Auditoría de seguridad en el proceso de desarrollo de software acorde a estándar ISO/IEC 15504 en una institución financiera.

MAESTRÍA EN AUDITORIA DE TECNOLOGÍA DE LA INFORMACIÓN

Propuesta de artículo presentado como requisito para la obtención del título:

Magíster en Auditoría de Tecnologías de la Información

Por la estudiante:
Blanca de Lourdes CÁRDENAS CANTOS

Bajo la dirección de:
Marco Vinicio SOTOMAYOR SÁNCHEZ

Universidad Espíritu Santo
Maestría en Auditoría de Tecnología de la Información
Samborondón - Ecuador
Abril del 2019

Auditoría de seguridad en el proceso de desarrollo de software acorde a estándares ISO/IEC 15504 en una institución financiera, año 2018.

Security audit in the software development process according to standards ISO/IEC 15504 at a financial institution

Blanca de Lourdes CÁRDENAS CANTOS [1]
Marco Vinicio SOTOMAYOR SÁNCHEZ [2]

Resumen

El presente estudio surge como una respuesta a la falta de aseguramiento de los procesos informáticos en ciertas instituciones financieras. Se planteó como objetivo: diseñar y aplicar una auditoría de seguridad en el proceso de desarrollo de software acorde al estándar ISO/IEC 15504, el mismo que ha demostrado una efectividad mayor en la obtención de información real y confiable, en una Cooperativa, durante el año 2018. La metodología aplicada asumió un enfoque mixto y se emplearon instrumentos como: encuesta sobre proceso de desarrollo de software, entrevista a la persona coordinadora del proceso de desarrollo de software, y una lista de verificación. Los resultados de permitieron observar que la mayoría de los subprocesos se encuentran completamente implementados; únicamente un número reducido estaría parcialmente implementado. A partir de ello se concluye el proceso auditado se realiza de manera consistente y bajo parámetros y lineamientos claramente definidos. La aplicación de la auditoría de seguridad informática al proceso de desarrollo de software permitió identificar varias problemáticas que, en caso de no ser solucionadas, ponen en riesgo la operatividad de los sistemas informáticos y, principalmente, la seguridad de los clientes y socios durante las transacciones económicas.

Palabras clave: Auditoría, seguridad informática, desarrollo de software, ISO/IEC 15504, framework.

Abstract

The investigation originates as a response to the lack of assurance of computer processes in certain financial institutions. The objective was to design and implement a security audit in the software development process according to ISO / IEC 15504 standards at a financial institution. The applied methodology assumed a mixed approach and instruments such as: survey about the software development process, interview with the coordinator of the software development process, and a checklist. The results allowed to observe that most of the sub-processes are fully implemented; only a small number would be partially implemented. Based on this, the audited process is concluded in a consistent manner and under clearly defined parameters and guidelines. The application of the computer security audit to the software development process made it possible to identify several problems that, if not solved, put at risk the operation of the computer systems and, mainly, the security of the clients and partners during the transactions. economic

Key words Audit, computer security, software development, ISO / IEC 15504,

[1] Estudiante de Maestría en Auditoría de Tecnología de Información, Universidad Espíritu Santo – Ecuador. E-mail bcardenas@uees.edu.ec

[2]

framework

INTRODUCCIÓN

Tamayo (2001) establece a la auditoría de seguridad informática como la revisión y evaluación de los controles, sistemas, procedimientos de informática, fijados en una organización para alcanzar la confiabilidad, oportunidad, seguridad y confidencialidad de la información procesada por medio de computadores. Para Cano (2004), es el resultado de una propiedad emergente de un sistema que conoce sus condiciones extremas, su operación límite, así como sus recursos y posibilidades para darle sentido a la razón de su misión. La auditoría de seguridad informática analiza todos los procesos relacionados a la seguridad informática, física y lógica: la seguridad física refiere a la protección de los elementos hardware, dispositivos, instalaciones y demás entornos; la seguridad lógica comprende la protección del software, los procesos y programas del sistema, por lo que su auditoría analizará la adecuada protección y actualización de estos (Chicano, 2014).

Por su parte, las cooperativas confiarían cada vez más en los Sistemas de Información (SI) para mejorar las operaciones, facilitar la toma de decisiones gerenciales y desplegar estrategias comerciales. La dependencia de estas entidades respecto de los SI ha llevado a un aumento en los abusos de seguridad (García, 2011). Varios estudios han documentado pérdidas reales y potenciales debidas a abusos de seguridad del SI. Una encuesta de 2002 del Instituto de Seguridad Informática indicó que el 90% de las entidades investigadas detectó violaciones de seguridad y pérdidas millonarias (Baca, 2016). Consecuencias negativas de los abusos de seguridad de los SI son la publicidad negativa, desventaja competitiva e, incluso, una menor viabilidad organizacional. La vulnerabilidad de las cooperativas aumentaría con el comercio electrónico y las arquitecturas de redes abiertas (Castellanos, 2014). Una mejor alfabetización informática, una mayor sofisticación de los usuarios de computadoras y la disponibilidad de herramientas de software avanzadas contribuirían a aumentar los abusos de seguridad de los IS para el futuro. Por lo tanto, las gerencias de las cooperativas requieren prestar más atención a los problemas de seguridad de los SI.

Sin embargo, como señalan Alarcón, González y Rodríguez (2011), existe una baja preocupación por la seguridad de los SI por parte de los gerentes de las cooperativas, debido a razones como: i) piensan que el riesgo de abusos de la seguridad de los SI es bajo; ii), son escépticos sobre la efectividad de la seguridad de los SI, debido a la dificultad de evaluar los beneficios; y iii), desconocen el rango de controles disponibles para reducir los abusos de seguridad de los SI. De ahí que es importante convencer a los gerentes sobre los beneficios de los esfuerzos de seguridad de los SI y hacerles saber qué tipos de medidas de seguridad son efectivas. Las cooperativas se sentirán completamente seguras cuando se demuestre que el sistema global es seguro (Rosado, Blanco, Sánchez, Fernández, & Piattinni, 2010).

Por otra parte, la seguridad del software permite que un producto previamente desarrollado funcione correctamente ante ataques maliciosos (Tovar, Carrillo, Vega, & Gasca, 2010). Existen varios modelos y estándares sobre la base de las características de calidad, los que consideran aspectos como la mantenibilidad del software, la reusabilidad, la corrección, la integridad, la eficiencia y la seguridad. Los problemas en la seguridad del software exigen distintas soluciones, las que se fundamentarían en tres pilares: la administración del riesgo, la aplicación de prácticas específicas en etapas del ciclo de vida de desarrollo y el conocimiento. Este último aspecto comprende la captura, encapsulamiento y distribución del conocimiento de seguridad que proveerá fundamentos para prácticas de seguridad de software (van Bon, 2008). A su vez, las fallas de un software serían resultado de cualquiera de las siguientes razones: i) la especificación puede ser incorrecta o puede que falten

requisitos, de manera que la especificación no indica exactamente lo que el cliente quiere o necesita; ii) las especificaciones contienen un requisito demasiado complicado de implementar, dados los escenarios de hardware y software prescritos; iii) el diseño del sistema contiene una falla, por ejemplo, la base de datos y los diseños de lenguaje de consulta hacen que sea imposible autorizar a los usuarios; iv) las descripciones de los componentes contienen un algoritmo de control de acceso que no maneja este caso correctamente; o, v) el código del programa puede estar equivocado, implementando el algoritmo de manera incorrecta o incompleta (Bhatti, 2005).

Con base en los estudios revisados se ha podido constatar la importancia que tiene para las cooperativas el aplicar una auditoría de seguridad en el proceso de desarrollo de software que asegure el eficaz desenvolvimiento de éste, pues no contar con dicha herramienta trae consigo la posibilidad de que estas instituciones se expongan a problemas y riesgos futuros, los que, a su vez, podrían redundar en una falta de seguridad en el diseño y aplicación de los software, arriesgando el manejo de recursos de los socios. Ante tal situación, cabe plantearse la siguiente pregunta de investigación, la misma que guiará cada uno de los pasos y procesos a implementarse en el presente trabajo de investigación:

¿Qué medidas y pasos deben seguirse para asegurar que el proceso de desarrollo de software en una Cooperativa cumpla los estándares establecidos por la ISO/IEC 15504?

Es importante señalar la organización en estudio, es una cooperativa de ahorro y crédito que se encuentra regulada por la Superintendencia de Economía Popular y Solidaria, y cuyos objetivos principales son fomentar en los socios mejores condiciones de trabajo, así como aumentar la productividad, a través de la prestación de servicios financieros competitivos y oportunos. Sin embargo, los fines para los cuales fue constituida la entidad podrían sufrir severas complicaciones si es que no se llevan a cabo procesos de auditoría y de control, particularmente a los programas de software implementados al interior de la entidad. Hasta el día de hoy el software que se emplea en la Cooperativa no ha sido auditado bajo estándares actualizados y consolidados como el ISO/IEC 15504, el cual según estudios previos, se constituye en una herramienta idónea para adquirir una visión real de los procesos informáticos de las organizaciones, por lo que se está exponiendo la institución financiera a una serie de errores informáticos que podrían redundar en falencias en los procesos y, por lo tanto, no se estaría asegurando un control adecuado de los ahorros e inversiones de todos los socios, al tiempo que se imposibilita que los objetivos económicos de la entidad lleguen a cumplirse. De ahí que resulta indispensable el desarrollo del presente estudio y su inmediata aplicación.

Para lo cual se ha planteado como objetivo general de la investigación: Diseñar y aplicar una auditoría de seguridad en el proceso de desarrollo de software acorde a los estándares ISO/IEC 15504 en la Cooperativa durante el año 2018. Para la consecución de este objetivo, la investigación se enfoca en la realización de los siguientes objetivos específicos: en primer lugar, efectuar una aproximación a estudios previos relacionados a la auditoría de seguridad y a distintos modelos de auditoría de seguridad al proceso de software, particularmente al estándar ISO/IEC 15504; en segunda instancia, diagnosticar la situación actual de la Cooperativa por medio de la aplicación de instrumentos de verificación del control en la seguridad informática; y, por último, aplicar una auditoría de seguridad informática al proceso de desarrollo de software en la Cooperativa.

MARCO TEÓRICO

Trabajos relacionados

Mas y Amengual (2005) estudiaron los modelos de auditoría en el contexto de las pymes desarrolladoras de software, al tiempo que presentaron un modelo para la implantación de un Sistema de Gestión de Calidad en Pymes de Desarrollo de Software basado en SPICE, detallándose su aplicación

a un conjunto de pymes de las Islas Baleares, España. Se evidenció la inexistencia una cultura de seguridad de la información al interior de las organizaciones, ausencia de sistemas de control de seguridad informática y procesos y procedimientos documentados para protección informativa.

Dussan (2006) evidenció que el 60% de las compañías a nivel de Colombia no cuentan con programas establecidos de seguridad informática. Mientras que Voutssas (2010) analizó la problemática actual de la producción y acumulación mundial de información en forma de documentos electrónicos o digitales, los riesgos, amenazas vulnerabilidades que afectan a esa información, al tiempo que planteó varias estrategias que permiten establecer una seguridad informática que preserve la información.

Solarte, Rosero y del Carmen (2015), a partir de la experiencia de aplicar las fases de auditoría de la seguridad informática en distintas empresas, evidenciaron que los problemas principales son: el desconocimiento sobre aplicación de las normas de seguridad de la información y las limitaciones en la administración de seguridad informática y de la información, mínima cultura en el tema de seguridad de información, la organización no formal del área informática, la no existencia de responsables de la seguridad, no existencia o falta de cumplimiento de políticas y procedimientos de seguridad dentro de la organización, falencias en el manejo de los inventarios de activos informáticos.

Naranjo (2013) aplicó la Metodología General de Auditoría (MGA) en la Cooperativa de Ahorro y Crédito “Educadores de Chimborazo”, observándose la seguridad existente en los servidores de la entidad alcanzan un nivel del 24%, lo que se constituye en un valor preocupante en razón de que no existe la seguridad adecuada en dicha área. Simbaya (2014), por su parte, a través de la aplicación de una auditoría a los sistemas de información financiera de la Cooperativa de Ahorro y Crédito Universitaria Limitada COPEU, pudo evidenciar que no se lleva registro y seguimiento de fallos del para poder dar soluciones adecuadas. Dicho sistema no responde con agilidad en el proceso por lo que provoca malestar en el personal y en los clientes

A su vez, una revisión bibliográfica a artículos científicos e indexados permite adquirir una percepción sobre el estado actual de las investigaciones en torno a ciertos estándares ISO / IEC. Los estudios más relevantes se detallan a continuación:

Modelos de seguridad para proceso de software

El Systems Security Engineering Capability Maturity Model (SSE-CMM) es un modelo de referencia que incorpora la Ingeniería de Seguridad en las empresas y entre cuyos alcances está la ejecución de una serie de actividades que permite el desarrollo de software confiables y un ciclo de vida para sistemas seguros (Ferraiolo, 1998). Clasifica la ingeniería de seguridad en tres apartados básicos: a) Riesgo, identificando y priorizando los peligros relacionados al desarrollo de productos o sistemas; b) Ingeniería, trabajando con otras disciplinas con la finalidad de plantear soluciones a los riesgos; c) Aseguramiento, cuyo objetivo es la certificación de que las soluciones incorporadas resultan confiables. Se encuentra estructurado en dos dimensiones: dominios y capacidades; la primera refiere a un conjunto de prácticas básicas que permiten definir la ingeniería de seguridad. La segunda, por su parte, alude a las prácticas genéricas que establecen la administración del proceso de desarrollo del software.

El Control Objectives for Information and related Technology (COBIT) organiza diferentes estándares, presenta varias mejoras prácticas, que se enfocan mayormente en el control que en la ejecución. Establece una serie de criterios de control, considerando para ello requisitos de calidad, confianza y seguridad. Divide la gobernanza de la tecnología de la información en 34 procesos y proporciona un objetivo de control (OC) de alto nivel para cada uno de estos 34 procesos. Cada OC se divide de nuevo en un conjunto de objetivos de control detallados (OCD), que especifican la forma en que se

debe gestionar el OC de alto nivel, con más detalle. En total, se definen 316 DCO para los 34 procesos (Von Solms, 2005). El fundamento es que si cada uno de estos 34 procesos se gestiona adecuadamente, se obtendrá una gestión adecuada de la tecnología de la información.

El Information Technology Infraestructure Library (ITIL) ofrece una descripción minuciosa de una serie de buenas prácticas, por medio de una amplia lista de roles, tareas, procedimientos y obligaciones que podrían ser adaptadas a cualquier empresa. La versión 3 de ITIL organiza los distintos procesos en cuatro categorías principales: estrategia, diseño, transición y operación del servicio. Además, hay un quinto: mejora continua del servicio, que aborda las actividades para mejorar los servicios y los procesos de forma continua (Eikebrokk & Iden, 2012). Proporciona un marco común para todas las actividades informáticas, las que se dividen en procesos, que empleados en conjunto se constituyen en un marco para lograr un gestión de servicios más madura. Entre los beneficios de la aplicación del modelo ITIL están: el área informática desarrolla una estructura más clara, se hace más eficaz y se centra más en los objetivos corporativos (van Bon, 2008).

El Informe técnico internacional para ISO / IEC 91261 describe un conjunto de métricas de calidad del software (métricas externas, internas y de calidad en uso) que se utilizarán con el modelo de calidad ISO / IEC 9126 (Jung, Kim, & Chung, 2004). Estas se relacionan con indicadores de calidad del proceso, desarrollo y tamaño de alto nivel que son de interés para la actividad de desarrollo y mantenimiento del software (Bhatti, 2005). El usuario de estos informes técnicos internacionales debe seleccionar las características de calidad y las características secundarias que se evaluarán de ISO / IEC 9126 (Zeiss *et al*, 2007), identificar las medidas directas e indirectas apropiadas que se aplicarán, identificar las métricas relevantes y luego interpretar la medición e interpretar el resultado de la medición de una manera objetiva (Behkamal, Kahani, & Akbari, 2009). Una métrica de funcionalidad externa mide los atributos, como el comportamiento de un sistema con respecto al criterio de precisión y adecuación (Lincke, Lundberg, & Löwe, 2008).

Por su parte, el estándar ISO IEC 27001 consiste en una guía para el análisis, implementación, control y mantenimiento de un sistema de gestión de seguridad de la información. Norma general aplicable a una amplia gama de empresas. Este estándar emplea la metodología denominada Ciclo de Deming, con el fin de establecer las fases de vida y mejora continua del sistema de software, por medio de un seguimiento que garantiza el mantenimiento de los controles y los cambios indispensables que permitan reducir los riesgos que aparezcan posterior a la implementación del sistema (Talavera, 2015).

Estándar ISO / IEC 15504

Norma propuesta en conjunto por la International Organization for Standardization (ISO) y la International Electrotechnical Commission (IEC) y que ofrece un marco de trabajo para la evaluación de procesos, además de establecer los requisitos para desarrollar un software con pautas de calidad (Alarcón, González, & Rodríguez, 2011). El estándar internacional emergente ISO / IEC 15504 es un intento de armonizar los modelos de evaluación existentes que son de uso común. Define un esquema para medir la capacidad de los procesos de software. Una premisa básica del 15504 es que el puntaje cuantitativo de la evaluación se asocia con el desempeño de la organización o proyecto. De hecho, esta es una premisa de todos los modelos de evaluación. Por lo tanto, se espera que la mejora de las prácticas de ingeniería de software, de acuerdo con el modelo de evaluación, mejore posteriormente el rendimiento. Esto se denomina validez predictiva del puntaje de capacidad del proceso. La validación empírica de la verosimilitud de tal premisa es de importancia práctica ya que las organizaciones que se guían por los resultados de la evaluación realizan importantes inversiones de mejora de procesos. Si bien se han realizado algunos estudios correlacionales que corroboran la premisa anterior, ninguno evaluó la validez

predictiva de las medidas de capacidad del proceso definidas en ISO / IEC 15504. La consecuencia es que no es posible sustanciar las afirmaciones de mejora mediante la adopción de las prácticas estipuladas en 15504 realmente resulta en mejoras de rendimiento (Pino, García, Serrano, & Piattini, 2006).

Por lo general, en el mejoramiento de la calidad de los procesos se involucran dos clases de modelos, el de procesos y el de evaluación; el primero establece un catálogo o colección de buenas prácticas que detallan las propiedades de un proceso efectivo, mientras que el modelo de evaluación ofrece los principios para evaluar la calidad y para implantar tal modelo en una entidad (García, Irrazabal, & Garzás, 2010).

La arquitectura de ISO / IEC 15504 es bidimensional. Una dimensión consiste en los procesos que se evalúan realmente (dimensión Proceso) agrupados en cinco categorías. La segunda dimensión consiste en la escala de capacidad que se utiliza para evaluar la capacidad del proceso (dimensión Capacidad). La misma escala de capacidad se usa en todos los procesos. El proceso de análisis de requisitos de software se define en la categoría Proceso de ingeniería en la dimensión Proceso. Durante una evaluación, no es necesario evaluar todo el proceso; una cooperativa puede determinar el alcance de una evaluación para cubrir solo el subconjunto de procesos que son relevantes para sus objetivos empresariales. Por lo tanto, no todas las organizaciones que realizan una evaluación basada en ISO / IEC 15504 cubrirán el proceso de análisis de requisitos (El Emam & Birk, 2000). Se determina el nivel de capacidad de los procesos correspondientes al nivel de madurez, mientras que a través del nivel de capacidad se derivará un nivel de madurez de acuerdo a las reglas de derivación (ver tabla 1).

Tabla 1. Nivel de madurez

Nivel de madurez	Descripción
Nivel de madurez 0	La entidad no posee una implementación efectiva de los procesos.
Nivel de madurez 1	Los procesos objeto de evaluación llegan a un nivel de capacidad 1, existiendo productos resultantes para aquellos y el proceso puede ser identificado.
Nivel de madurez 2	Los procesos poseen nivel de capacidad 2 o superior.
Nivel de madurez 3	Los procesos de los niveles de madurez 2 y 3 poseen nivel de capacidad 3 o mayor.
Nivel de madurez 4	Uno o más procesos poseen nivel de capacidad 4 o superior.
Nivel de madurez 5	Uno o más procesos poseen nivel de capacidad 5.

Siguiendo los aportes de Rout (2003), se desarrolla a continuación una explicación de cada uno de los niveles:

- Proceso incompleto - Nivel 0: Hay una falla general para lograr el propósito del proceso. No hay productos de trabajo o productos fácilmente identificables del proceso.
- Proceso realizado - Nivel 1: Generalmente se logra el objetivo del proceso. El logro no puede ser rigurosamente planificado y rastreado. Las personas dentro de la organización reconocen que se debe realizar una acción, y existe un acuerdo general de que esta acción se realiza cuando sea necesario. Existen productos de trabajo identificables para el proceso, y estos dan testimonio del logro del propósito.
- Proceso gestionado - Nivel 2: El proceso entrega productos de trabajo de calidad aceptable dentro de escalas de tiempo definidas. El rendimiento según los procedimientos especificados se planifica y se realiza un seguimiento. Los productos de trabajo cumplen con los estándares y requisitos especificados. La distinción principal con el Nivel 1 es que el rendimiento del proceso se planifica y gestiona, y avanza hacia un proceso definido.
- Proceso establecido - Nivel 3: El proceso se realiza y gestiona utilizando un proceso definido basado en buenos principios de ingeniería de software. Las implementaciones individuales del proceso utilizan versiones aprobadas y personalizadas de procesos documentados estándar. Los recursos necesarios para establecer la definición del proceso también están en su lugar. La distinción principal del nivel administrado

es que el proceso del nivel establecido se planifica y administra mediante un proceso estándar.

- Proceso predecible - Nivel 4: El proceso definido se lleva a cabo consistentemente en la práctica dentro de los límites de control definidos, para lograr sus objetivos. Se recopilan y analizan medidas detalladas de rendimiento. Esto lleva a una comprensión cuantitativa de la capacidad del proceso y una capacidad mejorada para predecir el rendimiento. El rendimiento se gestiona objetivamente. La calidad de los productos de trabajo es cuantitativamente conocida. La distinción principal con el Nivel 3 es que el proceso definido se entiende y se controla de forma cuantitativa.
- Proceso de optimización - Nivel 5: El rendimiento del proceso se optimiza para satisfacer las necesidades comerciales actuales y futuras, y el proceso logra la repetición para cumplir sus objetivos comerciales definidos. Se establecen objetivos cuantitativos de eficacia y eficiencia (objetivos) para el rendimiento, basados en los objetivos comerciales de la organización. El monitoreo continuo del proceso en contra de estos objetivos es posible mediante la obtención de retroalimentación cuantitativa y se logra una mejoría mediante el análisis de los resultados. La optimización de un proceso implica poner a prueba ideas y tecnologías innovadoras y cambiar los procesos no efectivos para alcanzar las metas u objetivos definidos. La distinción principal con el Nivel 4 es que el proceso definido y el proceso estándar se someten a refinamiento y mejora continuos, basados en una comprensión cuantitativa del impacto de los cambios en estos procesos.

Con la finalidad de medir la capacidad de un proceso, se emplea una serie de atributos de proceso (PAs), en la que cada atributo establece un aspecto específico de capacidad de proceso (ver tabla 2)

Tabla 2. Atributos de proceso

Nivel de capacidad	Atributo de proceso (PA)
Nivel 1: Proceso realizado	PA 1.1. Realización del proceso
Nivel 2: Proceso gestionado	PA 2.1. Gestión de la realización PA 2.2. Gestión del producto de trabajo
Nivel 3: Proceso establecido	PA 3.1. Definición del proceso PA 3.2. Despliegue del proceso
Nivel 4: Proceso predecible	PA 4.1. Medición del proceso PA 4.2. Control del proceso
Nivel 5: Proceso en optimización	PA 5.1. Innovación del proceso PA 5.2. Optimización continua

Por su parte, una revisión bibliográfica a artículos científicos e indexados permite adquirir una percepción sobre el estado actual de las investigaciones en torno al estándar ISO / IEC 15504. Los estudios más relevantes resaltan las ventajas del estándar para ofrecer una visión realista del proceso de desarrollo de software, particularmente en pequeñas y medianas empresas, como es el caso de la Cooperativa, objeto del presente estudio.

El Emam (1998) presentó una evaluación de seguimiento de la consistencia interna de la ISO / IEC 15504, cuyos resultados indican que la consistencia interna de la dimensión de capacidad no se deterioró, y que aún es lo suficientemente alta para fines prácticos. Emam y Garro (1999) estimaron el número de evaluaciones de procesos de software que se llevaron a cabo en todo el mundo entre septiembre de 1996 y junio de 1998 utilizando el estándar internacional emergente ISO / IEC 15504. Los resultados indican que se realizaron 1.264 evaluaciones con un intervalo de confianza del 90% de 916 y 1895. El método utilizado aquí se puede aplicar para estimar el alcance del uso de otras normas de ingeniería de software, y también de otras tecnologías de ingeniería de software. Dichas estimaciones pueden beneficiar a los desarrolladores de estándares (o tecnología), agencias de financiación e investigadores al centrar sus esfuerzos en los estándares (o tecnologías) más utilizados. Paulk (1999) discutió las similitudes y diferencias entre los modelos CMM y el ISO / IEC 15504 y cómo pueden influirse mutuamente a medida que ambos continúan evolucionando.

El Emam y Birk (2000) evaluaron la validez predictiva de la capacidad del proceso de análisis de requisitos de software (SRA). Se realizaron evaluaciones utilizando ISO / IEC

15504 en 56 proyectos en todo el mundo durante un período de dos años. Las medidas de rendimiento en cada proyecto también se recopilaron mediante cuestionarios, como la capacidad de cumplir los compromisos presupuestarios y la productividad del personal. Los resultados brindan una sólida evidencia de validez predictiva para la medida de capacidad de proceso de SRA utilizada en ISO / IEC 15504, pero solo para organizaciones con más de 50 empleados de TI. El Emam y Jung (2001) desarrollaron una evaluación empírica del modelo ISO / IEC 15504. Los datos se obtuvieron de 57 evaluaciones en todo el mundo. Los hallazgos indican que el modelo actual se puede usar con éxito en las evaluaciones. Sin embargo, también señalaron algunas debilidades en el esquema de calificación que deben rectificarse en futuras revisiones de ISO / IEC 15504.

Garzás, Fernández y Piattini (2009) presentaron una adaptación de ISO 15504 para la evaluación por niveles de madurez en PYMES y pequeños equipos de desarrollo. García, Irrazabal y Garzás (2010) estudiaron el grado de cobertura entre los procesos de ISO/IEC 15504 e ISO /IEC 122207-2008 y SCRUM, obteniéndose que con la implantación de este último se alcanzaría el 83% de la planificación del proyecto. Pino *et al* (2015) presentaron un modelo de evaluación de la calidad de procesos de desarrollo de software basado en la norma ISO/IEC 15504 aplicable a las micro, pequeñas y medianas empresas.

Anacleto, von Wangenheim, Salviano y Savi (2004) describieron algunas experiencias obtenidas de la aplicación de ISO / IEC 15504 para evaluaciones de procesos de software en cuatro pequeñas empresas de software en Brasil. Se evidenció la presencia de costos y beneficios relacionados con las evaluaciones. Jung y Hunter (2001) analizaron el nivel de capacidad ISO / IEC 15504 que espera una organización con certificación ISO 9001 y la existencia de diferencias significativas entre los niveles de capacidad ISO / IEC 15504 alcanzados por los procesos de las organizaciones certificadas con ISO 9001 y las de organizaciones sin certificación ISO 9001. Para lo cual se analizó un conjunto de datos de 1996 a junio de 1998. Los resultados muestran que los procesos ISO / IEC 15504 de las organizaciones certificadas ISO 9001 alcanzaron niveles mejores de capacidad. Los resultados también muestran diferencias entre los niveles de capacidad logrados por organizaciones certificadas ISO 9001 y organizaciones no certificadas ISO 9001, así como también entre organizaciones con un gran personal de TI y aquellas con un pequeño personal de TI.

METODOLOGÍA

Para el presente estudio se asumió un enfoque de tipo cuantitativo-cualitativo, es decir, mixto. Se alcanzó un nivel descriptivo, mientras que en relación al tipo de estudio, este sería observacional, transversal y prospectivo. Puesto que se basó en la revisión y evaluación de los controles, sistemas, y procedimientos en el desarrollo de software en una Cooperativa nacional, la investigación implicaría un estudio de caso.

Para el estudio de caso, la presente auditoría de seguridad informática siguió los criterios de evaluación propuestos en el estándar ISO / IEC 15504, que se dividen en los siguientes apartados:

Niveles de capacidad

- Nivel 0: El proceso de desarrollo de software no se implementó completamente y no alcanzó sus objetivos.
- Nivel 1: El proceso de desarrollo de software se ejecutó, se implementó y logró sus objetivos.
- Nivel 2: El proceso de desarrollo de software fue gestionado, controlado y su implementación está planificada, monitoreada y ajustada. Sus resultados (productos de trabajo) son establecidos, controlados y debidamente registrados y mantenidos.
- Nivel 3: El proceso de desarrollo de software está establecido y documentado con el fin de garantizar su capacidad para cumplir sus objetivos.
- Nivel 4: El proceso de desarrollo de software ha adquirido predictibilidad; es

decir, se ejecuta de acuerdo con los objetivos de rendimiento definidos.
- Nivel 5: El proceso de desarrollo de software se encuentra en grado de optimización.

Atributos de clasificación

Se estableció una escala de calificación con valores basados en el porcentaje de logro de los atributos:

- N: no implementado (0-15%)
- P: Parcialmente implementado (> 15-50%)
- L: Ampliamente implementado (> 50-85%)
- F: completamente implementado (> 85%)

Instrumentos

Para la auditoría informática se emplearon fundamentalmente tres herramientas de recopilación de información:

i. Encuesta sobre proceso de desarrollo de software en la Cooperativa.
ii. Una entrevista a la persona coordinadora del proceso de desarrollo de software en la Cooperativa
iii. Una lista de verificación a cada uno de los procesos considerados por el estándar ISO / IEC 15504. Con la finalidad de comparar los resultados del proceso se utilizaron listas de verificación, donde se señaló con una "x" si el criterio está de acuerdo con las siguientes categorías:

- Conforme (C)
- No Conforme (NC)
- Observación (OB)
- Oportunidad de Mejora (OM)

A continuación se describen y analizan los resultados obtenidos.

ANÁLISIS DE RESULTADOS

Suministro

Se auditó al proceso de suministro, con la finalidad de determinar si los directivos de la Cooperativa consideran que el software diseñado e implementado y actualmente en funcionamiento en la entidad cumple con las características acordadas (ver tabla 3).

Tabla 3. Suministro

Resultados del proceso	C	NC	OB	OM
Desarrollo del software	X			
Entrega del software	X			
Implantación del software	X			
Total	**3**			

Fuente: Lista de verificación del proceso

En torno al proceso de su suministro los resultados evidencian que la Cooperativa se encuentra conforme en los aspectos concernientes a desarrollo, la entrega y la implantación de software.

Definición de los requerimientos del usuario.

Se evaluó si se han definido los requerimientos del programa de desarrollo de software que permitan ofrecer los servicios útiles a los colaboradores (ver tabla 4).

Tabla 4. Definición de los requerimientos del usuario

Resultados del proceso	C	NC	OB	OM
Especificación características software	X			
Definición de restricciones	X			
Definición de requisitos	X			
Validación de conformidad a los servicios	X			
Base para la negociación y acuerdo de la entrega del software	X			
Total	**5**			

Fuente: Lista de verificación del proceso

Al observarse una conformidad por parte de la Cooperativa con respecto a las especificaciones de las características del software implementado, tanto en restricciones como en requisitos, así como en lo concerniente a la validación de los servicios, se constata que el proceso auditado habría cumplido satisfactoriamente las exigencias del nivel 1.

Análisis de los requerimientos del sistema.

Se analizó la transformación de los requisitos de los stakeholders[3] con respecto a los requisitos técnicos del software que guiarán el diseño del mismo (ver tabla 5).

Tabla 5. Análisis de los requerimientos del sistema

Resultados del proceso	C	NC	OB	OM
Definición de requisitos funcionales y no funcionales	X			
Aplicación de técnicas para solución del proyecto	X			
Comprobación de la precisión de los requisitos	X			
Costos, calendario e impacto de los requisitos del sistema en el entorno de exploración	X			
Aprobación requisitos del software	X			
Trazabilidad entre requisitos del software y de la Cooperativa	X			
Total	**5**			

Fuente: Lista de verificación del proceso

Para el análisis fue necesario, previamente, definir los requerimientos funcionales y no funcionales del proceso de desarrollo del software, para lo cual, posterior a la entrevista realizada se procedió a definirlos. Fue necesaria la elaboración y revisión de una Matriz de requerimientos, donde se detallaron todos aquellos requerimientos funcionales. Ello permitió constatar que se han definido los requisitos funcionales y no funcionales, que estos han sido planteados de manera precisa y que, al final, han sido aprobados. Con ello se ha logrado observar la existencia de una trazabilidad entre los requisitos del software y los otros procesos informáticos y administrativos de la Cooperativa.

Gestión del modelo del ciclo de vida

Se auditó si en la Cooperativa se han definido, mantenido y asegurado las políticas, procesos y modelos del ciclo de vida, que serán empleados por la entidad (ver tabla 6).

Tabla 6. Gestión del modelo del ciclo de vida

Resultados del proceso	C	NC	OB	OM
Establecimiento de políticas y procedimientos para la gestión	X			
Definición de autoridad y responsabilidades para la gestión		X		
Definición, mantenimiento e implementación de mejoras en los procesos.	X			
Total	**2**	**1**		

Fuente: Lista de verificación del proceso

Para el análisis de este proceso se revisaron los manuales proporcionados por la Cooperativa, en los cuales se especifica el procedimiento de mejora continua establecido por la entidad. Se pudo determinar que no existe una autoridad responsable de la coordinación del ciclo de vida, aunque sí un grupo de funcionarios que laboran bajo la coordinación de un responsable; ellos serían los encargados de dar seguimiento al proceso en cada una de sus fases. Se evidenció que las políticas y procedimientos para la gestión han sido implementados y mantenidos, pero el hecho de que no exista un funcionario legalmente asignado para su seguimiento, abre la posibilidad a que la gestión no se cumpla a cabalidad. Por tanto, el proceso de desarrollo de software estaría alcanzando de manera todavía no completa el nivel 2.

Planificación del proyecto

Se auditó si se han elaborado y comunicado los planes del desarrollo de software de manera efectiva y viable (ver tabla 7).

Tabla 7. Planificación del proyecto

Resultados del proceso	C	NC	OB	OM
Definición del alcance del proyecto de desarrollo de software	X			
Evaluación de la viabilidad de proyecto de desarrollo de software	X			
Estimación de los recursos, tamaño y esfuerzo de las tareas	X			
Identificación de la relación de los elementos del proyecto de desarrollo de software, con otras unidades de la Cooperativa	X			
Definición de plan de ejecución de desarrollo de software	X			
Iniciación de los planes	X			
Total	**6**			

Fuente: Lista de verificación del proceso

En líneas generales, se logró determinar que el proceso de Planificación del Proyecto de desarrollo de software se ha cumplido, hallazgo que se sustentó no solo gracias a la entrevista, el cuestionario y la lista de verificación que sintetizó la información obtenida, sino por medio de la revisión de ciertos documentos oficiales donde se definió las directrices del proceso de desarrollo del software en sus fases iniciales. El factor clave que permitió alcanzar este proceso fue el

[3] Quienes pueden afectar o son afectados por las actividades de una empresa.

contar con un método documentado para la estimación de esfuerzos para cada tarea preestablecida y no depender de consideraciones subjetivas.

Evaluación y control del proyecto

Con la auditoría de seguridad informática se pretendió determinar el estado del proyecto de desarrollo de software y constatar si su ejecución fue realizada de acuerdo con los planes y el calendario establecido, con los presupuestos planificados y respondiendo a los fines técnicos (ver tabla 8).

Tabla 8.Evaluación y control del proyecto

Resultados del proceso	C	NC	OB	OM
Control e informes sobre proceso del proyecto de desarrollo de software		X		
Control de la relación entre los elementos del proyecto de desarrollo de software, con otras unidades de la Cooperativa		X		
Acciones para la corrección de las desviaciones de los planes		X		
Registro de los objetivos del proyecto de desarrollo de software	X			
Total	**1**	**3**		

Fuente: Lista de verificación del proceso

La auditoría permitió constatar el incumplimiento de este proceso, básicamente evidenciándose la ausencia de controles sobre el proceso del proyecto de desarrollo de software y con respecto a la relación entre los componentes del proyecto de desarrollo de software y otras unidades de la Cooperativa. Así mismo, no se habrían tomado acciones que contribuyesen a la corrección de las desviaciones de los planes originales. A partir de estos hallazgos se comienza a evidenciar en dónde residen las principales falencias en el proceso de desarrollo de software en la Cooperativa: la ausencia de controles y seguimientos a los procesos y productos generados, vacío que abre la posibilidad a la presencia de riesgos en la seguridad informática.

Gestión de la configuración del software

La auditoría a la gestión de la configuración del software permitió determinar si existió integridad entre los elementos que componen el servicio al momento de entregarlo a la Cooperativa (ver tabla 9).

Tabla 9. Gestión de la configuración del software

Resultados del proceso	C	NC	OB	OM
Establecimiento de una estrategia de gestión de la configuración	X			
Definición de los productos generados por los procesos y el proyecto de desarrollo de software	X			
Control de cambios		X		
Informe sobre el estado de los elementos y cambios en el desarrollo de software		X		
Aseguramiento de la integridad y consistencia de los elementos	X			
Control del almacenamiento, tratamiento y entrega del software.		X		
Total	**3**	**3**		

Fuente: Lista de verificación del proceso

Los resultados permiten ratificar lo señalado en el análisis anterior (ver tabla 8): es en el apartado de control y el seguimiento donde existen los problemas más acuciantes en el proceso de desarrollo de software implementado en la Cooperativa. No se habría implementado un control de las modificaciones realizadas, ni un informe sobre el estado de los elementos y cambios en el desarrollo de software. A su vez, se pudo constatar la falta de control con respecto al almacenamiento, el tratamiento y la entrega del software. Con base en conversaciones con el funcionario responsable, se pudo confirmar que al momento en que la programación era actualizada a causa de una validación en los procesos informáticos de la entidad financiera, no se procedía a registrar dicha actualización, ni se comunicaba los cambios al resto de los involucrados.

Situación conflictiva, pues el buen desempeño en este subproceso permitiría asegurar la correcta evolución del software. Lo contrario implica exponer a la entidad a riesgos operativos futuros mediatos.

Gestión de la configuración

La auditoría a la gestión de la configuración permitió determinar si existió integridad en todos los productos de trabajo empleados durante el desarrollo del software y que fueron puestos en consideración de la Cooperativa (ver tabla 10).

Tabla 10. Gestión de la configuración

Resultados del proceso	C	NC	OB	OM
Definición de los elementos para la gestión de la configuración	X			
Gestión de cambios en los elementos	X			
Control de la configuración de los entregables		X		
Estado de elementos bajo gestión de la configuración está disponible todo ciclo de vida,	X			
Total	**3**	**1**		

Fuente: Lista de verificación del proceso

Con base en la observación se pudo determinar que existe un historial de cambios, el mismo que cuenta con la siguiente información: i) versión del software; ii) cambio realizado; iii) nombre del responsable del cambio y iv) fecha en que se realizó el cambio. Este contenido aseguraría la disponibilidad de la Cooperativa al historial de cambios; sin embargo, se constata que el seguimiento y, por ende, el control no es una práctica habitual. Sería indispensable delegar a uno de los funcionarios la responsabilidad de controlar y hacer seguimiento de cada uno de los subprocesos y cambios que vayan ocurriendo alrededor del desarrollo de software.

Medición

Por su parte, se evaluó si la recolección, el análisis y la información sobre los datos relacionados al desarrollo del software en la Cooperativa, se constituyeron en un apoyo a la gestión efectiva de los procesos, y si mostraron una objetiva calidad (ver tabla 11).

Tabla 11. Medición

Resultados del proceso	C	NC	OB	OM
Identificación de las necesidades que serán evaluadas de los procesos de desarrollo de software	X			
Desarrollo de un conjunto de medidas a partir de las necesidades	X			
Planificación de actividades de medición		X		
Datos son recogidos, almacenados, analizados e interpretados	X			
Resultados que facilitan toma de decisiones	X			
Evaluación de proceso de medición		X		
Mejoras comunicadas a responsable del proceso de medición	X			
Total	**5**	**2**		

Fuente: Lista de verificación del proceso

El hecho de que no se haya implementado una planificación de actividades de medición y que, al mismo tiempo, no exista una evaluación de proceso de medición, impide ubicar al proceso de desarrollo de software en un nivel 3 de manera satisfactoria. Como ha sido una constante en el presente análisis, las acciones de planificación, seguimiento y control son las que presentan serias deficiencias al interior de la Cooperativa. Y ello trae consigo la posibilidad de que se presenten ciertos riesgos, en especial, que no se asegure que la entidad financiera pueda evaluar el nivel de cumplimiento de los procesos de desarrollo de software desde una perspectiva afín a sus objetivos empresariales.

Aseguramiento de la calidad software

Se evaluó si el software implementado en la Cooperativa cumplió con los lineamientos y planes preestablecidos (ver tabla 12).

Tabla 12. Aseguramiento de la calidad software

Resultados del proceso	C	NC	OB	OM
Definición de la estrategia para el aseguramiento de la calidad.	X			
Producción y mantenimiento de evidencias que aseguren la calidad	X			
Identificación y registro de problemas con los requisitos	X			
Constatación de que el software cumple con estándares, procedimientos y requisitos	X			
Total	**4**			

Fuente: Lista de verificación del proceso

No existen hallazgos negativos con respecto a aseguramiento de la calidad software, más bien, se constató la presencia de un comportamiento esperado del proceso de desarrollo de software con respecto a los requerimientos definidos. Tales resultados permiten garantizar un proceso sistemático y planificado que asegura que las acciones y el software propiamente, estén acordes a lo que se señala en los estándares, procedimientos y

normas de referencia. Al mismo tiempo ofrece una herramienta de obtención de datos que fortalecen los procesos informáticos implementados en la entidad bancaria. Es importante recordar que contar con un proceso de aseguramiento de calidad garantiza un perfil de responsabilidad en la calidad del servicio y de la seguridad informática.

Gestión de requerimientos

Se analizó la gestión de los requerimientos del software implementado en la Cooperativa CAPCE Biblián, al tiempo que se revisó si existen inconsistencias entre los requisitos los planes y productos de trabajo del proyecto de desarrollo del software (ver tabla 13).

Tabla 13. Gestión de requerimientos

Resultados del proceso	C	NC	OB	OM
Obtención de una comprensión de los requerimientos	X			
Compromiso sobre los requerimientos		X		
Gestión de los cambios en los requerimientos		X		
Trazabilidad bidireccional de los requerimientos		X		
Identificación de las inconsistencias entre el trabajo del proyecto de desarrollo de software y los requerimientos	X			
Total	**2**	**3**		

Fuente: Lista de verificación del proceso

Partiendo de que el subproceso de gestión de requerimientos es importante para gestionar las exigencias generadas por el proyecto, tanto los técnicos como los no técnicos, resulta preocupante la ausencia de un compromiso sobre aquellos, así como a falta de una gestión frente a las modificaciones en los requerimientos. Tal situación impide que el proceso de desarrollo de software lleve a cabo una trazabilidad bidireccional de los requerimientos, necesaria para establecer una coherencia entre los objetivos del proceso de desarrollo de software y otros procesos de la entidad.

Análisis de requisitos del software

Los requisitos del software de los componentes del sistema fueron también auditados (ver tabla 14), y no se evidenciaron hallazgos problemáticos que podrían poner en riesgo la seguridad y operatividad de sistema.

Tabla 14. Análisis de requisitos del software

Resultados del proceso	C	NC	OB	OM
Los requisitos de los componentes de software y sus interfaces son definidos de modo que coinciden con las necesidades de la Cooperativa	X			
Los requisitos de software a ser desarrollados con analizados, corregidos y probados.	X			
Conocimiento del impacto de los requisitos de software en el entorno operativo	X			
La estrategia de lanzamiento de software define la prioridad para la implementación de los requisitos	X			
Los requisitos de software son aprobados y actualizados según necesidades	X			
Se establece consistencia entre requisitos del sistema y los de diseño y software	X			
Total	**6**			

Fuente: Lista de verificación del proceso

Diseño de la arquitectura del software

De igual manera que con respecto a los requerimientos, no se encontraron deficiencias en el diseño del software. Lo observado es el cumplimiento a cabalidad de cada una de las características técnicas necesarias para el adecuado funcionamiento del software, así como la implementación de los requisitos pertinentes (ver tabla 15).

Tabla 15. Diseño de la arquitectura del software

Resultados del proceso	C	NC	OB	OM
Diseño arquitectónico que describe los principales elementos del software	X			
Interfaces internas y externas definidas de los componentes software	X			
Diseño detallado describiendo unidades de software que pueden ser construidas y probadas	X			
Consistencia entre requerimientos de software y diseño del mismo	x			

Total	4			

Fuente: Lista de verificación del proceso

Diseño de la arquitectura del sistema

Se evaluó que la producción de unidades de software hayan sido ejecutables y que reflejasen correctamente el diseño (ver tabla 16) y en líneas generales se han cumplido con cada uno de los criterios; a excepción de la acción de verificar las unidades de software contra el diseño, lo que a criterio del funcionario responsable entrevistado resulta innecesario, pues señaló que el diseño se va adaptando a las necesidades operativas de la empresa, por lo que sería contraproducente comparar las actualizaciones con el diseño original.

Tabla 16. Diseño de la arquitectura del sistema

Resultados del proceso	C	NC	OB	OM
Establecidos criterios de verificación para las unidades de software	X			
Producidas unidades de software definidas para el diseño	X			
Consistencia establecida entre los requisitos del software y los componentes del diseño y software	X			
Verificación de las unidades de software contra el diseño		X		
Total	**3**	**1**		

Fuente: Lista de verificación del proceso

Gestión de infraestructuras

Se auditó el proceso denominado “gestión de infraestructura”, cuyo objetivo es el mantenimiento de una infraestructura estable y fiable que contribuya a la ejecución de los otros procesos informáticos de la Cooperativa (ver tabla 17). Se evidencia el cumplimiento en cada uno de los componentes de este proceso.

Tabla 17. Gestión de infraestructuras

Resultados del proceso	C	NC	OB	OM
Infraestructura coherente con los procedimientos de proceso, con las normas, las herramientas y las técnicas.	X			
Infraestructura cumple con requisitos de funcionalidad, rendimiento, seguridad, disponibilidad, espacio, equipos, costo, tiempo e integridad de datos.	X			
Total	**2**			

Fuente: Lista de verificación del proceso

Gestión de recursos humanos

Se analizaron las habilidades y conocimientos que el personal involucrado en el desarrollo del software posee y de qué manera estas les permiten llevar a cabo sus actividades (ver tabla 18).

Tabla 18. Gestión de recursos humanos

Resultados del proceso	C	NC	OB	OM
Funciones y competencias para el proyecto de desarrollo de software identificadas	X			
Formación para asegurar que colaboradores de la Cooperativa cuentan con conocimiento para realización de tareas.	X			
Reclutamiento de colaboradores con competencias para ejecutar el proyecto de desarrollo de software	X			
Interacción efectiva entre individuos y grupos	X			
Colaboradores comparten información y coordinan actividades de manera eficiente	X			
Definición de criterios objetivos para la supervisión del desempeño del equipo	X			
Total				

Fuente: Lista de verificación del proceso

Resulta decisivo que este subproceso haya sido cumplido a cabalidad, pues así se asegura una correcta gestión de los recursos humanos dentro de la Cooperativa, lo cual influye en el cumplimiento de los objetivos planeados. Es importante recordar que el factor humano es un componente importante dentro de las entidades financieras, pues de él depende el diseño, la aplicación y el seguimiento de un proceso de desarrollo de software. La asignación de funciones considerando las exigencias del puesto, así como las características del individuo, son fundamentales.

Gestión de riesgos

A continuación se procede a analizar el proceso de gestión de riesgos, particularmente

si se han identificado y mitigado los riesgos de proyecto de desarrollo de software de manera continua y a lo largo de ciclo de vida (ver tabla 19).

Tabla 19. Gestión de riesgo

Resultados del proceso	C	NC	OB	OM
Determinado el ámbito de la gestión de riesgos para el proyecto de desarrollo de software	X			
Estrategias de gestión de riesgo adecuadas				X
Identificados los posibles riesgos para el proyecto de desarrollo de software		X		
Priorizados recursos para monitorear los riesgos		X		
Definición, aplicación y evaluación de métricas de riesgo		X		
Reducción de impacto de riesgo por medidas correctas				X
Total	**1**	**3**		**2**

Fuente: Lista de verificación del proceso

Los resultados obtenidos son importantes en razón de que la implementación de una gestión de riesgos contribuye a que los procesos de desarrollo de software se ejecuten con mayor eficacia; sin embargo, no siempre es posible eludir todos los riesgos. De ahí que resulta preocupante que en el proceso de desarrollo de software en la Cooperativa no se hayan determinado los posibles riesgos para el proyecto de desarrollo de software, no se hayan priorizado los recursos que permitan el monitoreo de los riesgos y, fundamentalmente, que no se hayan definido, aplicado y evaluado las métricas de riesgo. Tales ausencias podría incidir negativamente en cada una de las áreas involucradas en el proceso de desarrollo del software

Gestión de la decisión

Se procede a auditar al proceso de la gestión de la decisión y observar si se ha asegurado el análisis y la resolución de aquellos problemas evidenciados (ver tabla 20). Los resultados permiten afirmar que existe la decisión por parte de los responsables en el proceso de desarrollo de software en la Cooperativa de implementar acciones de solución, de preparar los informes requeridos, y de aplicar los mecanismos necesarios.

Tabla 20. Gestión de la decisión

Resultados del proceso	C	NC	OB	OM
Actividades de resolución de problemas son identificadas	X			
Informes de problemas son preparados ante la detección de problemas en el software	X			
Mecanismos para actuar sobre problemas identificados	X			
Total	**3**			

Fuente: Lista de verificación del proceso

Integración del software

A continuación se revisa de qué manera se ha cumplido el propósito del proceso de integración del software, que fue combinar las unidades de software y la producción de software integrado; así como la verificación de que el software implementado en la Cooperativa refleje de manera correcta el diseño de software (ver tabla 21).

Tabla 21. Integración del software

Resultados del proceso	C	NC	OB	OM
Estrategia de integración elaborada para unidades de software	X			
Implementados criterios de verificación para los elementos de software	X			
Definidos elementos de software a través de criterios de aceptación	X			
Resultados de la prueba de integración registrados	X			
Coherencia entre requisitos y elementos de software	X			
Desarrollo de estrategia de regresión para la verificación de elementos de software el momento de producirse cambios en software	X			
Pruebas de regresión se ejecutan en caso de ser necesario	X			
Total	**7**			

Fuente: Lista de verificación del proceso

A observar estos resultados, podría afirmarse que el proceso de desarrollo de software en la Cooperativa se encuentra satisfactoriamente ensamblado. La información obtenida a través de la entrevista, la lista de verificabilidad y el cuestionario permitió constatar que el proceso, a pesar de ciertas falencias encontradas, habría alcanzado un nivel 3, lo que abre una serie de posibilidades de mejoramiento.

Integración del sistema

Se procede al análisis de la integración de los elementos del software implementado en la Cooperativa con los otros componentes, así como a la verificación de que el sistema haya satisfecho las expectativas de la entidad (ver tabla 22).

Tabla 22. Integración del sistema

Resultados del proceso	C	NC	OB	OM
Estrategia de integración se realiza para la construcción de unidades de agregados al software	X			
Criterios de aceptación son desarrollados para la verificación del cumplimiento de requisitos de software		X		
Agregados del sistema verificados a través de criterios de aceptación.		X		
Resultados de pruebas son registrados		X		
Estrategia de regresión se desarrolla para agregados de nuevas pruebas		X		
Pruebas de regresión ejecutadas cuando resulta necesario		X		
Total	**1**	**5**		

Fuente: Lista de verificación del proceso

A respecto de los resultados es conveniente recordar que la integración de los componentes del software conlleva al establecimiento y mantenimiento de lo que se denomina una secuencia de integración, lo que incluye al entorno para la ejecución de la integración, así como los procedimientos de integración. No obstante, la ausencia de criterios de aceptación para la verificación del cumplimiento de requisitos de software, la no verificación de los agregados del sistema por medio de criterios de aceptación, y que no exista una estrategia de regresión para agregados de nuevas pruebas estaría impidiendo la integración completa del software a los demás componentes de la entidad financiera.

Verificación del software

A continuación se procede a analizar si se ha confirmado que el software refleja correctamente los requisitos previamente establecidos (ver tabla 23). Los hallazgos reiteran lo evidenciado en el transcurso de la presente auditoría y que es la ausencia de acciones preocupadas de controlar, verificar y evitar posibles riesgos, pero realizadas de manera sistemática.

Tabla 23. Verificación del software

Resultados del proceso	C	NC	OB	OM
Implementación de estrategia de verificación		X		
Criterios para verificación de productos software son identificados		X		
Actividades de verificación son realizadas		X		
Se identifican y eliminan los defectos de los productos software		X		
Resultados de actividades de verificación son puestos a consideración de Cooperativa		X		
Total		**5**		

Fuente: Lista de verificación del proceso

Validación del software

Finalmente, a continuación se analiza el proceso de validación, esto es, constatar el cumplimiento de los requisitos para el uso del software (ver tabla 24).

Tabla 24. Validación del software

Resultados del proceso	C	NC	OB	OM
Estrategia de validación implementada	X			
Criterios de validación de productos software identificado	X			
Actividades de validación ejecutadas	X			
Problema identificados resueltos				X
Respaldos de que el software es adecuado para objetivo previsto				X
Resultados de la validación son puestos a consideración de la Cooperativa				X
Total	**3**			**3**

Fuente: Lista de verificación del proceso

La auditoría de seguridad informática ejecutada pretende constituirse en una oportunidad para que los funcionarios

responsables del proceso de desarrollo de software en la Cooperativa desarrollen acciones de mejoramiento en aquellos subprocesos que han tenido ciertas falencias, de ahí que algunas situaciones como problemas identificados todavía sin resolver, o respaldos de que el software es adecuado para los objetivos previstos o que los resultados de la validación sean puestos a consideración de la Cooperativa, han sido identificados como aspectos que pueden mejorarse.

Tabla 25. Calificación por procesos y nivel de madurez

Proceso	% de logro	Atributos de clasificación
Suministro	100%	F
Definición de los requerimientos del usuario	100%	F
Análisis de los requerimientos del sistema	100%	F
Gestión del modelo del ciclo de vida	67%	L
Planificación del proyecto	100%	F
Evaluación y control del proyecto	25%	P
Gestión de la configuración del software	50%	P
Gestión de la configuración	75%	L
Medición	71%	L
Aseguramiento de la calidad software	100%	F
Gestión de requerimientos	40%	P
Análisis de requisitos del software	100%	F
Diseño de la arquitectura del software	100%	F
Diseño de la arquitectura del sistema	75%	L
Gestión de infraestructuras	100%	F
Gestión de recursos humanos	100%	F
Gestión de riesgos	17%	P
Gestión de la decisión	100%	F
Integración del software	100%	F
Integración del sistema	17%	P
Verificación del software	100%	F
Validación del software	50%	P
Total	**77%**	**L**

Fuente: Auditoría ISO / IEC 15504

Los resultados de la auditoría al proceso de desarrollo de software de la Cooperativa permite observar que la mayoría de los subprocesos alcanzan el valor correspondiente a “F: completamente implementado”, mientras que solo un número reducido obtiene el valor correspondiente a “P: parcialmente implementado”. Ello permite establecer que el proceso de desarrollo de software auditado, alcanza un nivel 3, lo que lleva a establecer que el proceso se realiza de manera consistente y bajo parámetros y lineamientos claramente definidos.

CONCLUSIONES

La aproximación a los estudios previos relacionados a la auditoría de seguridad y a los distintos modelos de auditoría de seguridad al proceso de software, particularmente al estándar ISO/IEC 15504, permite definir a la auditoría de seguridad informática como la evaluación de los controles, sistemas, procedimientos de informática, establecidos en una Cooperativa de ahorros con la finalidad de obtener beneficios como la confiabilidad, oportunidad, seguridad y confidencialidad de la información. A su vez, se concluye el presente estudio con el señalamiento de que la seguridad del software permite que un producto previamente desarrollado funcione adecuadamente ante ataques maliciosos. Con respecto al estándar ISO / IEC 15504, el repaso bibliográfico a ciertas investigaciones en torno a este modelo de evaluación permite destacar su ventajas como instrumento para adquirir una visión realista del proceso de desarrollo de software, evidenciándose que aquellas empresas, pequeñas o medianas en el mejor de los casos, que aplicaron el estándar, obtuvieron mejores diagnósticos sobre su situación real.

Por su parte, a partir del diagnóstico preliminar a la realidad de la Cooperativa, se pudo determinar que los objetivos para los cuales se creó la entidad, podrían derivar en situaciones de riesgo si no se desarrollan procesos de auditoría y de control, particularmente a los programas de software implementados al interior de la entidad. El software implementado en la cooperativa no ha sido auditado bajo estándares actualizados y consolidados como el ISO/IEC 15504, ello deriva en la posibilidad de sufrir errores informáticos, falencias en los procesos. Tal situación conllevó a la necesidad de desarrollar la auditoría de seguridad informática objeto del presente estudio.

La aplicación de una auditoría de seguridad informática al proceso de desarrollo de software en la Cooperativa permitió identificar varias problemáticas que, en caso de no ser solucionadas, ponen en riesgo la operatividad de los sistemas informáticos y, principalmente, la seguridad de los clientes y socios durante las transacciones económicas. Se estableció que la mayoría de los subprocesos estaría completamente implementado, frente a un número reducido que estaría parcialmente implementado, lo que conlleva a que el proceso de desarrollo de software auditado alcance un nivel 3, observándose la realización consistente del proceso se realiza de manera consistente y bajo parámetros y lineamientos claramente definidos.

Por su parte, la única limitación a la que se vio expuesta el presente estudio fue la ausencia de auditorías previas, no solo a los procesos de desarrollo del software en la cooperativa, sino de los sistemas informáticos en general, lo que impidió contar con información relevante que permitiese observar la evolución de los procesos en la entidad auditada.

Finalmente, a partir de los resultados obtenidos, se plantea la posibilidad de futuros estudios en torno a las auditorías a los sistemas informáticos, no solo en el desarrollo de software, sino en todos los aspectos relacionados a la seguridad informática, particularmente en las entidades financieras pertenecientes al sector cooperativista, instituciones financieras que cumplen un rol decisivo al interior de las pequeñas comunidades del Ecuador.

Referencias bibliográficas

Alarcón, A., González, J., & Rodríguez, S. (2011). Guía para pymes desarrolladoras de software, basada en la norma ISO/IEC 15504. *Revista Virtual Universidad Católica del Norte*(34), 285-313. Recuperado el 1 de Agosto de 2018, de http://revistavirtual.ucn.edu.co/index.php/RevistaUCN/article/viewFile/339/651

Anacleto, A., von Wangenheim, C. G., Salviano, C. F., & Savi, R. (2004). Experiences gained from applying ISO/IEC 15504 to small software companies in Brazil. *Springer*, 33-37. Recuperado el 2 de Septiembre de 2018, de https://www.researchgate.net/profile/Christiane_Gresse_von_Wangenheim/publication/250215661_Experiences_Gained_from_Applying_ISOIEC_15504_to_Small_Software_Companies_in_Brazil/links/0deec53aebb5e5afd0000000/Experiences-Gained-from-Applying-ISO-IEC-15504-t

Baca, G. (2016). *Introducción a la seguridad informática.* México: Grupo Editorial Patria.

Behkamal, B., Kahani, M., & Akbari, M. (2009). Customizing ISO 9126 quality model for evaluation of B2B applications. . *Information and software technology, 51*(3), 599-609. Recuperado el 22 de Octubre de 2018, de http://www.academia.edu/download/42013641/Customizing_ISO_9126_quality_model_for_e20160203-20448-jwzv42.pdf

Bhatti, S. N. (2005). Why quality?: ISO 9126 software quality metrics (Functionality) support by UML suite. . *ACM SIGSOFT Software Engineering Notes, 30*(2), 1-5. Recuperado el 20 de Octubre de 2018, de https://www.researchgate.net/profile/Shahid_Bhatti3/publication/220631340_Why_quality_ISO_9126_software_quality_metrics_Functionality_support_by_UML_suite/links/58f461e8aca27289c21bda95/Why-quality-ISO-9126-software-quality-metrics-Functionality-support-b

Cano, J. (2004). *Inseguridad Informática: Un concepto dual en seguridad informática.* Recuperado el 16 de Septiembre de 2018, de https://ojsrevistaing.uniandes.edu.co/ojs/index.php/revista/article/download/437/640

Castellanos, L. (2014). *Seguridad en informática.* Madrid: EAE.

Chicano, E. (2014). *Auditoría de seguridad informática. IFCT0109.* Málaga: IC Editorial.

Dussan, C. (2006). Políticas de seguridad informática. *Entramado, 2*(1), 86-92. Recuperado el 10 de Septiembre de 2018, de http://www.redalyc.org/articulo.oa?id=265420388008

Eikebrokk, T. R., & Iden, J. (2012). ITIL implementation: The role of ITIL software and project quality. In Database and Expert Systems Applications (DEXA). *23rd International Workshop on* (págs. 60-64). IEEE. Recuperado el 16 de Octubre de 2018, de http://www.academia.edu/download/40429456/ITIL_implementation_The_Role_of_ITIL_sof20151127-10804-1prjbxp.pdf

El Emam, K. (1998). The internal consistency of the ISO/IEC 15504 software process capability scale. *Software Metrics Symposium, 1*, 72-81. Recuperado el 5 de Septiembre de 2018, de http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.198.1740&rep=rep1&type=pdf

El Emam, K., & Birk, A. (2000). Validating the ISO/IEC 15504 measure of software requirements analysis process capability. *IEEE transactions on Software Engineering, 26*(6), 541-566. Recuperado el 1 de Septiembre de 2018, de http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.38.5994&rep=rep1&type=pdf

El Emam, K., & Jung, H. W. (2001). An empirical evaluation of the ISO/IEC 15504 assessment model. . *Journal of Systems and Software, 59*(1), 23-41. Recuperado el 3 de Septiembre de 2018, de http://www.ehealthinformation.ca/wp-content/uploads/2014/07/2000-An-Empirical-Evaluation-of-the-ISO-IEC-15504.pdf

Emam, E., & Garro, I. (1999). *Estimating the EXtent of Standards Use: The Case of ISO/IEC 15504.* Recuperado el 1 de Septiembre de 2018, de https://pdfs.semanticscholar.org/038a/a4e122b502575f7a3c4af4473ca11347bcb8.pdf

Ferraiolo, K. (Octubre de 1998). *Tutorial: The Systems Security Engineering Capability Maturity Model*. (Arca Systems Inc.) Obtenido de https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/tutorb5.pdf

García, A. (2011). *Auditoria de seguridad informática (MF0487_3).* Madrid: Starbook.

García, M., Irrazabal, I., & Garzás, J. (2010). *Implantación de las normas ISO/IEC 15504 e ISO/IEC 12207 con métodos ágiles y Scrum.* Recuperado el 4 de Agosto de 2018, de http://www.kybeleconsulting.com/wp-content/uploads/2011/11/Implantacion-ISO-15504-con-SCRUM.pdf

Garzás, J., Fernández, C., & Piattini, M. (2009). Una aplicación de la norma ISO/IEC 15504 para la evaluación por niveles de madurez de Pymes y pequeños equipos de desarrollo. *Revista Española de Innovación, Calidad e Ingeniería del Software, 5*(2), 88-98. Recuperado el 3 de Agosto de 2018, de https://www.researchgate.net/publication/237042179/download

Jung, H. W., & Hunter, R. (2001). The relationship between ISO/IEC 15504 process capability levels, ISO 9001 certification and organization size: an

empirical study. *Journal of Systems and Software, 59*(1), 43-55. Recuperado el 4 de Septiembre de 2018, de https://www.sciencedirect.com/science/article/pii/S0164121201000474

Jung, H., Kim, S., & Chung, C. (2004). Measuring software product quality: A survey of ISO/IEC 9126. *IEEE software, 5*, 88-92. Recuperado el 20 de Octubre de 2018, de http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.455.533&rep=rep1&type=pdf

Lincke, R., Lundberg, J., & Löwe, W. (2008). Comparing software metrics tools. *Proceedings of the 2008 international symposium on Software testing and analysis* (págs. 131-142). ACM. Recuperado el 22 de Octubre de 2018, de http://www.cs.umd.edu/~pugh/ISSTA08/issta2008/p131.pdf

Mas, A., & Amengual, E. (2005). La mejora de los procesos de software en las pequeñas y medianas empresas (pyme). Un nuevo modelo y su aplicación a un caso real. *Revista Española de Innovación, Calidad e Ingeniería del Software, 1*(2). Recuperado el 13 de Septiembre de 2018, de http://www.redalyc.org/html/922/92210203/

Naranjo, M. (2013). *Análisis de metodologías de auditoria informática para la aplicación en entidades financieras. Caso práctico: auditoria informática en la cooperativa de ahorro y crédito "educadores de Chimborazo" de la ciudad de Riobamba.* Recuperado el 30 de Septiembre de 2018, de Universidad Nacional de Chimborazo: http://dspace.unach.edu.ec/bitstream/51000/677/1/UNACH-EC-IET-2013-0008.pdf

Paulk, M. (1999). *Analyzing the conceptual relationship between ISO/IEC 15504 (Software Process Assessment) and the capability maturity model for software.* Recuperado el 4 de Septiembre de 2018, de International Conference on Software Quality.: https://pdfs.semanticscholar.org/a6b6/be334179f60be5d28d565efd36b455618e6f.pdf

Pino, F. J., García, F., Serrano, M., & Piattini, M. (2006). Medidas para estimar el rendimiento y capacidad de los procesos software de conformidad con el estándar ISO/IEC 15504-5: 2006. REICIS. . *Revista Española de Innovación, Calidad e Ingeniería del Software, 2*(3).

Pino, F., García , F., Ruiz, F., & Piattini, M. (2015). *Adaptación de las normas ISO/IEC 12207:2002 e ISO/IEC 15504:2003 para la evaluación de la madurez de procesos software en países en desarrollo.* Recuperado el 5 de Agosto de 2018, de https://pdfs.semanticscholar.org/4b97/499853bf9e6e275b2e5d5da91c99337c73f1.pdf

Rosado, D., Blanco, C., Sánchez, L., Fernández, E., & Piattinni, M. (2010). La Seguridad como una asignatura indispensable para un Ingeniero del Software. *XVI Jornadas de Enseñanza Universitaria de la Informática*, (págs. 205-2012). Recuperado el 15 de Octubre de 2018, de https://upcommons.upc.edu/bitstream/handle/2099/11778/a25.pdf

Rout, T. P. (2003). ISO/IEC 15504—Evolution to an international standard. . *Software Process: Improvement and Practice , 8*(1), 27-40. Recuperado el 6 de Septiembre de 2018, de http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.875.9325&rep=rep1&type=pdf

Simbaya, C. (2014). *Auditoría Informática y su incidencia en la funcionalidad del Sistema de Información Financiera de la Cooperativa de Ahorro y Crédito*

Universitaria Limitada (COPEU). Recuperado el 1 de Octubre de 2018, de Universidad Técnica de Ambato.: http://repositorio.uta.edu.ec/bitstream/123456789/8102/1/Tesis_t920si.pdf

Solarte, F., Rosero, E., & del Carmen, M. (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, 28*(5), 492-507. Recuperado el 11 de Septiembre de 2018, de http://www.rte.espol.edu.ec/index.php/tecnologica/article/download/456/321

Talavera, V. (Mayo de 2015). *Diseño de un sistema de gestión de seguridad de la iformación para una entidad estatal de salud de acuerdo a la ISO/IEC 27001:2013.* Recuperado el 16 de Octubre de 2018, de http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/6092/TALAVERA_VASCO_DISE%C3%91O_SISTEMA_GESTION.pdf?sequence=1

Tamayo, A. (2001). *Auditoría de sistemas: Una visión práctica.* Recuperado el 17 de Septiembre de 2018, de http://bdigital.unal.edu.co/58517/11/9589322662.pdf

Tovar, E., Carrillo, J., Vega, V., & Gasca, G. (2010). DESARROLLO DE PRODUCTOS DE SOFTWARE SEGUROS EN SINTONÍA CON LOS MODELOS SSE-CMM, COBIT E ITIL. . *Revista de Procesos y Métricas de las tecnologías de la información, 3*(2), 62-72. Recuperado el 17 de Octubre de 2018, de 2006: https://www.researchgate.net/profile/Vianca_Vega/publication/309566968_Desarrollo_de_productos_de_software_seguros_en_sintonia_con_los_modelos_SSE-CMM_COBIT_E_ITIL/links/593f0eb5a6fdcc1b10a21b6f/Desarrollo-de-productos-de-software-seguros-en-sintonia-con-

van Bon, J. (2008). *Fundamentos de Gestión de Servicios TI basado en ITIL.* Van Haren Publishing. Recuperado el 19 de Octubre de 2018, de http://cdn.roelants.nl/7/B/F/C/9789087537159/pdf/9789087537159_h1.pdf

Von Solms, B. (2005). Information Security governance: COBIT or ISO 17799 or both? *Computers & Security, 24*(2), 99-104. Recuperado el 18 de Octubre de 2018, de http://t3mppu.kapsi.fi/tekisit_itse/Week%204-%20Information%20Security%20governance%20COBIT%20or%20ISO%2017799%20or%20both.pdf

Voutssas, J. (2010). Preservación documental digital y seguridad informática. *Investig. Bibl., 24*(50). Recuperado el 15 de Septiembre de 2018, de http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S0187-358X2010000100008

Zeiss, B., Vega, D., Schieferdecker, I., Neukirchen, H., & Grabowski, J. (2007). Applying the iso 9126 quality model to test specifications. *Software Engineering, 15*(6), 231-242. Recuperado el 24 de Octubre de 2018, de http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.406.6843&rep=rep1&type=pdf