DEPARTAMENTO DE ELECTRÍCA Y ELECTRÓNICA

CARRERA DE INGENIERÍA ELECTRÓNICA EN REDES Y COMUNICACIÓN DE DATOS

TRABAJO DE TITULACIÓN, PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO ELECTRÓNICO EN REDES Y COMUNICACIÓN DE DATOS

TEMA: VALIDACIÓN DE SEGURIDADES PARA APLICACIONES MÓVILES ORIENTADAS A COMPRA DE LÍNEA

AUTOR: ALVAREZ MENDOZA, BYRON RENE

DIRECTOR: ING. MONTOYA LARA LUIS HERNAN

SANGOLQUÍ, AGOSTO 2018

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA ELECTRÓNICA EN REDES Y COMUNICACIÓN DE DATOS

CERTIFICACIÓN

Certifico que el trabajo de titulación, ***"VALIDACIÓN DE SEGURIDADES PARA APLICACIONES MÓVILES ORIENTADAS A COMPRA DE LÍNEA"*** fue realizado por el señor ***ALVAREZ MENDOZA BYRON RENE*** el mismo que ha sido revisado en su totalidad, analizado por la herramienta de verificación de similitud de contenido; por lo tanto cumple con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, razón por la cual me permito acreditar y autorizar para que lo sustente públicamente.

Sangolquí, 28 de Agosto

Firma:

.....

Montoya Lara Luis Hernán

C.C 1715480412

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA ELECTRÓNICA EN REDES Y COMUNICACIÓN DE DATOS

AUTORÍA DE RESPONSABILIDAD

Yo, ***ALVAREZ MENDOZA, BYRON RENE***, declaro que el contenido, ideas y criterios del trabajo de titulación: ***"VALIDACIÓN DE SEGURIDADES PARA APLICACIONES MÓVILES ORIENTADAS A COMPRA DE LÍNEA"*** es de mi autoría y responsabilidad, cumpliendo con los requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de Fuerzas Armadas ESPE, respetando los derechos intelectuales de terceros y referenciando las citas bibliográficas.

Consecuentemente el contenido de la investigación mencionada es veraz.

Sangolquí, 28 de Agosto

Firma:

.....

ALVAREZ MENDOZA BYRON RENE

C. C 1719950915

DEPARTAMENTO DE ELÉCTRICA Y ELECTRÓNICA

CARRERA DE INGENIERÍA ELECTRÓNICA EN REDES Y COMUNICACIÓN DE DATOS

AUTORIZACIÓN

Yo, ***ALVAREZ MENDOZA, BYRON RENE***, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar el trabajo de titulación: Título:" ***VALIDACIÓN DE SEGURIDADES PARA APLICACIONES MÓVILES ORIENTADAS A COMPRA DE LÍNEA***" en el Repositorio Institucional, cuyo contenido, ideas y criterios son de mi responsabilidad.

Sangolquí, 28 de Agosto

Firma:

.....

ALVAREZ MENDOZA BYRON RENE

C. C 1719950915

DEDICATORIA

Dedico el presente trabajo de titulación, a Dios. A mis padres Cesar, Liduvina por su apoyo incondicional y paciencia desde el momento de mi nacimiento hasta la fecha actual de realización del proyecto. A mi hermano Iván, por ser mi ejemplo a seguir. Dedico a mis sobrinos Nathalie y Felipe, por su cariño y afecto hacia mí.

BYRON RENE ALVAREZ MENDOZA

AGRADECIMIENTO

Agradecimiento sincero al Ingeniero Luis Montoya, tutor del proyecto de titulación, por su guías y recomendaciones al desarrollo del proyecto.

Al Dr. Nicolay Espinoza, Director de la Carrera, por la agilización de los tramites de titulación.

Finalmente agradezco a los familiares y amigos que estuvieron pendientes de la culminación del proyecto.

BYRON RENE ALVAREZ MENDOZA

INDICE CONTENIDOS:

CERTIFICACIÓN i
AUTORÍA DE RESPONSABILIDAD ii
AUTORIZACIÓN iii
DEDICATORIA iv
AGRADECIMIENTO v
INDICE CONTENIDOS: vi
INDICE DE TABLAS: x
INDICE DE FIGURAS xi
RESUMEN xii
ABSTRACT xiii
CAPITULO I 1
INTRODUCCIÓN: 1
1.1 Antecedentes: 1
1.2 Justificación e Importancia: 2
1.3 Alcance del Proyecto: 3
1.4 Objetivos: 3
1.4.1 General: 3
1.4.2 Específicos: 4
CAPITULO II: 5
MARCO TEÓRICO 5
2.1 Definición Seguridad de Información. 5
2.2 Normas ISO 27000: 6
2.2.1 Origen: 6
2.2.2 Definición Norma ISO 27000: 10
2.3 Introducción Estándar ISO /IEC 27034: 11
2.3.1 Generalidades: 12
2.3.2 Propósito: 12
2.3.3 Público Objetivo: 14

2.3.4 Principios: 17
2.3.5 Relación con otras Normas Internacionales: 18
2.4 ISO/IEC 27034 Seguridad de Aplicación- Parte 1: Descripción y Conceptos 20
2.4.1 Objeto y Campo de Aplicación: 20
2.4.2 Referencias Normativas: 21
2.4.3 Términos, Definiciones y Abreviaciones: 21
2.4.4 Estructura de ISO /IEC 27034 25
2.5 Introducción a la Seguridad de la aplicación 26
2.5.1 Generalidades del campo de aplicación de seguridad de la aplicación: 27
2.5.2 Contexto de Negocio: 29
2.5.3 Contexto Regulatorio: 29
2.5.4 Proceso del ciclo de vida de la aplicación: 29
2.5.5 Procesos involucrados con la aplicación: 29
2.5.6 Contexto tecnológico: 30
2.5.7 Especificaciones de la aplicación: 30
2.5.8 Datos de Aplicaciones: 30
2.5.9 Datos de la organización y del usuario: 30
2.5.10 Roles y Permisos: 31
2.6 Requisitos para la seguridad de Aplicación: 31
2.6.1 Requisitos de seguridad para aplicación: 31
2.6.2 Requisitos de seguridad de la aplicación en Ingeniería: 31
2.6.3 Organización de SGSI: 32
2.7 Riesgo: 32
2.7.1 Riesgo de seguridad en la aplicación: 32
2.7.2 Vulnerabilidades de una aplicación: 32
2.7.3 Amenazas en las aplicaciones: 33
2.7.4 Gestión de Riesgo; 33
2.7.5 Costos: 34
2.7.6 Entorno Objetivo: 34
2.8 Proceso en general de ISO/IEC 27034: 35
2.8.1 Componentes, procesos y marco de trabajo 35

2.8.2 Procesos de Gestión MRNO: 35
2.8.3 Proceso de Gestión de Seguridad de la Aplicación (PGSA) 36
2.9 Marco de Referencia Normativo de la Organización. 37
2.9.1 Contexto de Negocio: 38
2.9.2 Contexto Regulatorio: 38
2.9.3 Especificaciones de la aplicación: 38
2.9.4 Contexto Tecnológico: 39
2.9.5 Roles, Responsabilidades y Calificaciones: 39
2.9.6 Control de Seguridad de Aplicación (CSA) 40
2.9.7 Modelo de Referencia del Ciclo de Vida de Seguridad de la Aplicación 43
2.9.8 Procesos relacionados con el Marco de Referencia Normativo de la Organización: 48
2.10 Evaluación de riesgo de seguridad de la aplicación: 51
2.10.1 Análisis de riesgo de la aplicación: 51
2.10.2 Evaluación de Riesgo: 52
2.10.3 Nivel de confianza objetivo de la aplicación: 52
2.10.4 Aceptación del propietario de la aplicación: 52
2.11 Marco de Referencia Normativo de la Aplicación (MRNA): 53
2.11.1 Componentes: 53
2.11.2 Ciclo de vida de la aplicación: 55
2.11.3 Procesos: 55
2.12 Aprovisionamiento y funcionamiento de la aplicación: 56
2.12.1 Impacto de ISO/IEC 27034 en un proyecto de aplicación: 56
2.12.2 Componentes de Aprovisionamiento: 57
2.12.3 Procesos: 58
2.13 AUDITORIA: 59
2.13.1 Componente de Auditoria: 60
CAPÍTULO 3 61
3 GUÍA DE VERIFICACIÓN DE CUMPLIMIENTO DEL ESTÁNDAR ISO/IEC 27034 61
3.1 Levantamiento de la información: 61
3.2 Método de transacción financieras por medio digitales: 62
3.3 Funcionamiento del aplicativo: 66

3.4 Propuesta. 68
Procedimiento 68
3.4.1 Diseño del MRNO: 68
CAPÍTULO 4 95
CONCLUSIONES Y RECOMENDACIONES 95
3.5 Conclusiones: 95
3.6 Recomendaciones: 97
BIBLIOGRAFÍA 99

INDICE DE TABLAS:

Tabla 1. Estándar Serie 27000.....7
Tabla 2. Relación ISO/IEC 27034 con Otras Normas Internacionales 18
Tabla 3. Descripción de partes de la norma ISO/IEC 27000 21
Tabla 4. Estructura ISO/IEC 27034 25
Tabla 5. Campos que deben ser protegidos en una aplicación. 28
Tabla 6. Mapeo de subprocesos de SGSI y de gestión de MRNO.....49
Tabla 7. Librería de Control de Seguridades de Aplicación. 86
Tabla 8. Consideraciones de Arquitectura y Diseño para desarrollo de aplicaciones móviles 87
Tabla 9. Consideraciones para el almacenamiento de datos y privacidad 87
Tabla 10. Consideraciones de Criptografía para Aplicaciones Móviles 90
Tabla 11. Consideraciones para Autenticación y Manejo de Sesiones 91
Tabla 12. Consideraciones de comunicación a través de la red para Aplicaciones Móviles 91
Tabla 13. Consideraciones para protección y manejo de tarjetas de crédito.....92
Tabla 14. Consideraciones de calidad de código, configuración de compilador 93
Tabla 15. Consideraciones de Control de Acceso para el diseño de aplicaciones Móviles.....93
Tabla 16. Manipulación de datos de entrada para aplicaciones móviles.....94
Tabla 17. Consideraciones de Requisitos de verificación Móvil para aplicaciones móviles.....94
Tabla 18. Consideraciones de verificación de Servicio Web.....94

INDICE DE FIGURAS

Figura 1. Procesamiento de datos.....5
Figura 2. Origen del Estandar ISO/IEC 27034 6
Figura 3. Relación Estándares Serie ISO 27000 18
Figura 4. Campo de Aplicación de seguridad de la aplicación. 28
Figura 5. Proceso de Gestión de la organización. 35
Figura 6. Marco de Referencia Normativo de la Organización(Simplificado) 37
Figura 7. Componente de un CSA. 42
Figura 8. Modelo de Referencia del Ciclo de vida de seguridad de la Aplicación 44
Figura 9. Proceso de Gestión de MRNO.....48
Figura 10. Marco de Referencia Normativo de la Aplicación 53
Figura 11. Impacto de ISO/IEC 27034 en un proyecto típico de la aplicación 57
Figura 12. El CSA utilizado como una actividad de seguridad 58
Figura 13 .EL CSA utilizado como una medición 59
Figura 14. Vista General del proceso de verificación de seguridad. 60
Figura 15. Estadística de activación de cuentas del dinero Electrónico 63
Figura 16. Funcionamiento de la Pasarela de Pagos 65
Figura 17. Ingreso y selección de producto en una aplicación móvil**.** 67
Figura 18. Autenticación para proceder al pago de producto 67
Figura 19. Ingreso de datos de tarjeta de crédito 68
Figura 20. Diagrama de bloques del Modelo de seguridad de la aplicación.....73
Figura 21 Propuesta de Control de Seguridad de la Aplicación para aplicaciones móviles. 85

RESUMEN

En los últimos años las organizaciones empezaron con la implementación de aplicaciones móviles con el objetivo de facilitar sus procesos comerciales realizando acciones como: compartición en tiempo real, movilidad, entre otras. A pesar de que ellas tengan tantos beneficios, el uso del mismo puede acarrear varios problemas de seguridad, ya que al igual que aplicaciones tradicionales pueden contener vulnerabilidades susceptibles ataques, que probablemente sean objeto de ataque, lo que acarrea fuga de información sensible de usuario. Para ayudar a minimizar estas falencias, las organizaciones deben desarrollar un plan de requisitos de seguridad especificando las posibles vulnerabilidades y/o fallos dependiendo del entorno de negocio a la cual está sujeta la aplicación. El presente trabajo propone un modelo de seguridad para aplicaciones móviles el cual ayuda a garantizar que una aplicación cumpla los requisitos para tener un proceso de evaluación correcto. El cual consiste en una serie de actividades que tienen como objetivo final determinar si una aplicación cumple con los requisitos de seguridad impuestos por una organización. Un auditor se encarga de la actividad de evaluación de la aplicación, la misma que consiste en probar las vulnerabilidades por servicios y así derivar un informe del mismo. La mencionada actividad implica la emisión de informes y evaluación de riesgos para determinar la aplicación de los requisitos de seguridad de la organización.

PALABRAS CLAVE:

- **REQUISITOS DE SEGURIDAD**
- **EVALUACIÓN DE SEGURIDAD**
- **EVALUACIÓN DE RIESGOS**

ABSTRACT

In the recent year´s organizations began with the implementation of mobile applications with the aim of facilitating their business processes by performing actions such as: real time sharing, mobility, among others. Although they have many benefits, the use of the same can lead to several security problems, because as traditional applications may contain vulnerabilities susceptible attacks, which are likely to be attacked, which leads to leakage of sensitive user information. To help minimize these shortcomings, organizations must develop a security requirements plan specifying potential vulnerabilities and / or failures depending on the business environment to which the application is subject. The present work proposes a security model for mobile applications which helps to guarantee that an application meets the requirements to have a correct evaluation process. Which consists of a series of activities whose ultimate goal is to determine if an application meets the security requirements imposed by an organization. An auditor is responsible for the evaluation activity of the application, which consists of testing the vulnerabilities for services and thus derive a report of the same. The aforementioned activity involves the issuance of reports and risk assessment to determine the application of the security requirements of the organization.

KEYWORDS:

- **SECURITY REQUIREMENTS**
- **SECURITY EVALUATION**
- **RISKS EVALUATION**

CAPITULO I

INTRODUCCIÓN:

1.1 Antecedentes:

Con el aparecimiento del internet en el siglo XX y el exponencial crecimiento de la tecnología de información han permitido el desarrollo de dispositivos innovadores como los celulares inteligentes (Smartphone) (Aranaz Tudela, 2009), los mismos que se han convertido en uno de los inventos tecnológicos más utilizados e importante en nuestra sociedad. Debido a que permite comunicar, el compartir información en tiempo real entre usuarios finales, tanto a nivel laboral además del personal.

Sin duda el desarrollo de la tecnología en los teléfonos celulares, permitió el aumento de características de los dispositivos electrónicos tales como memorias, procesador, sistema operativo, etc. Llegando a tener características similares a una computadora portátil. El sistema Operativo más utilizado para dispositivos móviles es Android, el mismo que es basado en software libre, por tanto, no tiene costo alguno. Es por ello que los programadores tienden a crear o desarrollar aplicaciones para empresas y/o personas independientes.

Con el fin de precautelar la información de los usuarios, La organización Internacional de Estandarización (ISO) publicó ISO/IEC 27034, que consiste en técnicas de seguridad de administración de información para aplicaciones con el fin de proteger la información que se maneja y llegar a tener el nivel deseado o adecuado de funcionamiento de las mismas. (iso27000).

1.2 Justificación e Importancia:

Al lanzar una aplicación al mercado, una organización debe considerar el impacto que generaría hacia su información, usuarios, recursos TI. Los desarrolladores deben estar conscientes de los riesgos y sus consecuentes vulnerabilidades que implicaría dicha acción. Para ayudar a minimizar los riesgos, las organizaciones deben emplear procesos de garantía de aplicación, es decir que el nivel de confianza de la aplicación, que se ofrece al usuario este en su posible sin vulnerabilidades. Esto en la práctica no se cumple, debido a que con el crecimiento exponencial de la tecnología genera que también que crezcan el número de vulnerabilidades.

Al utilizar aplicaciones para dispositivo móviles basados en Android, nos exponemos a la baja seguridad que poseen las mismas (Tutorialspoint, 2017) (Gomez, 2014). Además, la forma de transmisión de datos que utiliza es la inalámbrica, esto genera que exista mucha inseguridad al momento de intercambiar información importante o delicada como los usuarios y claves de cuentas bancarias, correos, etc. Por eso la encriptación de datos juega un papel importante en este tipo de transacciones.

Por lo tanto, se ve la necesidad de ejecutar un modelo de seguridades para aplicaciones móviles. Con el fin de proporcionar confiabilidad con los usuarios para el uso de la misma. Basados en la norma ISO/IEC 27034, en la cual indica definiciones, técnicas, validaciones, control de seguridad para aplicaciones.

1.3 Alcance del Proyecto:

Se realizará un estudio acerca de las formas de transacciones electrónicas seguras. Además de un análisis sobre los métodos y técnicas de encriptación de datos más utilizados para aplicaciones móviles orientadas a transacciones en línea.

Se propondrá un modelo de seguridad para aplicaciones móviles orientadas a compras en línea, el cual consiste en tener un formato de verificación de cumplimiento de una serie de guías y/o técnicas dados por el estándar ISO/IEC 27034. Como escenario de pruebas se utilizará una aplicación móvil dedicada a la compra en línea.

Si en la mencionada evaluación que se efectuará en la aplicación, existieran puntos faltantes y/o vulnerables con respecto al comercio en línea, se propondrá soluciones en la misma, basados en el estándar de seguridades ISO/IEC 27034.

Se realizará un análisis sobre los métodos y técnicas de encriptación de datos más utilizados para aplicaciones móviles y se empleará el más óptimo que cumpla las necesidades de la aplicación orientadas a transacciones en línea.

1.4 Objetivos:

1.4.1 General:

Aplicar una evaluación técnica de seguridades utilizando el estándar ISO/IEC 27034, para la validación de seguridad en aplicaciones móviles orientadas a compras en línea.

1.4.2 **Específicos:**

- Analizar el estándar ISO/ IEC 27034 de seguridades de aplicaciones.
- Realizar un estudio y evaluación de funcionamiento de una aplicación orientadas a de compra de en línea, bajo estándar ISO /IEC 27034.
- Analizar el método más óptimo de pago en línea en base al estándar ISO/IEC 27034.
- Analizar las técnicas de encriptación más utilizadas para aplicaciones móviles y determinar la más óptima para utilizarse en la aplicación de compras en línea.

CAPITULO II:

MARCO TEÓRICO

2.1 Definición Seguridad de Información.

La información de una empresa reflejada en un aplicativo o base de datos, es el activo más valioso e importante, considerado como invalorable. El cual siempre es el objetivo de personas malintencionadas que tratan de obtenerla de forma interna o externa a la organización.

El aseguramiento de la información y los procesos que intervienen, es lo primordial para la organización. Por lo tanto, para el acceso o manejo de información, se ha establecido un conjunto de estándares que ayuda a evitar peligros o daños de la información con ayuda de políticas de seguridades que reducirá posibles puntos vulnerables.

Entonces se puede definir a la seguridad de la información como el fin de protección de la información con medidas preventivas para evitar la divulgación, destrucción no autorizada de la misma. (iso27000)

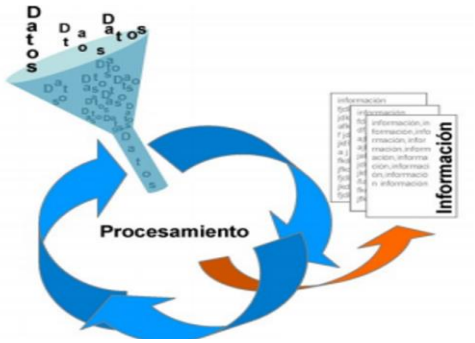


Figura 1. Procesamiento de datos
Fuente: www.iso27000.es

2.2 **Normas ISO 27000:**

2.2.1 **Origen:**

El instituto Británico de Estandarización (BSI), publico en 1995 la norma BS7999 con el objetivo de proporcionar a las empresas británicas, un conjunto de recomendaciones para la gestión de seguridad de la información. La primera parte de esta norma fue BS 7999-1, que fue enfocada a códigos de buenas prácticas de seguridad, la cual no establecía certificación alguna. La segunda parte fue BS 7999-2, la cual fue desarrollada en 1998 y planteo requisitos de los SGSI para poder tener una certificación. Ambas partes fueron revisadas por ISO y la primera fue adoptada como ISO 17799. (Morales, 2015). La segunda parte se adoptó como estándar ISO en el 2005.

Finalmente, en el año 2007, fue revisada, actualizada y publicada como ISO 27001. Periódicamente cada año existe las respectivas actualizaciones y se siguen desarrollando estándares de la serie 27000, teniendo en cuenta que las empresas u organizaciones se pueden certificar con el estándar ISO/IEC 27001. (Ramirez Jaramillo & Moreira Zambrano, 2017)

Figura 2. Origen del Estandar ISO/IEC 27034
Fuente: www.iso27000.es

Los estándares de la serie 27000, son los siguientes:

Tabla 1.
Estándar Serie 27000

Estándar	Fecha Publicación	Descripción (Guía)
ISO /IEC 27001	15 de Octubre 2005	• Norma Principal de la Serie. • Contiene requisitos de un SGSI.
ISO /IEC 27002	1 de Julio del 2007	• Buenas prácticas que describe objetivos de control para la seguridad de información.
ISO /IEC 27003	1 de Febrero del 2010	• Aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI.
ISO /IEC 27004	15 de Diciembre del 2009	• Desarrollo de utilización de métricas y técnicas de medida aplicadas a la eficiencia de un SGSI.
ISO /IEC 27005	1 de Junio del 2011	• Proporciona Directrices para la gestión de los riesgos en la seguridad de la información.
ISO /IEC 27006	1 de Diciembre del 2011	• Especifica requisitos para la acreditación de entidades de auditoria y certificación de sistemas de gestión de seguridad de la información.
ISO /IEC 27007	14 de Noviembre del 2011	• Auditoria de un SGSI.
ISO /IEC 27008	15 de Octubre del 2011	• Auditoria de los controles seleccionados en la implantación de SGSI.
ISO /IEC 27009	En desarrollo	• Uso y aplicación de los principios de ISO /IEC 27001, para el sector de servicios.
ISO /IEC 27010	20 de Octubre del 2012	• Gestión de la seguridad de información cuando se comparte entre organizaciones o sectores.
ISO /IEC 27011	15 de Diciembre del 2008	• Implementación y gestión de seguridad de información en organizaciones de telecomunicaciones.

CONTINÚA

ISO /IEC 27013	**24 de Noviembre 2015**	• **Implementación integrada a ISO /IEC 27001 y de ISO/IEC 20000 (Gestión de Servicios TI)**
ISO /IEC 27014	23 de Abril del 2013	• Gobierno corporativo de la seguridad de información.
ISO /IEC 27015	23 de Noviembre del 2012	• SGSI orientada a organizaciones financieras y aseguradoras.
ISO /IEC 27016	20 de Febrero del 2014	• Valoración de los aspectos financieros de la seguridad de la información.
ISO /IEC 27017	15 de Diciembre del 2015	• Seguridad para Cloud Computing.
ISO /IEC 27018	29 de Julio del 2014	• Código de buenas prácticas en controles de protección de datos para Cloud Computing.
ISO /IEC 27019	17 de Julio del 2015	• Referencia para el proceso de sistemas de control relacionados con el sector energético.
ISO /IEC 27023	2 de Julio del 2015	• Correspondencias a transiciones de versiones entre ISO/IEC 27001 y 27002.
ISO /IEC 27031	1 de Marzo del 2011	• Apoyo para la adecuación de las Tecnologías de Información y Comunicación de la organización para la continuación de negocio.
ISO /IEC 27032	16 de Julio del 2012	• Proporciona orientación para la mejora del estado de seguridad cibernética, cubriendo aspectos básicos para los interesados en el ciberespacio
ISO /IEC 27033	15 de Diciembre 2009	• Norma dedicada a la seguridad en Redes.
ISO /IEC 27034	Parcialmente desarrollada	• Norma dedicada a la seguridad en aplicaciones informáticas
ISO /IEC 27035	17 de Agosto del 2011	• Gestión de incidentes de seguridad de la información.
ISO /IEC 27036	8 de Noviembre del 2013	• Seguridad en relaciones con proveedores.

CONTINÚA 

ISO /IEC 27037	15 de Octubre del 2012	• Proporciona directrices para las actividades relacionadas con la identificación, recopilación, consolidación y preservación de evidencias digitales.
ISO /IEC 27038	13 de Marzo del 2014	• Especificaciones para seguridad en la redacción digital
ISO /IEC 27039	11 de Febrero del 2015	• Selección, despliegue y operativa de IDS/IPS. Continua
ISO /IEC 27040	05 de Enero del 2015	• Seguridad en medios de almacenamiento.
ISO /IEC 27041	19 de Junio del 2015	• Garantizar la idoneidad y adecuación de métodos de investigación.
ISO /IEC 27042	19 de Junio del 2015	• Directrices para el análisis e interpretación de evidencias digitales.
ISO /IEC 27043	04 de Marzo del 2015	• Desarrolla principios y procesos de investigación para la recopilación de evidencias digitales.
ISO /IEC 27044	En desarrollo	• Gestión de eventos y de la seguridad de información
ISO /IEC 27799	12 de Junio del 2008	• Proporciona directrices para apoyar la interpretación y aplicación en el sector sanitario.

Vocabulario:

TI: Tecnologías de Información y Comunicación

ISO: International Organization for Standarization

IEC: International Electrotechnical Commission.

IDS/IPS: Sistema de detección y prevención de intrusión.

SGSI: Sistema de Gestión de Sistemas de Información

2.2.2 **Definición Norma ISO 27000:**

Conjunto de estándares desarrollado por ISO (International Standarization Organization) y por IEC (International Electrotechnical Commisssion), la cual establece un marco de gestión de la seguridad de la información utilizable para empresas u organizaciones, con el fin de establecer practicas recomendadas para reforzar los posibles puntos vulnerables.

Estos estándares de la serie ISO 27000 tiene como resultado llegar a que una organización pueda implantar un sistema de gestión de seguridad de la información.

Sistema De Gestión De Seguridad De La Información (SGIS):

Como su nombre lo dice consiste en una herramienta para dirigir y controlar la seguridad de la información preservando aspectos relevantes que permitan garantizar la confidencialidad, integridad y disponibilidad.

Para garantizar que la información se gestiona de manera correcta se hace uso de procesos sistemáticos y documentos desde un enfoque empresarial. A esto se denomina un SGIS. (Ramirez Jaramillo & Moreira Zambrano, 2017)

Para el presente proyecto, se va a enfocar en el estándar ISO /IEC 27034 de seguridades para aplicaciones de organizaciones. Para lo cual se va a detallar en que consiste el mencionado estándar.

2.3 Introducción Estándar ISO /IEC 27034:

ISO/IEC 27034, es un estándar desarrollado por sistema especializado de norma mundial conformado por ISO (International Standarization Organization) y por IEC (International Electrotechnical Commisssion). La misma que establece una guía sobre seguridad de la información enfocados a aplicaciones, dirigidas a administradores TI, desarrolladores, auditores o usuarios finales de TIC.

En la mencionada guía proporciona orientación sobre diseño, programación, implementación de controles de seguridad de la información a través de un conjunto de procesos integrados y orientados, denominado SDLC (System Development Life Cycle). (iso27000)

SDLC: Conocido como el ciclo de vida del desarrollo del sistema, consiste esencialmente en una serie de actividades planeadas para el desarrollo de productos. Usado por las industrias de diseño para el desarrollo y evaluación de programas de alta calidad, con el fin de cumplir las expectativas de los clientes. (Tutorialspoint, 2017)

El estándar ISO /IEC 27034 no asume todos los modelos de desarrollo de SDLC, sino que los complementa con algunos estándares de la serie ISO 27000. Obteniendo un enfoque hibrido sin entrar en conflictos entre ellos. Con el objetivo final de cumplir los requisitos de seguridad de la información que se accede por las aplicaciones informáticas, proporcionando un nivel necesario y óptimo de la seguridad. Para lograr integrar un Sistema de Gestión de Seguridad de la información (SGSI) en una organización. (Karakeneva, 2014).

2.3.1 **Generalidades:**

Las organizaciones deben proteger su información y sus infraestructuras tecnológicas (TI) con el fin de permanecer en el negocio.

Actualmente las organizaciones se ven obligadas a proteger su información mediante sus aplicaciones, debido a que ellas manejan la evidencia informativa de los negocios de la organización. Las mismas se pueden adquirir a través de un desarrollo interno, contratación de terceros (producto comercial) o combinación de estos enfoques. Lo que se podría introducir nuevas implicaciones de seguridad, las mismas que se debería tener en cuenta para su gestionamiento.

A través de su ciclo de vida, una aplicación segura muestra características como ejecución y conformidad predecible. A más de cumplir requisitos desde el punto de vista de desarrollo, gestión, Infraestructura Tecnológica y auditoria.

Una aplicación segura toma en cuenta los requisitos de seguridad dependiendo del tipo de información, actores y especificaciones de la misma.

2.3.2 **Propósito:**

"El propósito del estándar ISO/IEC 27034 es de ayudar a las organizaciones a integrar la seguridad en forma clara y transparente durante el ciclo de vida de sus aplicaciones" (NTE INEN-ISO/IEC 27034-1, 2014).

Proporcionando:

- Conceptos, principios, marcos, componentes y procesos.
- Guía para establecer criterios de aceptación en las organizaciones que subcontratan el desarrollo, operación de las aplicaciones.

Mecanismos orientados a procesos para:

- Establecer requisitos de seguridad, evaluando los riesgos, asignando un nivel de confianza objetivo y seleccionando los controles de seguridad y medidas para las verificaciones correspondientes.
- Determinar, generar y coleccionar la evidencia necesaria para demostrar que las aplicaciones se pueden utilizar de forma segura bajo un entorno definido.
- Apoyando a los conceptos generales especificados en ISO /IEC 27001 y ayudando con la implementación satisfactoria de la seguridad de la información basado en un enfoque de gestión de riesgo.
- Marco de referencia que ayude a la implementación de los controles de seguridad.

El Estándar ISO/IEC 27034, se aplica:

- A la Aplicación y factores que contribuyen al impacto en su seguridad.
- A toda clase de organizaciones ya sean empresas comerciales, gubernamentales, o sin fines de lucro. Propensas a los riesgos asociados a las aplicaciones.

El Estándar ISO IEC/27034, no proporciona: normas para la seguridad física y de la red, controles o mediciones, especificaciones de código seguro para ningún lenguaje de programación.

El Estándar ISO IEC/27034, no es una norma: de desarrollo de aplicaciones, gestión de Proyectos de aplicación y Ciclo de vida de desarrollo de software.

Los procesos publicados por el estándar ISO /IEC 27034 no están destinados a ser implementados aisladamente, sino que deben ser integrados en el proceso existente en la organización. Para conseguir esto se debe realizar un seguimiento a sus propios procesos y marcos de referencias existentes para así reducir el impacto de la implementación del estándar en mención. (NTE INEN-ISO/IEC 27034-1, 2014).

2.3.3 **Público Objetivo:**

Generalidades:

Los aspectos a mejorar en las organizaciones son los siguientes:

a) **Gestión**: Conformada por personas involucrada en la gestión de la aplicación durante su ciclo de vida completo. Esta etapa aplicable del ciclo de vida incluye las etapas de aprovisionamiento y de producción, por ejemplo, gerentes de seguridad de aplicación, gerente de proyectos, administradores, propietarios del software, etc.

   Normalmente la gestión necesita:

- Equilibrar costos de la implementación y mantenimiento de la seguridad de la aplicación con los riesgos y el valor que representa para su organización.
- Revisar informes del auditor recomendando la aceptación o rechazo que ha alcanzado la aplicación, basado en el nivel de Confianza objetivo de la misma.
- Aseguramiento de reglamentos propios de la organización.

- Supervisión de la implementación de una aplicación segura.
- Autorizar el nivel de confianza Objetivo según el contexto de la organización.
- Determinar controles de seguridad y mediciones deberían implementar y probar con respecto a la verificación.
- Minimizar los costos de verificación de la aplicación
- Documentar las políticas y procedimientos de seguridad para la aplicación.
- Proporcionar capacitación, socialización y supervisión para los actores.
- Estar al tanto de todos los planes de seguridad relacionado con el sistema de la organización.

b) <u>Equipos de Aprovisionamiento y de operación:</u> Son el equipo del proyecto, quienes son personas involucradas en el diseño, desarrollo y mantenimiento de una aplicación a lo largo de su ciclo de vida completo, por ejemplo, arquitectos, analistas, programadores, administradores de sistema, administradores base de datos, administradores de red, técnicos.

Estos miembros necesitan:

- Entender que controles se deberían aplicar e implementar en cada etapa del ciclo de vida de la aplicación.
- Asegurar que los controles introducidos cumplan con los requisitos de las mediciones.
- Obtener acceso a las herramientas con el fin de agilizar el desarrollo de pruebas y documentación.
- Participar en la planificación y en las estrategias de adquisición
- Adquirientes: Personas involucradas en la adquisición de un producto o servicio. Los adquirientes necesitan:

- Preparar las solicitudes para las propuestas que incluyen los requisitos para los controles de seguridad
- Seleccionar proveedores que cumplan con los requisitos.
- Verificar la evidencia de los controles de seguridad aplicados por los servicios subcontratados.
- Evaluar productos mediante la verificación de los controles de seguridad de la aplicación implementados correctamente.

c) **Proveedores:** Personas involucradas en el abastecimiento del producto o servicio. Proveedores necesitan:

- Cumplir con los requisitos de seguridad de la aplicación
- Selecciona adecuados controles de seguridad de la aplicación con respecto a su impacto en el costo
- Proporcionar evidencia de que los controles de seguridad requeridos estén implementados en el producto y servicio propuesto.

d) **Auditores:** Son personas que necesitan:

- Entender el campo de la aplicación y procedimientos involucrados en las mediciones de verificación para los controles correspondientes para asegurar los resultados de la auditoria sean repetibles.
- Establecer una lista de mediciones de verificación para generar evidencias verificables de que una aplicación ha alcanzado el nivel de confianza objetivo requerido por la gestión.

e) **Usuarios:** Los usuarios requieren confiar en:

- La aplicación produzca resultados seguros de manera oportuna.

- En los controles y mediciones correspondientes a su verificación funcionen correctamente. (NTE INEN-ISO/IEC 27034-1, 2014)

2.3.4 **Principios:**

La seguridad como requisito

Los requisitos de seguridad se deberían ser definidos, analizados y manejados para cada etapa de un ciclo de vida de una aplicación. Además, se deberá establecer los requisitos relacionados con la seguridad para ajustarse a las limitaciones actuales. Los requisitos deberían ser claros, no ambiguos, consistentes, completo, rastreables y verificables. Estas mismas características se aplican a los requisitos de seguridad en este estándar ISO /IEC 27034 con el fin de que: El desarrollador debería descubrir todos los riesgos importantes de seguridad para la aplicación. (Cuenca Diaz)

El proceso de auditoría de la aplicación en él hace uso de evidencias verificables proporcionadas por los controles de seguridad de la aplicación. Por tanto, no se puede declarar segura a la misma a menos que el auditor este de acuerdo en que la aplicación cumpla con las mediciones correspondientes de verificación de los controles aplicables de seguridad de la aplicación y así alcanzar el nivel de confianza objetivo.

2.3.5 Relación con otras Normas Internacionales:

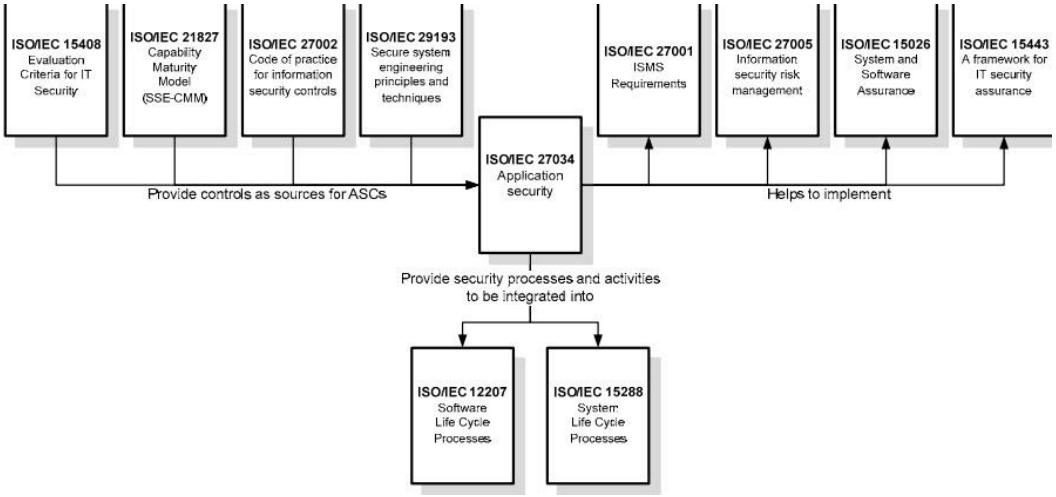


Figura 3. Relación Estándares Serie ISO 27000
Fuente: ISO/IEC27034

Como se mencionó anteriormente el estándar ISO /IEC 27034, es basado en algunos estándares y/o normas como se puede observar en la figura 3. En la siguiente tabla se describe brevemente qué relación existe entre ellos. (NTE INEN-ISO/IEC 27034-1, 2014)

Tabla 2.
Relación ISO/IEC 27034 con Otras Normas Internacionales

Norma	Nombre	Relación
ISO/IEC 27001	Sistemas de Gestión de seguridad de Información (SGSI)	ISO /IEC 27034 ayuda a implementar con un campo limitado en la seguridad las siguientes recomendaciones de ISO /IEC27001 • Enfoque sistemático para la gestión de seguridad. • Enfoque de proceso "Planificar, Hacer, Verificar, Actuar" • Implementación de seguridad de la información basada en la gestión de riesgo.

CONTINÚA

ISO/IEC 27002	Guía de buenas prácticas para SGSI	Ayuda con la implementación de Controles de Seguridad de la aplicación de ISO /IEC 27034 con recomendaciones de ISO /IEC 27002 como: • Gestión de Comunicaciones y Operaciones • Control de Acceso • Adquisición, Desarrollo y Mantenimiento de Sistema de Información.
ISO /IEC 27005	Gestión de Riesgo de seguridad de Información.	ISO /IEC 27034 ayuda con la implementación el proceso de gestión de riesgo de ISO /IEC 27005
ISO /IEC 21827	Ingeniería de Seguridad de Sistemas – Modelo de Madurez de Capacidad (SSE-CMM).	ISO /IEC 21827, proporciona prácticas de ingeniería de seguridad que una organización puede implementar como los niveles de capacidades para controles de seguridad de aplicación propuestos en ISO /IEC 27034.
ISO/IEC 15408-3	Criterios de evaluación para la seguridad TI- Parte 3: Componentes de garantía de seguridad.	ISO /IEC 15408-3, proporciona requisitos y elementos de acción que una organización puede implementar evaluar la seguridad de TI.
ISO/IEC 15443-1	Marco de Referencia para el aseguramiento de TI- Parte 1. Descripción y marco de referencia para el aseguramiento de TI. Parte 3: Análisis de los métodos de aseguramiento	ISO /IEC 27034 ayuda a cumplir y refleja los principios del aseguramiento de seguridad.

CONTINÚA

ISO/IEC 15026-2	Ingeniería de Sistemas y Software – Aseguramiento de sistemas y Software. Parte2: Caso de aseguramiento	El uso de los procesos de controles de seguridad de la aplicación de ISO /IEC 27034 en los proyectos de la aplicación proporciona directamente es de aseguramiento acerca de la seguridad de la aplicación, Las afirmaciones y justificaciones son proporcionadas por el proceso de análisis de riesgo de seguridad de la aplicación. Las evidencias se proporcionan por las mediciones de verificación de los controles de seguridad de aplicación.
ISO /IEC 15288	Ingeniería de Sistemas y Software – Procesos de ciclo de vida de sistemas e ISO /IEC 12207- Proceso de ciclo de vida de software	ISO /IEC 27034 proporciona los procesos para el control de seguridad de aplicación de una organización añadiendo procesos de ciclo de vida de ingeniería de sistemas y software.
ISO /IEC TR 29193 (Desarrollo)	Principios y técnicas de ingeniería de sistemas seguros	ISO /IEC TR 29193 proporciona una guía para ingeniera de sistemas seguros o productos TIC que una organización puede implementar.

2.4 ISO/IEC 27034 Seguridad de Aplicación- Parte 1: Descripción y Conceptos

2.4.1 Objeto y Campo de Aplicación:

- ISO/IEC 27034 proporciona una guía para ayudar a las organizaciones a integrar la seguridad en los procesos utilizado para gestionar sus aplicaciones.
- En esta primera parte se presenta una descripción de la seguridad de la aplicación, introduciendo definiciones, conceptos, principios y procesos involucrados en la seguridad

de la aplicación. Aplicable a las aplicaciones desarrolladas internamente, adquirida por tercera parte y cuando se desarrolla por subcontratación.

2.4.2 Referencias Normativas:

El estándar ISO/IEC 27034, esta descrito por algunas normas tanto parcial o totalmente. Las normas bases de la serie ISO /IEC 27000 son:

Tabla 3.
Descripción de partes de la norma ISO/IEC 27000

Norma	Descripción
ISO /IEC 27000	Técnicas de Seguridad- Sistemas de Gestión de seguridad de la información – Descripción y vocabulario
	Técnicas de Seguridad - Gestión de seguridad de la información – Requisitos.
	Técnicas de Seguridad – Código de prácticas para la gestión de seguridad de la información.
	Técnicas de Seguridad - Gestión en Riesgo de seguridad de la información.

2.4.3 Términos, Definiciones y Abreviaciones:

Actor: Persona que realiza una actividad durante el ciclo de vida de una aplicación, ya sea interactuando con cualquier proceso de una aplicación.

Nivel de Confianza Actual: Resultado de un proceso de auditoria proporcionando evidencia del soporte. Indicando todos los controles de seguridad de la aplicación requeridos por el nivel de confianza objetivo de la aplicación tanto los que fueron implementados y verificados, como los resultados esperados. (NTE INEN-ISO/IEC 27034-1, 2014)

Aplicación: Producto o solución de TI, que incluye el software de aplicación, datos y procedimientos de la aplicación para ayudar a los usuarios de una organización a realizar actividades o solución problemas TI mediante la automatización de un proceso o función de negocio.

Modelo de Referencia de Ciclo de Vida de seguridad de la Aplicación: Utilizado como referencia para la introducción de las actividades de seguridad en los procesos involucrados en la gestión de la aplicación, el aprovisamiento y la operación de la aplicación, gestión de infraestructura y la auditoria de la aplicación

Marco de Referencia Normativo de la Aplicación (MRNA): Conjunto de elementos normativos referente a un proyecto específico de la aplicación, seleccionado del Marco de referencia normativo de la organización.

Propietario de la Aplicación: Rol organizacional responsable de la gestión, utilización y protección de la aplicación y sus datos. Además, toma todas las decisiones relacionadas con la seguridad de la aplicación.

Proyecto de la Aplicación: Criterios definidos de inicio y de fin, ejecutado para adquirir una aplicación de acuerdo con los recursos y requisitos especificados. (ISO/IEC 12207:2008, 2008)

Control de Seguridad de la Aplicación (CSA): Estructura de datos que contiene la descripción precisa de una actividad de seguridad y sus mediciones asociadas de verificación para ser realizada en un punto específico en el ciclo de vida de una aplicación.

Proceso de Gestión de Seguridad de la Aplicación PGSA: Proceso general de gestión para las actividades de seguridad, actores, productos y la auditoria de seguridad para cada aplicación utilizada por una organización.

Software de Aplicación: "Software diseñado para ayudar a los usuarios a realizar tareas particulares". (ISO/IEC 24765, 2010)

Auditoria: Proceso sistemático y documentado para obtener la evidencia y evaluación objetiva con el fin de determinar el grado de cumplimiento de los criterios de medición. (ISO 9000, 2005)

Entorno: Contexto regulatorio, tecnológico y de negocio en el cual se utiliza una aplicación, incluyendo todos los procesos, información y actores involucrados en la aplicación.

Ciclo de Vida: Evolución de un sistema, producto. Servicio o proyecto desde la concepción hasta su retiro de la producción. (ISO/IEC 12207:2008, 2008)

Modelo de Ciclo de Vida: Marco de procesos y actividades relacionadas con el ciclo de ida que puede ser organizado en etapas.

Mantenimiento: Cambio realizado en una aplicación después de su entrega

Marco de Referencia Normativo de la Organización MRNO: Estructura interna de toda organización, que contiene un conjunto de procesos y elementos normativos de seguridad de la aplicación.

Comité de MRNO: Responsable de mantener y aprobar los componentes relacionados con la seguridad de la aplicación dentro de MRNO.

Entorno Operativo: Alrededores externos de un software existente durante su ejecución.

Aplicación Segura: Aplicación para la cual el nivel de confianza actual es igual al nivel de confianza objetivo.

Nivel de Confianza Objetivo: Nombre de un conjunto de controles de seguridad de la aplicación considerado por el propietario de la aplicación para bajar el riesgo asociado con una aplicación específica a un nivel aceptable, seguido por un análisis de riesgo de seguridad de la aplicación.

Validación: Confirmación a través de la provisión de una evidencia objetiva, cumpliendo los requisitos de una aplicación. Estas condiciones pueden ser reales o simulada.

Verificación: Confirmación a través de la provisión de la evidencia objetiva, de que los requisitos específicos se han cumplidos.

BackOffice (Trastienda): Conjunto de actividades de apoyo al negocio realizando tareas para la gestión de la empresa y que no tiene contacto con el cliente. Ejemplo labores informativas y de comunicaciones.

Abreviaciones:

MRNA: Marco de Referencia Normativo de la Aplicaciones

CSA: Control de Seguridad de la aplicación

PGSA: Proceso de Gestión de Seguridad de la Aplicación.

CDDG: Comercial de Distribución General

TIC: Tecnología de la información y Comunicación

SGSI: Sistema de Gestión de Seguridad de la información

MRNO: Marco de Referencia Normativo de la Organización

XML: Lenguaje de Marcas Extensible.

2.4.4 Estructura de ISO /IEC 27034

ISO /IEC 27034 está dividido en 6 documentos o secciones, que se detallan a continuación:

Tabla 4.
Estructura ISO/IEC 27034

Parte	Nombre	Descripción
ISO /IEC 27034-1	Descripción y conceptos	Seguridad de la aplicación. Introduciendo definiciones, conceptos, principios y procesos involucradas.
ISO /IEC 27034-2	Marco de Referencia Normativo de la Organización	Discusión del Marco de Referencia normativo de la organización, sus componentes y procesos a nivel de organización para gestionarlo. Aquí se detalla las relaciones entre proceso, actividades y medios mediante los cuales se apoyan al Procesos de gestión de seguridad de la aplicación.
ISO /IEC 27034-3	Proceso de Gestión de Seguridad de la Aplicación	Debate de los procesos involucrados en un proyecto de la aplicación: Determinar los requisitos y el entorno de la aplicación. Evaluar los riesgos de seguridad de la aplicación. Crear y mantener el Marco referencia normativo (MRNA) Realizar y operar la aplicación. Validar su seguridad a través del ciclo de vida, explicado las relaciones entre procesos, actividades e interdependencias. A más de cómo se introduce la seguridad en un proyecto de aplicación.

CONTINÚA

ISO /IEC 27034-4	Validación de seguridad de la aplicación	Debate acerca del proceso de validación y certificación de seguridad que mide el nivel de confianza actual de la aplicación, comparado con el Nivel de confianza objetivo de la aplicación seleccionada o desarrollada por la organización.
ISO /IEC 27034-5	Protocolos y estructurad de datos de control de seguridad de la aplicación	Presenta protocolos y esquemas XML (Lenguaje marcado extensible) para el control de seguridad de la aplicación CSA. Se utilizará para ayudar a las organizaciones a validar, automatizar, actualizar la estructura de datos de sus CSA.
ISO /IEC 27034-6	Guía de Seguridad para Aplicaciones Especificas	Proporciona ejemplos de CSA adaptados a requisitos específicos de aplicaciones.

Fuente: (NTE INEN-ISO/IEC 27034-1, 2014)

2.5 Introducción a la Seguridad de la aplicación

Al lanzar una aplicación al mercado, una organización debe considerar el impacto que generaría hacia su información, usuarios, recursos TI. Los desarrolladores deben estar conscientes de los riesgos y sus consecuentes vulnerabilidades que implicaría dicha acción. Para ayudar a minimizar los riesgos, las organizaciones deben emplear procesos de garantía de aplicación, es decir que el nivel de confianza de la aplicación este en su posible sin vulnerabilidades.

Esto en teoría no se cumple debido a que con los avances de la tecnología genera que también existan nuevas vulnerabilidades. Las organizaciones deben desarrollar requisitos que especifiquen como deben protege los datos según el entorno en el cual se desarrolla. (Quirolgico, Voas, Karygiannis, Michael, & Scarfone, 2015)

La seguridad de la aplicación es un proceso ejecutado para aplicar controles y mediciones a las aplicaciones de una organización con el fin de gestionar el riesgo que existe en su utilización.

Estos controles y mediciones se pueden aplicar a:

- La propia aplicación, es decir, a sus procesos, componentes, programas, resultados.
- A sus datos (configuración, datos de usuario y/u organización).
- A toda su tecnología, procesos y actores involucrados en el ciclo de vida de la aplicación.

2.5.1 **Generalidades del campo de aplicación de seguridad de la aplicación:**

La seguridad de la aplicación consiste en proteger los datos críticos utilizados, almacenados y transferidos por una aplicación según el requerimiento de una organización. Dicha protección asegura la disponibilidad, integridad y confidencialidad de los datos, además de la autenticación de los usuarios que acceden. El criterio de los datos y otros activos se debe definir por la organización a través de su proceso de evaluación de riesgos de seguridad.

Los datos críticos que requiere de protección también incluyen el código fuente de la aplicación, código binario y el código de ejecución. (NTE INEN-ISO/IEC 27034-1, 2014)

En la siguiente figura se muestra una representación gráfica del campo de aplicación de seguridad de la aplicación.

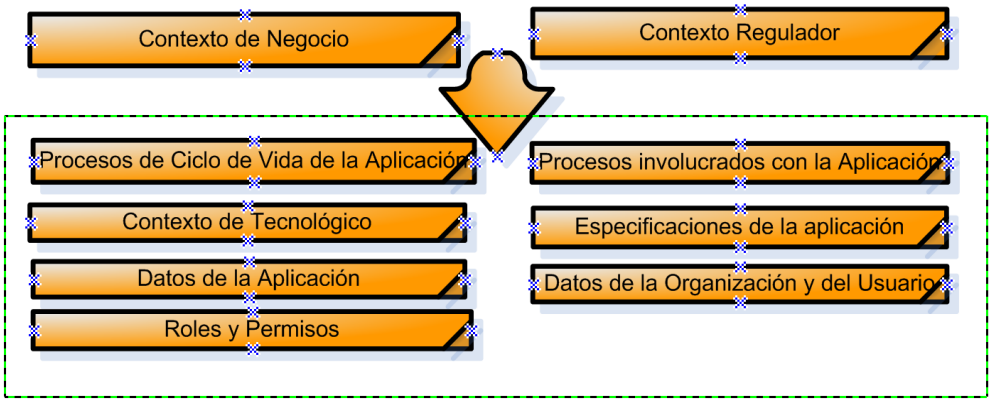


Figura 4. Campo de Aplicación de seguridad de la aplicación.
Fuente: ISO/IEC27034

Generalmente todos estos elementos no son parte de una aplicación, pero estos campos deberían ser protegidos con el fin de asegurar la aplicación.

Tabla 5.
Campos que deben ser protegidos en una aplicación.

Elementos Relacionados	En el campo de aplicación propiamente dicha	En el campo de aplicación con controles de seguridades
Datos de la Organización y del usuario		✓
Datos de la Aplicación	✓	✓
Roles y Permisos	✓	✓
Especificaciones de la aplicación	✓	✓
Contexto tecnológico		✓
Procesos involucrados con la aplicación		✓
Procesos del ciclo de vida de la aplicación		✓
Contexto de negocio		✓
Contexto regulatorio		✓

Como se mencionó anteriormente los siguientes procesos y datos son los que se deben proteger:

2.5.2 Contexto de Negocio:

Se refiere a todas las mejores prácticas, regulaciones y restricciones relacionadas con el negocio de la organización.

2.5.3 Contexto Regulatorio:

Se refiere a las leyes, regulaciones y reglas comunes, en el campo de la jurisdicción y que tienen un impacto en la funcionalidad de la aplicación.

2.5.4 Proceso del ciclo de vida de la aplicación:

Todos los procesos organizacionales están involucrados en el ciclo de vida de vida de aplicaciones se deberían protegeré, tales como proceso de:

- Capacitación, auditoria y de calificación
- Realización (desarrollo, mantenimiento, control de pruebas, etc.)
- Operacionales.

2.5.5 Procesos involucrados con la aplicación:

Todos los procesos organizacionales requeridos por las especificaciones y datos críticos de la aplicación que se debería proteger tales como los procesos de: Utilización y de Gestión, Mantenimiento y respaldo, distribución y de lanzamiento, requeridos por la aplicación.

2.5.6 **Contexto tecnológico:**

Todos los componentes del producto y de tecnología que ayudan a los datos críticos a protegerse como: Periféricos termínales de red, Sistema operativo, enlaces y puertos de comunicación autorizados, Sistemas de Gestión de base de datos SGBD, productos utilizados por la aplicación

2.5.7 **Especificaciones de la aplicación:**

Todas las especificaciones de la aplicación se deberían proteger contra modificaciones no autorizadas, tales como: Especificaciones de hardware, Especificaciones de seguridad, Funcionalidades de la aplicación, Especificaciones del a terminal del cliente, Especificaciones de BackOffice.

2.5.8 **Datos de Aplicaciones:**

Toda la información crítica de la aplicación se debería proteger como: configuración de la aplicación, código binario de la aplicación, código fuente de la aplicación, componentes de la aplicación y librerías, documentación de la aplicación de los componentes y funcionalidades críticas.

2.5.9 **Datos de la organización y del usuario:**

Toda información crítica de la organización y del usuario se debe proteger: certificados, Claves Privadas, datos críticos, Datos Personales, Datos de configuración del usuario.

2.5.10 **Roles y Permisos:**

Toda la información crítica de gestión de identidad y de permisos se debe proteger: datos de Gestión de Identidad, datos de identificación y autenticación, datos de autorización.

2.6 **Requisitos para la seguridad de Aplicación:**

2.6.1 **Requisitos de seguridad para aplicación:**

Son identificados por la evaluación de riesgo y tratamiento de riesgo. Estos factores son efecto de las especificaciones de la aplicación, entorno objetivo, datos críticos y decisiones tomadas por el propietario de la aplicación.

Los requisitos funcionales se establecen que las funcionalidades de seguridad se implementan en la aplicación. Los requisitos no funcionales de seguridad tratan las cualidades de seguridad que la aplicación debería exhibir. Estos controles deberían ser aprobados por la organización a nivel global. (INEN-ISO/IEC 27005)

2.6.2 **Requisitos de seguridad de la aplicación en Ingeniería:**

Es el proceso para reunir, analizar y especificar los requisitos para una aplicación. Se debe mejorar con la evaluación del riesgo para así incorporar los requisitos de seguridad más específicos. La evaluación de riesgo debería involucrar el uso de procedimientos repetibles y sistemáticos que aseguraran que los conjuntos de requisitos obtenidos sean completos, consistentes, entendibles y analizable por el propietario de la aplicación. (INEN-ISO/IEC 27005)

2.6.3 **Organización de SGSI:**

Toda la información obtenida y procesada por una organización esta sujetas a riesgos y peligros relacionadas con la tecnología. La Seguridad de la información es sinónimo de un activo inestimable de la organización que requiere una protección adecuada.

"Un sistema de gestión de seguridad de la información proporciona un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la protección de los activos de la información de una organización basado en un enfoque de riesgo de negocio". (NTE INEN-ISO/IEC 27001, 2011).

ISO/IEC, apoya a los objetivos de un SGSI de toda organización. Además, debería proporcionar los controles y las evidencias adecuadas para demostrar a la gerencia de la organización que los riesgos involucrados en el uso de la aplicación se gestionan adecuadamente.

2.7 **Riesgo:**

2.7.1 **Riesgo de seguridad en la aplicación:**

El riesgo es una magnitud a danos frente a un peligro, por lo tanto, el riesgo de una aplicación es el riesgo de toda organización. Una aplicación puede presentar los siguientes riesgos:

2.7.2 **Vulnerabilidades de una aplicación:**

Viene como consecuencia de los controles inadecuados o no existentes en una aplicación. La vulnerabilidad se puede dar por:

- Actores, tales como programadores, quienes escriben un código de forma de manera incorrecta.

- Usuarios que cometen errores en la utilización del software.
- Técnicos y desarrolladores que comenten errores durante el mantenimiento de la aplicación.
- Procesos como los procedimientos inadecuados de prueba, gestión de proyecto, atención insuficiente a la seguridad a lo largo del proceso de ciclo de vida, procesos de gestión de cambios inadecuados.
- Contexto tecnológico, tal como la mala decisión de infraestructura tecnológica o de productos.
- Especificaciones, tales como el diseño inadecuado, vulnerabilidades debido a las interacciones de los sistemas o errores de interfaces. (NTE INEN-ISO/IEC 27034-1, 2014)

2.7.3 **Amenazas en las aplicaciones:**

Una amenaza tiene el potencial de dañar a la información crítica en el campo de aplicación de la misma y así a la organización. La amenaza se puede dar por el entorno de la aplicación y/o actores.

2.7.4 **Gestión de Riesgo;**

Proceso de mantener los riesgos de seguridad de la aplicación con ayuda del tratamiento de los riesgos de seguridad, aplicando controles a los riesgos para que se encuentren dentro de los niveles aceptables.

"*La gestión de riesgo es un concepto clave debido a que se puede aplicar a una organización en su conjunto, a cualquier parte discreta de la misma (departamento, servicio, etc) a cualquier sistema de información, existente o planificado o a los aspectos de control*". (NTE INEN-ISO/IEC 27005)

El proceso de gestión de riesgo son el establecimiento del contexto, la evaluación de riesgo, tratamiento de riesgo, aceptación de riesgo, comunicación del riesgo, monitoreo y revisión del riesgo. En el proceso de gestión de riesgo de seguridad en aplicaciones se usa los mismos elementos con un campo de entorno ajustado al nivel de la aplicación. (NTE INEN-ISO/IEC 27034-1, 2014)

2.7.5 **Costos:**

El costo de seguridades viene dado por la relación entre las amenazas y vulnerabilidades. El precio viene dado por el control de seguridad de aplicación a implementar en el producto de la organización.

2.7.6 **Entorno Objetivo:**

Compuesto por contextos regulatorios, negocio y tecnológicos dentro de los cuales la organización utilizara la aplicación. Todas las amenazas pueden dañar a una organización por tanto se deben definir claramente al inicio de un proyecto de la aplicación.

El contexto tecnológico de la organización debería cumplir con los requisitos del entorno objetivo de la aplicación, con el fin de publicar o lanzar al mercado una aplicación de forma segura.

Después de implementar la aplicación se puede definir nuevos requisitos de seguridad para la aplicación (Actualizacion), con el objetivo de abordar estos nuevos riesgos y seleccionar los controles que mitigan esos riesgos a un nivel aceptable. Estos controles de seguridad pueden ser introducidos en los procesos del ciclo de vida de la aplicación agregado al código fuente de la aplicación.

2.8 Proceso en general de ISO/IEC 27034:

2.8.1 Componentes, procesos y marco de trabajo

Todo el componente y marcos de referencia son parte de dos procesos generales:

- Procesos de Gestión de MRNO.
- Proceso de Gestión de Seguridad de la Aplicación (PGSA).

El proceso de Gestión MRNO es un proceso continuo a nivel organizacional y el PGSA se utiliza para gestionar la seguridad en los proyectos específicos del a aplicación. (NTE INEN-ISO/IEC 27034-1, 2014)

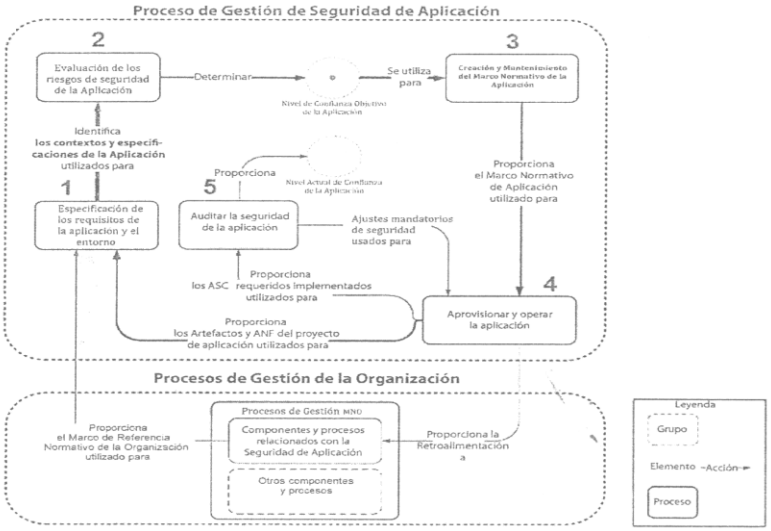


Figura 5. Proceso de Gestión de la organización.
Fuente: ISO/IEC27034

2.8.2 Procesos de Gestión MRNO:

Utilizado para gestionar los aspectos relacionados con la seguridad de la aplicación. Establece todos los contextos de la organización y se convierte en la única referencia para la seguridad de las aplicaciones dentro de la organización. MRNO contiene procesos involucrados en

la seguridad de la aplicación, como son las regulaciones, leyes, mejores prácticas, roles y responsabilidades aceptadas por la organización.

2.8.3 Proceso de Gestión de Seguridad de la Aplicación (PGSA)

Gestiona la seguridad de la aplicación utilizado por una organización, se realiza en cinco pasos:

2.8.3.1 Especificación de los requisitos de la Aplicación y del Entorno

El primer paso de PGSA es especificar todos los requisitos de la aplicación, incluyendo: actores, especificaciones, información y entorno.

2.8.3.2 Evaluación de los riesgos de seguridad de la aplicación

El segundo paso consiste en la identificación del riesgo, análisis del riesgo, tratamiento de riesgo y evaluación del riesgo.

Aquí también se produce requisitos de seguridad que se usan para obtener el nivel deseado de confianza para la aplicación, a lo que se denomina nivel de confianza objetivo de la aplicación. (NTE INEN-ISO/IEC 27005)

2.8.3.3 Creación y mantenimiento del Marco de Referencia Normativo de la Aplicación

El tercer paso selecciona todos los elementos del MRNO que se aplica a un proyecto específico de la aplicación. El nivel de confianza objetivo de la aplicación, contextos, responsabilidades y especificaciones de la aplicación determinan los contenidos exactos de MRNA. Con esto la organización selecciona los controles aplicables de la seguridad de aplicación para el proyecto de aplicación.

2.8.3.4 Provisión y operación de la aplicación:

El cuarto paso es el uso de los controles de Seguridad de la aplicación. El equipo de proyecto implementa los CSA bajo el Marco de referencia normativo de la aplicación, en dos sub-pasos: Actividad y Medición de seguridad de CSA.

2.8.3.5 Auditorías a la seguridad de la aplicación

Un equipo de verificación prueba de monitoreo y revisión de todas las mediciones de verificación proporcionadas por todos los CSA en el MRNA.

2.9 Marco de Referencia Normativo de la Organización.

Marco donde todas las mejores prácticas de seguridad de la aplicación reconocidas por la organización se definirán. El MRNO es el fundamento de la seguridad de la aplicación y de todas las decisiones de seguridad de la aplicación se basan en él. Además, es el inicio de un PGSA que se realiza para cada proyecto como se puede observar en la figura 6:

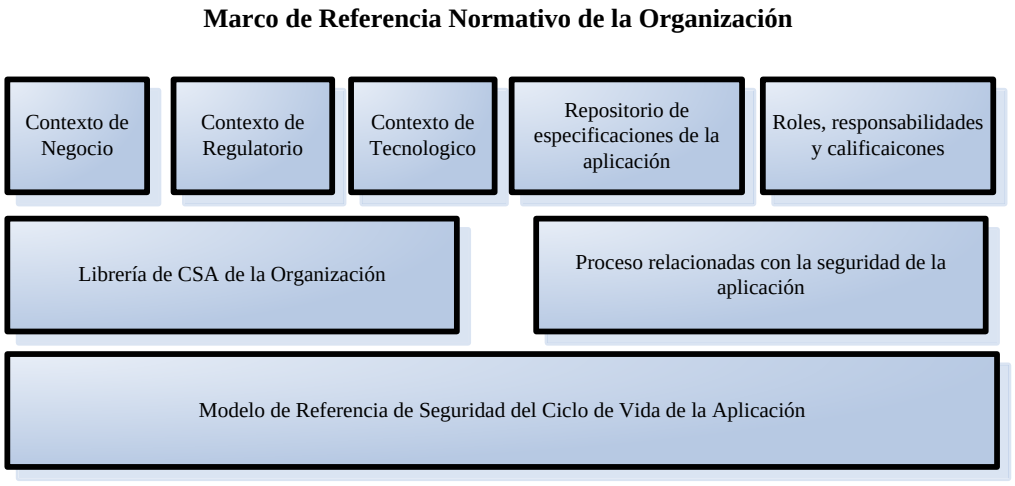


Figura 6. Marco de Referencia Normativo de la Organización(Simplificado)
Fuente: ISO/IEC 27034

Componentes:

2.9.1 Contexto de Negocio:

Lista y documenta todas las normas y mejores prácticas aceptadas por la organización que podría tener impacto en los proyectos de organización. Además, incluye:

a) Procesos de gestión de proyecto, desarrollo, análisis de riesgo, operación, autoría y control.
b) Políticas de seguridad de la organización
c) Prácticas para el dominio de negocio
d) Metodología de desarrollo de la organización
e) Mejores prácticas de programación empleados por la organización en el contexto tecnológico
f) Proceso formal de gestión de proyecto de la organización (NTE INEN-ISO/IEC 27034-1, 2014)

2.9.2 Contexto Regulatorio:

Lista y documenta cualquier ley o regulación, para cualquiera negocio de una organización. Teniendo impacto en los proyectos de aplicaciones.

2.9.3 Especificaciones de la aplicación:

Lista y documenta los requisitos generales funcionales de TI y las soluciones aprobadas por la organización, que debería cumplir.

- Especificaciones sobre como las aplicaciones deberían calcular, almacenar y transferir la información.

- Parámetros, funciones, servicios y requisitos usuales de la aplicación.
- Código fuente, binario, librerías y productos utilizados por las aplicaciones.

2.9.4 **Contexto Tecnológico:**

Inventario de todos los productos, servicios y tecnologías de TI disponible para la organización para los proyectos de aplicación. Incluye computadoras, herramientas, productos y servicios TI, infraestructura de comunicación, etc.

Además, el Contexto Tecnológico debe incluir:

- Tecnología disponible: Debe estar actualizada por la MRNO a través de la retroalimentación de proyectos anteriores.
- Tecnología requerida por una aplicación: cumpliendo los requisitos funcionales agregados por MRNO, especificados en la planificación de investigación de un proyecto de aplicación. Deben ser entendidas y documentadas antes de ser aprobadas.
- Tecnología disponible: investigación, análisis y monitoreo de tecnologías.

2.9.5 **Roles, Responsabilidades y Calificaciones:**

El MRNO debe contener la lista y descripciones de todos los roles, responsabilidades y calificaciones profesionales requeridas para los actores involucrados en:

- Creación y mantenimiento del MRNO.
- El ciclo de vida de la aplicación de la organización, tal como gerente de seguridad de la información, proyectos, administradores de base de datos, compradores de software, dirección de desarrollo de software, base de datos, etc. (ISO/IEC 27034-2)

2.9.6 Control de Seguridad de Aplicación (CSA)

Las organizaciones deben definir una librería de controles para la seguridad de la aplicación, para listar y documentar todos los CSA reconocidos por la organización.

Las CSA dentro de esta librería están organizadas en conjuntos según el nivel de protección que proporciona contra las amenazas de seguridad. Cada conjunto lleva consigo una etiqueta que informa a los administradores, el grado de seguridad obtenido de un conjunto de controles particulares, a esto se denomina "nivel de confianza". (NTE INEN-ISO/IEC 27034-1, 2014)

2.9.6.1 Proceso Creación CSA:

Las CSA se agregan agrupándolos según el nivel de confianza. Es responsabilidad del MRNO construir una librería CSA, que satisfaga las necesidades y requisitos particulares de la organización.

Este objetivo se consigue mediante un análisis de las aplicaciones nuevas o existentes de la organización. Además, involucra la determinación de los riesgos y requisitos de seguridad de la aplicación, el resultado es un conjunto de CSA.

2.9.6.2 Nivel de Confianza de la Aplicación:

Es una etiqueta que simplifica la comunicación entre actores con diferentes formas de participación de la seguridad de la aplicación dentro de la organización. Se debe definir con el propósito de identificar sin ambigüedades a un conjunto de controles.

Un nivel de confianza tiene un concepto parecido a un plan de seguridad, el cual es un conjunto de controles autorizados por una organización con el fin de reducir los riesgos.

Una organización debe definir su propio domino o escala de niveles de confianza aprobado por la MRNO y así obtener un nivel de confianza Objetivo de aplicación que es el destino de la aplicación. Además, se tiene que definir cuál es el nivel de confianza cero, el cual es el nivel mínimo aceptable para cada aplicación desarrollada por la aplicación.

La organización debe monitorear estos niveles de confianza de las aplicaciones para así tomar acciones adecuadas si, la misma no se encuentra o cae por debajo del nivel cero de confianza. (NTE INEN-ISO/IEC 27034-1, 2014)

2.9.6.3 **Control de seguridad de la Aplicación:**

Medio por el cual se puede realizar la verificación de una aplicación.

Los CSA se pueden utilizar para:

- Asegurar los componentes de la aplicación, incluyendo software, datos, infraestructura.
- Agregar actividades de seguridad a los procesos utilizados durante el ciclo de vida de la aplicación.
- Verificación de roles, responsabilidades de todos los actores involucrados en el proyecto.
- Determinar los criterios de evaluación para componentes.
- Ayudar a determinar el nivel Real de confianza de la aplicación.
- Proporcionar información pertinente a diferentes actores.
- Facilitar la comunicación, agrupando los CSA de acuerdo al lenguaje de nivel de negocio.
- Facilitar distribución de CSA agrupando en conjuntos relacionados.
- Asegurar que todas las actividades de seguridad de CSA vinculados sean realizadas.

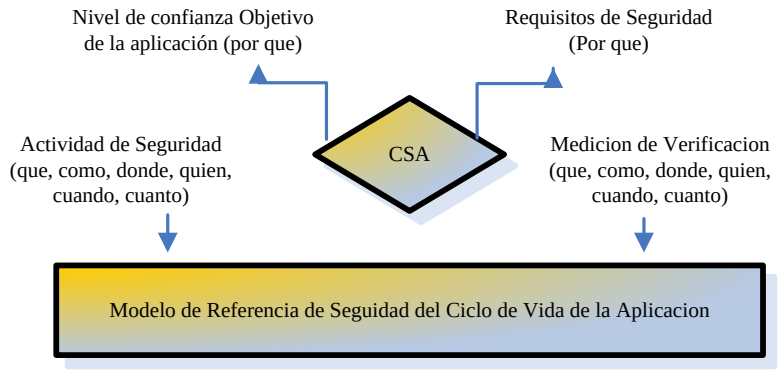


Figura 7. Componente de un CSA.
Fuente: ISO/IEC 27034

Para identificar una CSA debe tener información como: nombre, identificación, actor, fecha, descripción de CSA. Además de señales de elementos raíces o derivados. Finalmente debe tener contextos pertinentes de negocios, reglamentos y tecnología, así como especificaciones de la aplicación que proporcionan los requisitos de seguridad.

Objetivo: Especifica porque este CSA existe, esto quiere decir que expresa los requisitos de seguridad para los cuales fue diseñado. Además, especifica:

- Elementos de su actividad de seguridad necesita para producir la evidencia que soporta sus mediciones de verificación
- Para que niveles de confianza el CSA es obligatorio
- Especificaciones de la aplicación con los cuales el CSA está asociado y cuales se pueden referir a las regulaciones y normas.
- Amenazas de seguridad sobre el entorno operativos de la aplicación.

2.9.6.4 **Actividades/Verificación de CSA:**

Una CSA debe tener los siguientes procedimientos o pasos para ser implementada:

- Que: Descripción completa de actividad y/o verificación de seguridad, complejidad de la actividad, artefactos de actividad, los cuales son las pruebas necesarias para demostrar la presencia de procesos de seguridad de aplicación de controles y resultados esperados
- Como: Técnica para realizar actividad/verificación y obtención de artefacto.
- Dónde: Objetivo de la actividad/ verificación de seguridad.
- Quien: Calificaciones requeridas para los actores que deben llevar a cabo esta actividad/verificación.
- Cuando: Actividad específica en una etapa en la vida del modelo de referencia del ciclo de vida de seguridad de la aplicación
- Cuánto: Costo para llevar la actividad/verificación de CSA.

2.9.7 **Modelo de Referencia del Ciclo de Vida de Seguridad de la Aplicación**

Cuando una organización quiere desarrollar o adquirir aplicaciones debe utilizar un marco de referencia de procesos y actividades definidas, dados en dos etapas. La primera es el "Modelo de ciclo de Vida de la aplicación", el cual es el marco de referencia único y personalizados de una organización. Dicho modelo viene dado desde la concepción de la aplicación hasta su retiro de la organización. La segunda es el Control de Seguridad de la Aplicación (CSA), que se agregan a actividades definidas por el Ciclo de vida de la aplicación. (NTE INEN-ISO/IEC 27034-1, 2014)

El propósito del Modelo de Referencias del ciclo de vida es ayudar a la organización:

- Validar cada uno de los ciclos de vidas especificando las actividades.
- Asegurar que los problemas de seguridad sean realizados correctamente en todas las etapas del ciclo de vida.
- Minimizar los costos.
- Proporcionar un modelo normal para compartir los CSA entre equipos de proyectos
- Proporcionar un modelo normalizado para compartir CSA.

Una organización debería definir un mapeo constante entre las etapas y actividades definidas en este modelo de referencia y las etapas. El comité de la MRNO de la organización definirá la colocación del os CSA en el modelo de referencia del ciclo de vida de seguridad de la aplicación. (NTE INEN-ISO/IEC 27034-1, 2014)

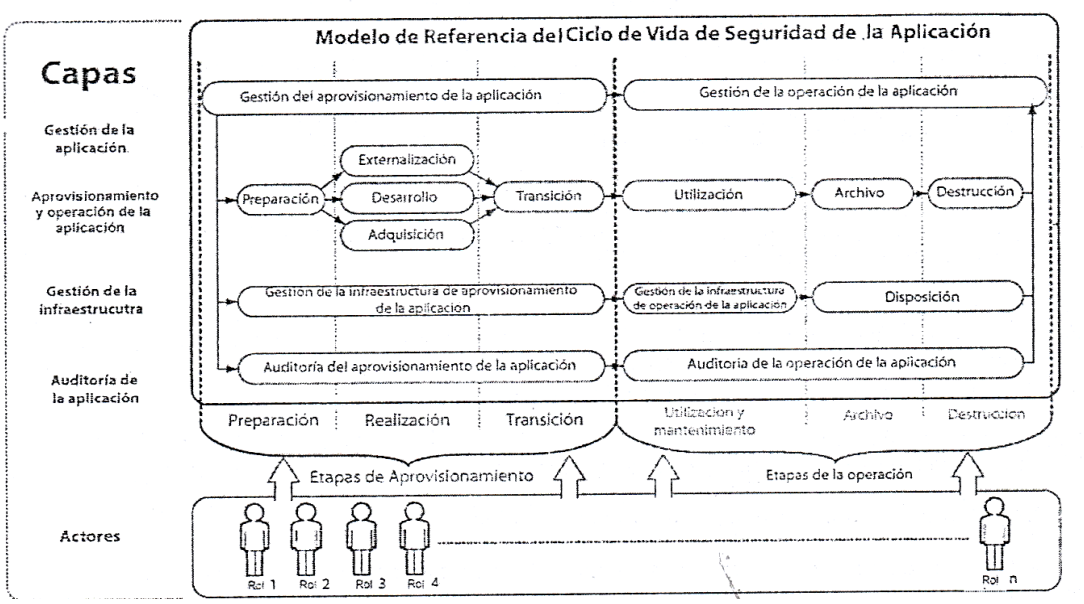


Figura 8. Modelo de Referencia del Ciclo de vida de seguridad de la Aplicación
Fuente: ISO/IEC 27034

Como se puede observar en la figura se tiene varias etapas del modelo de referencia las cuales son las siguientes:

2.9.7.1 **Gestión de aprovisamiento de la aplicación:**

Se lleva a cabo por la dirección de proyecto. Incluye procesos de ingeniería de software, tal como Proceso de gestión de recursos humanos, proceso de planificación de proyecto, proceso de evaluación de proyecto de control, Procesos de gestión de decisión (ISO/IEC 12207:2008, 2008)

2.9.7.2 **Gestión de operación de la aplicación:**

Están relacionadas con las gestión y uso de aplicación durante las etapas de operación. Las actividades que se realización son el Proceso de gestión de decisión y Gestión de la información.

2.9.7.3 **Subcontratación:**

Las actividades relacionadas con la implementación del software cuando la organización externaliza la implementación. Dichas actividades son Proceso de adquisición, procesos de gestión de documentación de software, proceso de gestión de configuración de software y proceso de gestión de riesgo.

2.9.7.4 **Desarrollo:**

Ejecuta el equipo de aprovisionamiento. Las actividades que se realización son proceso de gestión de riesgo, diseño arquitectónico del sistema, proceso de diseño detallado del software, proceso de gestión de configuración del software proceso de verificación del software, proceso de validación y revisión del software, y proceso de gestión del archivo para reusó.

2.9.7.5 **Adquisición:**

Se lleva a cabo por el equipo de aprovisionamiento con el propósito de obtener externamente o comprar el producto que satisfagan las necesidades de la organización. Las actividades que se manejan son el Proceso de adquisición, proceso de gestión de documentación y configuración del software, gestión de riesgo y el proceso de implementación.

2.9.7.6 **Transición:**

Realizada por el equipo de aprovisamiento para la preparación, configuración y pruebas de la aplicación en el entorno operativo definido por la organización. Las actividades que se realización son Proceso de gestión de configuración de software, proceso de integración de sistemas y proceso de prueba de calificaciones de sistemas.

2.9.7.7 **Utilización:**

Actividades que ocurren en el momento de uso de la aplicación que incluyen gestión de usuario y acceso, registro, monitoreo, capacitación de seguridad, mantenimiento de software. Además, incluye la corrección de errores y posibles adaptaciones de software. Los procesos que sean manejan son Proceso de operación de software y Mantenimiento de Software.

2.9.7.8 **Archivo:**

Ejecuta equipo de operación cuando ya no se necesita en su estado activo. Incluye toda la información de la aplicación, incluyendo herramientas y procesos para proteger y acceder de forma segura a la información e incluso la aplicación que ya no se ejecuta en el entorno operativo. Los procesos que se manejan son el deshecho del software. (ISO/IEC 12207:2008, 2008)

2.9.7.9 **Destrucción:**

Destrucción segura de toda la información de la aplicación, incluyendo datos del usuario, información de organización, etc. A este proceso se conoce como Proceso de deshecho de Software.

2.9.7.10 **Gestión de infraestructura de aprovisionamiento de la aplicación:**

Esta etapa incluye actividades involucradas en el aprovisionamiento y el mantenimiento de una infraestructura tecnológica. Incluye servicios, facilidades, herramientas, y activos de tecnologías de comunicaciones información en el entorno de desarrollo. Dichas actividades son parte de la Gestión de infraestructura y el proceso de gestión de configuración.

2.9.7.11 **Gestión de infraestructura de operación de la aplicación:**

Incluye actividades en el aprovisionamiento y mantenimiento de una infraestructura tecnológica segura para las etapas de operación del ciclo de vida de una aplicación. Además de incluir servicios, facilidades, herramientas y activos de tecnologías de comunicaciones e información en el entorno operativo de la aplicación. Otras actividades que se deben llevar acabo en la etapa de operación es el mantenimiento de infraestructura (Sistemas y red), copias de seguridad y recuperación. (ISO/IEC 15288, 2015)

2.9.7.12 **Eliminación:**

Tienen el fin de proporcionar una garantía de que toda la información almacenada en los servidores, sistemas utilizadas por la aplicación sean eliminada de forma segura. A esto se lo conoce como proceso de eliminación.

2.9.7.13 **Auditoria de aprovisionamiento de la aplicación:**

Las actividades de auditorio se realización en todos los procesos durante el ciclo de vida de la aplicación. Se realizan periódicamente por los equipos internos o externo según el nivel de confianza objetivo del proyecto de lea aplicación, proporcionando así la garantía y evidencia necesaria de los requisitos de seguridad para la aplicación que se espera. (ISO/IEC 12207:2008, 2008)

2.9.8 **Procesos relacionados con el Marco de Referencia Normativo de la Organización:**

El comité del MRNO de la organización debe definir, documentar y autorizar los procesos para la aprobación de MRNO y sus componentes (Tecnológicos, negocio y reglamentarios).

Los roles y responsabilidades y las calificaciones profesionales de los actores involucrados deben estar especificados.

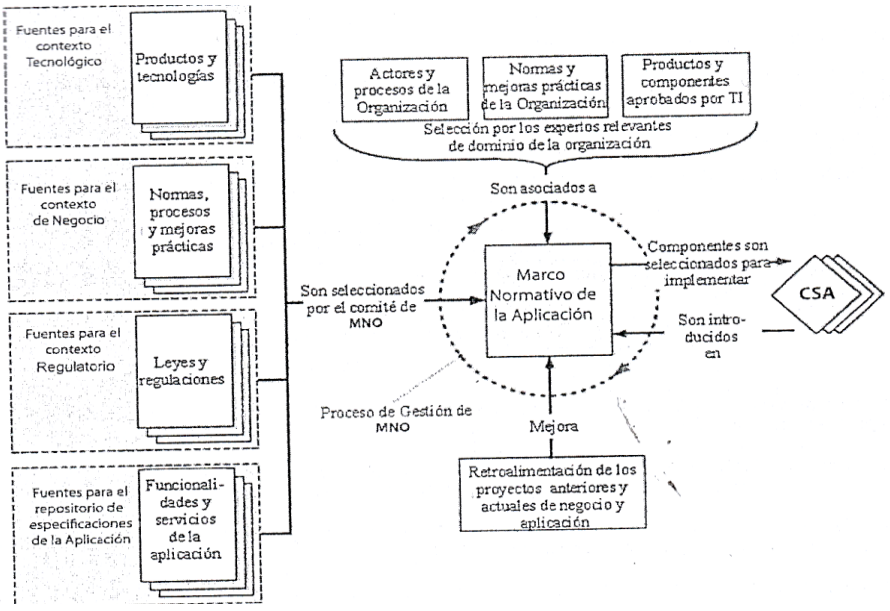


Figura 9. Proceso de Gestión de MRNO
Fuente: ISO/IEC 27034

2.9.8.1 **Objetivos:**

- Aseguramiento de las necesidades de la aplicación y aprobación de la librería CSA y niveles de confianza, alineadas a las necesidades de negocio de la organización
- Aseguramiento de los componentes MRNO
- Aprobación de alta dirección de las políticas de seguridad de la organización
- Aseguramiento de que CSA se cumpla de forma adecuada en toda la organización
- Comunicación de los componentes de MRNO a todos los equipos en la organización.
- Prestación de una retroalimentación al MRNO

2.9.8.2 **Subproceso de Gestión del MRNO:**

Estos subprocesos están relacionados con los procesos de SGSI

Tabla 6.
Mapeo de subprocesos de SGSI y de gestión de MRNO

Procesos de SGSI	Sub-Procesos de Gestión de MRNO
Planificar	Diseñar el MRNO
Hacer	Implementar el MRNO
Verificar	Supervisar y revisar MRNO
Actuar	Mejorar continuamente el MRNO

Fuente: ISO/IEC 27034

Diseño del MRNO:

Consiste en establecer los componentes del MRNO relacionados con la aplicación incluyendo el PGSA, librería CSA y todos los procesos relacionados.

a) Especificar y documentar los contextos posibles en el cual se utilizará.
b) Crear, documentar y mantener el repositorio de las especificaciones de la aplicación. Analizando las especificaciones para cada nueva aplicación y de las existentes.
c) Especificar actores y proceso involucrados en el ciclo de vida de la aplicación
d) Analizar mejores prácticas y normas para definir los CSA.
e) Creación y actualización de CSA: Un CSA se crea o actualiza para abordar los requisitos específicos de la seguridad. Los expertos deben definir la actividad y la mención de verificación.
f) Validación e integración de CSA: Un equipo de verificación compuesto por la dirección, desarrollador, auditores TI, deberá ser responsable de CSA, asegurando que sea comprensible para los que utilizan. Además, el equipo debe especificar en qué niveles definidos de confianza se requiere este CSA.
g) Analizar y comparar el modelo de referencia del ciclo de vida de seguridad de la aplicación y como se quiere adaptar el modelo actual del ciclo de vida de la aplicación de la organización otros procesos.
h) Definir e implementar la librería CSA de la organización
i) Desarrollar, actualizar y validar los CSA requeridos por la organización e integrarlos en la librería CSA.
j) Analizar, adaptar y validar la retroalimentación de los proyectos de la aplicación.

Implementar MRNO: implementar y comunicar el MRNO.

Supervisar y revisar el MRNO: garantizar los proyectos de la aplicación utilicen correctamente los componentes del MRNO y que reúna la retroalimentación de los proyectos.

a) Requerir un nivel de confianza objetivo y un nivel de confianza actual para todas las aplicaciones utilizadas por la organización,
b) Requerir una evaluación periódica de riesgo de la aplicación para todas las aplicaciones utilizadas por la organización.

Mejorar continuamente el MRNO: mantener y mejorar todos los componentes en el MRNO, mediante la revisión de contextos, procesos y tecnología de la organización encontrando todos los cambios en el PGSA e integrarnos en el MRNO. (NTE INEN-ISO/IEC 27034-1, 2014)

2.10 Evaluación de riesgo de seguridad de la aplicación:

"La evaluación de riesgo determina el valor de los activos de la información, identifica las amenazas y vulnerabilidades aplicables que existen, identifica los controles existentes y en su efecto en el riesgo identificado, determina las consecuencias potenciales y finalmente prioriza los riesgos derivados y los clasifica contra el conjunto de criterios de evaluación del riesgo en el establecimiento del contexto" (INEN-ISO/IEC 27005) .

2.10.1 Análisis de riesgo de la aplicación:

De Alto nivel: El nivel de confianza objetivo de la aplicación según las especificaciones básicas de la aplicación y los contextos tecnológicos regulatorios y de negocio de la aplicación.

Detallado: Identifica más precisamente los riesgos residuales asociados con las aplicaciones específicas antes de considerar cualquier CSA para la aplicación y reconfirma el nivel de confianza objetivo de la aplicación.

Como resultado del análisis, el propietario de la aplicación poder cambiar el nivel de confianza objetivo de la aplicación para el proyecto.

2.10.2 **Evaluación de Riesgo:**

"*La evaluación de riesgo utiliza la comprensión del riesgo que se detiene mediante el análisis de riesgo para tomar decisiones sobre las acciones futuras. Estas decisiones deberían incluir: si una actividad se lleva a cabo y prioridades para el tratamiento de riesgo, considerando los niveles estimados de ellos*" (NTE INEN-ISO/IEC 27005).

2.10.3 **Nivel de confianza objetivo de la aplicación:**

Ayuda a lograr el nivel de confianza requerido por la organización con el fin de utilizar o lanzar la aplicación de una forma segura. Es vital para la seguridad de la aplicación por que determina directamente los CSA apropiados a ser seleccionados de la librería de CSA implementados en el ciclo de vida de la aplicación.

"El proceso de evaluación de riesgo produce los requisitos de seguridad los cuales se deriva el nivel de confianza objetivo de la aplicación, y este a su vez se convierte en el objetivo de proyecto de aplicación" (NTE INEN-ISO/IEC 27034-1, 2014).

2.10.4 **Aceptación del propietario de la aplicación:**

El propietario de la aplicación tiene la responsabilidad de aceptar los riesgos asociados a la aplicación mediante aprobación de: Nivel de Confianza Objetivo y resultados de la auditoria de seguridad de la aplicación comparando niveles de confianza objetivo con el inicial.

2.11 Marco de Referencia Normativo de la Aplicación (MRNA):

Es un subconjunto del MRNO que contiene solo información detallada de la aplicación con el fin de lograr el nivel de confianza objetivo pedido por el propietario de la aplicación. Para cada proyecto de la aplicación, un MRNA es creado y completado con los contextos pertinentes tecnológicos, reglamentarios y de negocio, las especificaciones de la aplicación y los CSA apropiados. Este MRNA puede cambiar en el trayecto ya sea por cambios en las leyes del contexto regulatorio u otro nivel de confianza. Los cambios en MRNA tiene un impacto en la aplicación.

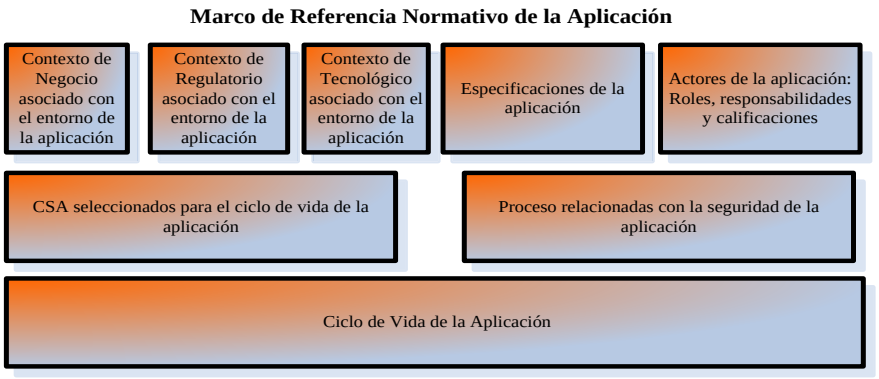


Figura 10. Marco de Referencia Normativo de la Aplicación
Fuente: ISO/IEC 27034

2.11.1 Componentes:

2.11.1.1 Contexto de negocio asociado con el entorno de la aplicación:

"Todos los procesos, metodologías, normas y actores de negocio involucrados en el proyecto de la aplicación, incluyendo los procesos externos de negocio, requerido para proporcionar una integridad adecuada de negocio en los entornos operativos" (NTE INEN-ISO/IEC 27034-1, 2014).

2.11.1.2 **Contexto regulatorio asociado con el entorno de aplicación:**

Todo los requisitos legales y regulatorios aplicables donde se ejecuta la aplicación.

2.11.1.3 **Contexto tecnológico asociado con el entorno de aplicación:**

Todos los componentes tecnológicos de la aplicación: arquitectura, infraestructura, protocolos y lenguajes.

2.11.1.4 **Especificaciones de la aplicación**

Se debe listar y clasificar los datos utilizados, almacenados, calculados, compartidos y transferidos por la aplicación. Incluyendo los datos organizacionales, datos de usuarios, etc.

2.11.1.5 **Actores de la aplicación:**

Se debe determinar todos los actores que interactuaran con la aplicación durante su ciclo de vida, tanto como propietarios de la aplicación, dirección de proyecto, auditores, desarrolladores.

2.11.1.6 **CSA seleccionados para el ciclo de vida de la aplicación:**

Las CSA son seleccionadas bajo los siguientes criterios: Nivel de confianza Objetivo de la aplicación, requisitos de la organización para la aplicación, contextos y especificación específicos de la aplicación.

Cada CSA proporciona tanto una actividad de seguridad realizada por equipo del proyecto con el fin de minimizar un riesgo en específico de seguridad como una medición de la misma realizada por el equipo de verificación para confirmar que la actividad se lleva a cabo con éxito, mediante evidencia.

Los CSA son definidos y aprobados por la organización antes de su desarrollo. Cada uno de ellos deberían incluir como mínimo todos los CSA que el comité de MRNO ha actualizado para el nivel cero de confianza que se definió como el mínimo de confianza que la organización aceptara. (NTE INEN-ISO/IEC 27034-1, 2014)

2.11.2 **Ciclo de vida de la aplicación:**

Designa las etapas y actividades seleccionadas del MRNO par aun proyecto de la aplicación específica. Mencionando de otra manera el ciclo de vida de la aplicación es un subconjunto del modelo de referencia del ciclo de vida de la aplicación contenida en le MRNO.

2.11.3 **Procesos:**

2.11.3.1 **Procesos relacionados con el Marco de referencia normativo de la aplicación.**

La organización debería definir y documentar los procesos para crear, aprobar y mantener el MRNA. En los cuales debe especificar los roles, responsabilidades y calificaciones profesionales de los actores involucrados en el MRNA de la organicen para el enfoque especifico.

El proceso de creación de MRNA para una aplicación específica es vital. Este proceso transforma la información genérica contenida en el MRNO en una información específica requerida por el MRNA para una aplicación específica y sus requisitos.

2.11.3.2 **Proceso de Retroalimentación:**

La organización debe definir un proceso para la mejora a través de la retroalimentación de nuevo conocimiento, sugerencia de control de seguridad de la aplicación ganados.

2.12 Aprovisionamiento y funcionamiento de la aplicación:

El cuarto paso del PGSA involucra el seguimiento y despliegue, el equipo de proyecto implementa sus actividades de seguridad específica, esto se hace más sencillo al suminístrales solo aquellos CSA requeridos para lograr el nivel de confianza objetivo para su proyecto específico. La dirección de proyecto utiliza la herramienta eficaz CSA porque en el detalla recursos y calificaciones requeridas.

Además, el equipo de verificación entrara que CSA es eficaz porque proporciona la información detallada sobre que mediciones de verificación se debería realizar para proporcionar la evidencia de que actividades de seguridad se han realizado correctamente con los resultados. (NTE INEN-ISO/IEC 27034-1, 2014)

2.12.1 Impacto de ISO/IEC 27034 en un proyecto de aplicación:

Un proyecto sin la utilización de ISO/IEC 27034 es manejado por un equipo de proyecto, apoyado por procesos automatizados por la tecnología, con el objetivo de generar la aplicación.

Se agregan nuevos campos en el desarrollo de una aplicación con la utilización de ISO/IEC 27034 como el MRNO y el MRNA. El MRNO no actúa directamente en la aplicación, sino que es la referencia de la organización. El equipo de proyecto, verificación y los usuarios son afectados por el MRNA, siendo este el marco de referencia proporciona los controles de seguridad es de aplicación precisos.

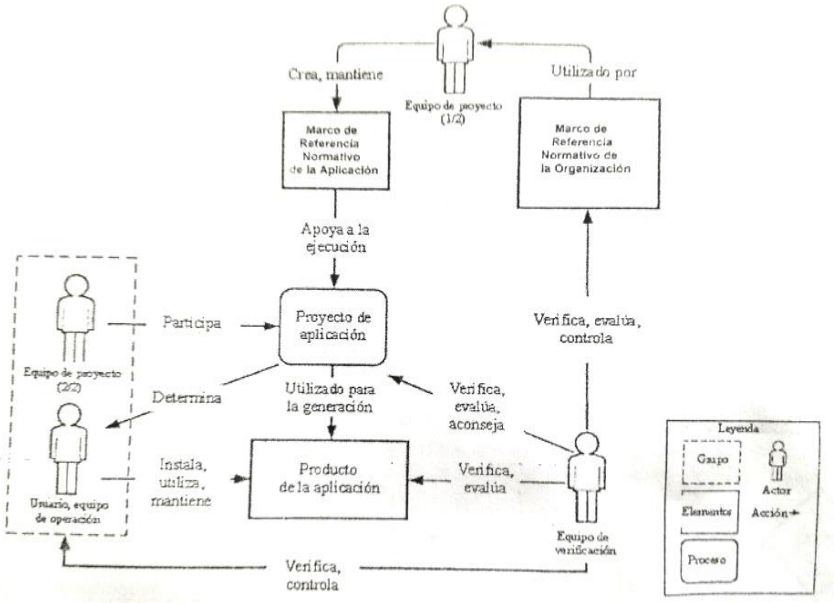


Figura 11. Impacto de ISO/IEC 27034 en un proyecto típico de la aplicación
Fuente: ISO/IEC 27034

2.12.2 **Componentes de Aprovisionamiento:**

2.12.2.1 **Equipo de proyecto:**

Compuesto por personas involucradas en la aplicación durante las etapas de aprovisionamiento.

2.12.2.2 **Equipo de operación:**

Compuesto por personas involucradas en la gestión y mantenimiento de la aplicación durante la etapa de operación del ciclo de vida como en la administración de sistema, base de datos, red.

2.12.3 **Procesos:**

2.12.3.1 **Realización de actividades de seguridad en el curso de un proyecto de aplicación:**

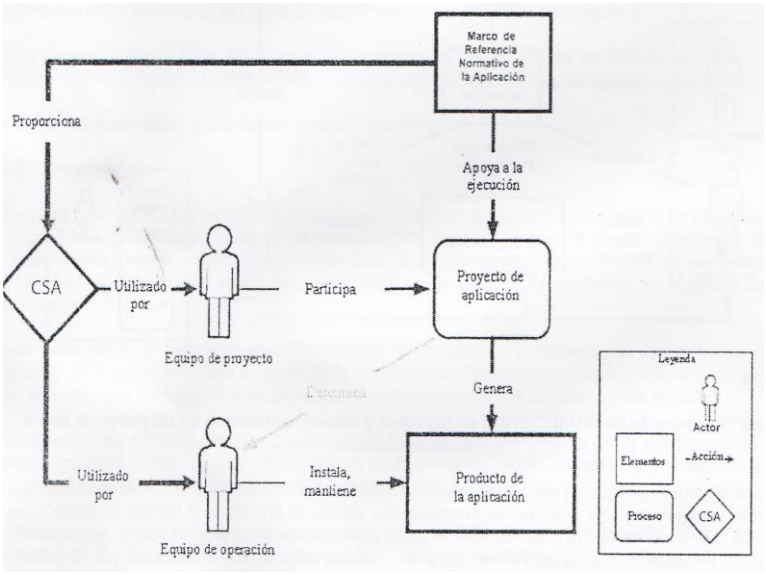


Figura 12. El CSA utilizado como una actividad de seguridad
Fuente: ISO/IEC 27034

2.12.3.2 **Relación de mediciones de verificación en el curso de un proyecto de aplicación**

Implementa el principio de que todas las actividades de seguridad se deberían verificar para proporcionar la evidencia de que la actividad se realizó correctamente, alcanzando así los resultados esperados.

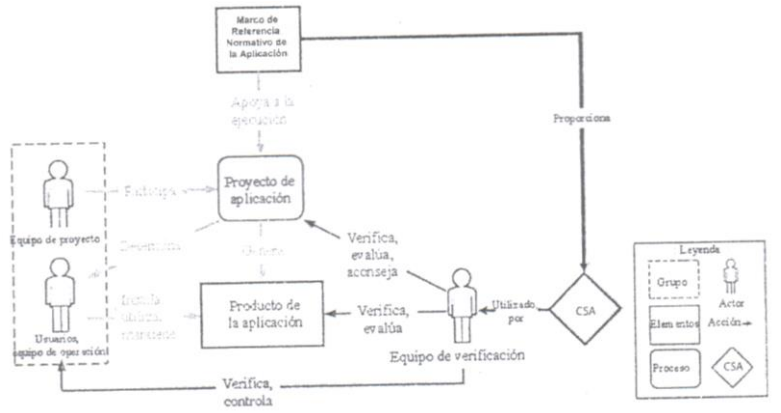


Figura 13 .EL CSA utilizado como una medición
Fuente: ISO/IEC 27034

Como se puede observar en la figura 13, la medición de verificación de un Control de seguridad de Aplicación es la puerta de un ciclo de vida de un proyecto de la aplicación para que el equipo de verificación pueda verificar y validar la aplicación del proyecto. Y así asesorar al propietario para que pueda decidir si autoriza o no el proyecto de aplicación para proceder a su ejecución.

2.13 **AUDITORIA:**

El propósito de que paso es verificar y registrar formalmente la evidencia, que apoya si una aplicación a alcanzado y está manteniendo el nivel de confianza objetivo de la aplicación. Esto se puede realizar en cualquier momento del ciclo de vida de la aplicación tanto periódicamente como eventualmente.

El equipo interno o externo de verificación comprueba que todas las mediciones de verificación proporcionada por los CSA en el MRNA, se hayan realizado y que los resultados sean verificados. Una organización puede declararse como segura cuando su nivel de confianza Actual es igual a su nivel de confianza Objetivo. (NTE INEN-ISO/IEC 27034-1, 2014)

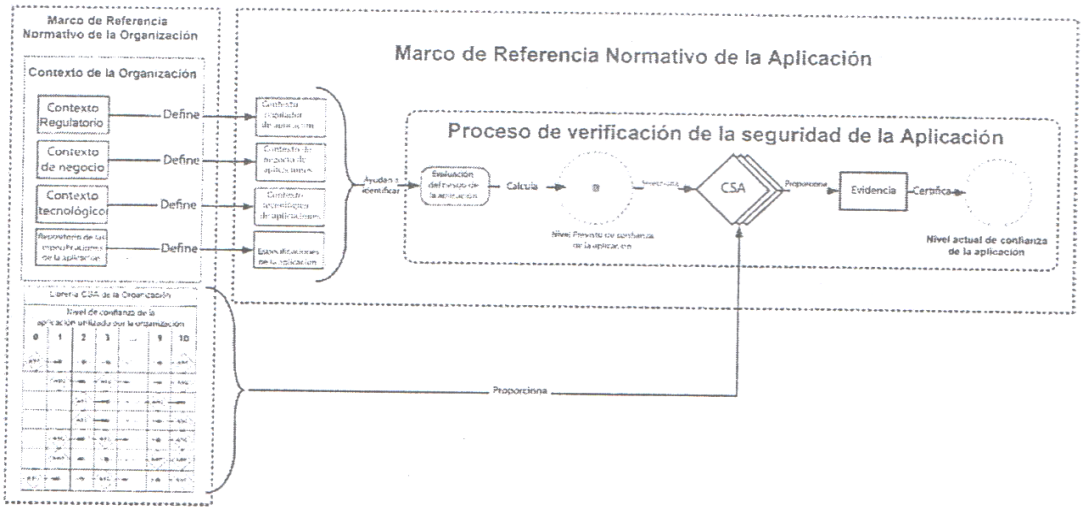


Figura 14. Vista General del proceso de verificación de seguridad.
Fuente: ISO/IEC 27034

2.13.1 **Componente de Auditoria:**

2.13.1.1 **Nivel de Confianza Actual de la aplicación:**

Es el nivel de confianza máximo demostrado por el equipo de verificación según las mediciones de verificación de todos los CSA de la aplicación. Cada CSA proporciona una actividad de medición específica y detallada a ser realizada por el equipo de verificación.

El logro exitoso del nivel de confianza objetivo de la aplicación se confianza cuando la verificación de la evidencia de soporte de las actividades de medición de verificación de todos los CSA esperados se han realizado con éxito. (NTE INEN-ISO/IEC 27034-1, 2014).

CAPÍTULO 3
3 GUÍA DE VERIFICACIÓN DE CUMPLIMIENTO DEL ESTÁNDAR ISO/IEC 27034

3.1 Levantamiento de la información:

Se realizó un análisis actual de un aplicativo de dispositivo móvil, orientado a compras en línea. Para esta verificación se utilizó la aplicación de la empresa "Supercines" dedicadas a la comercialización de venta de boletos de cinematografía.

La mencionada aplicación a analizar fue desarrollada por un agente externo a la organización, en este caso "Bayteq" que se dedica a la "*implementación de soluciones creativas con agilidad y calidad y nuevas tecnologías para generar soluciones innovadoras en múltiples industrias."* (Bayteq, 2018)

Por lo que se puede asumir que "Supercines" no poseen:

- Políticas documentadas relacionada a la seguridad de la información, para garantizar la confidencialidad, Integridad y Disponibilidad.
- Modelo de Gestión de Seguridad de la Información
- Las infraestructuras Tecnológicas no se encuentran normados, ni con criterios de seguridad.
- Control de Vulnerabilidades documentadas
- Documentación de Roles y Responsabilidades.
- Control de Acceso.
- Adquisición, Desarrollo y Mantenimiento de la Información.
- Gestión de Activos.

3.2 Método de transacción financieras por medio digitales:

En la actualidad las aplicaciones manejan gran cantidad de datos, entre ellos los sensibles, como, por ejemplo, usuarios, contraseñas, información de tarjetas de crédito, cuentas bancarias, etc. Por lo que las personas deben usar un medio confiable para la realización de sus transacciones financieras.

En el Ecuador el 73 % de las transacciones bancarias o financieras, se realizan por medio de canales electrónicos (banca en línea). Este crecimiento fue del 16 % en el 2016 y de 30% en el 2017. Con la gran acogida de este sistema de transacciones, las agencias de los respectivos bancos quedaran solamente para atención personalizada, ya que se puede realización transacciones financieras desde cualquier dispositivo móvil.

Con el aumento exponencial de la banca digital trajo consigo una disminución en el analfabetismo digital que se ha reducido en un porcentaje considerable, teniendo como referencia el año 2016 que existe un 11%. (El Comercio, 2018)

Cuando una empresa u organización necesita desarrollar un proyecto de aplicación móvil, orientada a compras o transacciones en línea. Necesita realizar él envió de confirmación de pago para lo cual se puede realizar de las siguientes formas:

Banca en línea (e-banking):

Es un servicio de las instituciones financieras, está disponible con el objetivo de facilitar a los usuarios realizar sus transacciones cotidianas por medio del internet. Entre sus beneficios tenemos que se puede ahorrar tiempo, pago se servicios y tarjetas de créditos, etc. (Banco Pichincha, 2018)

Dinero Electrónico:

Es un medio de pago electrónico, implementado por el banco central del Ecuador y que se utiliza a través de teléfonos celulares, sea dispositivo inteligente o normal. El dinero electrónico es un conjunto de operaciones y normativas que facilita el almacenamiento y transferencia en tiempo real, entre agentes económicos. (Auquilla, 2015). Sustituye al dinero físico y utiliza la red de telefónica celular. (SRI, 2018)

Con la ley de reactivación Económica, establecida por el gobierno ecuatoriano en el 2018. El dinero electrónico dejará de ser gestionada por el Banco Central y pasará a la administración de banca privada. Cerca de 408000 cuentas fueron cerradas, como se puede observar en la figura 15. se tiene los datos estadísticos de las activaciones de cuentas según rangos de edad. (El Universo, 2018)

Figura 15. *Estadística de activación de cuentas del dinero Electrónico*
Fuente: Banco Central del Ecuador

Tarjetas bancarias:

Corresponde a las tarjetas de crédito o débito, son herramientas emitidas por una institución financiera, que permiten al usuario realizar compras en tiendas físicas, virtuales, tanto nacional como internacionales. El establecimiento comercial necesita tener un terminal electrónico de pagos. (Sanca, 2013)

Pasarela de pago o TPV (Terminal Punto Venta):

Pasarela de pago es un término asociado a tarjeta de crédito, usado en internet. Es un método en el que se procesan y autorizan pagos de clientes. Además, son plataformas contratadas por una entidad financiera o empresas de seguridad de información. Las pasarelas de pagos son una porción de código que va anidado al código fuente de la aplicación a desarrollarse, utilizando funciones de validación de información, sistemas y protocolos de seguridad para así garantizar la transacción. (Cecarm, 2008)

Las pasarelas de pagos utilizan servidores seguros proporcionando autenticidad, confiabilidad, integridad. Utiliza protocolo SSL (Secure Socket Layer), con el fin de cifrar las tarjetas de crédito, datos sensibles, etc. Además, maneja normas de seguridad de transacción (SET), cuyo objetivo es proteger la información de usuario para que no exista manipulación durante la transferencia, autenticándolos con firmas digitales. Entre las más conocidas tenemos a PayPal, Stripe, kushkipagos, entre otros. (Filippi, 2013)

Funcionamiento:

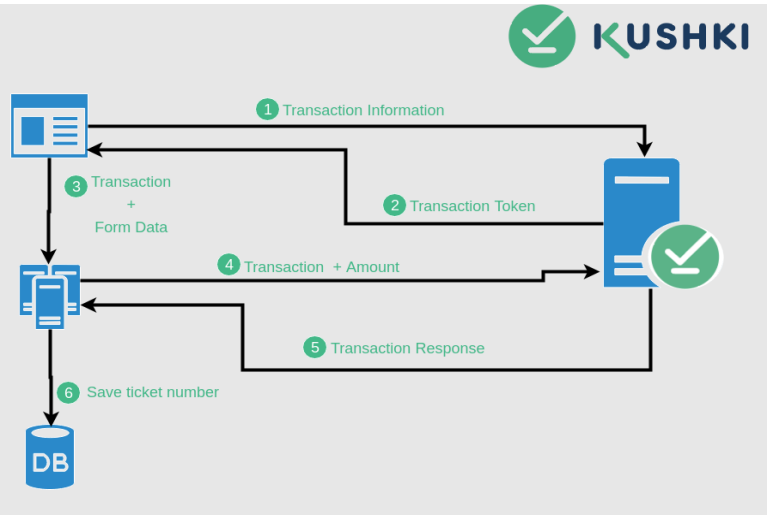


Figura 16. *Funcionamiento de la Pasarela de Pagos*
Fuente: www.kushkipagos.com

- Se integra el widget en el front-end (parte visible) de la aplicación de la organización por medio de un fragmento de código que se deberá añadir al código fuente de la aplicación.
- Se utiliza una biblioteca en el lado del back-end (servidor) de la organización, en el lenguaje de programación en el cual está desarrollado.
- El usuario de la aplicación ingresa los datos de su tarjeta de crédito y procede con el pago.
- La información de la tarjeta de crédito es encriptada y envidad vía HTTPS, a la empresa de pasarela de pago.
- Si la verificación es exitosa, se envía un Token valido solo para la mencionada transacción, la cual tiene un tiempo de expiración.
- En la cuenta contratada por la pasarela de pagos se puede verificar las transferencias realizadas.

La mayoría de aplicaciones de dispositivos móviles orientadas a compras en línea, sus desarrolladores utilizan el método pasarela de pagos debido a que las empresas que ofrece el mencionado servicio se encargan de la confiabilidad de manejo de transacciones financieras.

Para la aplicación de estudio, en lo que se refiere a las transacciones financieras en línea, Supercines maneja el estándar PCI- DSS, que es "un *estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS) fue desarrollado para alentar y mejorar la seguridad de los datos del titular de la tarjeta y facilitar la amplia adopción de medidas consistentes de seguridad de datos a nivel mundial. PCI DSS proporciona una línea base de requisitos técnicos y operativos diseñado para proteger los datos de la cuenta*" (Payment Card Industry (PCI) Data Security Standard, 2018). Sus consideraciones y criterios se indicarán en la propuesta del modelo.

3.3 **Funcionamiento del aplicativo:**

El procedimiento para realizar cualquier compra en línea es semejante al de Supercines:

1. Se escoge la ciudad o lugar en el cual se va a realizar la compra y el correspondiente producto, en este ejemplo, la película y la hora.

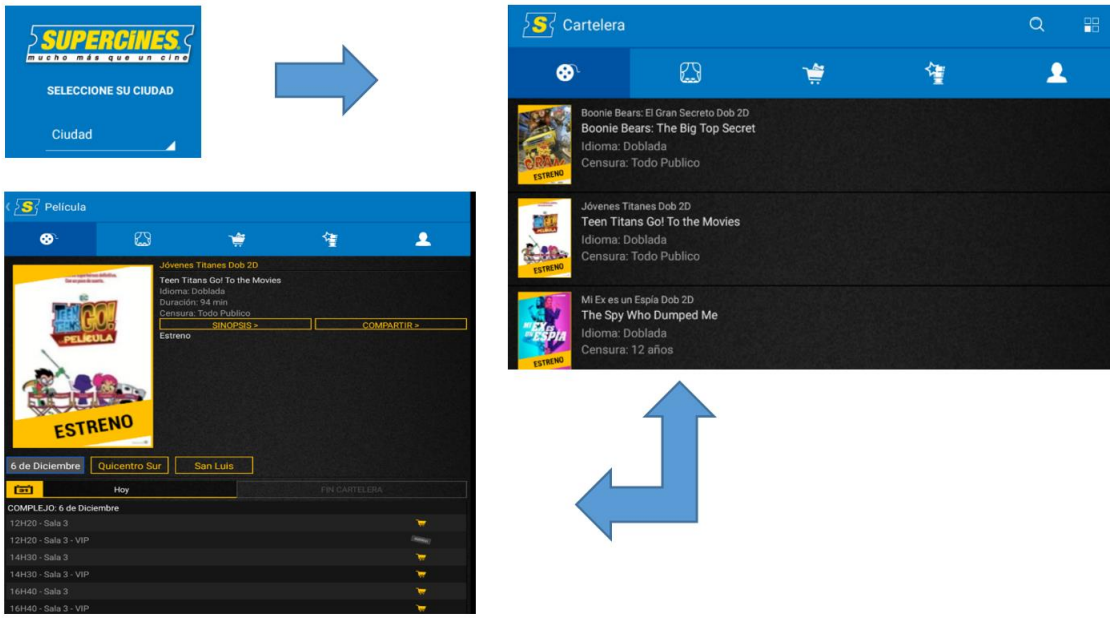


Figura 17. Ingreso y selección de producto en una aplicación móvil**.**
Fuente:www.supercines.com

2. Se procede con la autenticación de sesión, y especificamos el número de asientos que se va a realizar la compra.

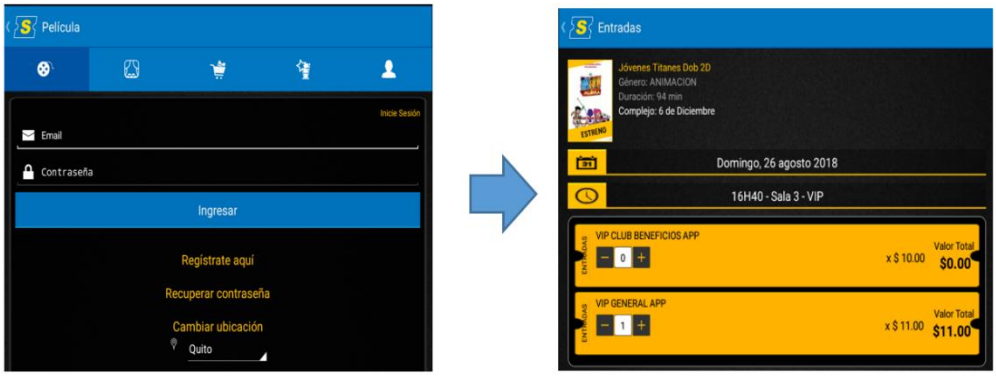


Figura 18. Autenticación para proceder al pago de producto
Fuente:www.supercines.com

3. Se selecciona el asiento en el establecimiento. Y finalmente ingresamos los datos de la tarjeta de crédito o débito que se va a utilizar en la transacción.

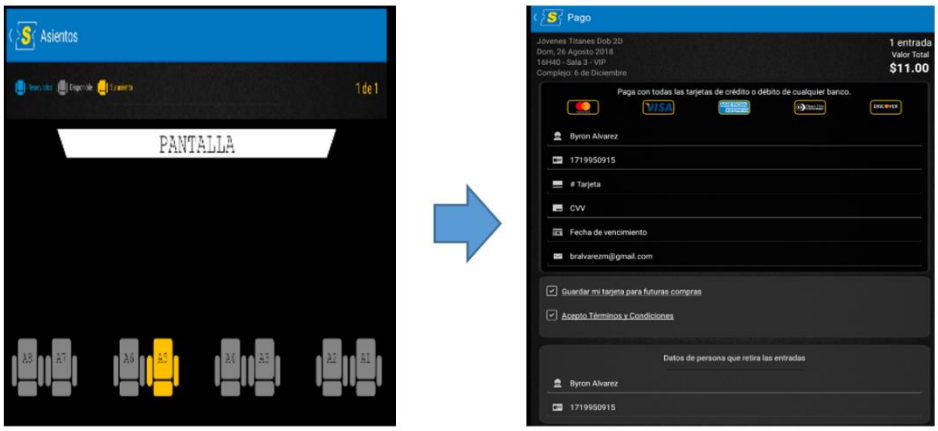


Figura 19. *Ingreso de datos de tarjeta de crédito*
Fuente:www.supercines.com

3.4 **Propuesta.**

El presente trabajo busca obtener una guía práctica de la implementación de la norma ISO/IEC 27034, en los procesos de Marco de Referencia Normativo de la Organización y Proceso de Gestión de Seguridad de la Aplicación.

Procedimiento

A continuación, se describe como se realiza el MRNO para las aplicaciones orientadas a compras en líneas, para lo cual tenemos los siguiente:

3.4.1 **Diseño del MRNO:**

Consiste en establecer los componentes del MRNO relacionados con la aplicación incluyendo el PGSA, librería CSA y todos los procesos relacionados:

3.4.1.1 **Contexto de Negocio:**

Para el objeto de estudio de este proyecto, el contexto de negocio de esta aplicación, es la de la comercialización de boletos de cinematografía, teniendo como objetivo es realizar la compra de forma segura del producto.

Este contexto de negocio varía según la misión de la organización. Con fines de estudio se utiliza la empresa Supercines, que tiene el siguiente contexto que es "Ofrecer la mejor selección de películas con tecnología de punta en imagen y sonido, además de brindar toda la comodidad, diversión y un servicio personalizado para todos nuestros clientes. Cumpliendo con los estándares de innovación que el mercado requiere, nuestra principal misión es lograr que la experiencia de ir al cine sea mucho más que un cine." (Supercines, 2018)

El contexto de negocio está disponible a través de combinaciones de políticas en toda organización, corporación o empresa, con políticas específicas de región, contexto técnico y de varios factores de mercado o de negocio dentro de la organización.

3.4.1.2 **Contexto Regulatorio:**

Cumplimiento con las regulaciones que se cubren por los procesos existentes de negocio. Las políticas deben ser analizadas por las unidades de negocio, asuntos legales y corporativos para asegurar que todos los aspectos de la creación y lanzamiento de software cumplan cualquier criterio legal o regulatorio, según la región en donde se desarrollara el aplicativo.

En el Ecuador en la constitución de la república, no manifiesta impedimentos ni regulaciones para la utilización de aplicaciones móviles en las organizaciones, se enfoca más el régimen general de telecomunicaciones (administrar, regular y controlar sectores estratégicos de telecomunicaciones) y la utilización del espectro radioeléctrico del Ecuador. (Asamblea Nacional, 2015). Las instituciones que rigen el contexto Regulatorio son:

Ministerio de Telecomunicaciones:

"Es el órgano rector del desarrollo de las tecnologías de la información y comunicación en el Ecuador, que incluyen las telecomunicaciones y el espectro radioeléctrico, que emite políticas, planes generales y realiza el seguimiento y evaluación de su implementación, coordinando acciones con los actores de los sectores estratégicos para garantizar el acceso igualitario a los servicios y promover su uso efectivo, eficiente y eficaz, que asegure el avance hacia la sociedad de la información para el buen vivir de la población ecuatoriana." (Ministerio de Telecomunicaciones y de la sociedad de la información, s.f.)

ARCOTEL:

"Regula el uso del espectro radioeléctrico y los servicios de telecomunicaciones con la finalidad de garantizar el derecho de acceso a servicios de calidad, convergentes, con precios y tarifas equitativas; gestionar los recursos inherentes a las telecomunicaciones mediante su asignación transparente, equitativa, eficiente y ambientalmente sostenible; controlar el uso del espectro radioeléctrico, y la prestación de servicios de telecomunicaciones con calidad, universalidad, accesibilidad, continuidad, seguridad en las comunicaciones y protección de datos personales." (ARCOTEL, s.f.)

En ambas instituciones y en la ley Orgánica de telecomunicaciones, aprobada en febrero del 2015, no ponen en consideración o regulación el desarrollo de aplicaciones móviles. Pero debemos tomar en cuenta la utilización de datos que genera la aplicación, dicha información es manejada por las empresas de telefonía móvil e internet.

Existe la ley de Comercio Electrónico, firmas electrónicas y mensajes de texto. La cual menciona que un mensaje de texto, tiene la misma validez que un documento físico, esto en el ámbito jurídico. Mas no en el ámbito de protocolos de seguridades. (Congreso Nacional, 2002)

3.4.1.3 **Repositorio de especificaciones de la aplicación:**

Estas especificaciones consisten tanto de una guía funcional como una guía tecnológica. Creando políticas para componentes y otras tecnologías que tienen un contexto de seguridad.

3.4.1.4 **Contexto Tecnológico:**

Esto varía según las unidades de negocio. y se depende de combinación de factores de mercado. Concluyendo un contexto tecnológico se fija de forma independiente por cada unidad de negocio para cumplir las necesidades con el fin cumplir los criterios de seguridad y privacidad fijados en el contexto de negocio.

3.4.1.5 **Roles y Responsabilidades:**

Según las unidades de negocio se especifica las categorías laborales con respecto a las competencias de seguridad y privacidad para la delegación de responsabilidades. Estas actividades deben ser creadas y dirigidas por Recursos Humanos en las organizaciones. Cada una de las especificaciones, tareas y roles se especificación antes de la etapa de desarrollo del proyecto.

Roles de Supervisión:

Proporciona la vigilancia tanto cualitativa como cuantitativa al proyecto con el fin de manejar los niveles mínimos aceptables de seguridad y privacidad para un proyecto de software.

- **Asesor de Seguridad**: Experto en la materia de seguridad, ajeno al proyecto u organización, puede ser conformado por un grupo de personas calificadas o por medio de servicios de expertos externos y debe ocupar los siguientes roles:
- **Auditor**: Supervisa cada fase del proceso de seguridad, debe dar cumplimiento exitoso a cada requisito. Da el cumplimento o no de los requisitos de seguridad previamente establecidos.
- **Experto**: Persona elegida como tutor de seguridad, debe tener experiencia en el tema.
- **Asesor de privacidad**: Experto en la materia de privacidad, ajeno al proyecto y organización. Conformado por uno o grupo de personas o por expertos externos. Cumpliendo los siguientes roles:
- **Auditor**: Supervisa cada fase del proyecto del desarrollo de la privacidad, dando cumplimiento o no de los requisitos previamente establecidos.
- **Experto**: Persona elegida para el rol de privacidad, debería tener experiencia en temas de privacidad.

El rol del asesor de seguridad puede ser combinado con el de privacidad, asumiendo que un individuo posea las habilidades y experiencia apropiadas.

- **Roles de Líder de Equipo**: Expertos en la materia que representan a todo el equipo de desarrollo del proyecto tomando las decisiones durante el tiempo que dure el proyecto en desarrollarse. Además, es responsable de negociaciones, aceptaciones y seguimientos de los requisitos de seguridad.
- **Líder de equipo de Seguridad y privacidad**: Persona o grupo de personas que no tienen la responsabilidad de asegurar que la aplicación haya abordados los asuntos de seguridad o privacidad. Pero debe garantizar la coordinación y seguimiento de los asuntos de seguridad o privacidad del proyecto. Además, debe de reportar a los asesores en el proyecto. Una sola persona o grupo puede ser líder de seguridad y privacidad siempre y cuando posea experiencia y habilidades en la misma, caso contrario se debería designar funciones por separado.

Cada rol descrito anteriormente debe aplicarse y documentarse en las organizaciones, hayan o no desarrollado la aplicación móvil. Por tanto, se sugiere establecer los roles y tareas para la administración eficaz del producto adquirido por subcontratación o terceros.

3.4.1.6 Librería CSA de la organización.

El modelo de seguridades que se propone en el proyecto de titulación, es el siguiente:

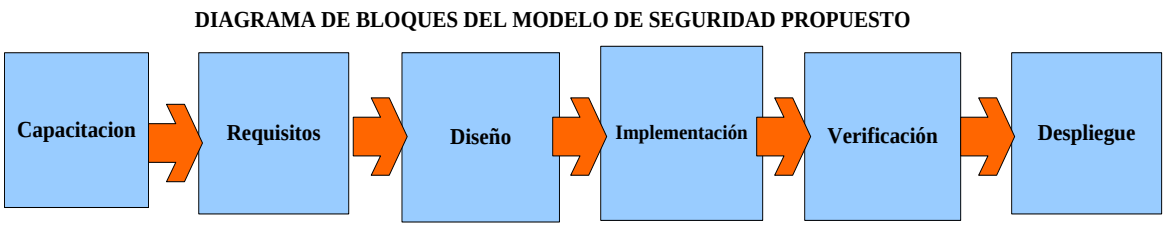


Figura 20. Diagrama de bloques del Modelo de seguridad de la aplicación

Veinte CSA se han identificado parte del proceso para la implementación de aplicaciones móviles orientadas a compras en línea. A continuación, se describe cada uno de los bloques con sus respectivas tareas o controles tanto obligatorias como opcionales. Las tareas opcionales se pueden agregar dependiendo del contexto de negocio hacia cual va dirigido la aplicación, con el objetivo de cumplir los objetivos deseados de seguridad y privacidad.

CAPACITACIÓN

1. **Capacitación**:

Es necesario tener al personal de una organización capacitados en aspectos básicos de seguridad. La seguridad de la información es una actividad que se debe llevar periódicamente en una organización con el fin de socializar, fomentar y concientizar aspectos básicos de seguridades de la información para evitar posibles incorrectas utilizaciones de aplicaciones, por desconocimiento o simplemente por travesura. Se debe tener énfasis en las capacitaciones de los miembros de los equipos de desarrollo de la aplicación o software, sobre elementos de seguridad y tendencias recientes de privacidad. Teniendo una capacitación mínima de una vez al ano cubriendo mínimamente los temas de diseño seguro, modelado de amenazas, vulnerabilidades, codificación segura, pruebas y privacidad, entre otros temas.

REQUISITOS

2. Requisitos de seguridad:

Las aplicaciones deben ser protegidas contra las vulnerabilidades que pueden ser propias de la misma aplicación como defectos del programa. O las que aparecen durante su ciclo de vida (cambios de aplicación o actualizaciones). Para cubrir la necesidad descrita anteriormente desde

un punto de vista más óptimo debemos acordar los requisitos de confiabilidad para el proyecto, esto se dará durante las etapas iniciales de planificaron del proyecto, lo que permitirá al equipo de desarrollo identificar los puntos clave y entregables que permitan la integración de seguridad y privacidad.

El análisis de requisitos de seguridad y privacidad se realiza al inicio de proyecto, teniendo en cuenta varios aspectos como determinación de personas responsables de control de acceso, seguridad mínima, especificación y despliegue de un sistema de seguimiento de vulnerabilidades.

3. Nivel de Confianza Objetivo de la Aplicación:

Utilizado para definir o establecer los niveles mínimos aceptables de seguridad y calidad de privacidad que tiene una aplicación. Estos criterios se deber realizar al inicio de proyecto con el fin de mejorar la comprensión de riesgos que son involucrado con asuntos de seguridad. Esto ayuda a identificar los errores durante el desarrollo. El equipo de proyecto debe negociar con el asesor de seguridad, el nivel de confianza para cada una de las fases de desarrollo. El nivel de confianza es una puerta de calidad que se aplica a cualquier proyecto de software, ayuda a definir lo límites de gravedad de los errores de seguridad. Siempre debe estar presente así se haya lanzado o finalizado el proyecto o aplicación.

4. Evaluación del Riesgo de Seguridad y Privacidad:

Procesos obligatorios para identificar la funcionalidad de la aplicación que podrían requerir una profunda inspección para su análisis. Es procedente realizar evaluaciones simples como primera consideración de riesgo y luego expandir según los requerimientos que se hayan establecido. Debería incluir:

a) ¿Qué porciones del proyecto requerirán las revisiones del diseño de seguridad antes del lanzamiento?

b) ¿Qué porciones del proyecto requerirán las pruebas de penetración ejecutadas por un proyecto netamente acordado que sea externo al equipo de proyecto? Cualquier porción del proyecto que requiera de pruebas de penetración debería resolver los problemas idénticos durante las pruebas de penetración antes de que se apruebe para el lanzamiento.

c) Cualquier requisito adicional de prueba o análisis que el asesor de seguridad considera como necesario para mitigar los riesgos de seguridad.

d) Determinación del Impacto de Privacidad.

a. P1- Riesgo Alto de Privacidad: La característica, producto o servicio almacena o transfiere la información Personalmente Identificable

b. P-2 Riesgo Moderado de Privacidad: una única trasferencia de datos anónimos iniciada por un usuario.

c. P3- Riesgo Bajo de Privacidad: Ningún dato anónimo o personal es transferido, ninguna información es almacenada en la máquina, ninguna configuración se cambia en el perfil del usuario, y ningún software es instalado.

DISEÑO

5. Requisitos de Diseño:

En el inicio del ciclo de vida de la aplicación, es el momento idóneo para realizar un diseño que mantenga una confianza aceptable.

- Se tiene que considerar los problemas de seguridad y privacidad durante la fase de diseño.
- Realizar una investigación profunda de problemas de seguridad y privacidad, ya que es menos costosa cuando se realiza durante el inicio de una etapa de un ciclo de vida de una aplicación.
- El equipo del proyecto debe implementar características seguras que son definidas como elementos cuya funcionalidad está bien diseñada con respecto a la seguridad, validadas rigurosamente a todo su dato antes del procesamiento o implementación de la misma, en forma criptográfica de las librerías o servicios.
- En el diseño debemos tener en cuenta algunas especificaciones funcionales que describen características de seguridad tales como:
  a) Describir de forma precisa y completa como implementar estas características
  b) Describir cómo implementar de forma segura todas las funcionalidades habilitadas por una característica determinada.
  c) Describir cómo desplegar la característica de una manera segura.
- Dentro de los requisitos de diseño debe contiene algunas tareas como: revisión del diseño de seguridad, la revisión y especificación del diseño de privacidad y la implementación de los requisitos del diseño mínimo criptográfico. Teniendo en cuenta que no solo se puede limitar a las expuestas.

6. <u>Reducción de la superficie de ataque:</u>

Medición para reducir el riesgo, con el fin de que el atacante tenga menos posibilidades de encontrar una vulnerabilidad. Para minimizar el campo de ataque se tiene que emplear defensas por capas, restricción de acceso a los servicios de sistemas y aplicar mínimos privilegios mientras se contrarresta un ataque.

7. **Modelado de Amenazas:**

Proceso obligatorio realizado durante la fase de diseño en donde los equipos de proyecto puedan considerar, documentar y debatir las consideraciones de seguridad de los diseños en forma estructurada. Este es un ejercicio que interviene la dirección de proyecto, desarrolladores y representa la primera acción para analizar la seguridad realizada durante la etapa de diseño.

IMPLEMENTACIÓN

8. **Herramienta Aprobada de uso:**

El equipo de desarrollo debe publicar una lista de herramientas aprobadas por el Gerente y equipo de desarrollo. Las mismas que deben estar en su última versión, para ser utilizadas y aprovechadas con sus funcionalidades en la ejecución de la aplicación.

9. **Funciones Integradas Desaprobada:**

El equipo de proyecto y desarrollo debe analizar todas las funciones y API que se utilizaran y prohibir las inseguras. Verificando la existencia de funciones prohibidas y reemplazar por alternativa más seguras.

10. **Análisis Estadístico:**

Consiste en verificación del código fuente. Este análisis proporciona una solución escalable para revisión del código y se puede usar para asegurar que las políticas de codificación aceptadas por el equipo de proyecto, sigan. Un análisis estático no es suficiente para revisión de seguridades.

VERIFICACIÓN

11. Análisis de Software Dinámico:

El tiempo de ejecución de una aplicación es una consideración necesaria para realizar un análisis de diseño de la misma. El análisis dinámico funciona operando un programa manejando parámetros de entrada y verificando el comportamiento en tiempo de ejecución. Es poco probable que con este tipo de análisis proporcione una cobertura completa.

12. Debilidades Comunes Enumeradas(CWE):

Es una lista desarrollada por un proyecto comunitario con el fin de entender las debilidades y defectos de software con el fin de crear herramientas automatizadas para ser utilizada para la identificación, mitigación, corrección y prevención de estos defectos. (MITRE Corporation, 2018)

13. Vulnerabilidades Comunes Expuestas:

Esquema de nombres para las vulnerabilidades de seguridad conocidas, para el conocimiento público de vulnerabilidades. Estas entradas son usadas por servicios de ciberseguridad de todo el mundo incluyendo la base de datos nacional de vulnerabilidades(NVD). (MITRE Corporation, 2018)

14. Sistema Común de Puntuaciones de Vulnerabilidades (CVSS):

El modelo CVSS intenta garantizar un medición repetible y precisa. Utiliza un algoritmo para calcular los puntajes y se puede utilizar ese puntaje para estimar el impacto de las vulnerabilidades sobre la aplicación. El objetivo según su fuente oficial es “proporcionar una forma de capturar las características principales de una vulnerabilidad y producir una puntuación numérica que refleje

su gravedad. El puntaje numérico puede traducirse en una representación cualitativa (como baja, media, alta y crítica) para ayudar a las organizaciones a evaluar y priorizar adecuadamente sus procesos de gestión de vulnerabilidad." (Common Vulnerability Scoring System SIG, s.f.)

15. Pruebas de Fuzz:

Las pruebas Fuzz se utilizan para inducir fallas del software mediante la inyección deliberada de datos con formatos incorrectos o aleatorios automatizados en las entradas de una aplicación.

16. Modelo de Amenazas/Revisión de la Superficie de Ataque:

Esta revisión asegurara que cualquier cambio en el sistema se haya detectado y cualquier dirección de ataque nuevo haya sido revisado y mitigado.

17. Revisión Manual del Código:

Se realiza normalmente por el equipo de seguridad de la aplicación por la recomendación del asesor de seguridad. La revisión manual del código se centra normalmente en los componentes "críticos" de una aplicación. Más a menudo, esta se utiliza cuando los datos sensibles tales como la información personalmente identificable están involucrados.

DESPLIEGUE:

18. Plan de Respuestas a Incidentes:

Cada consideración del software está sujeta a los requisitos de la aplicación y debe incluir un plan de respuesta a incidentes. Incluso una aplicación sin vulnerabilidades conocidas al momento del lanzamiento, puede estar sujeto a nuevas amenazas que surgen con el tiempo. El plan de respuesta de incidentes debería incluir como mínimo:

a) Un equipo de ingeniería de soporte. Si el equipo es demasiado pequeño se tiene que designar de tres hasta cinco miembros del personal de ingeniería, de tres hasta cinco miembros del personal de comunicaciones de mercado y cliente, para que actúen como los puntos de primer contacto en una emergencia de seguridad.
b) Disponibilidad 24 x 7 x 365.
c) Los planes de servicio de seguridad para el código heredado de otros grupos dentro de la organización
d) Los planes de servicio de seguridad para el código incluyendo los nombres del archivo, las versiones, el código fuente, la información de contacto de la tercera parte y el permiso contractual para hacer cambios.

19. Revisión final de Seguridad (Nivel de Confianza Real):

Se realiza por el asesor de seguridad con la asistencia del personal regular de desarrollo y los líderes del equipo de seguridad y privacidad. Consiste en evaluar las consideraciones de las actividades de seguridad, antes de su lanzamiento. No es la oportunidad de realizar actividades olvidadas o ignoradas. Incluye rendimiento de herramientas contra errores previamente determinados. Teniendo como resultado:

Aprobada: Consideraciones de seguridad y privacidad identificadas son arregladas

Aprobada con excepciones: Consideraciones de seguridad que no se puedan abordar son registradas y corregidas en el siguiente despliegue.

Rechazada: Si no cumple con todos los requisitos y consideraciones para alcanzar un nivel aceptable.

20. <u>Despliegue / Archivo:</u>

Condicionada por la finalización de la aplicación. Los asesores deben certificar que el equipo de proyecto ha cumplido los requisitos de seguridad y privacidad. Toda la información, datos, especificaciones, código fuente, planes de respuesta a emergencia se debe archivar para poder realizar tareas posteriores al lanzamiento.

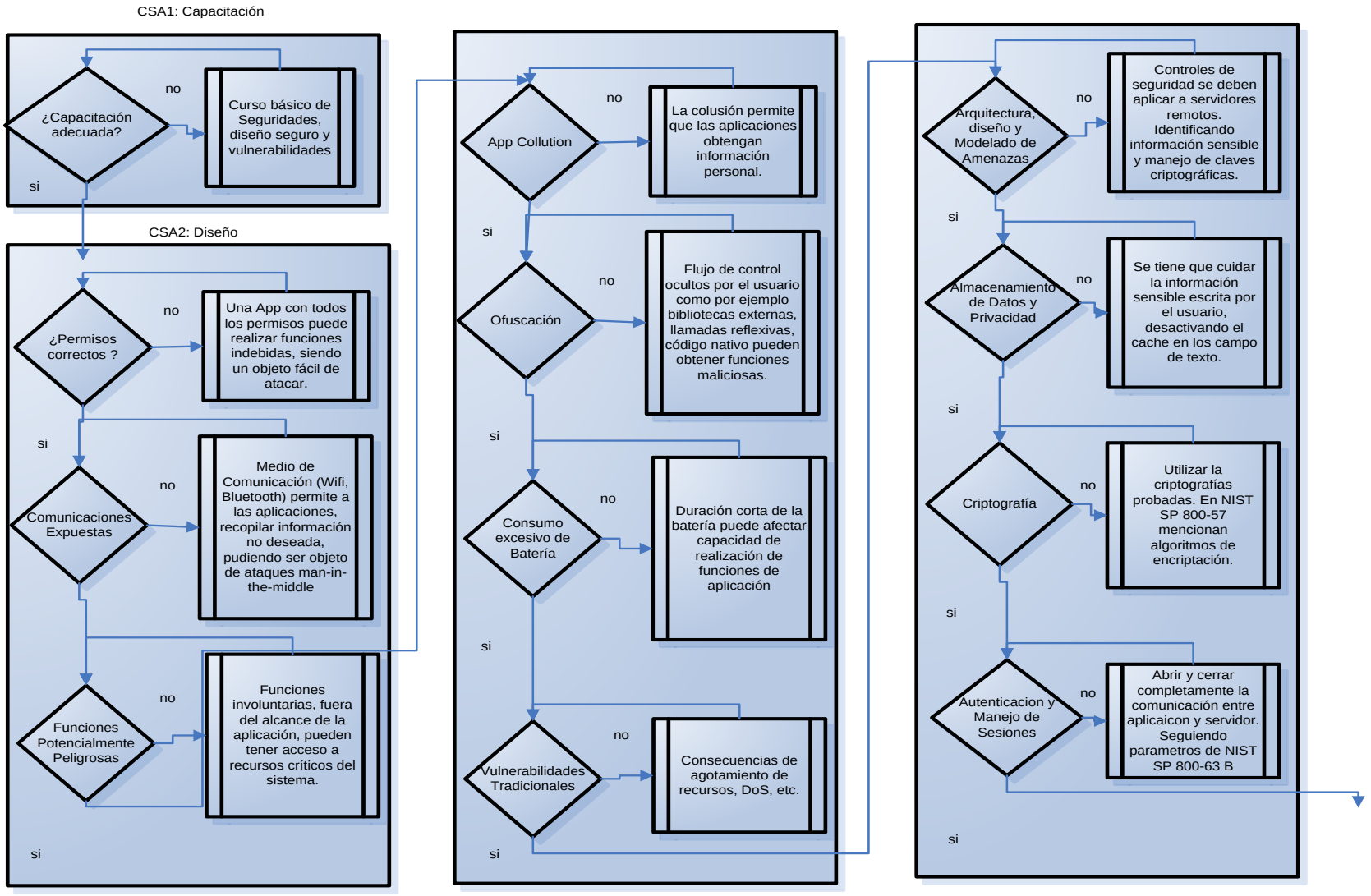
AUDITORIA:

Consiste en medir el nivel de confianza actual:

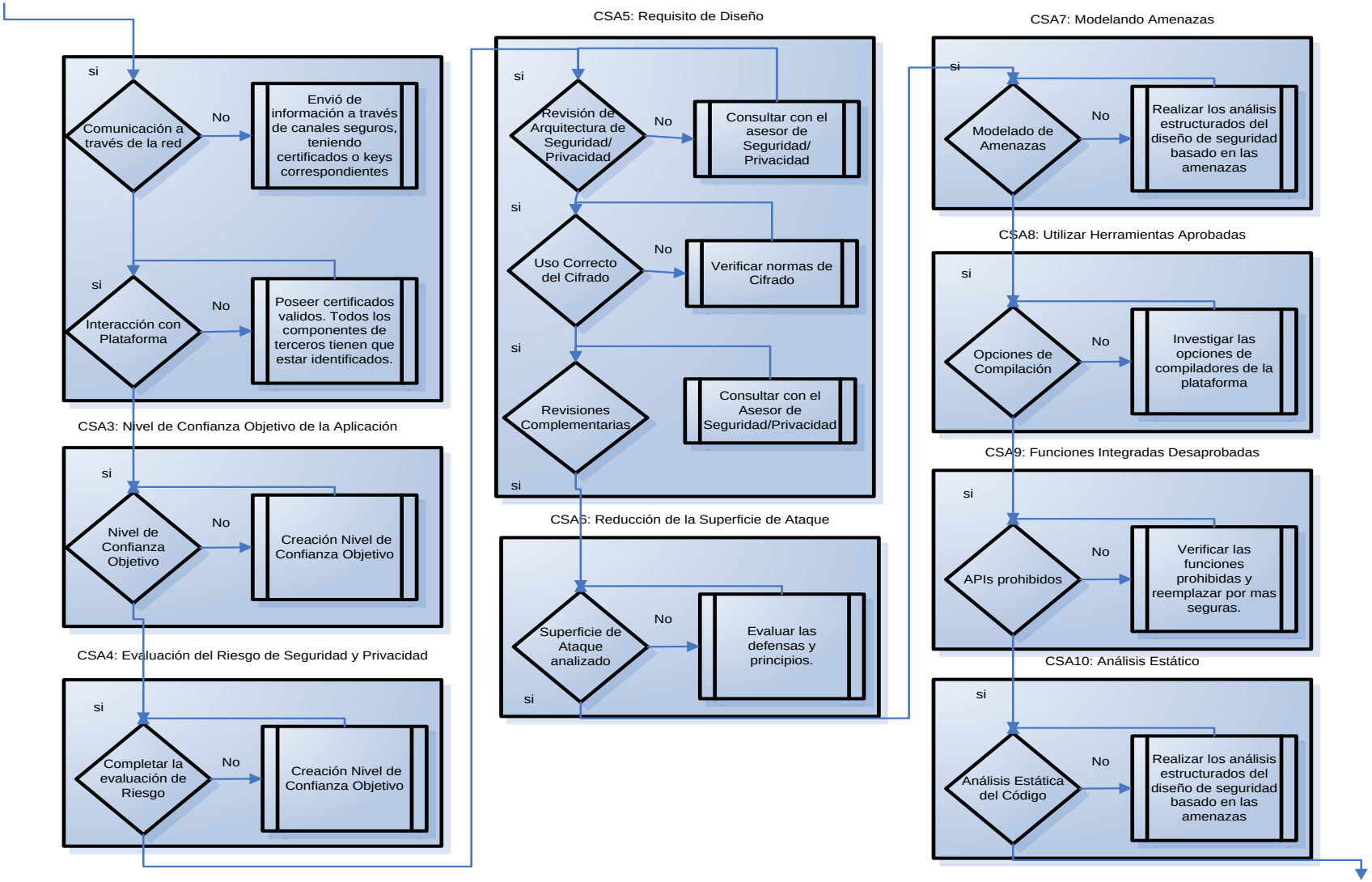
- Se debe realizar un seguimiento al cumplimiento de las consideraciones de diseño.
- Un líder de equipo de seguridad y privacidad son responsables de asegurar que los datos necesarios para una valoración sean categorizados e introducidos en la aplicación de seguimiento.
- La información de la aplicación es utilizada por los asesores de seguridad y privacidad para la revisión final de seguridad
- Los asesores de seguridad y privacidad son responsables de revisar los datos introducidos en la aplicación de seguimiento.

MODELO DE CICLO DE VIDA DE LA APLICACIÓN

Es utilizado para mapear todas las actividades seguras de la aplicación. Se puede visualizar en el siguiente diagrama no exhaustivo, una visualización de controles de seguridad de la aplicación utilizados en un proyecto hipotético. Teniendo en cuenta que se pueden agregar más tareas de seguridad y privacidad, específicas para otros proyectos a implementar.


CSA1: Capacitación
¿Capacitación adecuada?
no
Curso básico de Seguridades, diseño seguro y vulnerabilidades
si
CSA2: Diseño
¿Permisos correctos ?
no
Una App con todos los permisos puede realizar funciones indebidas, siendo un objeto fácil de atacar.
si
Comunicaciones Expuestas
no
Medio de Comunicación (Wifi, Bluetooth) permite a las aplicaciones, recopilar información no deseada, pudiendo ser objeto de ataques man-in-the-middle
Funciones Potencialmente Peligrosas
no
Funciones involuntarias, fuera del alcance de la aplicación, pueden tener acceso a recursos críticos del sistema.
si
App Collution
no
La colusión permite que las aplicaciones obtengan información personal.
si
Ofuscación
no
Flujo de control ocultos por el usuario como por ejemplo bibliotecas externas, llamadas reflexivas, código nativo pueden obtener funciones maliciosas.
si
Consumo excesivo de Batería
no
Duración corta de la batería puede afectar capacidad de realización de funciones de aplicación
si
Vulnerabilidades Tradicionales
no
Consecuencias de agotamiento de recursos, DoS, etc.
si
Arquitectura, diseño y Modelado de Amenazas
no
Controles de seguridad se deben aplicar a servidores remotos. Identificando información sensible y manejo de claves criptográficas.
si
Almacenamiento de Datos y Privacidad
no
Se tiene que cuidar la información sensible escrita por el usuario, desactivando el cache en los campo de texto.
si
Criptografía
no
Utilizar la criptografías probadas. En NIST SP 800-57 mencionan algoritmos de encriptación.
si
Autenticacion y Manejo de Sesiones
no
Abrir y cerrar completamente la comunicación entre aplicaicon y servidor. Seguiendo parametros de NIST SP 800-63 B
si

CONTINÚA


si
Comunicación a través de la red
No
Envió de información a través de canales seguros, teniendo certificados o keys correspondientes
si
Interacción con Plataforma
No
Poseer certificados validos. Todos los componentes de terceros tienen que estar identificados.
CSA3: Nivel de Confianza Objetivo de la Aplicación
si
Nivel de Confianza Objetivo
No
Creación Nivel de Confianza Objetivo
CSA4: Evaluación del Riesgo de Seguridad y Privacidad
si
Completar la evaluación de Riesgo
No
Creación Nivel de Confianza Objetivo
CSA5: Requisito de Diseño
si
Revisión de Arquitectura de Seguridad/ Privacidad
No
Consultar con el asesor de Seguridad/ Privacidad
si
Uso Correcto del Cifrado
No
Verificar normas de Cifrado
si
Revisiones Complementarias
Consultar con el Asesor de Seguridad/Privacidad
si
CSA6: Reducción de la Superficie de Ataque
Superficie de Ataque analizado
No
Evaluar las defensas y principios.
si
CSA7: Modelando Amenazas
si
Modelado de Amenazas
No
Realizar los análisis estructurados del diseño de seguridad basado en las amenazas
CSA8: Utilizar Herramientas Aprobadas
si
Opciones de Compilación
No
Investigar las opciones de compiladores de la plataforma
CSA9: Funciones Integradas Desaprobadas
si
APIs prohibidos
No
Verificar las funciones prohibidas y reemplazar por mas seguras.
CSA10: Análisis Estático
si
Análisis Estática del Código
No
Realizar los análisis estructurados del diseño de seguridad basado en las amenazas

CONTINÚA

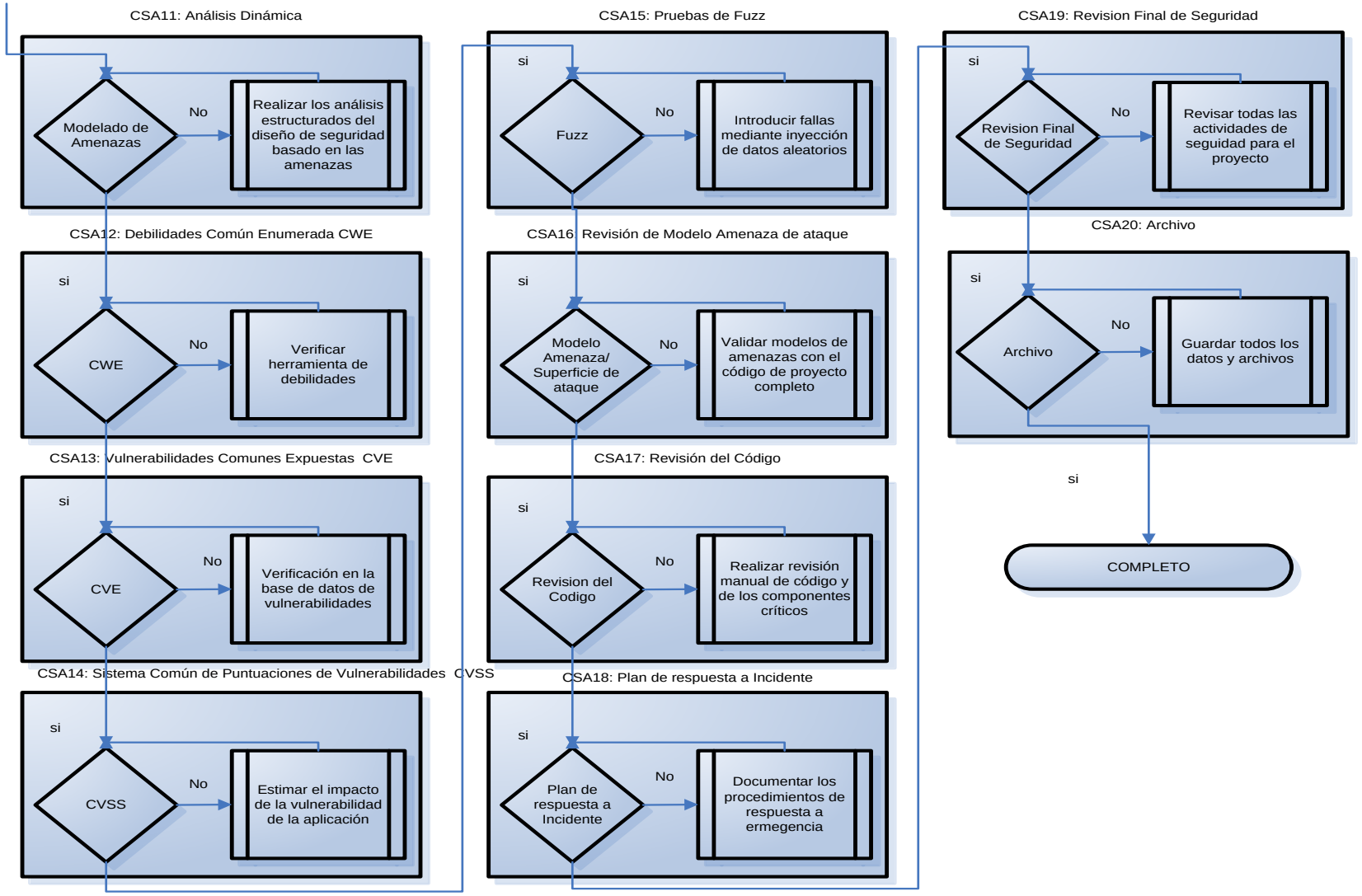
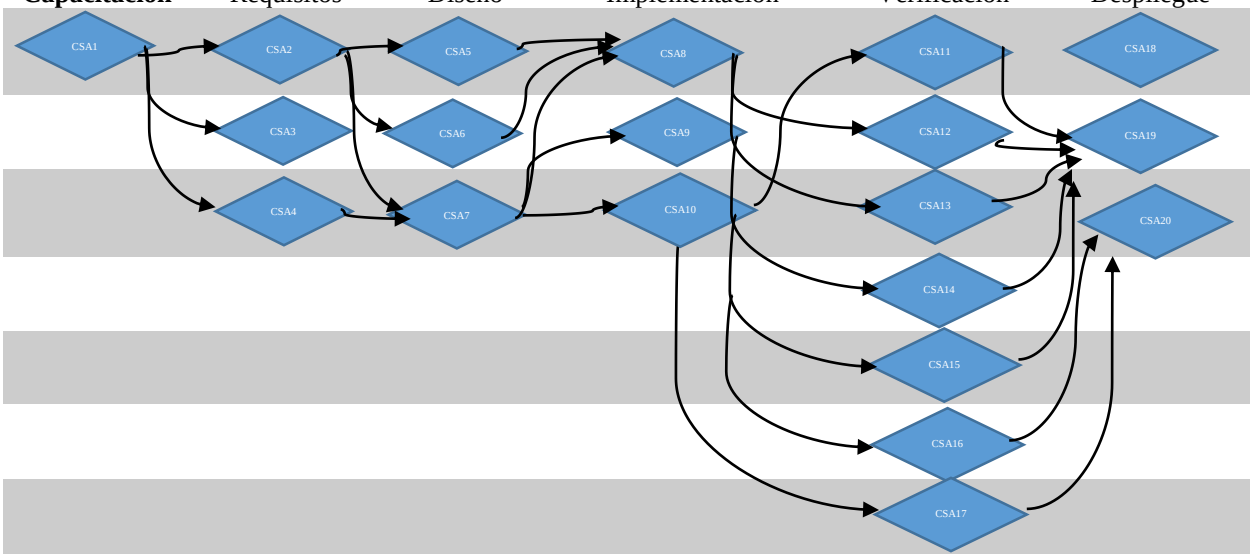


Figura 21 Propuesta de Control de Seguridad de la Aplicación para aplicaciones móviles.

Como se puede observar en la figura 21. Se tiene todos los controles de seguridad para aplicaciones móviles, teniendo en cuenta que se pueden aplicar muchos más dependiendo del entorno en el que se desempeña la organización. Cada CSA está separada por niveles de confianza de la aplicación, la misma que indica que tan confiable es la aplicación móvil. Teniendo en cuenta que el nivel de confianza cero (0), no significa que es insegura, sino que es el nivel base en el cual se va a realizar las consideraciones pertinentes de la aplicación. A continuación, se puede observar la clasificación de los CSA por niveles de Confianza

Tabla 7.
Librería de Control de Seguridades de Aplicación.

Librería CSA de la Organización					
Niveles de Confianza de la aplicación utilizada por la organización					
0	1	2	3	4	5
Capacitación	Requisitos	Diseño	Implementación	Verificación	Despliegue



Dentro de cada CSA se puede tener en cuenta algunos criterios los cuales ayudaran a cumplir cada uno de los Controles de forma eficiente. Los mismos que basados en algunos estándares publicados en NIST (National Institute Standars and Technology), se propone las siguientes consideraciones a tomar en cuenta:

Tabla 8.
Consideraciones de Arquitectura y Diseño para desarrollo de aplicaciones móviles

	Consideración	SI	NO
1	Los componentes TI se encuentran con su respectiva etiqueta y asegurados físicamente.		
2	Controles de Seguridad aplicados tanto en el lado de cliente como en sus respectivos servidores remotos.		
3	Se incluyeron controles de Seguridad en la arquitectura de alto nivel, previamente definida		
4	Se definió cual es la información crítica de alta sensibilidad manejada por la aplicación móvil.		
5	Los componentes de la aplicación están identificadas en el contexto de negocio de la organización.		
6	Se consideró plantear los modelos de amenazas y servicios con sus respectivas contramedidas.		
7	Los CSA se administran de forma centralizadas		
8	Hay política de manejo criptográfico de la información		
9	Se especifica la forma de actualización de la aplicación en móvil		
10	Se realiza mantenimiento de seguridad en el ciclo de vida de la aplicación		

Fuente: (Muller & Scheleier, 2018).

Tabla 9.
Consideraciones para el almacenamiento de datos y privacidad

	Consideración	**SI**	**NO**
1	Credenciales del sistema son utilizadas como almacenamiento de información sensible de usuario y claves criptográficas		
2	No se escribe información sensible en los registros de la aplicación		
3	No se debe compartir información sensible de servicios externos		
4	Desactivación de cache de teclado en los campos de texto		
5	Desactivación de portapapeles, para evitar envió de información sensible		
6	No se debe exponer información sensible como contraseñas y número de tarjetas de crédito a través de interfaz.		
7	No se incluye información de respaldos generados por Sistema Operativo		
8	Remover toda información sensible, cuando se ejecuta la aplicación en segundo plano.		
9	No conservar información sensible en la memoria tras él envió de la misma.		
10	Aplicación debe exigir política mínima de seguridad al usuario		
11	Aplicación capacita al usuario sobre la información personal que procesa.		
12	Protección de copias almacenadas en el servidor.		

Fuente: (Meucci & Muller, 2014)

Criptografía:

Es un papel muy importante en el ámbito de seguridad de datos de usuario. El objetivo de la criptografía es proporcionar confidencialidad, integridad y autenticidad. Los algoritmos de cifrado (codificar y decodificar datos), consiste en convertir los todos de texto plano a texto cifrado ocultando el contenido original. Existe de forma simétrica (clave secreta) y asimétrica (Clave pública).

Los algoritmos de cifrado de clave simétrica utilizan la misma clave tanto en origen y destino de la conexión. Es un cifrado rápido y necesita un manejo adecuado de las claves. Los algoritmos asimétricos utilizan dos llaves, una privada y una pública. La publica se puede compartir libremente mientras que la privada se reserva. En este tipo de encriptación un mensaje con clave pública solo se puede descifrar con clave privada.

Para la verificación de integridad de cifrado mapeando los datos de forma arbitraria, a esto se lo conoce como hashing. Este método no proporción garantía de autenticidad.

Cuando se intercambian mensajes se utilizan códigos de autenticación denominados MAC, que combinan a códigos criptográficos con claves secretas con el objetivo de proporcionar protección de integridad como autenticidad, entre los más comunes tenemos el HMAC-SHA256, que utiliza SHA-256 como función de hashing.

Otro tipo de cifrado asimétrico son las firmas, que manejan un par de claves una publica y una privada con hashing, lo que diferencia con MAC es que la clave privada se utiliza en cuando firma los datos. Además, se tiene funciones de derivación de clave KDF, semejantes a las funciones de hashing para aumentar su longitud.

Cuando se desarrolla una aplicación móvil, se debe tener la certeza de que no utilice algoritmos criptográficos que tengan debilidades importantes. Los algoritmos que consideramos seguros en la actualidad, al cabo de poco tiempo pueden no serlo, por lo tanto, es importante controlar periódicamente los mejores estándares de la industria para encriptación. Para elegir un correcto algoritmo para el desarrollo de aplicaciones móviles tenemos que verificar que sean aprobados o certificados por NIST y que estén actualizados. Recordando que una certificación no reemplaza la verificación de un algoritmo.

Se recomienda los siguientes algoritmos que son certificados y actualizados, son los siguientes:

- Confidencialidad: AES-GCM-256 o ChaCha20-Poly1305
- Integridad: SHA-256, SHA-394, SHA-512, Blake2
- Firma Digital: RSA, DH (ambos de 3072 bits en adelante), ECDSA P384
- Clave de Establecimiento: RSA, DH, ECCDH con p384. (NIST Special Publication 800-57, 2016), (BlueKrypt, 2018)

Problemas Comunes:

Longitud de clave insuficiente: Se debe tener la certeza que el algoritmo cumpla con los estándares de la industria

Encriptación Simétrica con claves criptográficas codificadas: No se debe almacenar las claves secretas en el mismo lugar de datos cifrados. Esto es un error común debido a que los desarrolladores almacenan todo su código en un mismo archivo o carpeta. Por lo tanto, lo que se tiene que hacer es asegurar que la clave o llave no este almacenada dentro del código fuente.

Funciones de generación de claves débiles: esto se da cuan un usuario genera la contraseña, si esta es más pequeña que la clave, para evitar estos problemas se debe asegurar que la contraseña pase por un proceso criptográfico.

Implementación personalizada de criptografía: Sucede cuando se crea desde cero un algoritmo criptográfico, por lo tanto, se recomienda usar algoritmos conocidas seguros para desde ahí partir con la personalización del algoritmo, tenido en cuenta las recomendaciones criptográficas de Android e IOS.

Configuración de AES inadecuada: Advanced Encryption Standard (AES), es el estándar más aceptado para el cifrado de aplicaciones móviles. Se basa en operaciones matemáticas, simulando entradas, las cuales utiliza una clave derivada de la original. (Elenkov, 2014)

Tabla 10.
Consideraciones de Criptografía para Aplicaciones Móviles

	Consideración	SI	NO
1	Sebe utilizar implementaciones de criptografías probadas		
2	Utilizar mejores prácticas de seguridad		
3	No utilizar algoritmos criptográficos depreciados o no actuales		
4	No utilizar una misma llave criptográfica para todos los procesos		
5	Aislar procesos criptográficos.		

Fuente: (NIST Special Publication 800-57, 2016), (NIST Special Publication 800-107, 2012), (NIST 800-131A Revision 1, 2015), (NIST Special Publication 800-132, 2010)

Tabla 11.
Consideraciones para Autenticación y Manejo de Sesiones

	Consideración	SI	NO
1	Autenticación de usuario y contraseña en servidor remoto		
2	Verificar que los controles de autenticación se realice por el servidor		
3	Verificar que los usuarios y contraseñas no sean generado por software generadores de frases o claves.		
4	El registro de usuario debe ser resistente a ataques.		
5	Cambio de contraseña debe de ser diferente a la actual, no manejar componentes por defecto.		
6	Implementar funcionalidades de recuperación de contraseña.		
7	Usar Tokens en servidor remoto con el fin de evitar Envio de credenciales de usuario		
8	Token debe estar firmado usando algoritmo seguro		
9	Llaves, contraseñas no deben ser incluida en el código fuente.		
10	Cerrar sesión tanto en el lado de cliente como servidor		
11	Interfaces de administración de aplicación no deben ser vulnerable		
12	Numero de intento de autenticación limitadas		
13	Expiración de tokens y sesiones por inactividad		
14	Autenticación biométrico o keystore para firmar aplicación		
15	Aplicar Autenticación de dos pasos (2FA).		
16	Verificar que la sesión no se revele en URL.		
17	Para transacciones como compras en línea realizar una re-autenticación		
18	Manejar datos estadísticos de acceso a cuenta para verificar que lista de dispositivos y bloquear.		

Fuente: (Developer Android, 2018), (NIST 800-38B, 2016)

Tabla 12.
Consideraciones de comunicación a través de la red para Aplicaciones Móviles

	Consideración	SI	NO
1	Información cifrada TLS usando canal exclusivo para aplicación		
2	Usar mejores prácticas de protocolo TLS(Transport Layer Security)		
3	Usar certificación X.509 (llaves públicas) en el lado del servidor		
4	No depender de un único canal de comunicaciones, para recuperación de cuentas		
5	Aplicación solo depende de bibliotecas de conectividad (datos móviles, WIFI).		
6	Verificar fallos de conexión TSL en el vacíen.		

Fuente: (NIST Special Publication 800-52 Revision 1, 2014), (NIST Special Publication 800-53 Revision 4, 2015)

Tabla 13.
Consideraciones para protección y manejo de tarjetas de crédito

	Consideración	SI	NO
	Construir y mantener la red y sistemas seguros		
1	Instalar y administrar configuraciones de Firewall para protección de tarjeta de crédito		
2	No usar contraseñas, usuarios y parámetros sensibles, entregados por proveedores		
3	Analizar el tráfico que viaja con información sensible		
4	En cada conexión a internet configurar firewall con sus respectivas vlans de entrada, salida y dmz para protección de información		
5	Documentación de roles y responsabilidades, servicios inseguros y sus justificaciones		
6	Limitar el ancho de banda de internet por usuario		
7	Prohibir acceso directo entre internet y el componente de manejo de tarjeta.		
	Protección de datos de Titular de tarjeta		
8	Proteger datos de la tarjeta de crédito		
9	Encriptar la transmisión de datos a través de redes abiertas		
	Administración de Vulnerabilidades		
10	Proteger todos los sistemas contra virus y malware, actualizando programas, paquetes, antivirus		
11	Desarrollar y mantener seguro sistemas y aplicaciones		
	Medidas de Control de Acceso		
12	Restringir los datos de Tarjeta de Crédito a empresas que quieran conocerlos		
13	Identificar y autenticar el acceso		
14	Restringir el acceso físico a los datos del titular de tarjeta		
15	Asegurarse que las fallas de control de seguridad sean detectadas, resueltas y documentadas en el menor tiempo posible.		
	Supervisar periódicamente la red interna		
16	Seguimiento y monitoreo a todos los recursos de red y datos de titular de tarjeta		
17	Pruebas de seguridad y procesos periódicos		
	Políticas de Seguridad		
18	Mantener una política de seguridad de la información al personal		

Fuente: *(Payment Card Industry (PCI) Data Security Standard, 2018)*

Tabla 14.
Consideraciones de calidad de código, configuración de compilador

	Consideración	SI	NO
1	Aplicación firmada y entregada con su respectivo certificado		
2	Aplicación liberada apropiadamente (Release)		
3	Debugs eliminados de los binario nativos		
4	Aplicación no debe contener el código de prueba, ni logs o mensajes debug.		
5	Elementos de fuentes externas son identificados y analizadas sus respectivas posibles vulnerabilidades.		
6	Manejar las posibles excepciones.		
7	Por defecto denegar el acceso		
8	Aplicación requiere mínimos permisos		
9	Fuentes externas validadas		
10	No exportar funcionalidades sensibles vía URL.		
11	Si utiliza serialización de objetos, implementar API seguras		
12	Todos los componente deben de estar actualizados a sus versiones adecuadas		
13	Conexión entre servidor de aplicación y base de datos deben estar cifradas.		
14	Procesos de compilación debe realizarse de forma segura.		
15	Administradores verifican la integridad de las configuraciones de seguridad		

Fuente: (Meucci & Muller, 2014)

Tabla 15.
Consideraciones de Control de Acceso para el diseño de aplicaciones Móviles

	Consideración	SI	NO
1	Protección contra suplantación de identidad y elevación de privilegios		
2	Proteger contra manipulación de registros sensibles		
3	Evitar navegación de directorios en el servidor		
4	Verificar que las acciones de control de acceso queden registradas		
5	Verificación de emisión de tokens anti-CSRF (exploit malicioso)		

Fuente: (Meucci & Muller, 2014)

Tabla 16.
Manipulación de datos de entrada para aplicaciones móviles.

	Consideración	SI	NO
1	En el entorno de ejecución, no exista desbordamiento de buffer		
2	Validación de entradas datos rechazadas sean registradas		
3	Consultas a base de datos, no sean susceptibles a inyección SQL		
4	Aplicación no susceptible a inyección LDAP(Lightweight Directory Access Protocol)		
5	Aplicación no susceptible a inyección de comandos de Sistemas Operativos		
6	Validaciones lado cliente entran a validación luego del servidor. W		
7	Datos validados en la entrada de información a formularios		

Fuente: (Meucci & Muller, 2014), (Chell, Erasmus, Colley, & Whitehouse, 2015)

Tabla 17.
Consideraciones de Requisitos de verificación Móvil para aplicaciones móviles.

	Consideración	SI	NO
1	No utilizar datos propio del móvil (IMEI), no se utilicen como Token		
2	No almacenar datos compartidos o sensibles en tarjetas SD		
3	Verificar que contraseñas y tokens se generen dinámicamente en el móvil.		
4	Revisar que no exista fugas de información sensible		
5	Explorar que aplicación no exporte contenido de información sensible a otras aplicaciones en el mismo dispositivo		
6	Información almacenada en el equipo debe ser sobrescrita con ceros.		
7	Verificar que actividades realicen validación de datos		

Fuente: (Meucci & Muller, 2014), (Chell, Erasmus, Colley, & Whitehouse, 2015)

Tabla 18.
Consideraciones de verificación de Servicio Web

	Consideración	SI	NO
1	Mismo tipo de codificación entre cliente y servidor		
2	Verificar esquemas XML o JSON(JavaScript Object Notation) sean verificados antes de aceptarlos		
3	Datos de entrada con tamaño adecuado		
4	Verificar servicios REST (representational state transfer) se encuentren protegidos contra Sitios Cruzados o CSRF (Cross-siete Request forgery).		
5	Verificar que no existan rutas de acceso alternativas o inseguras.		

Fuente: (Meucci & Muller, 2014), (Chell, Erasmus, Colley, & Whitehouse, 2015), (Muller & Scheleier, 2018)

CAPÍTULO 4

CONCLUSIONES Y RECOMENDACIONES

3.5 Conclusiones:

- Se logró analizar las seguridades de una aplicación móvil para la comercialización de tickets basándose en la norma ISO/IEC 27034.
- Se realizó unas guías y checklist para evaluar el funcionamiento de una aplicación para transacciones electrónicas en línea.
- Las tecnologías de la información se están desarrollado rápidamente, por tanto, el análisis de las técnicas de encriptación desarrollado en este proyecto es de fundamental importancia para determinar la más óptima al momento de desarrollar aplicaciones móviles.
- Cada organización debe establecer su marco de referencia Normativo, con el fin de establecer su entorno de operación y consideraciones.
- ISO/IEC 27034 puede ayudar a administrar los costos de la seguridad de la aplicación, ofreciendo una visión más comprensiva e inclusiva para garantizar una seguridad efectiva.
- ISO/IEC 27034 puede ayudar a minimizar costos en la seguridad de la aplicación, promoviendo la integración de actividades de seguridad en procesos de la organización, esto ayudaría reducir los impactos de seguridad y la resistencia a cambios futuros.
- ISO/IEC 27034 ayuda a las organizaciones a plantear y/o administrar los CSA y niveles de confianza, respecto a los recursos y prioridades de la organización. Implementando conocimiento y mejores prácticas a la interna de la misma.
- Seguridad de la información es basada en la administración del riesgo. El mismo que no puede ser eliminado, pero puede solo ser minimizado a un nivel aceptable.

- En la seguridad de la aplicación se tiene el riesgo y se debe definir los requerimientos de seguridad que significa como se va a mitigar el riesgo. Dentro de los requerimientos se debe diseñar e implementar un control de seguridad de aplicación que tiene que proveer la evidencia esperada que soporte la reducción de riesgos.

3.6 **Recomendaciones:**

- Definir claramente el entorno de negocio para así poder establecer de forma clara y especifica sus respectivos contextos. Esto conlleva a tener unas especificaciones de seguridad más claras para así poder desarrollar una aplicación que cumpla con los parámetros y requisitos propios de la organización.
- Para evitar nuevas vulnerabilidades no detectadas en una aplicación. Se recomienda la periódica actualización de la aplicación. Además de realizar pruebas de software de vulnerabilidades o verificar en la Base de datos de vulnerabilidades, en donde publican todas las actualizaciones de las mismas y proceder con las respectivas correcciones.
- Se recomienda revisar las últimas actualizaciones criptográficas, en fuentes oficiales de estandarización como en National Institute Standars and Technology (NIST).
- Documentar todos los procedimientos operativos y disponer de un área en el departamento de TI de seguridad de la información/aplicación, para que realice funciones de monitoreo, actualizaciones y resuelvas incidencias presentadas en las aplicaciones. Esta área debe de estar compuesta por un grupo de trabajo, no solo una persona.
- La seguridad es un aspecto primordial que se debe tener encuentra en una organización, debido a que cada día aparecen o se desarrollan nuevos tipos de amenazas en la tecnología, por tanto, se recomienda capacitar a los miembros de la organización sobre conceptos básicos de seguridades, mientras que a las personas o grupo de trabajo del departamento TI, deben capacitarse en temas más complejos de seguridad.
- Se recomienda identificar áreas que manejan información crítica o sensible.

- Es necesario seguir los estándares que siguen otros países para el desarrollo de aplicaciones comerciales y transaccionales en línea, ya que en el Ecuador no se establecen unas normas y un marco regulatorio para este tipo de operaciones financieras.

BIBLIOGRAFÍA

Aranaz Tudela, J. (2009). Desarrollo de Aplicaciones para dispositivos móviles sobre la plataforma Android de Google. *(Tesis de pregrado).* Universidad Carlos II de Madrid, Madrid.

ARCOTEL. (s.f.). *Misión*. Obtenido de Arcotel: http://www.arcotel.gob.ec/mision-vision-principios-y-valores/

Asamblea Nacional. (2015). *Ley orgánica de Telecomunicaciones.*

Auquilla, D. (2015). Diseño e Implementación de una aplicación móvil para comercialización de boletos para empresas de transporte terrestre del Ecuador. *(Tesis de Pregrado).* Escuela Politécnica de las Fuerzas Armadas, Sangolqui.

Banco Pichincha. (2018). *Transacciones Electrónicas.* Obtenido de Pichincha: https://www.pichincha.com/portal/Informacion/Canales-de-atencion/Banca-electronica

Bayteq. (Agosto de 2018). *Conocenos.* Obtenido de Bayteq: http://www.bayteq.com

BlueKrypt. (10 de Junio de 2018). *Cryptographic Key Length Recommendation.* Obtenido de keylength: https://www.keylength.com/en/4/

Cecarm. (2008). *Guia Funcionamiento y contratacion de una pasarela de pago.* Obtenido de Cecarm: https://www.cecarm.com/Guia_Funcionamiento_y_contratacion_de_una_pasarela_de_pago.pdf-6535

Chell, D., Erasmus, T., Colley, S., & Whitehouse, O. (2015). *The Mobile Application Hacker's Handbook.* Wiley.

Common Vulnerability Scoring System SIG. (s.f.). *Common Vulnerability Scoring System SIG*. Obtenido de First.org: https://www.first.org/cvss/

Congreso Nacional. (2002). *ReglamentoComercioElectronico.* Obtenido de sri.gob.ec: http://www.sri.gob.ec/DocumentosAlfrescoPortlet/descargar/69c4134c-204a-4b35-a702-428a07711b34/ReglamentoComercioElectronico.doc

Cuenca Diaz, C. (s.f.). *Desarrollo Seguro: Principios y Buenas Prácticas.* Obtenido de The Open Web Aplication Security Project : https://www.owasp.org/images/9/93/Desarrollo_Seguro_Principios_y_Buenas_Pr%C3%A1cticas..pdf

Developer Android. (25 de Abril de 2018). *Certificados y keystores*. Obtenido de Developer Android: https://developer.android.com/studio/publish/app-signing?hl=es-419

El Comercio. (12 de Febrero de 2018). *73% de las transacciones bancarias se realizan en línea.* Obtenido de El comercio: https://www.elcomercio.com/actualidad/transacciones-banca-internet-aplicaciones-digitales.html

El Universo. (26 de Marzo de 2018). *Cuentas de dinero electrónico dejarán de funciona.* Obtenido de El Universo: https://www.eluniverso.com/noticias/2018/03/26/nota/6685168/cinco-dias-que-se-deje-usar-dinero-electronico

Elenkov, N. (2014). *Android Security Internals.*

Filippi, S. (01 de Diciembre de 2013). *Protocolo SET. El Protocolo de Seguridad en las transacciones electrónicas.* Obtenido de internetlab: https://www.internetlab.es/post/2640/protocolo-set/

Gomez, I. (30 de Julio de 2014). *Decenas de aplicaciones de Android podrían ser vulnerables*. Obtenido de Genbeta: https://www.genbeta.com/seguridad/decenas-de-aplicaciones-de-android-podrian-ser-vulnerables

Guanín, B. (2014). Estudio, Diseño E Implementación De Un Portal Web Dinámico Para La Comercialización De Boletos Para Rutas Y Frecuencias De Cooperativas Interprovinciales De Transporte Terrestre En El País . *(Tesis de Pregrado).* Escuela Politécnica de las Fuerzas Armadas ESPE, Sangolqui.

INEN-ISO/IEC 27005. (s.f.). *Tecnología de información – Técnicas de seguridad – Gestión de riesgos de seguridad de información.*

ISO 9000. (2005). *Sistemas de gestión de la calidad — Fundamentos y vocabulario.*

ISO/IEC 12207:2008. (2008). *Information Technology / Software Life Cycle Processes.*

ISO/IEC 15288. (2015). *Systems and software engineering -- System life cycle processes.*

ISO/IEC 24765. (2010). *Systems and software engineering -- Vocabulary.*

ISO/IEC 27034-2. (s.f.). *Tecnología de información – Técnicas de seguridad – Seguridad de información. Parte 2: Marco de Referencia Normativo de La Organización.*

iso27000. (s.f.). *Sistema de Gestión de la Seguridad de la Información.* Obtenido de iso27000: Sistema de Gestión de la Seguridad de la

Karakeneva, J. (2014). Software Application Security. *Trakia Journal of Sciences*, 1-7.

Meucci, M., & Muller, A. (2014). *Guia de pruebas.* Obtenido de OWASP: https://www.owasp.org/images/1/19/OTGv4.pdf

Ministerio de Telecomunicaciones y de la sociedad de la información. (s.f.). *Valores Mision Visión*. Obtenido de Ministerio de Telecomunicaciones y de la sociedad de la información: https://www.telecomunicaciones.gob.ec/valores-mision-vision/

MITRE Corporation. (20 de Agosto de 2018). *About*. Obtenido de CVE: https://cve.mitre.org/

MITRE Corporation. (03 de Abril de 2018). *About*. Obtenido de CWE: https://cwe.mitre.org

Morales, R. F. (2015). Diseño para implementación de dominios de un sistema de gestión de la información. *(Tesis Postgrado).* Escuela Politécnica de las Fuerzas Armadas ESPE, Sangolqui.

Muller, B., & Scheleier, S. (2018). *OWAPS-Mobile Security Testing Guide.*

NIST 800-131A Revision 1. (Noviembre de 2015). *Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*. Obtenido de NIST: http://dx.doi.org/10.6028/NIST.SP.800-131Ar1

NIST 800-38B. (Octubre de 2016). *Recommendation for Block Cipher Modes of Operation the CMAC Mode for Authentication*. Obtenido de NIST: http://dx.doi.org/10.6028/NIST.SP.800-38B.

NIST Special Publication 800-107. (Agosto de 2012). *Revision 1, Recommendation for Applications Using Approved Hash Algorithms*. Obtenido de NIST: , August 2012, http://dx.doi.org/10.6028/NIST.SP.800-107r1.

NIST Special Publication 800-132. (Diciembre de 2010). *Recommendation for Password-Based Key Derivation*. Obtenido de http://dx.doi.org/10.6028/NIST.SP.800-132.

NIST Special Publication 800-52 Revision 1. (Abril de 2014). *Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations*. Obtenido de NIST: http://dx.doi.org/10.6028/NIST.SP.800-52r1

NIST Special Publication 800-53 Revision 4. (22 de Enero de 2015). *Recommended Security and Privacy Controls for Federal Information Systems and Organizations*. Obtenido de NIST: http://dx.doi.org/10.6028/NIST.SP.800-53r4.

NIST Special Publication 800-57. (Enero de 2016). *Part 1, Revision 4, Recommendation for Key Management, Part 1: General*. Obtenido de NIST: http://dx.doi.org/10.6028/NIST.SP.800-57pt1r4.

NTE INEN-ISO/IEC 27001. (2011). *Tecnología de la información. Técnicas de seguridad — Sistema de gestión de la seguridad de la información. Requisitos.*

NTE INEN-ISO/IEC 27005. (s.f.). *Tecnología de información – Técnicas de seguridad – Gestión de riesgos de seguridad de información.*

NTE INEN-ISO/IEC 27034-1. (2014). *Técnologia de la información-Técnicas de seguridad-Seguiridad de la Aplicación-Parte1:Descripción de Conceptos.*

Payment Card Industry (PCI) Data Security Standard. (Mayo de 2018). *Requirements and Security Assessment Procedures*. Obtenido de pcisecuritystandard: https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf?agreement=true&time=1535336228388

Quirolgico, S., Voas, J., Karygiannis, T., Michael, C., & Scarfone, K. (2015). *Vetting the Security of Mobile Applications.* National Institute of Standards and Technology .

Ramirez Jaramillo, C. D., & Moreira Zambrano, R. M. (2017). Diseño para la implementacion de los dominios de cifrado y seguridad fisica y ambiental basados en la norma iso27001 e iso27002. *(Tesis de Posgrado).* Escuela Politécnica de las Fuerzas Armadas ESPE, Sangolqui.

Sanca, F. D. (2013). Comercio electrónico y pago mediante tarjeta de crédito en el ordenamiento jurídico español:. *(Tesis Doctoral).* Universidad Carlos III, Madrid.

SRI. (2018). *Efectivo desde mi celular (dinero electrónico).* Obtenido de SRI: http://www.sri.gob.ec/web/guest/dinero-electronico1

Supercines. (2018). *Nuestra Mision*. Obtenido de Supercines: https://www.supercines.com/SupercinesInformation/InformationPage?section=whoWeAre

Tutorialspoint. (2017). *SDLC-Overview*. Obtenido de tutorialspoint: http://www.tutorialspoint.com/sdlc/sdlc_overview.htm