica
		Solicitar Aval en PAPP 2020
		Elaborar términos de referencia
		Solicitar inicio de proceso
		asignar y elaborar Ficha técnica
		Solicitar certificación de catálogo electrónico
		Solicitar constancia en el plan anual de compras
		Solicitar certificación de fondos
		Solicitar de autorización para la adquisición
		Administrar la adjudicación y firma de contrato realizada
		Elaborar entrega - recepción de los bienes objeto del contrato
		Solicitar pago final
	Plan de acción y mejoras de los servicios tecnológicos	Análisis para actualización de versiones de la base de datos de MySql
		Análisis para actualización de versiones de PHP
		Diseño de la nueva BD
		Scripts de migracion de data
		Actualización de PHP
	Planes de reposición de software y hardware	Aálisis de HW y SW a reponer
		Solicitar Aval en PAPP 2020
		Elaborar términos de referencia
		Solicitar inicio de proceso
		asignar y elaborar Ficha técnica
		Solicitar certificación de catálogo electrónico
		Solicitar constancia en el plan anual de compras
		Solicitar certificación de fondos
		Solicitar de autorización para la adquisición
		Administrar la adjudicación y firma de contrato realizada
		Elaborar entrega - recepción de los bienes objeto del contrato
		Solicitar pago final
	Portafolio de desarrollo de soluciones tecnológicas propias, adquiridas y adaptadas, proceso y proyectos informáticos gestionados y administrados por TIC, así como los estándares de programación relacionados con el ciclo de vida de desarrollo o gestión de cambio de nuevas aplicaciones y sistemas informáticos;	Recibir documentos y formularios de requerimientos a los sistemas de informacion enviado por la Direccón Nacional de Planificación y actualizacion de la matriz de priorización.
		Validar documentos, formularios y delegado o delegados de las areas requirentes, habilitantes para atención del requerimiento
		Disponer al coordinador del área de proyectos de TIC's para efectuar estudio de viabilidad.
		Disponer al equipo de trabajo el analisis de viabilidad
		Analizar la viabilidad del proyecto.
		Aprobar documento análisis de viabilidad de proyectos

		Delegar al equipo de desarrollo para atencion del requerimiento
		Desarrollar aplicativo de acuerdo al requerimiento
		Desarrollar guion de pruebas del requerimiento
		Realizar pruebas y certificacion funcional del requerimiento desarrollad
		Apoyar a los delegados de las areas requirentes en la capacitacion a usuarios finales, sobre el requerimiento desarrollado
		Apoyar a los delegados de las areas requirentes en la elaboración de los manuales de usuario
		Elaboracion de la documentacion tecnica relacionado al requerimiento
		Solicitar autoriazacion para paso aproduccion con copia a la dirección de Planificación para conocimiento y actualizacion de la matriz de priorización
		Realizar paso a produccion y notificacion a las areas involucradas en el requerimiento
	Repositorios e inventarios de códigos fuente versionados, scripts de base de datos versionados, instaladores, archivos de configuración y parametrización, reportes de control de cambio y versiones del desarrollo de los aplicativos y sistemas informáticos desarrollados, adquiridos o adaptados	Disponer la revisón documentos tecnicos y versionamientos realizados en los sistemas de informacion de acuerdo a los requerimientos solicitados
		Delegar y coordinar equipo tecnico para revision de los requerimientos atrendidos y en ejecucion para validar documentacion y versionamientos realizados
		Inventariar códigos fuentes versionados, scripts de base de datos, reportes de control de cambios y versiones de aplicativos y sistemas informáticos, desarrollados, adquiridos o adaptados.
	Términos de referencia, especificaciones funcionales y técnicas para la contratación del desarrollo de sistemas informáticos, servicios, servicios web, consultorías y demás contrataciones requeridas por la coordinación en base a la normativa legal vigente para este fin	Disponer y analizar las especificaciones para la contratación del desarrollo de sistemas informáticos
		Realizar solicitud de cotizaciones
		Elaborar los tdr
		Aprobar tdr
	Servicios web y documentación relacionada para compartir e intercambiar datos e información electrónica por medio de la plataforma gubernamental; dispositivos electrónicos, hardware y software, enfocados a brindar seguridad a la información institucional	Recibir documentos y formularios de requerimientos a los sistemas de informacion enviado por la Direccón Nacional de Planificación y actualizacion de la matriz de priorización.
		Validar documentos, formularios y delegado o delegados de las areas requirentes, habilitantes para atención del requerimiento
		Disponer al coordinador del área de proyectos de TIC's para efectuar estudio de viabilidad.
		Disponer al equipo de trabajo el analisis de viabilidad
		Analizar la viabilidad del proyecto.
		Aprobar documento análisis de viabilidad de proyectos
		Delegar al equipo de desarrollo para atencion del requerimiento
		Desarrollar aplicativo de acuerdo al requerimiento
		Desarrollar guion de pruebas del requerimiento

		Realizar pruebas y certificacion funcional del requerimiento desarrollad
		Apoyar a los delegados de las areas requirentes en la capacitacion a usuarios finales, sobre el requerimiento desarrollado
		Apoyar a los delegados de las areas requirentes en la elaboración de los manuales de usuario
		Elaborcion de la documentacion tecnica relacionado al requerimiento
		Solicitar autoriazcion para paso aproduccion con copia a la dirección de Planificación para conocimiento y actualizacion de la matriz de priorización
		Realizar paso a produccion y notificacion a las areas involucradas en el requerimiento
	Informes de gestión de paso a producción de los sistemas informáticos desarrollados, proyectos informáticos y seguimiento y control de incidentes de las aplicaciones, sistemas informáticos desarrollados, adquiridos o adoptados, herramientas para gestión de soporte técnico y reportes	Elaborar informes de GLPI reportados y atendidos
		Elaborar informe de requerimientos y controles de cambios de los sistemas de informacion
		Elaborar informes de sistemas de informacion adquiridos
	Informes de administración, transferencia de conocimiento y fiscalización de sistemas informáticos, manuales de usuario, instructivos y procedimientos de uso de sistemas y aplicativos institucionales.	disponer se realice auditoría interna al sistema informático
		Coordinar auditoría interna al sistema informático
		Realizar auditoría interna al sistema informático

Anexo 3: Resultado de análisis de campo y comprobación de controles implementados

PREGUNTAS	RESPUESTAS	
	Implementación	Cumplimiento
5. POLÍTICAS DE SEGURIDAD:		
¿Existen documento(s) de políticas de seguridad de Sistema de Información?	2	4
¿Existe normativa relativa a la seguridad del Sistema de Información?	2	4
¿Existen procedimientos relativos a la seguridad de Sistema de Información?	2	4
¿Existe un responsable de las políticas, normas y procedimientos?	3	5
¿Existen controles regulares para verificar la efectividad de las políticas?	1	3
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN:		
¿Existen roles y responsabilidades definidos para las personas implicadas en la seguridad?	2	5
¿Existe un responsable encargado de evaluar la adquisición y cambios de Sistema de Información?	3	5
¿Participan la Dirección y las áreas de la Organización en temas de seguridad?	3	5
¿Existen condiciones contractuales de seguridad con terceros y outsourcing?	5	5
¿Existen criterios de seguridad en el manejo de terceras partes?	5	5
¿Existen programas de formación en seguridad para los empleados, clientes y terceros?	2	4
¿Existe un acuerdo de confidencialidad de la información que se accede?	4	5
¿Se revisa la organización de la seguridad de forma periódica por una empresa externa?	2	3
7. SEGURIDAD DE RECURSOS HUMANOS:		
¿Se tienen definidas responsabilidades y roles de seguridad?	3	4
¿Se tiene en cuenta la seguridad en la selección y baja del personal?	3	4
¿Se plasman las condiciones de confidencialidad y responsabilidades en los contratos?	4	5
¿Se imparte la formación adecuada de seguridad y tratamiento de activos?	2	4
¿Existe un canal y procedimientos claros a seguir en caso de incidente de seguridad?	4	3

¿Se recogen los datos de los incidentes de forma detallada?	3	3
¿Informan los usuarios de las vulnerabilidades observadas o sospechadas?	3	4
¿Se informa a los usuarios de que no deben, bajo ninguna circunstancia, probar las vulnerabilidades?	2	3
¿Existe un proceso disciplinario de la seguridad de la información?	3	3
8. GESTIÓN DE ACTIVOS:		
¿Existen un inventario de activos actualizado?	3	5
¿El Inventario contiene activos de datos, software, equipos y servicios?	3	5
¿Se dispone de una clasificación de la información según la criticidad de la misma?	4	4
¿Existe un responsable de los activos?	4	5
¿Existen procedimientos para clasificar la información?	4	4
¿Existen procedimientos de etiquetado de la información?	4	5
¿Existen procedimientos para el manejo de activos?	4	5
¿Se realiza gestión en medios extraíbles?	4	4
¿Existen procedimientos para la transferencia de medios físicos?	4	4
9. CONTROL DE ACCESOS:		
¿Existe una política de control de accesos?	4	4
¿Existe una política de uso de los servicios de red?	4	5
¿Existe un procedimiento formal de registro y baja de accesos?	4	5
¿Se controla y restringe la asignación y uso de privilegios en entornos multi-usuario?	4	5
¿Existe una gestión de los privilegios de usuarios?	3	3
¿Existe una revisión de los derechos de acceso de los usuarios?	4	3
¿Existe el uso del password?	4	5
¿Se controla el uso de información secreta de autenticación?	3	3
¿Existe restricción de acceso a la información?	4	4
¿Se han establecido procedimientos para el inicio de sesión seguros?	2	2
¿Existe un control de acceso al código fuente del programa?	3	2

¿Existe una autenticación de usuarios en conexiones externas?	4	5
¿Existe un control de la conexión de redes?	4	5
¿Existen procedimientos de log-on al terminal?	4	5
¿Se ha incorporado medidas de seguridad a la computación móvil?	3	4
¿Está controlado el teletrabajo por la organización?	4	4
10. CRIPTOGRAFÍA:		
¿Existen políticas sobre el uso de controles criptográficos?	2	3
¿Se realizan procedimientos adecuados para la gestión de claves?	3	3
11. SEGURIDAD FÍSICA Y AMBIENTAL:		
¿Existe perímetro de seguridad física (una pared, puerta con llave)?	4	5
¿Existen controles físicos de entrada?	4	5
¿Existe un área segura cerrada, aislada y protegida de eventos naturales?	1	2
¿En las áreas seguras existen controles adicionales al personal propio y ajeno?	3	4
¿La ubicación de los equipos está de tal manera para minimizar accesos innecesarios?	3	4
¿Existen protecciones frente a fallos en la alimentación eléctrica?	4	4
¿Existe seguridad en el cableado frente a daños e intercepciones?	3	4
¿Se asegura la disponibilidad e integridad de todos los equipos?	3	4
¿Existe algún tipo de seguridad para los equipos retirados o ubicados en el exterior?	3	4
¿Se incluye la seguridad en equipos móviles?	3	4
12. SEGURIDAD DE OPERACIONES:		
¿Existen procedimientos operativos documentados?	3	3
¿Se realiza gestión de cambio?	3	3
¿Existe Gestión de capacidad?	3	3
¿Se han definido separación de los entornos de desarrollo, prueba y operación?	3	3
¿Existen controles contra malware?	4	4
¿Se han establecido parámetros para realizar copia de seguridad de la información?	4	4

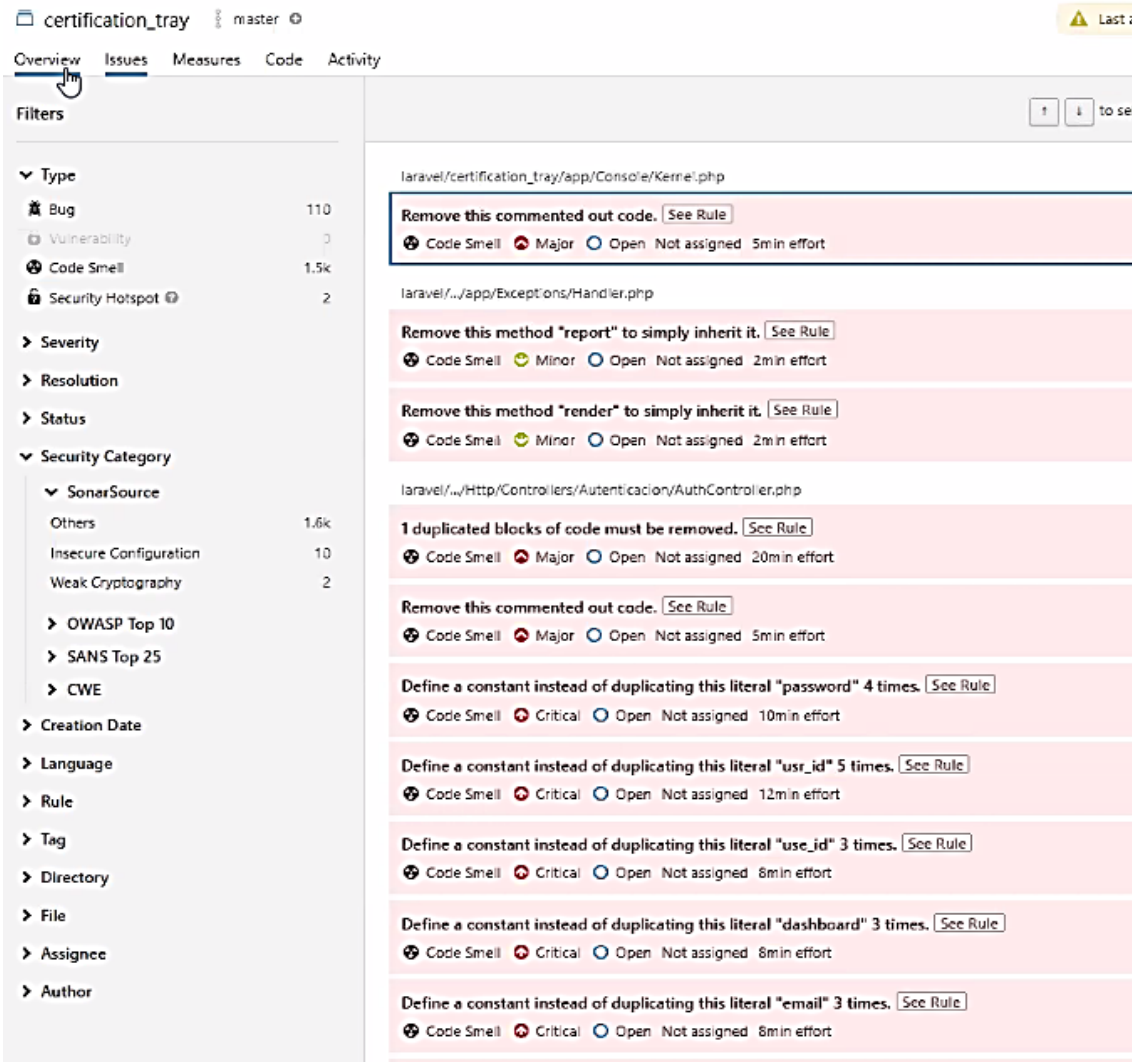
¿Existe un registro de eventos?	3	4
¿Se realizan procedimientos para la protección de la información de registro?	3	4
¿Se realizan controles para la instalación de software en sistemas operativos?	3	4
¿Existen restricciones en la instalación de software?	3	4
¿Existen controles de auditoría de sistemas de información?	3	4
¿Existe Gestión de vulnerabilidades técnicas?	3	4
¿Se definen y establecen los roles y responsabilidades asociados con la gestión de vulnerabilidades técnicas?	2	3
¿Se supervisan las vulnerabilidades?	2	3
¿Se aplican parches?	3	3
¿Se han identificado los recursos de información que se utilizaran para vulnerabilidades?	1	2
¿Los recursos de información se actualizan basándose en los cambios del inventario?	1	2
¿Existe un cronograma para reaccionar a las notificaciones de vulnerabilidades relevantes?	1	2
¿Existen procedimientos para riesgos asociados y acciones a ser tomadas?	2	3
¿Si está disponible un parche (patch), los riesgos asociados con la instalación del parche (patch) son evaluados?	2	2
¿Se prueban y evalúan los parches antes de ser instalados?	2	2
Si no está disponible ningún parche:		
• ¿Existen procedimientos para bajar servicios o funcionalidades relacionadas con la vulnerabilidad?	1	1
• ¿Se adaptan o agregan controles de acceso, por ejemplo: cortafuegos (firewalfs), ¿en los bordes de la red?	1	1
• ¿Se aumenta el seguimiento para descubrir ataques reales?	1	1
• ·¿Se fomentar conciencia de la vulnerabilidad?	1	1
¿Existe un registro de auditoría para todos los procedimientos emprendidos?	2	2
¿Se supervisa y evaluá con regularidad el proceso de gestión de vulnerabilidades técnicas para asegurar su eficacia y eficiencia?	1	2
¿Existe una gestión de los sistemas de riesgo alto?	2	2

¿La vulnerabilidad técnica está alineada con las actividades de gestión de incidentes?	1	2
¿Existen procedimientos técnicos si ocurre un incidente?	2	2
¿Existen procedimientos para vulnerabilidades identificadas?	2	2
¿Se evalúan los riesgos relacionados con la vulnerabilidad conocida y se definen las acciones de investigación y correctivas adecuadas?	2	2
13. SEGURIDAD EN LAS TELECOMUNICACIONES:		
¿Todos los procedimientos operativos identificados en la política de seguridad están documentados?	2	2
¿Están establecidas responsabilidades para controlar los cambios en equipos?	2	2
¿Están establecidas responsabilidades para asegurar una respuesta rápida, ordenada y efectiva frente a incidentes de seguridad?	2	2
¿Existe algún método para reducir el mal uso accidental o deliberado de los Sistemas?	2	2
¿Existe una segregación en redes?	3	3
¿Existen políticas y procedimientos de transferencia de información?	3	3
¿Existen controles contra software maligno?	1	2
¿Se realizar copias de backup de la información?	3	4
¿Existen logs para las actividades realizadas por los operadores y administradores?	3	4
¿Se ha establecidos controles para realizar la gestión de los medios informáticos (cintas, discos, removibles, informes impresos)?	2	2
¿Existen medidas de seguridad en el comercio electrónico?	2	2
¿Se han establecido e implantado medidas para proteger la confidencialidad e integridad de información publicada?	3	3
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS:		
¿Se asegura que la seguridad está implantada en los Sistemas de Información?	3	3
¿Existe seguridad en las aplicaciones?	4	4
¿Existe seguridad en los ficheros de los sistemas?	4	4
¿Existe seguridad en los procesos de desarrollo, testing y soporte?	2	3

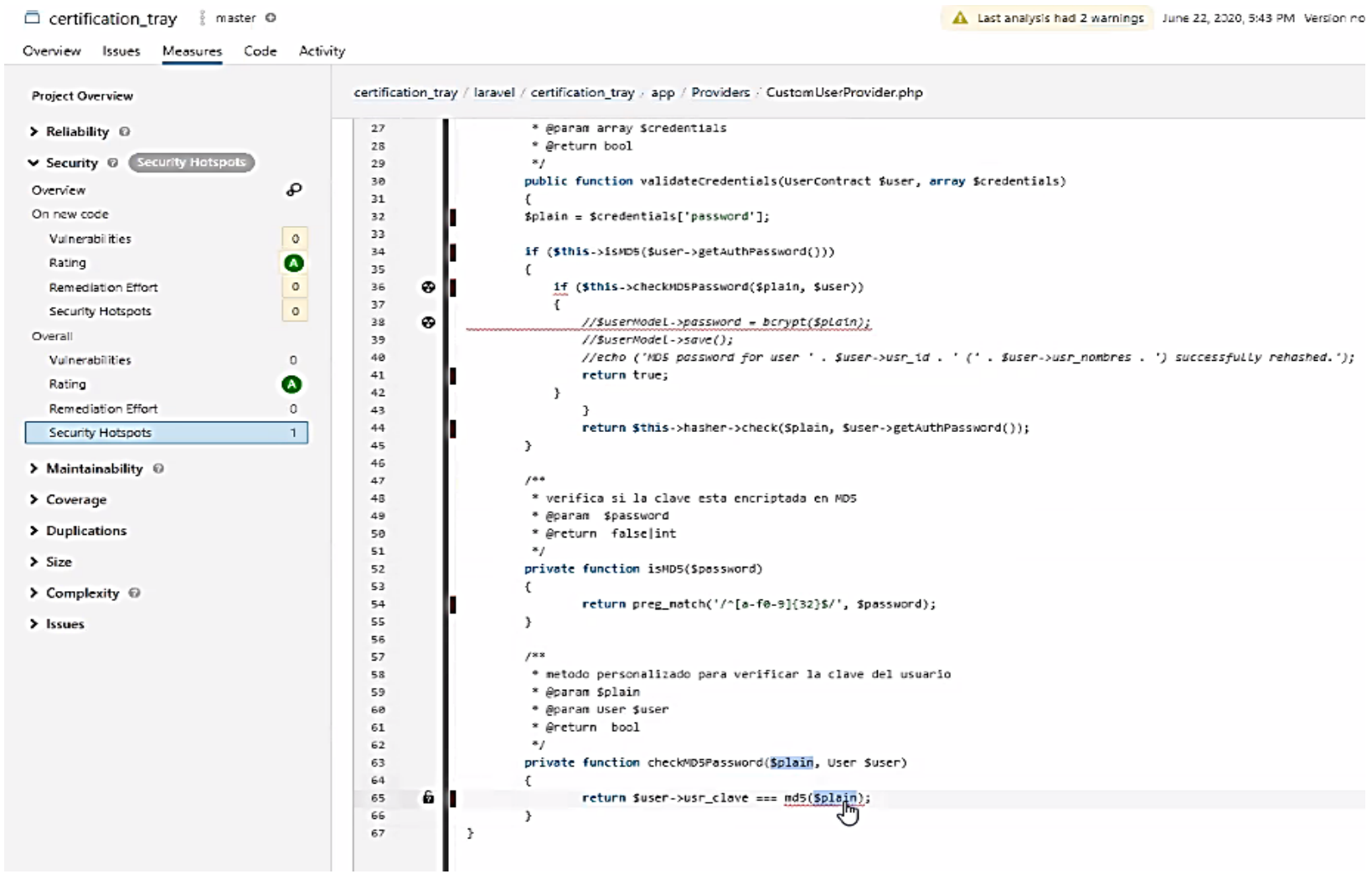
¿Existen controles de seguridad para los resultados de los sistemas?	2	3
¿Existe la gestión de los cambios en los Sistemas Operativos?	2	3
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN:		
¿Se comunican los eventos de seguridad?	2	3
¿Se comunican las debilidades de seguridad?	2	3
¿Existe definidas las responsabilidades antes un incidente?	2	3
¿Existe un procedimiento formal de respuesta?	2	3
¿Existe la gestión de incidentes?	3	3
17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO:		
¿Existen procesos para la gestión de la continuidad?	2	2
¿Existe un plan de continuidad del negocio y análisis de impacto?	2	2
¿Existe un diseño, redacción e implantación de planes de continuidad?	2	2
¿Existe un marco de planificación para la continuidad del negocio?	2	2
¿Existen prueba, mantenimiento y reevaluación de los planes de continuidad del negocio?	2	2

Fuente: (ISO/IEC 27002, 2013)

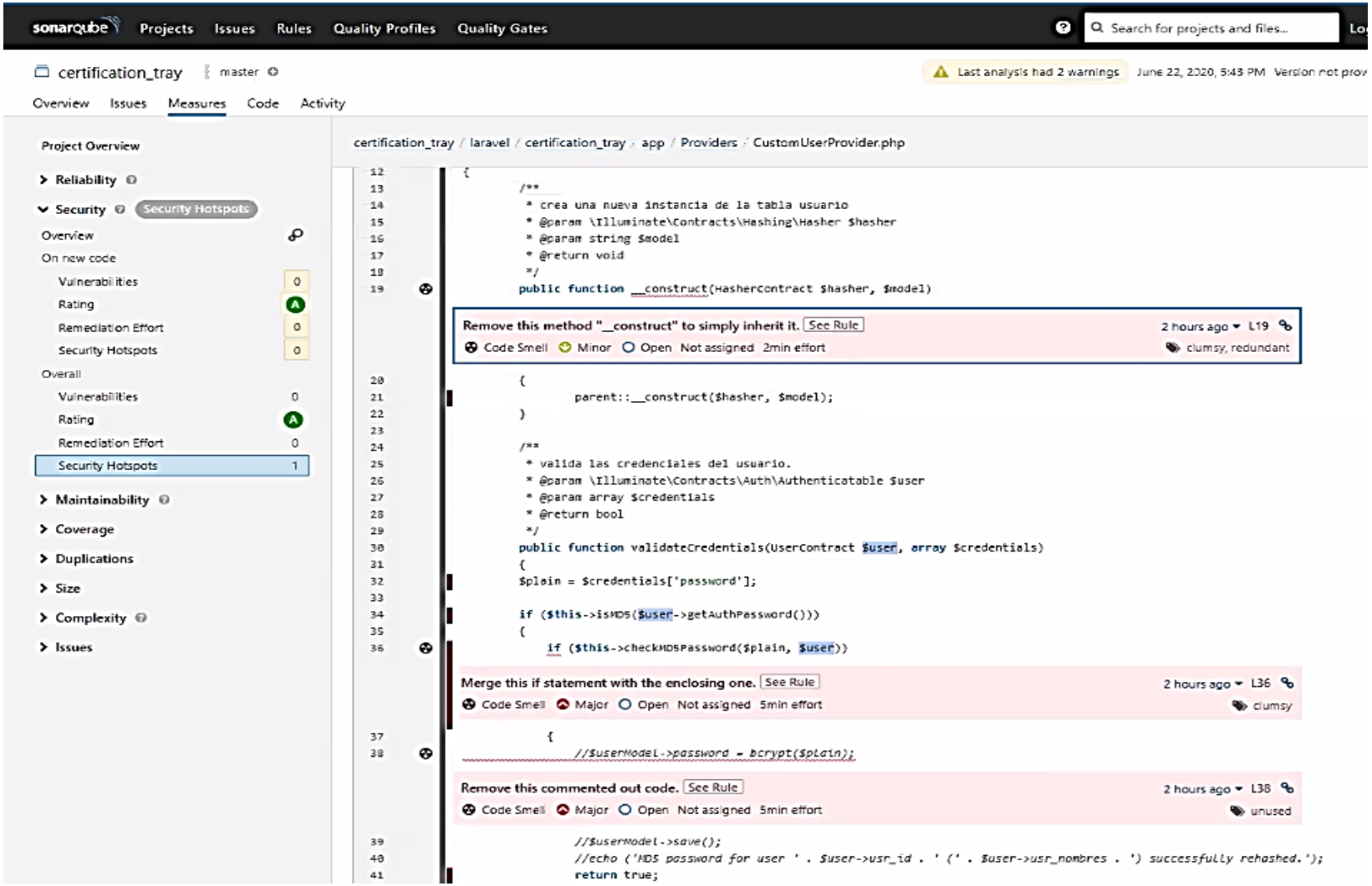
Anexo 4: Resultado SonarQube CodeSmells



Code Smell


certification_tray
master
Last analysis had 2 warnings
June 22, 2020, 5:43 PM
Version no
Overview
Issues
Measures
Code
Activity
Project Overview
Reliability
Security
Security Hotspots
Overview
On new code
Vulnerabilities 0
Rating A
Remediation Effort 0
Security Hotspots 0
Overall
Vulnerabilities 0
Rating A
Remediation Effort 0
Security Hotspots 1
Maintainability
Coverage
Duplications
Size
Complexity
Issues
certification_tray / laravel / certification_tray / app / Providers / CustomUserProvider.php
* @param array $credentials
* @return bool
*/
public function validateCredentials(UserContract $user, array $credentials)
{
$plain = $credentials['password'];
if ($this->isMD5($user->getAuthPassword()))
{
if ($this->checkMD5Password($plain, $user))
{
//$userModel->password = bcrypt($plain);
//$userModel->save();
//echo ('MD5 password for user ' . $user->usr_id . ' (' . $user->usr_nombres . ') successfully rehashed.');
return true;
}
}
return $this->hasher->check($plain, $user->getAuthPassword());
}
/**
* verifica si la clave esta encriptada en MD5
* @param $password
* @return false|int
*/
private function isMD5($password)
{
return preg_match('/^[a-f0-9]{32}$/', $password);
}
/**
* metodo personalizado para verificar la clave del usuario
* @param $plain
* @param User $user
* @return bool
*/
private function checkMD5Password($plain, User $user)
{
return $user->usr_clave === md5($plain);
}
}

Hotspots


sonarqube
Projects
Issues
Rules
Quality Profiles
Quality Gates
Search for projects and files...
certification_tray
master
Last analysis had 2 warnings
June 22, 2020, 5:43 PM
Overview
Issues
Measures
Code
Activity
Project Overview
Reliability
Security
Security Hotspots
Overview
On new code
Vulnerabilities 0
Rating A
Remediation Effort 0
Security Hotspots 0
Overall
Vulnerabilities 0
Rating A
Remediation Effort 0
Security Hotspots 1
Maintainability
Coverage
Duplications
Size
Complexity
Issues
certification_tray / laravel / certification_tray / app / Providers / CustomUserProvider.php
Remove this method "__construct" to simply inherit it. See Rule
2 hours ago L19
Code Smell Minor Open Not assigned 2min effort
clumsy, redundant
Merge this if statement with the enclosing one. See Rule
2 hours ago L36
Code Smell Major Open Not assigned 5min effort
clumsy
Remove this commented out code. See Rule
2 hours ago L38
Code Smell Major Open Not assigned 5min effort
unused

Hotspots

5.1. GUIA DE MEJORAS DE LA EVALUACIÓN REALIZADA AL MODULO DE AUTENTICACIÓN DEL SISTEMA SISECAP PARA DATOS SENSIBLES

5.1.1. Alcance

Esta guía de mejoras se aplicará con base a la evaluación realizada de datos confidenciales del módulo de autenticación del sistema académico SISECAP, habiendo utilizado las normas ISO 27002 y 27701. Basándose en las vulnerabilidades encontradas en tus datos más sensibles como son usuarios y contraseñas.

Además, brindará sugerencias para obtener un nivel de seguridad aceptable al momento de ingresar al sistema principal del módulo de autenticación y mitigar varias vulnerabilidades encontradas.

5.1.1.1. Consideraciones Generales

- Esta guía se aplicará a todos los integrantes del equipo de desarrollo de TI como personas que interactúen directamente con el sistema académico del SECAP llamado SISECAP.
- La dirección de tecnologías de la información y comunicación debe coordinar con la dirección ejecutiva para la difusión, cambios y mantenimiento de las políticas aplicadas de esta guía.
- Los nuevos usuarios del aplicativo académico en general, deberán ser informados sobre estas políticas de seguridad, al momento de que firmen un contrato en el que acepten las condiciones de las mismas, como también que son responsables únicos de las acciones y consecuencias que generen al utilizar el sistema del SECAP con sus cuentas personales de ingreso.

Esta guía deberá ser revisada cada 6 meses por parte de la dirección de tecnologías de la información, en que sus directrices o políticas deban ser evaluadas y si es necesario reformadas. Acordes las nuevas tendencias, formas de autenticación actuales y a la evolución del negocio.

5.1.1.2. Nombres de usuarios y perfiles de usuario para acceso al sistema

- Cuando una persona se le otorga acceso al aplicativo SISECAP con tu perfil respectivo como es: estudiante, docente o directivo.
- Se deberá crear un nombre de usuario con una cuenta genérica de servicios de directorio para un estudiante, o una cuenta propia para un docente o directivo del instituto.
- El aplicativo debe permitir el acceso a las diferentes opciones dependiendo el tipo de perfil asignado al usuario.

5.1.1.3. Políticas de ingreso de contraseñas

- Se le deberá asignar una contraseña por defecto al usuario, y el mismo tendrá la obligación de cambiarlo por una nueva clave para poder ingresar al aplicativo.
- La contraseña deberá tener las siguientes características:
  - Un mínimo de 8 caracteres ingresados.
  - Ingresar por lo menos una mayúscula.
  - Ingreso de por lo menos un número.
  - Ingreso de por lo menos un carácter especial.
- Que tenga un tiempo de caducidad de por lo menos tres meses.

5.1.1.4. Segundo Factor de autenticación

- Implementar un segundo factor de autenticación adicional a la contraseña como:
  - Authy.
  - Google Authenticator.
  - Sms para recibir clave temporal.
  - Mail para recibir clave temporal.
  - FreeOTP.
- En caso de olvido de contraseña, utilizar algunas de las sugerencias del segundo factor de autenticación, y en el aplicativo solicitar el ingreso de una nueva clave de ingreso.

5.1.1.5. Caducidad de sesión de usuario

- El aplicativo deberá tener una caducidad de sesión por inactividad de 10 minutos.
- En caso se ingresar al sistema con el mismo usuario desde otro dispositivo, deberá generar un cierre automático de la sesión iniciada en el dispositivo anterior.

5.1.1.6. Path o URL del aplicativo SISECAP

- Aplicar la herramienta PowerCenter para el enmascaramiento del path del sistema académico.