UNIVERSIDAD TÉCNICA DEL NORTE

Facultad de Ingeniería en Ciencias Aplicadas

Carrera de Ingeniería en Sistemas Computacionales

TEMA:

IMPLEMENTACIÓN DEL MÓDULO DE FIRMAS DIGITALES PARA EL SISTEMA INTEGRADO DE ACTIVIDAD DOCENTE (SIAD) DE LA CARRERA DE SOFTWARE DE LA UNIVERSIDAD TÉCNICA DEL NORTE MEDIANTE EL USO DE UN TOKEN CRIPTOGRÁFICO APLICANDO EL ESTÁNDAR DE INFRAESTRUCTURA DE CLAVE PÚBLICA X.509 PARA AUTOMATIZAR EL PROCESO DE ENTREGA DE DOCUMENTOS.

TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERA EN SISTEMAS COMPUTACIONALES

AUTORA:

Otavalo Arrayan Lizeth Marlene

DIRECTOR:

MSc. Xavier Mauricio Rea Peñafiel

Ibarra, 2020

UNIVERSIDAD TÉCNICA DEL NORTE

BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	172760650-9		
APELLIDOS Y NOMBRES:	OTAVALO ARRAYAN LIZETH MARLENE		
DIRECCIÓN:	OTAVALO-ILUMAN, BARRIO STO DOMINGO		
EMAIL:	lmotavaloa@utn.edu.ec		
TELÉFONO FIJO:	(06) 2946754	**TELÉFONO MÓVIL:**	0969603520

DATOS DE LA OBRA	
TÍTULO:	IMPLEMENTACIÓN DEL MÓDULO DE FIRMAS DIGITALES PARA EL SISTEMA INTEGRADO DE ACTIVIDAD DOCENTE (SIAD) DE LA CARRERA DE SOFTWARE DE LA UNIVERSIDAD TÉCNICA DEL NORTE MEDIANTE EL USO DE UN TOKEN CRIPTOGRÁFICO APLICANDO EL ESTÁNDAR DE INFRAESTRUCTURA DE CLAVE PÚBLICA X.509 PARA AUTOMATIZAR EL PROCESO DE ENTREGA DE DOCUMENTOS.
AUTOR (ES):	OTAVALO ARRAYAN LIZETH MARLENE
FECHA: DD/MM/AAAA	18/02/2020
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA:	[x] PREGRADO [ ] POSGRADO
TITULO POR EL QUE OPTA:	INGENIERA EN SISTEMAS COMPUTACIONALES
ASESOR /DIRECTOR:	MSc. REA PEÑAFIEL XAVIER MAURICIO

2. CONSTANCIAS

La autora manifiesta que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es la titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de esta y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 18 días del mes de febrero del 2020

LA AUTORA:

Nombre: LIZETH MARLENE OTAVALO ARRAYAN
CI: 172760650-9

Ibarra, 18 de febrero del 2020

CERTIFICACIÓN DEL DIRECTOR

Por medio del presente, yo MSc. Mauricio Rea, certifico que la Srta. **LIZETH MARLENE OTAVALO ARRAYAN**, portadora de la cédula de identidad Nro. 172760650-9. Ha trabajado en el desarrollo del proyecto de grado denominado: "**IMPLEMENTACIÓN DEL MÓDULO DE FIRMAS DIGITALES PARA EL SISTEMA INTEGRADO DE ACTIVIDAD DOCENTE (SIAD) DE LA CARRERA DE SOFTWARE DE LA UNIVERSIDAD TÉCNICA DEL NORTE MEDIANTE EL USO DE UN TOKEN CRIPTOGRÁFICO APLICANDO EL ESTÁNDAR DE INFRAESTRUCTURA DE CLAVE PÚBLICA X.509 PARA AUTOMATIZAR EL PROCESO DE ENTREGA DE DOCUMENTOS"**, previo a la obtención del Título de Ingeniería en Sistemas Computacionales, lo cual ha realizado en su totalidad con responsabilidad.

Es todo en cuanto puedo certificar en honor a la verdad.

Atentamente,

MSc. Mauricio Rea

DIRECTOR DE TESIS

REPUBLICA DEL ECUADOR

UNIVERSIDAD TÉCNICA DEL NORTE

Resolución No. 001-073 CEAACES-2013-13

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

El MSc. Pedro Granda, Coordinador de la Carrera CISIC/CSOFT de la Universidad Técnica del Norte

CERTIFICA:

Que: La Srta. LIZETH MARLENE OTAVALO ARRAYAN, portadora de la cédula de ciudadanía 172760650-9, Estudiante de la Carrera de Ingeniería en Sistemas Computacionales de la Universidad Técnica del Norte, ha desarrollado con el levantamiento de procesos entregados por la Coordinación de la Carrera CISIC/CSOFT, el Proyecto de Tesis "IMPLEMENTACIÓN DEL MÓDULO DE FIRMAS DIGITALES PARA EL SISTEMA INTEGRADO DE ACTIVIDAD DOCENTE (SIAD) DE LA CARRERA DE SOFTWARE DE LA UNIVERSIDAD TÉCNICA DEL NORTE MEDIANTE EL USO DE UN TOKEN CRIPTOGRÁFICO APLICANDO EL ESTÁNDAR DE INFRAESTRUCTURA DE CLAVE PÚBLICA X.509 PARA AUTOMATIZAR EL PROCESO DE ENTREGA DE DOCUMENTOS", el software se encuentra funcional y el código fuente se ha registrado en el repositorio de proyectos de software de la carrera.

Que: El estudio del proyecto fue entregado a la Coordinación de la Carrera CISIC/CSOFT el 18 de febrero del 2020.

Es todo cuanto puedo certificar, facultando a la interesada hacer uso de este certificado como estime conveniente.

Ibarra, 18 de febrero del 2020

Atentamente,

MSc. Pedro Granda

COORDINADOR DE CARRERA CISIC/CSOFT

Av. 17 de Julio s-21 y José María Córdova
Ciudadela Universitaria Barrio El Olivo
Teléfono: (06)2997800 Casilla 199
E-mail: info@utn.edu.ec
www.utn.edu.ec
Ibarra - Ecuador

DEDICATORIA

A Dios, por ser luz en muchos momentos oscuros, cuando el camino se volvía duro de recorrer, a Él, por haberme permitido llegar hasta este punto.

A mis padres Antonio Otavalo y Luzmila Arrayan por todo su amor, su paciencia, por sus consejos, por ser ejemplo de perseverancia y constancia, a ellos, por apoyarme y confiar en mí incondicionalmente.

A mis hermanos Carlos, Coly y Laly, por compartir conmigo momentos especiales que me llenan el corazón de alegría, a ellos, por creer en mí.

A mis angelitos del cielo, a ellos, porque sé que están orgullos de verme alcanzar esta meta.

AGRADECIMIENTO

Gracias a Dios por la vida que me ha dado, por darme salud y su bendición para poder formarme y alcanzar una de mis metas como persona y profesional. Gracias por permitirme compartir este logro con mis padres y mis hermanos, no puedo pedirte más, sino más bien agradecerte por demostrarme tu amor en todo momento.

Mi agradecimiento eterno a mi papá y mi mamá, soy lo que soy gracias a sus esfuerzos y sus sacrificios, lucharon por mi bienestar, mi educación y mi salud, les agradezco infinitamente por todo el amor que siempre me han dado, por darme a mis cómplices de vida, mis hermanos, sin ellos mí vida estaría incompleta, no conozco a nadie en este mundo a quienes les deba tanto, gracias a ustedes soy feliz.

Gracias “Qiinteto”, “Las 3”, “Nosotr@s” y “Zappy”, por brindarme su amistad, por compartir conmigo muchos momentos especiales, por ser quiénes me han levantado y me han ayudado a seguir adelante estando lejos de casa, definitivamente Dios pone a las personas correctas en nuestro camino en el momento indicado, gracias por este tiempo compartido y por formar parte de mi vida y de mi historia, su amistad me hace bien.

Agradezco especialmente a mis docentes Ing. Mauricio Rea e Ing. Pedro Granda, por la oportunidad de trabajar en este proyecto junto a ustedes, por permitirme aprender e incentivarme en muchos sentidos a continuar, sin su apoyo esto no hubiera sido posible.

Tabla de Contenido

Índice de Figuras

Índice de Tablas

RESUMEN

La presente investigación tiene como objetivo mostrar la importancia de la Firma Digital como complemento del Sistema Integrado de Actividad Docente (SIAD) de la Universidad Técnica del Norte de la Carrera de Ingeniería en Sistemas Computacionales (CISIC) y Carrera de Ingeniería de Software (CSOFT) la misma que presenta varias ventajas, una de estas es el beneficio al medio ambiente al evitar el uso de papel, al usar esta aplicación, también se puede evidenciar otros beneficios como son la disminución de documentos físicos y recursos materiales y económicos.

El uso de este software además de las ventajas nombradas anteriormente provee mayor seguridad y validez jurídica a los documentos firmados, de esta manera se evita la alteración de estos.

Para el desarrollo de esta aplicación se utilizó como marco de trabajo SCRUM, que es una metodología ágil y flexible que permite gestionar proyectos de software con planificaciones de trabajo en sprints o pequeños bloques, dando como resultado el diseño de un plan de implementación de la Firma Digital en los principales procesos de entrega y recepción de documentos en la CISIC/CSOFT. El proceso de desarrollo de este software se realizó mediante la API proporcionada por el Registro Civil del Ecuador.

La aplicación desarrollada permite firmar y verificar documentos firmados, así como también permite verificar si el certificado digital otorgado por la Autoridad Certificadora es válido y aún no ha sido revocado. Por otra parte, se desarrolló una aplicación extra en la que se permite la creación de un certificado digital y la firma de documentos con dicho certificado, ambas aplicaciones cumplen con las características del Estándar X.509.

ABSTRACT

This investigation have how objective to show the importance of the Digital Signature as a complement to the Integrated Teaching Activity System (SIAD) of the Technical University of the North of the Computer Systems Engineering Degree (CISIC) and Software Engineering Degree (CSOFT) the same that presents several advantages, one of these is the benefit to the environment by avoiding the use of paper, by using this application, other benefits can also be evidenced, such as the decrease of physical documents and material and economic resources.

The use of this software in addition to the advantages mentioned above provides greater security and legal validity to the signed documents, thus preventing their alteration.

For the development of this application, SCRUM is established as a framework, which is an agile and flexible methodology that allows managing software projects with work schedules in sprints or small blocks, resulting in the design of an implementation plan for the Firm Digital in the main processes of delivery and reception of documents in the CISIC/CSOFT. The development process of this software was carried out through the API controlled by the Civil Registry of Ecuador.

The developed application allows to sign and verify signed documents, as well as to verify if the digital certificate granted by the Certificate Authority is valid and has not yet been revoked. On the other hand, an extra application is required in which the creation of a digital certificate and the signing of documents with said certificate are allowed, the required applications are established with the characteristics of the X.509 Standard.

INTRODUCCIÓN

Antecedentes

En la Carrera de Software (CSOFT) de la Universidad Técnica del Norte (UTN) se está desarrollando el Sistema Integrado de Actividad Docente (SIAD), con el propósito de mejorar el proceso de actividades de los 22 docentes que laboran en la carrera, los mismos que generan alrededor de 50 documentos al mes, de los cuales 2 o 3 son generados por cada uno. En secretaría de la Coordinación se recibe, despacha y archiva un expediente de cada uno por cada semestre, y a su vez, se escanea y guarda en el disco duro de el equipo de la carrera, debido a esto se busca implementar el módulo de firmas digitales por la necesidad de automatizar procesos de trámites documentales, puesto que se ha visto que al realizar este procedimiento se requiere que el docente imprima y firme personalmente dicho documento generando gastos de papel innecesarios y pérdida de tiempo, también se da por la falta de eficiencia de gestiones administrativas dado que la documentación ingresada a la CSOFT no sigue un proceso de filtrado y validación de firmas, entre otras causas por la insuficiente seguridad de informes firmados debido a la falta de autentificación de los documentos, consecuente a esto el contenido podría ser cambiado o reemplazado y la legalidad del documento podría verse afectada así como también se correría el riesgo de la pérdida de documentación importante.

A nivel tecnológico existen proyectos conocidos sobre el tema a tratar como es el caso de Quipux, que es un servicio web proporcionado por la Subsecretaria de Tecnologías de la Información de la Secretaria Nacional de la Administración Pública (Quipux, 2015). Dicho servicio se encuentra instalado en la Universidad Técnica del Norte, esta aplicación permite gestionar documentos de una manera rápida y legal, sin embargo, Quipux no está incorporado a ningún sistema interno de la UTN.

Situación Actual

Actualmente la Carrera de Software no cuenta con un método para automatizar, validar y verificar la firma de documentos de actividad docente, por lo que el proceso de entrega de informes hacia la coordinación se hace manualmente, por consiguiente, las vulnerabilidades en cuanto a modificación de contenido, pérdida de documentación, falsificación de firmas, incendios o inundaciones, entre otros tiene un riesgo de alto nivel, también tomando en cuenta que se consume en exceso recursos como papel y tinta de impresora, entre otros gastos económicos al adquirir dichos recursos.

Cabe recalcar que, siendo una carrera orientada al uso e implementación de tecnologías, aún se puede evidenciar procesos que se realizan en papel o archivos de texto convencionales.

Prospectiva

La Coordinación de la Carrera de Software de la UTN contará con un módulo de firmas digitales seguro, que garantizará la identidad del docente firmante, y que además después de enviado el mismo con la firma digitalizada la información contenida no podrá ser modificada y se validará automáticamente, por otra parte, mejorará el proceso de firmas evitando la movilidad del usuario pues no hará falta un desplazamiento físico como para ir a hacer uso de la impresora. Concluido el desarrollo del proyecto, en el sistema general se podrá visualizar la opción que permita generar la firma digital en documentos PDF y no será una aplicación extra como lo es Quipux, a la vez, después de implementado este proyecto disminuirá notablemente la impresión en hojas de papel, porque los documentos ya estarán registrados en la base de datos del sistema con su respectiva firma digital, de esta manera se podrá realizar esta tarea con mayor eficiencia e incidir positivamente en al menos un proceso de la gestión de trámites de la CSOFT (María de los Ángeles Valle C., 2014).

Planteamiento del problema

En la Coordinación de la Carrera de Software de la UTN se requiere un módulo de firmas digitales que se integre al SIAD que se está desarrollando en dicha Coordinación, el mismo que permita que el documento se genere y sea firmado dentro del mismo sistema, sin la necesidad de usar una aplicación extra que permita realizar este procedimiento.

El proyecto planteado se podrá crear aplicando el estándar de Infraestructura de Clave Pública X.509 (ITU, 2018). Al contar con este módulo se podrá evitar inconvenientes de inseguridad por el intercambio de información privada, además que por medio de esta automatización se facilitará el proceso de documentación acelerando la tarea de firmas, validación y formalización de los documentos, a la vez se podrá contribuir de alguna manera en el cuidado del medio ambiente teniendo en cuenta que tras la implementación de este proyecto se podrá disminuir notablemente el consumo excesivo de hojas de papel, el mismo que al ser bastante empleado para realizar impresiones (a veces innecesarias) es uno de los atentados inconscientes más comunes que conlleva consecuencias negativas para la naturaleza como por ejemplo, deforestación que provoca no solo la pérdida de árboles, sino también la pérdida de especies tanto animales como vegetales,

contaminación ambiental, entre otros, además se disminuirían los gastos que se generan al adquirir este tipo de recursos y otros extras con impresoras como son mantenimiento y reparación de las mismas en el caso de ser necesarios (López Ruiz, 2018). La automatización de este proceso representaría un resultado de impacto en cuanto a la satisfacción de los docentes que es a quienes va dirigido el desarrollo de este tema, haciéndose notar de manera importante la disminución de tiempos de espera, costos y papel.

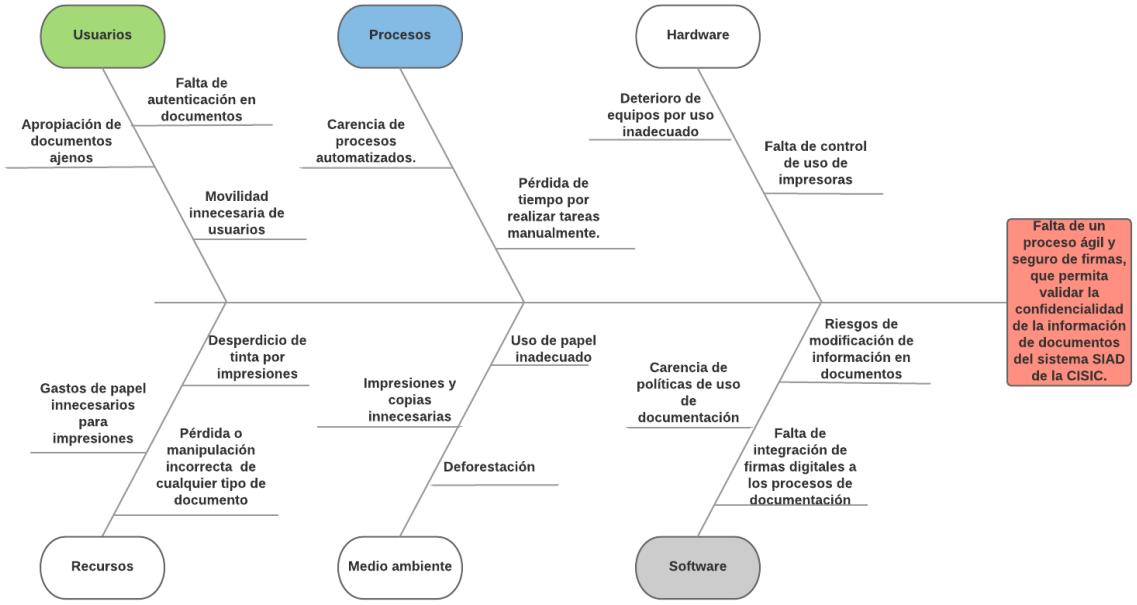


Figura 1: Diagrama de problemas

Fuente: Propia

Objetivos

Objetivo general

Implementar el módulo de firmas digitales para el Sistema Integrado de Actividad Docente (SIAD) de la Carrera de Software de la Universidad Técnica del Norte mediante el uso de un token criptográfico aplicando el estándar de Infraestructura de Clave Pública X.509 para automatizar el proceso de entrega de documentos.

Objetivos específicos

- Elaborar un marco teórico del uso de firmas digitales en la gestión documental del proceso de la actividad docente.
- Desarrollar el módulo de firmas digitales para el sistema SIAD aplicando el estándar de Infraestructura de Clave Pública X.509 y la metodología SCRUM como marco de trabajo para el desarrollo de software.
- Implementar el algoritmo de encriptación SHA-256 para validar la confidencialidad y seguridad de la información.
- Validar los resultados.

Alcance

El proyecto planteado tiene como finalidad utilizar un algoritmo de criptología de datos SHA-256 para fortalecer la seguridad de la documentación generada en el proceso de actividad docente, mediante la adquisición de un dispositivo criptográfico portable seguro (Token) proporcionada por el Registro Civil del Ecuador (Registro Civíl, 2019), el mismo que puede ser utilizado únicamente por el propietario original , permitiendo de esta manera validar la información del documento y la autenticación del docente firmante, por lo tanto, poder garantizar que únicamente el poseedor del dispositivo fue quien generó la firma en el documento que será entregado (Carlos De Luca, 2015), esto se realizará con el fin de automatizar el proceso de firmas de docentes de la Carrera de Software de la Universidad Técnica del Norte. Luego del estudio se determinará el método estadístico que se ajuste a las características del trabajo realizado que permitirá validar los resultados.

Por otra parte, se utilizará la metodología de desarrollo ágil SCRUM, la misma que permitirá cumplir con las actividades requeridas para el desarrollo del proyecto que será integrado al sistema SIAD.

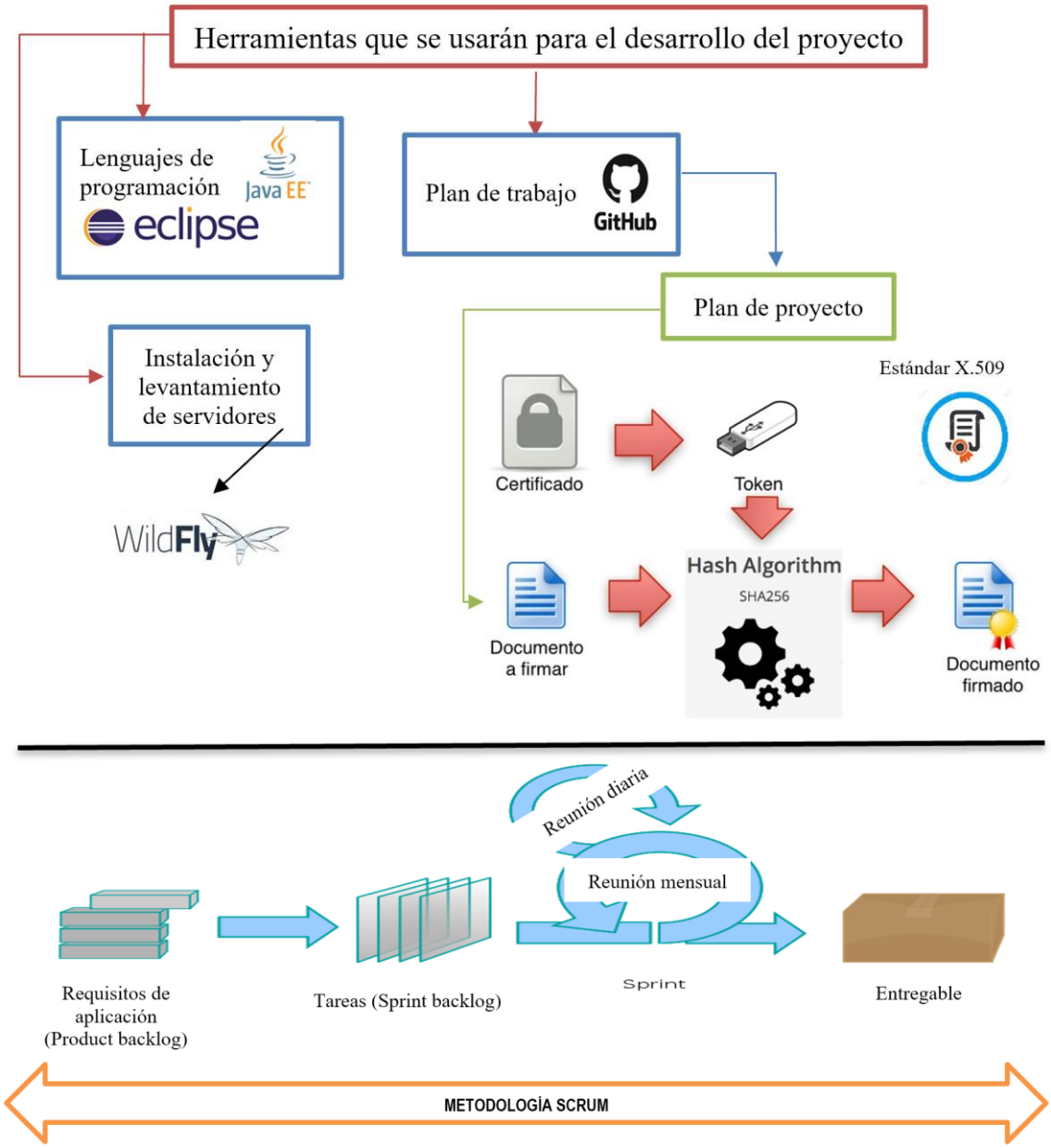


Figura 2: Arquitectura del sistema

Fuente: Propia

Justificación

El presente proyecto tiene un enfoque hacia los objetivos de desarrollo sostenible:

Nº4: Educación de calidad:

El acceso a una educación de calidad es crucial para mejorar la vida de las personas y el desarrollo sostenible (ODS, 2018).

Nº9: Industria, Innovación e Infraestructura:

9.b Apoyar el desarrollo de tecnologías, la investigación y la innovación nacionales en los países en desarrollo, incluso garantizando un entorno normativo propicio a la diversificación industrial y la adición de valor a los productos básicos, entre otras cosas.

9.c Aumentar significativamente el acceso a la tecnología de la información y las comunicaciones y esforzarse por proporcionar acceso universal y asequible a Internet en los países menos adelantados de aquí a 2020 (ODS, 2018).

Económico

El impacto a nivel económico implica evitar gastos que se pueden producir por la compra de material para impresiones que pueden ser tinta y papel para impresiones, además también de mantenimientos de impresoras.

Ambiental

La automatización del proceso de firmas ayuda a reducir el consumo de recursos, principalmente el papel con lo que aportamos directamente a la preservación del medio ambiente.

Social

Los beneficiados directos de este proyecto en este caso los docentes de la Carrera de Software de la Universidad Técnica del Norte evitarán la pérdida, plagio y el deterioro de documentos haciendo uso de este proceso automatizado, validando de esta manera la seguridad de la información.

CAPÍTULO I

1. MARCO TEÓRICO

1.1. Fundamentos generales

1.1.1. Criptografía

Según el Diccionario de la Real Academia, la palabra Criptografía proviene del griego “kryptós”, que significa oculto, y “gráphein”, escritura, lo que quiere decir *“Escritura oculta”.* (López, 2008)

La Criptografía se ha convertido en una técnica que se aplica a la protección de la información, utilizando matemáticas complejas se ha desarrollado algoritmos criptográficos que permiten cifrar (modificar) un mensaje descifrable con el uso de una clave, después de la modificación, dicho mensaje es indescifrable para aquel que no posea una clave, de esta manera la transferencia de la información es segura y sólo puede ser leída por las personas a quienes está dirigida. Esto indica que no se emplea solamente para proteger información sino también para permitir su autentificación, lo que quiere decir que, identifica el autor de un mensaje e impide que nadie suplante su identidad. (López, 2008)

El criptoanálisis rompe esos procedimientos para poder recuperar la información, la criptología y el criptoanálisis están ligadas ya que cualquier método de cifrado lleva siempre emparejado su criptoanálisis correspondiente. (Sanjuan, 2016)

1.1.2. Objetivo de la Criptografía

La UNAD (2007) menciona que, el objetivo de la Criptología es garantizar que se cumplan las siguientes características:

- Confidencialidad: Asegura que solo las personas autorizadas tienen acceso a la información.
- Integridad: Asegura que el contenido original del mensaje enviado no haya sido modificado en el transcurso del envío.
- Autenticación: Asegura que el que envía el mensaje es realmente quien dice ser.

1.1.3. Tipos Criptográficos

Teniendo en cuenta el tipo de clave, se pueden identificar tres tipos de métodos criptográficos.

Criptografía Simétrica o clave secreta

Un algoritmo criptográfico simétrico utiliza un método matemático conocido como algoritmo de cifrado, para cifrar y descifrar un mensaje utilizando una sola clave. Con este tipo de criptografía se puede asegurar la confidencialidad ya que el mensaje puede ser visto únicamente por quien posea la clave secreta. (Krugman & Wells, 2015)

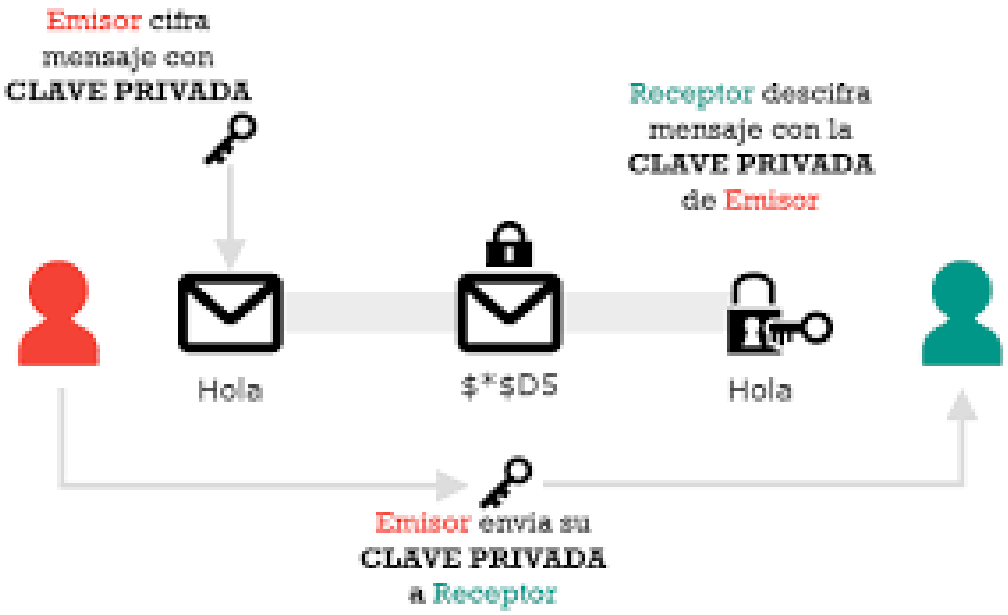


Figura 3: Criptografía simétrica

Fuente: (Informática, 2015)

Criptografía Asimétrica o clave pública

Un algoritmo criptográfico asimétrico maneja métodos matemáticos más complejos que los que son utilizados en los algoritmos simétricos. López (2008) menciona que este algoritmo demanda la generación de dos claves distintas, una privada y otra pública, una sirve para codificar y la otra para descodificar, estas están relacionadas entre sí matemáticamente.

Para cifrar y descifrar un mensaje se debe considerar que si un mensaje es cifrado con una clave pública solo se puede descifrarlo con una clave privada, y si se cifra con una clave privada esta se descifra con una clave pública. (Rafael Palacios, 2012)

Es importante mencionar que una clave no puede cifrar o descifrar por si sola un mensaje, además no se puede obtener una clave a partir de la otra, esto permite que la clave pública pueda estar disponible para todos los usuarios, mientras que la clave privada debe estar disponible solamente para el dueño de la pareja de claves. (Naranjo, 2010)

En la página web Informática (2015) mencionan que otro propósito de este algoritmo es también el poder firmar documentos digitalmente, certificando que el emisor es quien dice ser, firmando con la clave privada y verificando su identidad con la clave pública, esto se puede realizar con la ayuda de funciones hash (ver sección 1.1.4.).

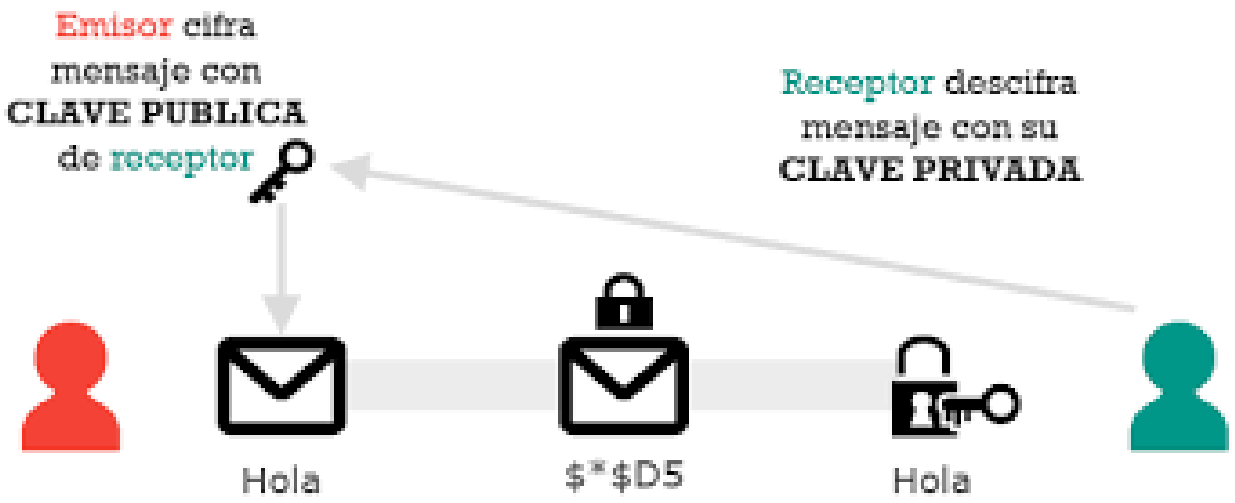


Figura 4: Criptografía asimétrica

Fuente: (Informática, 2015)

Tabla 1.1: Tipos de Algoritmos Asimétricos

Algoritmos Criptográficos Asimétricos	
Diffie-Hellman (Whitfield Diffie y Martin Hellman - 1976)	Utilizado aún como punto de partida para la explicación de protocolos de seguridad Naranjo (2010) estable que este algoritmo basa su seguridad en la dificultad de calcular logaritmos discretos en un campo limitado, se usa para la distribución de claves, pero no para cifrar y descifrar. También menciona que, es computacionalmente imposible calcular la clave secreta a partir de los valores públicos compartidos. Actualmente se conoce que es vulnerable a ataques. (Campos, 2011)
RSA (Rivest, Shamir y Adleman - 1978)	Crearon su algoritmo basándose en el artículo de llaves públicas de Diffie y Martin Hellman. (Aguirre & Lucen, 2019)

	Este algoritmo es el más sencillo de entender y más fácil de complementar. También garantiza los servicios de autenticación (firmas digitales) y confidencialidad (cifrado). (Sanchez, 2015)
DSA (Instituto Nacional de Tecnología y Estándares NIST - 1994)	Este algoritmo tiene como finalidad la generación de firmas digitales, no cifra información, es más rápido que un RSA, pero la comparación de la firma es más lenta. (Sanchez, 2015)
HASH	Función que genera claves que representen de manera casi unívoca un conjunto de datos con un algoritmo o función hash. Un hash, es el resultado de dicha función o algoritmo. (Sanchez, 2015)

Fuente: Propia

1.1.4. Función HASH o de resumen

Según Pedro Gutierrez (2013) un algoritmo Hash, es un algoritmo matemático que consigue crear a partir de una entrada (textos, archivos, contraseñas, etc.) una salida alfanumérica única (ver figura 5), el mismo que presenta un resumen de la información que se ha recopilado, mismo que al realizar un mínimo cambio se alteraría la cadena alfanumérica (ver Figura 6).

Este algoritmo no tiene las mismas funciones que los algoritmos de encriptación simétrica o asimétrica, entre una de sus funciones está el asegurar que los archivos no han sido modificados durante el envío, hacer ilegible una contraseña o firmar digitalmente un documento. (Universidad de Murcia, 2011)

Figura 5: Ejemplo de cadena alfanumérica

Fuente: (Kike Torné, 2017)

Figura 6: Ejemplo de una cadena alfanumérica con un cambio

Fuente: (Kike Torné, 2017)

Tabla 1.2: Tipos de Algoritmos Hash

Algoritmos Hash	
MD5 **(Ron Rivest - 1992)**	Según Naranjo (2010), esta función es la última versión de algoritmos Hash de RSA, es uno de los algoritmos más difundidos, proporciona un buen nivel de seguridad y resulta más rápido que SHA.
SHA **(National Security Agency NSA - 1993)**	Secure Hash Algorithm, según Sanchez (2015), esta función es un poco más lenta que el algoritmo MD5, pero presenta mayor resistencia ante ataques. Se utiliza en la mayoría de las aplicaciones de firmas electrónicas. El primer miembro de la familia de este algoritmo fue publicado en 1993. (EcuRed, 2011)

Fuente: Propia

1.1.5. Algoritmo de Encriptación SHA-256

SHA significa: algoritmo de hash seguro, utilizado para la seguridad criptográfica. Este algoritmo es uno de los sucesores de Sha-1, es una de las funciones más fuertes de los algoritmos Hash, el mismo que ha sido elegido actualmente para la generación de certificados que serán utilizados para las firmas digitales. Está compuesto por un hash de 64 bits hexadecimales, de un tamaño fijo de 256 bits. (P. Sumalatha & Prof. B. Sathyanarayana, 2015)

1.2. Infraestructura de Clave Pública (PKI)

Abobeah, Ezz, & Harb (2015) definen a la Infraestructura de Clave Pública como: "Una combinación de software, hardware, políticas y personas que tienen como objetivos administrar (crear, emitir, modificar, almacenar y eliminar) certificados digitales, autenticar la identidad del remitente y el receptor, y proporcionar la integridad de los datos."

Según Cantero (citado por Holguín García, 2018), el objetivo de una PKI es crear un documento que permita verificar la autenticidad de una clave pública, denominado como Certificado Digital emitido por una Autoridad Certificadora que como ejemplo se citará al Banco Central del Ecuador (BCE).

1.2.1. Elementos de Infraestructura de Clave Pública del BCE

Tabla 1.3: Elementos de PKI

Usuario	Autoridades	Destinatario
Un usuario se denomina a cualquier persona natural, jurídica o servidor público que hace uso de los certificados emitidos por una Autoridad Certificadora.	Personal que otorga validez a los certificados emitidos.	Se hace referencia a los usuarios quienes reciben los datos cifrados.

Fuente: (Holguín García, 2018)

1.2.2. Componentes de Infraestructura de Clave Pública del BCE

López (2008) asegura que, aunque la complejidad de una arquitectura PKI depende de los servicios a los que se destinará, cuenta con componentes que le permiten mantener un buen nivel de confianza como son:

Certificado digital

Ramos (citado por Holguín García, 2018) hace referencia a un certificado digital como un documento digital, el mismo que contiene datos informativos del usuario y que se encuentran debidamente autentificados por una Autoridad Certificadora, de esta manera garantiza la vinculación entre la identidad del usuario y una clave pública. Además, de que su función principal es la de emitir certificados de firmas digitales que permiten la firma electrónica. (Universidad Politécnica de Valencia, 2012)

Tabla 1.4: Contenido de un certificado digital

Identificación de la Entidad de Certificación de Información.
Los datos del titular del certificado que permitan su ubicación e identificación.
Las fechas de emisión y expiración del certificado.
El número único de serie que identifica el certificado.
Clave pública del titular del certificado.
Puntos de distribución (URL) para verificación de la CRL.

Fuente: (BCE, 2016)

Autoridad de registro (RA)

La Autoridad de Registro se encarga de garantizar el servicio de identificación dentro de la PKI, siendo responsables de facilitar el proceso de registro tanto de solicitantes como de suscriptores de certificados, valida datos y finalmente envía la información necesaria a la Autoridad Certificadora. (Reyes Krafft & Preciado Briseño, 2009)

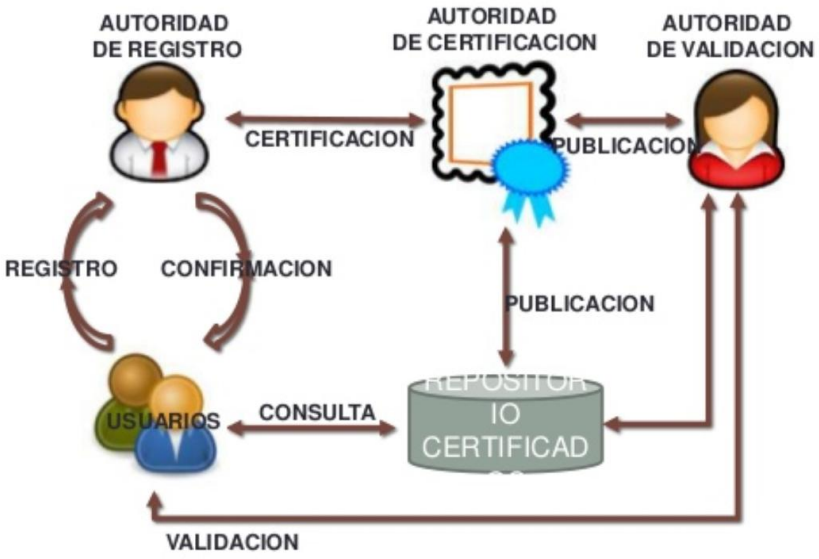


Figura 7: Autoridad de registro

Fuente: Fuente: (José Ortega, 2013)

Autoridad certificadora (CA)

El Banco Central del Ecuador es una Entidad de Certificación, misma que fue acreditada como tal por el Consejo Nacional de Telecomunicaciones, mediante la Resolución 481-20-CONATEL-2008 del 08 de octubre de 2008 y renovada mediante la Resolución ARCOTEL-2018-0902 de 25 de octubre de 2018**.** (BCE, 2016)

Esta entidad Certificadora se encarga de emitir y revocar certificados digitales, mismas que son usadas en las firmas digitales, para la que se emplea la criptografía de clave pública. (Universidad de Murcia, 2011). Cuando una CA emite un certificado lo genera en un formato X.509 (ver sección 1.2.4.). Cutanda (citado por Holguín García, 2018)

Figura 8: Autoridad certificadora

Fuente: (Hugo David Calderon Vilca, 2011)

Renovación de certificado

El proceso de renovación de certificados se realiza cuando las claves se han expirado o cuando la clave privada se vio comprometida o vulnerada, en otro caso también se pueden dar en algún caso de alguna actualización importante del propietario. (García, 2014)

Revocación de certificado

La entidad certificadora debe notificar a todas las entidades cuando un certificado es suspendido, debido a que los certificados digitales son utilizados como credenciales de identificación como propietario con un sistema u otros sistemas. (García, 2014)

Aplicaciones habilitadas para PKI

Hace referencia a los programas o softwares que son aptos para el uso de certificados digitales. (Holguín García, 2018)

1.2.3. Tipos de Certificados emitidos por el BCE

Según mencionan en la página web del BCE (2016), los tipos de certificados emitidos por esta entidad certificadora son:

Tabla 1.5: Tipos de certificados

Certificado de firma digital de Persona Natural	Certifica la identidad del titular dentro del entorno de sus negocios, el mismo que será responsable como propietario de todo lo que firme.
Certificado de firma digital de Persona Jurídica	Identifica una empresa o sociedad como tal y cumple con sus obligaciones administrativas o institucionales a nombre de la misma.
Certificado de firma digital de Funcionario Público	Identifica a un funcionario o servidor público, quien se hará responsable a nivel institucional de todo lo que firme.

Fuente: Propia

1.2.4. Estándar X.509 de Infraestructura de Clave Pública

La Unión Internacional de Telecomunicaciones (2016) (UIT), construyó un directorio que pudiera almacenar claves y dispositivos de todos los usuarios a nivel mundial, lo que dio origen al estándar X.500 según (Albarqi, Alzaid, Ghamdi, Asiri, & Kar, 2015).

Reshma Afshar (2015) manifiesta que ante la necesidad de garantizar autenticación para el uso de certificados digitales nace el modelo X.509, a su vez, bajo la recomendación de la UIT especifica que se debe manejar directorios que cumplan la norma UIT-T X.509, debido a que esta se adapta al formato de certificados digitales emitidos por el BCE. (Sector & Itu, 2016)

Este estándar define la sintaxis de los certificados como se puede observar en la Figura 9. Los campos principales del certificado se describen en la Tabla 6, estas descripciones dan una idea general de la función que cumple cada campo que contiene el certificado digital. (María Laura Irigoitia, 2016)

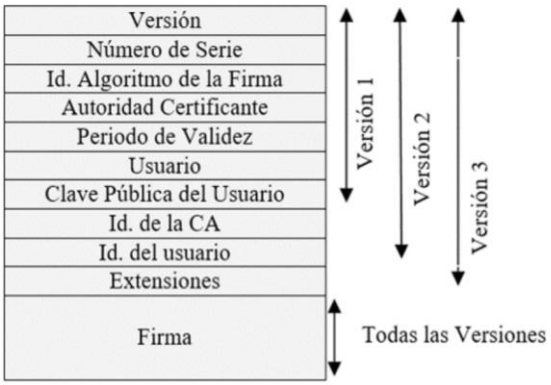


Figura 9: Formato de certificado X.509 versión 3

Fuente: (Holguín García, 2018)

Tabla 1.6: Campos de un certificado X.509

Campo	Significado
Versión	Versión del estándar X.509.
Número de serie	Este número junto al nombre de la CA identifican de manera única al certificado.
Algoritmo de firma	Algoritmo utilizado para firmar el certificado.
Emisor	El nombre de la CA.
Validez	Fecha inicio y fecha fin de validez del certificado.
Usuario	Datos del usuario firmador
Clave pública	Clave pública del usuario e ID del algoritmo usado para generar dicha clave.
ID del emisor	Identificador único de la CA.
ID del usuario	Identificador único del usuario firmador.
Extensiones	Extensiones permitidas del certificado.
Firma	Firma digital, firmada por la clave privada de la CA.

Fuente: (María Laura Irigoitia, 2016)

1.3. Introducción a las firmas digitales

1.3.1. Integridad de los datos

Naranjo (2010) anuncia que, el servicio de integridad se puede garantizar gracias al uso de funciones hash y criptografía asimétrica. Mencionada la función de un algoritmo hash (ver sección 1.1.4.), se entiende que, si se aplica una función hash a un mensaje, el valor hash que se obtiene es como la huella digital del mensaje; con tan solo un bit alterado del mensaje original, el valor hash será diferente (ver Figura 6).

1.3.2. Firma electrónica y firma digital

Tabla 1.7: Diferencias entre firma electrónica y firma digital

Firma electrónica	Firma digital
Según la página web BlogNeothek (2017) la firma electrónica equivale a una firma manuscrita digitalizada , hace referencia a un concepto jurídico, es un método de identificación, que puede utilizar varios medios electrónicos como puede ser una firma digital o un lápiz electrónico.	Es el resultado de aplicar algoritmos de una función hash seguros al contenido del documento, de esta manera se genera la firma del documento electrónico.

Fuente: (AprenderCompartiendo, 2016)

1.3.3. Firma digital

La firma digital es un método criptográfico que permite garantizar la identidad del firmante, así como también permite asegurar la integridad, la confidencialidad de los datos y el no repudio de la información. (María Laura Irigoitia, 2016)

Para firmar un documento digital, el autor cifra dicho documento con su clave privada. La validez de dicha firma en el documento podrá ser verificada por cualquier persona que disponga de la clave pública del autor. (Mike Ashley, 2016)

La firma digital es capaz de confirmar que el documento es auténtico y confiable, debido a que una Autoridad Certificadora actúa como intermediaria en términos de verificar la identidad del firmante. (BlogNeothek, 2017)

Objetivo

García (2014) menciona que, el objetivo principal de la firma digital es la optimización de los trámites, ya que permite una transacción segura de información en documentos computacionales garantizando los siguientes aspectos:

Figura 10: Objetivos de la firma digital

Fuente: (Leones, 2018)

1.3.4. Generación de una firma digital

El usuario firmante genera o aplica un algoritmo matemático llamado función hash, el cual se cifra con la clave privada del mismo dando como resultado una firma digital, la misma que se enviará adjunta al mensaje original. De esta manera el firmante, adjuntará al documento una marca que es única para dicho documento y que sólo él es capaz de producir. (Gijón, 2014)

Figura 11: Proceso de firma digital
Fuente: (HermesSoft, 2011)

1.3.5. Aplicación de la Firma Digital

iProfesional (2018) menciona en su página web algunas posibilidades de uso de la firma digital, como los siguientes:

- Trámites del gobierno (Gobierno Electrónico)
- Gestión documental (Cero papeles)
- Compras públicas
- Dinero electrónico
- Balances electrónicos
- Trámites judiciales y notariales
- Comercio electrónico

- Facturación electrónica
- Solicitud y contratos electrónicos
- Servicios web
- Transacciones bancarias

Para la elaboración del presente trabajo, se usará como referencia de uso a la Gestión Documental.

1.4. Contenedores de almacenamiento de un certificado digital

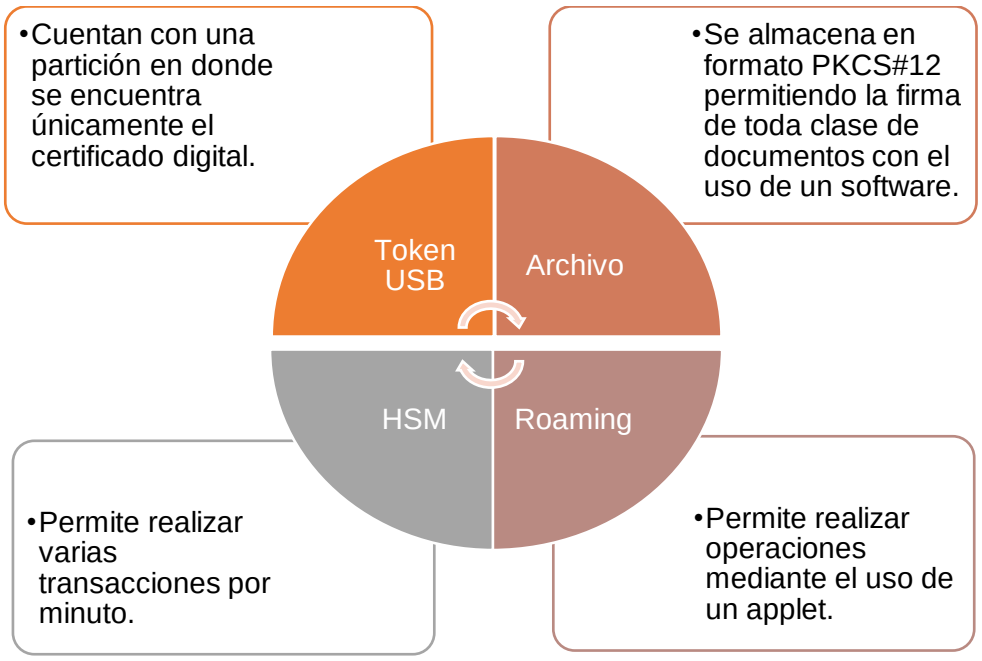


Figura 12: Contenedores de un certificado digital

Fuente: (Chulde, 2016)

Entre los más usados están: certificado tipo token y certificado tipo archivo.

1.4.1. Tipos de token de seguridad

Tabla 8: Principales tokens

Token OTP	Password	Token USB
Contraseña de un solo uso, se requiere una contraseña nueva para cada inicio de sesión, de esta manera se evita que	Es una forma de autenticación que usa información secreta para controlar los accesos a ciertos recursos. (Keitling	Se usan para almacenar no solo contraseñas, sino también claves criptográficas como firmas digitales o datos biométricos. (Keitling

un atacante que haya capturado el usuario y la contraseña pueda volver a reutilizarla. (Salmón Corp. Blog, 2016)	Daysi Salinas Hinojosa, 2013)	Daysi Salinas Hinojosa, 2013)

Figura 13: Token se seguridad

Fuente: (Solidpass, 2013)

Figura 14: La contraseña perfecta

Fuente: (Santiago Campillo, 2015)

Figura 15: Tokens USB de PKI

Fuente: (Registro Civíl, 2019)

Fuente: Propia

1.4.2. Certificado almacenado en dispositivo token USB

El dispositivo token USB es un contenedor en el que se almacena de manera segura las claves privadas de los usuarios, estas se utilizan para su autenticación y portabilidad del certificado digital. (María Laura Irigoitia, 2016)

Para firmar con este tipo de certificado, el usuario tendrá que estar conectado obligatoriamente a una red con acceso a internet, ya que, al ser un certificado emitido por una Entidad Certificadora autorizada requiere que los datos que se sellarán en el documento sean migrados desde la API del Registro Civil.

El dispositivo que se usará es el Token USB “SafeNet eToken touch 5300|Gemalto”, el cual contiene una forma adicional de autenticación por *touch*, para poder firmar un documento además de tener el token y conocer la contraseña hay que tocarlo para confirmar la presencia del usuario. (Sitepro, 2019)

1.4.3. Certificado almacenado en archivo

"Contenedor en el que se almacena en formato de archivo PKCS#12 lo que permite la firma de toda clase de documentos con el uso de un software específico para el procedimiento" (ICERT-EC Entidad de Certificación, 2017).

1.4.4. Java Keytool

Es una herramienta de línea de comandos que administra un almacén de claves criptográficas, cadena de certificados X.509, entre otros certificados de confianza. Permite manejar certificados para habilitar el SSL en un servidor. (Oracle, 2017)

Protocolo SSL: Protocolo de Capa de Sockets Seguros. En la página web DigiCert (2018) menciona que este protocolo permite cifrar el tráfico de datos entre dos servidores web protegiendo la conexión, de esta manera impide que un hacker pueda acceder a la información que se transmite de un punto a otro.

El certificado digital tipo archivo se generará a partir de esta herramienta.

1.4.5. Tipos de extensiones de archivos de certificados

IBM (2017) indica que los certificados y las claves se almacenan en distintos tipos de archivos, pero, los archivos que almacenan certificados y claves que mantienen el estándar X.509 pueden tener las siguientes extensiones:

- .cer: Es una solicitud de firma del certificado, incluye los detalles clave del certificado solicitado.
- .pem: Contiene una línea de encabezado y pie de página, los datos en el medio son los datos de base 64.
- .arm: Contiene una representación ASCII codificada en base 64 de un certificado. Incluye clave pública, pero no clave privada.
- .der: Contiene datos binarios
- .pfx (PKCS#12): Contiene un certificado emitido por una Autoridad Certificadora y la clave privada correspondiente.

```
-----BEGIN CERTIFICATE-----
... base 64 encoding of the DER encoded certificate
    with line endings and padding with equals signs ...
-----END CERTIFICATE-----
```

Figura 16: Codificación de extensión .pem

Autor: (StackOverflow, 2017)

1.4.6. Proceso de uso de un certificado digital

Según la página web Yofacturo.bo (2015), el proceso que se sigue para firmar un documento digitalmente con un archivo es el siguiente:

- Poseer un certificado digital, el cual es un documento informático que certifica la identidad del usuario. Este documento está firmado por una Autoridad Certificadora (ver sección 1.2.2.).
- El usuario remitente usando un certificado de manera segura y una contraseña, aplica un algoritmo hash sobre el documento a firmar.
- Mediante un programa que hará la firma leyendo el certificado, el usuario remitente encripta el resultado del hash generando así la firma digital sobre el documento.
- La firma digital se añade al final del texto original.

Figura 17: Diagrama de firma digital

Fuente: (Yofacturo.bo, 2015)

1.5. Sellado de tiempo o Time-Stamping y su relación con las firmas digitales

Un sellado de tiempo permite probar la integridad de una persona, es decir, prueba que los datos existieron en algún momento y que no han sido alterados por ningún motivo. (Signaturit, 2017)

Uno de los requisitos que hacen que un proceso de firmas digitales sea seguro es la integridad, por lo tanto, garantiza que un documento firmado no haya sido modificado.

Las Autoridades de Sellado de Tiempo (TSA) utilizan la Infraestructura de Clave Pública (PKI). Un TSA actúa como tercera parte de confianza testificando la existencia de dichos datos electrónicos en una fecha y hora exacta, permitiendo incorporar la hora a la que fue firmado dentro del documento.

Mientras que en la página web del Consejo de la Judicatura (2017), menciona lo siguiente:

> El servicio TSP de los equipos de la TSA(Autoridad de Sellado de Tiempo) procesa las peticiones TSP enviadas, sobre HTTP, por las aplicaciones y los servicios que solicitan sellos de tiempo a la TSA (por ejemplo, para incorporarlos en firmas), enviando las correspondientes respuestas TSP que contienen los correspondientes sellos de tiempo emitidos por la TSA, conforme al estándar [RFC3161].
> Los sellos de tiempo emitidos están firmados con la clave privada correspondiente al certificado de firma de sellos de tiempo de la TSA.

1.6. Normativa de la firma electrónica

1.6.1. Declaración de Prácticas de Certificación (DPC)

Esta DPC cumple con lo dispuesto en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos de la República del Ecuador. (BCE, 2016)

1.6.2. Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos

En el año 2002 se aprobó la ley que protege y garantiza el uso de firmas electrónicas y mensajería de datos, debido a que se ha considerado que el uso de la información y redes eléctrica son herramientas fundamentales para el desarrollo del comercio y producción. Por esta razón, el análisis de la Ley de Comercio Electrónico, Firmas Electrónicas y

Mensajes de Datos es importante para la fundamentación del presente trabajo. (García, 2014)

En el título II de las Firmas Electrónicas, Certificados de Firma Electrónica, Entidades de Certificación de Información, Organismos de Promoción de los Servicios Electrónicos, y de Regulación y Control de las Entidades de Certificación Acreditadas; capítulo I de las Firmas Electrónicas, citadas en la Ley de Comercio Electrónico (2011) se establece que:

> Art. 13.- Firma electrónica. - Son los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que puedan ser utilizados para identificar al titular de la firma en relación con el mensaje de datos, e indicar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos. (p.4).

En el siguiente Artículo proporcionado por la Ley de Comercio Electrónico (2011) se detalla los efectos que posee una firma electrónica al momento de su uso:

> Art. 14.- Efectos de la firma electrónica. - La firma electrónica tendrá igual validez y se le reconocerán los mismos efectos jurídicos que a una firma manuscrita en relación con los datos consignados en documentos escritos, y será admitida como prueba en juicio. (p. 5).

A continuación, para la verificación y validación de los artículos mencionados y revisión de otros artículos relacionados a las firmas electrónicas se adjunta el enlace de la página oficial del Banco Central del Ecuador, en la que se adjuntan las Leyes mencionadas anteriormente así como también los Reglamentos de la Ley de Comercio Electrónico: https://www.eci.bce.ec/marco-normativo

1.7. Metodologías de trabajo

Actualmente el mundo se enfrenta a varios cambios respecto a negocios y tecnología, por esta razón, se debe cambiar también la forma en la que se genera proyectos nuevos adoptando una metodología ágil de trabajo.

Las metodologías ágiles se definen como un conjunto de tareas y procesos, que son dirigidos a la gestión de proyectos, tanto necesidades como las soluciones que se dan a estas evolucionan con el tiempo. (Quonext, 2018)

Existen diferentes opciones para trabajar con una metodología ágil, entre las cuales se puede destacar a las siguientes:

Tabla 1.9: Tipos de metodologías de trabajo

Scrum	Kanban	XP
Trabajo por iteraciones, herramienta ágil para aumentar la productividad. Adoptan una estrategia de desarrollo incremental planificando bloques temporales, incluyendo en sus iteraciones: planificación, requisitos, diseño, análisis, codificación, etc.	Herramienta orientada a la gestión de proyectos especialmente complejos o en los que se presenta un cuello de botella, es decir, acumulación de tareas y funciones.	Las técnicas de Xtreme Programming permite flexibilidad y cambios en los requisitos de trabajo. Su esencia es la adaptabilidad ante todo, pensada en agregar valor y calidad al proyecto.

Fuente:(OBS Business School, 2019)

Después de analizar las diferentes metodologías de trabajo propuestas, se decidió usar la Metodología SCRUM por adaptarse a las condiciones de trabajo requeridos.

1.8. Metodología SCRUM

Una metodología ágil para el desarrollo de Software es Scrum, la misma que se define como un “marco de trabajo para el desarrollo y el mantenimiento de productos complejos” (Schwaber & Sutherland, 2014, p.4), esta metodología es ligera, fácil de entender y moderadamente difícil de llegar a dominar. Mientras que La Organización Mundial de Scrum (citado por Alejandro Frechina, 2018) afirma que:

> Scrum es un proceso de gestión que reduce la complejidad en el desarrollo de productos para satisfacer las necesidades de los clientes. Los Scrum Masters, equipos de desarrollo y Product Owners trabajan juntos alrededor de requisitos y tecnologías para entregar productos funcionando de manera incremental aplicando su experiencia.

Schwaber & Sutherland (2014) aseguran que scrum es simple pero complejo, y que las compañías que consiguen implementar esta metodología consiguen mejoras de 4 a 10 veces en productividad y competitividad.

Se planifica actividades semanales, al final de cada Sprint o iteración se va revisando el trabajo y así se va validando si se cumplió con el objetivo planteado para dicha semana. En función de esto, se priorizan y planifican nuevas actividades en las que se invertirá recursos en el siguiente Sprint (Anónimo, 2019). Se conoce como Sprint a un bloque de tiempo llamado “time-box” que consiste en una definición de lo que se va a construir, un diseño y un plan flexible que guiará la construcción, el trabajo y el producto resultante. (Schwaber & Sutherland, 2014)

Figura 18: La metodología SCRUM

Fuente: (Alejandro Frechina, 2018)

La implementación de este proyecto será desarrollada bajo esta metodología.

CAPÍTULO II

2. DESARROLLO

2.1. Metodología de desarrollo

La metodología de desarrollo usada para la implementación de este proyecto es SCRUM, debido a que se trata de una metodología ágil, misma que permite que el desarrollo de un proyecto se haga de una forma incremental.

Se debe mencionar que cada Sprint será de dos semanas, en las que se desarrollarán 28 horas por sprint.

2.2. Roles SCRUM

Product Owner: Ing. Pedro Granda

Scrum Master: Ing. Mauricio Rea

Team: Lizeth Otavalo

2.3. Artefactos SCRUM

2.3.1. Matriz de planificación

El desarrollo del presente proyecto se encuentra planificado en seis sprints, en los que se detallan las actividades que se irán cumpliendo a lo largo de la implementación de esta aplicación, estas actividades permitirán evidenciar los resultados que se obtendrán al finalizar este proyecto, la planificación de trabajo se detalla a continuación:

PLANIFICACIÓN DE TRABAJOS DE DESARROLLO

Sprint **1**
Total horas **28**
Fecha Inicio SP1: 29/05/2019
Fecha Final SP1: 12/06/2019

Historia de usuario	Desarrollador	Fase Desarrollo	Tipo	TAREA	TIEMPO ESTIMADO (Horas)	TIEMPO REAL (Horas)	ESTADO
Matriz de planificación	Lizeth Otavalo	Planificación	Nueva	Formalización de la matriz de planificación	1:00	1:00	Hecho
				Organización y análisis de los documentos para los Sprints 1,2,3 y 4	1:30	2:00	Hecho
Acta de constitución	Lizeth Otavalo	Desarrollo	Nueva	Recolección de información del proyecto	0:30	0:45	Hecho
				Identificación del propósito y la justificación del proyecto	0:30	0:30	Hecho
				Descripción del proyecto y entregable	0:30	0:30	Hecho
				Requerimientos de alto nivel (requisitos del producto y proyecto)	1:20	1:00	Hecho

				Cronograma de hitos principales	0:30	0:30	Hecho
				Definición del presupuesto estimado	0:20	0:20	Hecho
				Lista de interesados (stakeholders)	0:20	0:20	Hecho
				Identificación de requisitos de aprobación del proyecto	0:30	0:30	Hecho
				Asignación del gerente de proyecto y nivel de autoridad	0:20	0:15	Hecho
				Asignación de personal y recursos preasignados	0:30	0:20	Hecho
Especificaciones de requisitos	Lizeth Otavalo	Desarrollo	Nueva	Introducción	1:30	1:00	Hecho
				Descripción general	2:00	1:00	Hecho
				Análisis de los requisitos específicos	3:00	2:30	Hecho
				Análisis de los requisitos funcionales	1:20	2:00	Hecho
				Análisis de los requisitos no funcionales	1:20	1:00	Hecho
Historias de usuario	Lizeth Otavalo	Desarrollo	Nueva	Creación de las historias de usuario: generales	2:00	1:00	Hecho
				Creación de las historias de usuario: específicas	3:00	3:00	Hecho
Casos de uso y diagrama de actividades	Lizeth Otavalo	Desarrollo	Nueva	Desarrollo de casos de uso	3:00	2:30	Hecho
				Diagrama de actividades	3:00	2:00	Hecho
				TOTAL	**28:00:00**	**24:00:00**	

Sprint **2**
Total horas **28**
Fecha inicio SP2: 13/06/2019
Fecha Final SP2: 27/06/2019

Historia de usuario	Desarrollador	Fase Desarrollo	Tipo	TAREA	TIEMPO ESTIMADO (Horas)	TIEMPO REAL (Horas)	ESTADO
Diagrama de actividades	Lizeth Otavalo	Desarrollo	Nueva	Desarrollo de diagrama de actividades	3:00	3:30	Hecho
Arquitectura de software	Lizeth Otavalo	Desarrollo	Nueva	Introducción de la arquitectura de software	1:00	1:00	Hecho
				Descripción de la arquitectura de software	1:00	1:00	Hecho
				Definición de la herramienta en el entorno de desarrollo	0:30	0:20	Hecho
				Base de datos y herramienta case para el manejo de la BDD	0:30	0:30	Hecho
				Sistema operativo	0:10	0:10	Hecho
				Diagrama de arquitectura de Software	1:00	1:40	Hecho
Wireframe	Lizeth Otavalo	Desarrollo	Nueva	Prototipo de pantalla general	2:00	1:30	Hecho
				Prototipo de pantalla de repositorio de archivos	1:30	1:30	Hecho
				Prototipo de pantalla de selección de archivo	1:00	0:45	Hecho
				Prototipo de pantalla de inserción de firmas	1:30	2:15	Hecho
				Prototipo de pantalla de documento firmado	1:00	1:30	Hecho
Instalación y configuración de herramientas a usar	Lizeth Otavalo	Desarrollo	Nueva	Instalación de Sistema Operativo Fedora	2:00	8:00	Hecho
				Instalación de servidor de aplicaciones WildFly, IDE de desarrollo Eclipse	2:00	4:00	Hecho
				Configuración de Jboos, WildFly y git en Eclipse	2:00	3:00	Hecho
				Configuración de PostgreSQL y PgModeler	1:00	10:00	Hecho
		Desarrollo	Nueva	Creación del proyecto en un Workspace	0:30	0:10	Hecho

Creación y configuración del proyecto	Lizeth Otavalo			Creación de la BDD en pgModeler y pgAdmin	1:30	2:00	Hecho
				Verificación e importación de librerías a usar	0:30	0:10	Hecho
				Mapeo de la BDD en el proyecto	0:30	0:15	Hecho
				Configuración de JPA, JSF	1:00	0:15	Hecho
Diseño y codificación general	Lizeth Otavalo	Desarrollo	Nueva	Diseño y codificación de la vista del repositorio de archivos	3:00	3:15	Por hacer
				TOTAL	**28:00:00**	**43:30:00**	

Sprint **3**
Total horas **28**
Fecha Inicio SP3: 28/06/2019
Fecha Final SP3: 12/07/2019

Historia de usuario	Desarrollador	Fase Desarrollo	Tipo	TAREA	TIEMPO ESTIMADO (Horas)	TIEMPO REAL (Horas)	ESTADO
Codificación de proyecto general	Lizeth Otavalo	Desarrollo	Nueva	Codificación de manager y controller para el repositorio	5:00	6:00	Hecho
				Vinculación de la vista de la pantalla principal con la vista del repositorio de archivos	2:00	1:30	Hecho
Pruebas de funcionamiento y correcciones	Lizeth Otavalo	Pruebas	Nueva	Pruebas de funcionamiento del repositorio de archivos	3:00	2:00	Hecho
				Corrección de errores	5:00	6:00	Hecho
				Pruebas de funcionamiento del repositorio de archivos	4:00	2:30	Hecho
Codificación de proyecto general	Lizeth Otavalo	Desarrollo	Nueva	Diseño y codificación de la vista de firmas digitales	4:00	4:30	Hecho
				Codificación de manager y controller de firmas digitales	5:00	6:30	Hecho
				TOTAL	**28**	**29:00:00**	

Sprint **4**
Total horas **28**
Fecha Inicio SP4: 13/07/2019
Fecha Final SP4: 27/07/2019

Historia de usuario	Desarrollador	Fase Desarrollo	Tipo	TAREA	TIEMPO ESTIMADO (Horas)	TIEMPO REAL (Horas)	ESTADO
Codificación de proyecto general	Lizeth Otavalo	Desarrollo	Nueva	Codificación de reconocimiento de extensiones de documento permitidos para firmas electrónicas	5:00	4:30	Hecho
				Codificación de reconocimiento de token USB e ingreso de contraseña	8:00	10:00	Hecho
				Vinculación de la vista de firmas digitales con el repositorio	4:00	3:40	Hecho
Instalación y configuración de certificados y drivers para firma digital	Lizeth Otavalo	Desarrollo	Nueva	Instalación de complementos necesarios para la firma electrónica, emitidos por el Banco Central del Ecuador	2:00	0:20	Hecho
Pruebas de funcionamiento y correcciones	Lizeth Otavalo	Desarrollo	Nueva	Pruebas de funcionamiento	2:00	1:30	Hecho
				Corrección de errores	5:00	6:30	Hecho
				Pruebas de funcionamiento	2:00	2:30	Hecho
				TOTAL	**28**	**29:00:00**	

Sprint **5**
Total horas **28**
Fecha Inicio SP5: 28/07/2019
Fecha Final SP5: 11/08/2019

Historia de usuario	Desarrollador	Fase Desarrollo	Tipo	TAREA	TIEMPO ESTIMADO (Horas)	TIEMPO REAL (Horas)	ESTADO
Instalación y configuración de herramientas a usar	Lizeth Otavalo	Desarrollo	Nueva	Instalación de IDE de desarrollo Netbeans	1:00	0:30	Hecho
				Instalación de OpenSSL, creador de certificados digitales	1:30	1:00	Hecho
Creación y configuración del proyecto	Lizeth Otavalo	Desarrollo	Nueva	Importar jar's necesarios para la firma digital	0:30	0:10	Hecho
Diseño y codificación de proyecto	Lizeth Otavalo	Desarrollo	Nueva	Generación de certificado digital con OpenSSL	1:00	1:00	Hecho
				Diseño de interfaz gráfica de firmas digitales con archivo	3:00	3:30	Hecho
				Codificación de clase de firmas digitales	5:00	6:30	Hecho
				Codificación de método de estampado de firmas	2:00	2:30	Hecho
				Codificación de método de reconocimiento de archivo digital	5:00	6:00	Hecho
Pruebas de funcionamiento y correcciones	Lizeth Otavalo	Desarrollo	Nueva	Pruebas de funcionamiento	2:00	1:00	Hecho
				Corrección de errores	5:00	3:30	Hecho
				Pruebas de funcionamiento	2:00	1:30	Hecho
				TOTAL	**28:00:00**	**27:10:00**	

Sprint **6**
Total horas **28**
Fecha Inicio SP6: 03/09/2019
Fecha Final SP6: 17/09/2019

Historia de usuario	Desarrollador	Fase Desarrollo	Tipo	TAREA	TIEMPO ESTIMADO (Horas)	TIEMPO REAL (Horas)	ESTADO
Creación y configuración del proyecto	Lizeth Otavalo	Desarrollo	Nueva	Creación de proyecto Maven de firmas digitales	1:00	1:00	Hecho
				Implementación de librería rúbrica para reconocimiento de token digital de firmas electrónicas	2:00	2:30	Hecho
Instalación y configuración de certificados y drivers para firma digital	Lizeth Otavalo	Desarrollo	Nueva	Diseño de interfaz gráfica de firmas digitales con token	2:00	3:00	Hecho
				Implementación de métodos de firma con token	5:00	8:30	Hecho
				Codificación de estampado de firma en la última hoja	3:00	4:30	Hecho
				Codificación de generación de certificado digital	4:00	5:00	Hecho
				Codificación de datos necesarios para la firma	4:00	3:00	Hecho
Pruebas de funcionamiento y correcciones	Lizeth Otavalo	Desarrollo	Nueva	Pruebas de funcionamiento	2:00	1:00	Hecho
				Corrección de errores	3:00	6:00	Hecho
				Pruebas de funcionamiento	2:00	1:00	Hecho
				TOTAL	**28:00:00**	**35:30:00**	

2.3.2. Cartillas de Historias de Usuario

En las siguientes cartillas de historias de usuario se podrá visualizar de una manera explícita y detallada lo que se implementará en el software final.

Historias de Usuario Nro. 1| Diseño de la página principal

Historia de Usuario		
Número:	**1**	**Usuario:** Usuario validador
Nombre historia: Diseño de la página principal		
Prioridad en negocio: Alta		**Riesgo en desarrollo:** Media
Puntos estimados: 5		**Sprint asignada:** 5
Programador responsable: Lizeth Otavalo		
Descripción: Creación de la vista del proyecto, al que tendrán acceso los usuarios validadores del mismo. En esta pantalla se podrá visualizar opciones como: buscar documento, seleccionar certificado digital (token o archivo), campo de contraseña, firmar documento y verificar documento firmado.		
Observaciones: *Esta pantalla podrá ser visualizada únicamente por usuarios que tengan acceso al sistema y puedan hacer uso de la aplicación de firmas digitales.*		

Historias de Usuario Nro. 2| Creación de certificado digital con Keytool de java

Historia de Usuario		
Número:	**2**	**Usuario:** Usuario validador
Nombre historia: Creación de certificado digital con Java Keytool		
Prioridad en negocio: Alta		**Riesgo en desarrollo:** Media
Puntos estimados: 5		**Sprint asignada:** 5

Programador responsable: Lizeth Otavalo
Descripción: La creación de un certificado digital tipo archivo mediante la aplicación de generador de certificado, permite que el usuario validador pueda crear su propio certificado sin hacer uso de una herramienta externa. Este certificado contendrá los siguientes datos: Datos del usuario, razón social, país, provincia, correo electrónico y número de cédula.
Observaciones: *La contraseña del certificado únicamente debe conocerla el usuario quien creo el certificado digital, por ningún motivo se compartirá dicha clave.*

Historias de Usuario Nro. 3| Firmar documento antes de subir como evidencia al repositorio

Historia de Usuario		
Número:	**3**	**Usuario:** Usuario validador
Nombre historia: Firmar documento antes de subir como evidencia al repositorio		
Prioridad en negocio: Alta		**Riesgo en desarrollo:** Alta
Puntos estimados: 5		**Sprint asignada:** 3
Programador responsable: Lizeth Otavalo		
Descripción: El usuario validador podrá firmar el documento que desee y una vez firmados subirlo al SIAD.		
Observaciones: *Los documentos firmados serán listados en el repositorio de archivos del SIAD.*		

Historias de Usuario Nro. 4| Firmar documento con certificado tipo archivo

Historia de Usuario		
Número:	**4**	**Usuario:** Usuario validador
Nombre historia: Firmar documento con certificado tipo archivo		
Prioridad en negocio: Alta		**Riesgo en desarrollo:** Media
Puntos estimados: 5		**Sprint asignada:** 5
Programador responsable: Lizeth Otavalo		
Descripción: El usuario validador que opte firmar con un certificado tipo archivo, deberá primero crear el certificado digital con la herramienta Keytool incorporado en el FirmadorSIAD. Este certificado digital podrá ser utilizado únicamente si el documento a firmar es de extensión pdf.		
Observaciones: *Los documentos firmados con este certificado únicamente serán válidos a nivel institucional.*		

Historias de Usuario Nro. 5| Firmar documento con certificado tipo token

Historia de Usuario		
Número:	**5**	**Usuario:** Usuario validador
Nombre historia: Firmar documento con certificado tipo token		
Prioridad en negocio: Alta		**Riesgo en desarrollo:** Media
Puntos estimados: 5		**Sprint asignada:** 6
Programador responsable: Lizeth Otavalo		
Descripción: El usuario validador que opte firmar con un certificado tipo token, deberá hacer la adquisición del mismo en alguna Entidad Certificadora, este tipo de certificado firmará documentos con extensión pdf.		
Observaciones: *Los documentos firmados con este certificado serán válidos a nivel nacional.*		

2.3.3. Casos de Uso

En esta sección de puede evidenciar de una forma gráfica los detalles explicados en las cartillas de historias de usuario, de esta manera se puede entender mejor el funcionamiento del software.

En la Figura 19 se presenta el caso de uso para el acceso por parte de un validador a las funciones del firmador con token.

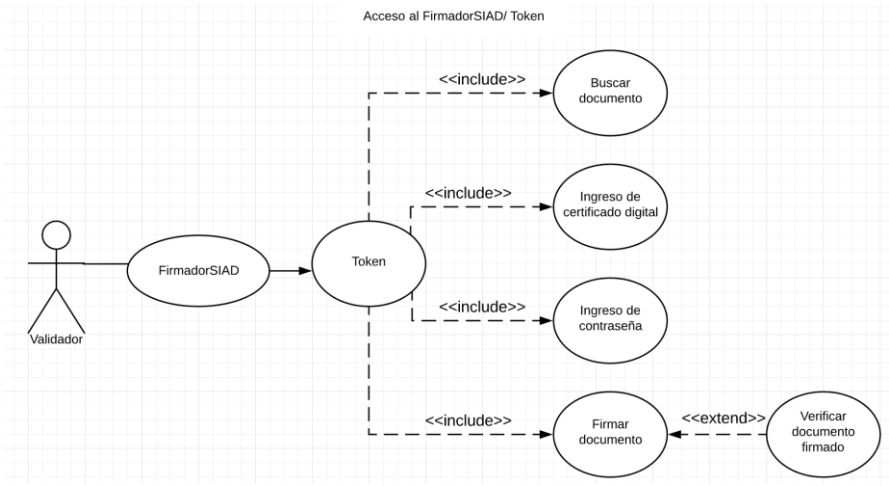


Figura 19: Caso de uso 1- Acceso al Firmador SIAD con token

Fuente: Propia

En la Figura 20 se presenta el caso de uso para el acceso por parte de un validador a las funciones del firmador con archivo.

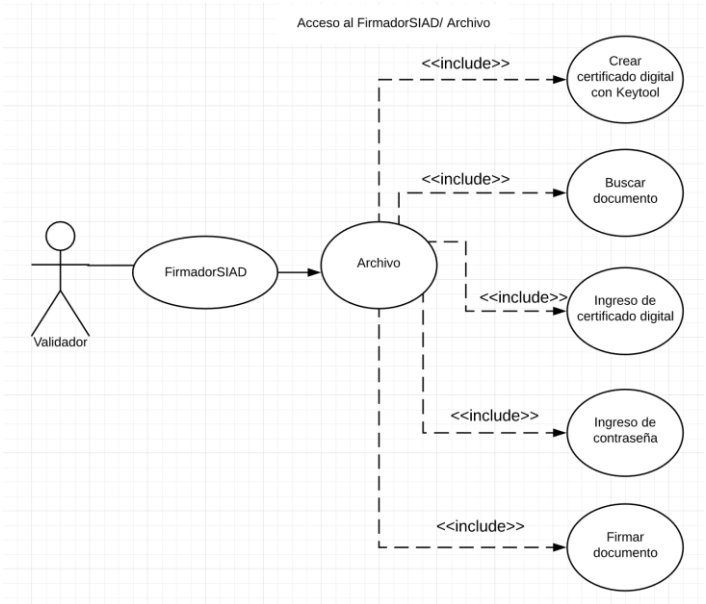


Figura 20: Caso de uso 2- Acceso al Firmador SIAD con archivo

Fuente: Propia

En la Figura 21 de presenta el caso de uso en el que se representa el proceso de uso de un documento firmado en el Firmador SIAD.

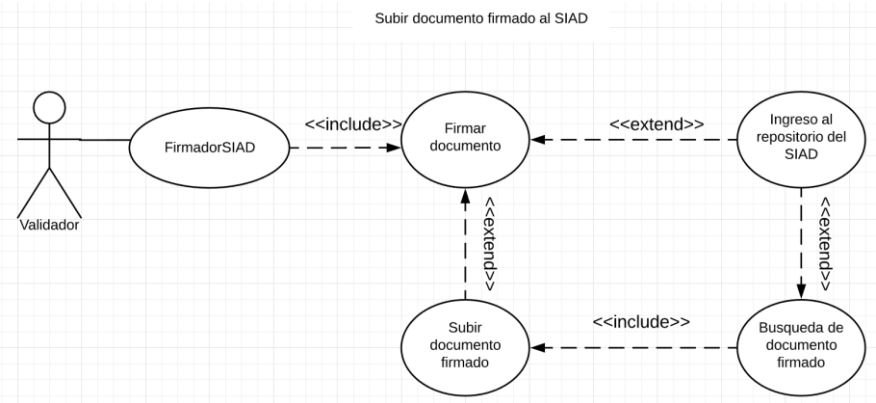


Figura 21: Caso de uso 3- Documento firmado

Fuente: Propia

2.3.4. Diagrama de actividades

El diagrama de actividades permite ver el proceso interno (validador) y externo (interfaz) que realiza el software al ejecutar la aplicación.

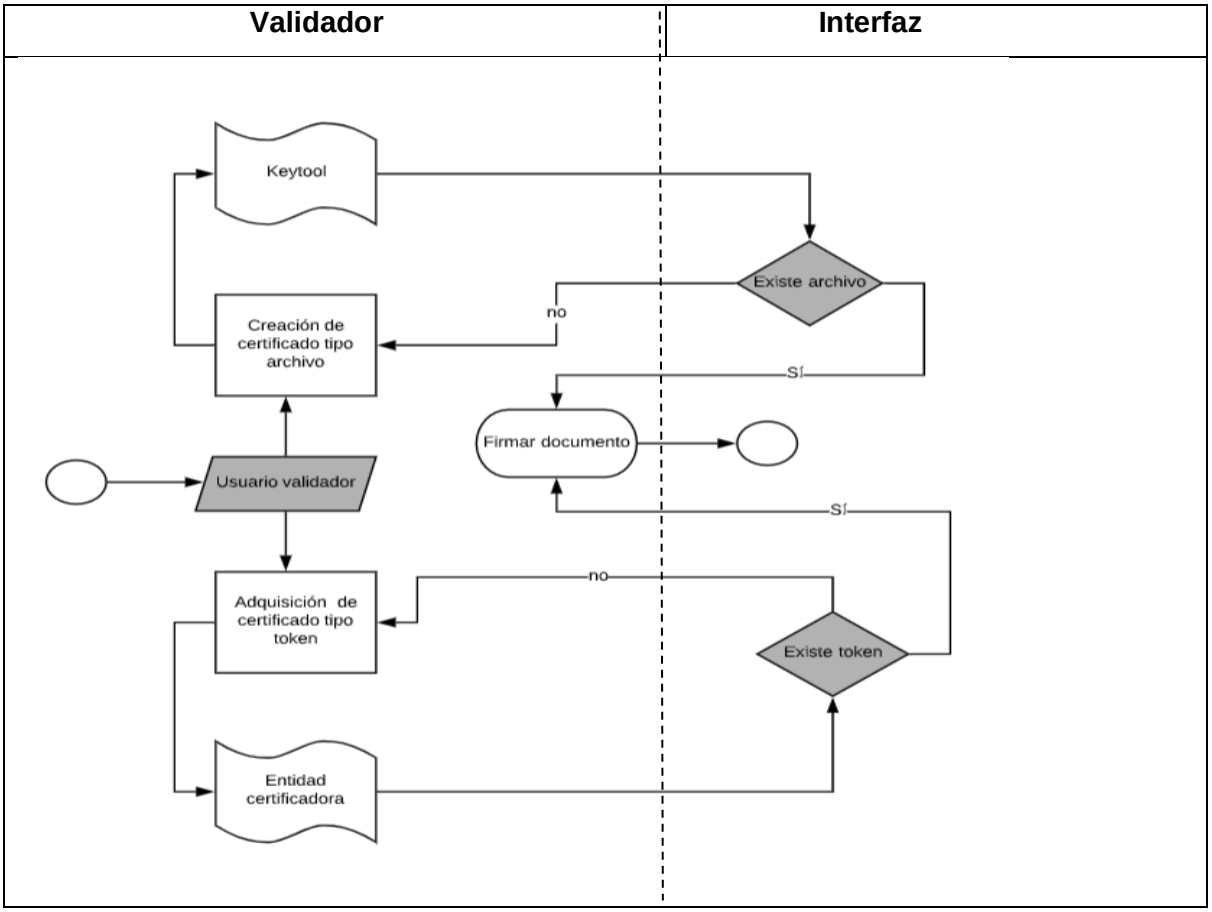


Figura 22: Diagrama de actividades

Fuente: Propia

2.3.5. Arquitectura de Software

Introducción de la Arquitectura de Software

Lenguaje de Descripción Arquitectónica: Diagramas UML

- Diagrama de Casos de Uso
- Diagrama de Actividades

Arquitectura de Software para el desarrollo del proyecto

Herramientas y Tecnologías

- Entorno de desarrollo: IDE Eclipse JEE 2018-09 y Netbeans
- Entorno de producción: Servidor Web WildFly 14.0.1. Final, Apache Tomcat
- Sistema Operativo: Windows 7, 8, 8.1, 10 y Linux
- Firmador de documentos: SafeNet eToken touch USB 5300|Gemalto
- Generador de certificados: Java Keytool
- Metodología de desarrollo: SCRUM

2.4. Pruebas de funcionamiento

2.4.1. Plan de Pruebas

Pruebas funcionales

El objetivo del plan de pruebas de funcionalidad es, validar los casos de uso que fueron anteriormente aprobados, por lo cual, se realizaron las pruebas correspondientes.

Tabla 2.1: Objetivo 1. Pruebas funcionales de diseño

Objetivo de la Prueba:	Crear el diseño visual del FirmadorSIAD.
Estrategia:	Mediante técnicas de frontend se logró definir un diseño de interfaz de software que sea llamativo y similar al SIAD.
Herramientas Requeridas:	Se requiere del servidor Wildfly
Observaciones:	El diseño visual de este software es una adaptación del SIAD, el cuál cumple con el estándar establecido por el sistema general.

Fuente: Propia

Tabla 2.2: Objetivo 2. Pruebas funcionales de codificación con Token USB

Objetivo de la Prueba:	Crear el FirmadorSIAD con certificado Token USB.
Estrategia:	Mediante la codificación de métodos que permitan la firma de documentos con dispositivo Token USB, verificador de documentos firmados y verificador de certificados vigentes, se logró desarrollar un software bastante útil y fácil de usar por el usuario, permitiendo que estos documentos sean válidos a nivel nacional.
Herramientas Requeridas:	Se requiere del servidor Wildfly, entorno de desarrollo Eclipse, Token USB y conexión a internet.
Observaciones:	Se requiere de una API proporcionada por el Registro Civil del Ecuador.

Fuente: Propia

Tabla 2.3: Objetivo 3. Pruebas funcionales de codificación con Archivo

Objetivo de la Prueba:	Crear el FirmadorSIAD con certificado en Archivo.
Estrategia:	Mediante la codificación de métodos que permitan la generación de certificados digitales tipo archivo con extensión .p12 y firmador de documentos, se logró obtener un software fácil de usar por el usuario, permitiendo que estos documentos sean válidos únicamente a nivel institucional.
Herramientas Requeridas:	Se requiere del servidor Wildfly Tomcat y entorno de desarrollo Eclipse.
Observaciones:	Se requiere generar primero el certificado para poder firmar un documento.

Fuente: Propia

Tabla 2.4: Objetivo 4. Pruebas funcionales con documentos firmados

Objetivo de la Prueba:	Subir documento firmado al repositorio del SIAD.
Estrategia:	Mediante el uso del FirmadorSIAD se logró firmar documentos, los mismos que pueden ser subidos al repositorio del sistema si el usuario lo requiere.
Herramientas Requeridas:	Se requiere del servidor Wildfly para que el repositorio sea visualizado en un navegador.
Observaciones:	El documento que se subirá al repositorio como evidencia, puede o no estar firmado por el usuario.

Fuente: Propia

Pruebas de seguridad

El objetivo del plan de pruebas de seguridad es, validar la autenticidad del usuario firmante y la verificación de que un documento no ha sido modificado después de haber sido firmado.

Tabla 2.5: Objetivo 1. Pruebas de seguridad de identidad de usuario

Objetivo de la Prueba:	Verificar que los datos del usuario firmante sean correctos.
Estrategia:	Abrir el documento firmado, mismo que contendrá los datos del usuario que firmó el documento digitalmente.
Herramientas Requeridas:	Se requiere de un documento PDF firmado por el FirmadorSIAD.
Observaciones:	El documento firmado debe tener una asignación de nombre *signed* aparte del original, que deberá abrirse sin ningún inconveniente.

Fuente: Propia

Tabla 2.6: Objetivo 2. Pruebas de seguridad de reconocimiento de CA.

Objetivo de la Prueba:	Verificar que el documento firmado sea reconocido por una Autoridad Certificadora.
Estrategia:	Abrir el documento en un visor PDF y verificar que en el contenido del panel de firmas se visualice que la validez de la firma es reconocida por una Autoridad Certificadora.
Herramientas Requeridas:	Se requiere de un documento PDF firmado.
Observaciones:	El documento firmado debe tener una asignación de nombre *signed* para poder abrir el panel de firmas digitales.

Fuente: Propia

Tabla 2.7: Objetivo 3. Prueba de seguridad de modificación de documentos firmados

Objetivo de la Prueba:	Verificar que el documento firmado no pueda ser modificado.
Estrategia:	Realizar alguna modificación en el documento firmado y guardarlo, no se permite guardar un documento firmado con algún tipo de cambio de contenido.
Herramientas Requeridas:	Se requiere de un documento PDF firmado.
Observaciones:	El documento firmado debe tener una asignación de nombre *signed* para poder abrir el panel de firmas digitales.

Fuente: Propia

Tabla 2.8: Objetivo 4. Prueba de seguridad de claves privadas

Objetivo de la Prueba:	Verificar que un documento pueda ser firmado únicamente por el usuario que contenga la clave privada.
Estrategia:	Verificar la seguridad de la clave privada del usuario ingresando el Token USB o Archivo en el FirmadorSIAD y probar distintas contraseñas.
Herramientas Requeridas:	Se requiere del FirmadorSIAD.
Observaciones:	El dispositivo Token USB puede llegar a bloquearse 3er intento de ingresar distintas contraseñas.

Fuente: Propia

Recurso Humano de Plan de Pruebas

En la Tabla 2.9 se muestra el perfil de los usuarios responsables del plan de pruebas.

Tabla 2.9: Recurso Humano - Plan de Pruebas

Nombres	Perfil
Lizeth Otavalo	Desarrollador - Estudiante UTN
Ing. Mauricio Rea	Tester – Docente UTN
Ing. Pedro Granda	Tester – Docente UTN
Ing. Daysi Imbaquingo	Tester – Docente UTN

Fuente: Propia

2.4.2. Informe de Plan de Pruebas

Pruebas del Sistema

El resultado de las pruebas de software se verá en el informe reflejado en la Tabla 2.10.

Tabla 2.10: Resultado de Pruebas de Software

Caso de Uso	<Identificador del Caso de uso>	<Número total de casos de prueba ejecutados de acuerdo al escenario>
FirmadorSIAD con Token USB	Caso de Uso – Gestión 1	5
FirmadorSIAD con Archivo	Caso de Uso – Gestión 2	3
Documento firmado	Caso de Uso – Gestión 3	5

Fuente: Propia

Pruebas de Interfaz de Usuario

El resultado de las pruebas de interfaz de usuario se puede ver reflejado en la lista de chequeo o informe representada en la Tabla 2.11.

Tabla 2.11: Resultado de pruebas de interfaz

Elemento a Revisar	Sí	No	Observaciones
Apariencia de software.	x		S/O
Contraste de colores.	x		S/O
Botones que identifican la función que cumplen.	x		Errores corregidos.

Fuente: Propia

Pruebas de Seguridad

El resultado de las pruebas de seguridad se puede ver reflejado en la lista de chequeo o informe representada en la Tabla 2.12.

Tabla 2.12: Resultado de las pruebas de seguridad

Elemento a Revisar	Sí	No	Observaciones
Datos del firmante visuales en el documento.	x		Errores corregidos.
Reconocimiento de la firma por una Autoridad Certificadora.	x		S/O
Integridad del documento.			S/O
Seguridad de claves privadas.	x		S/O

Fuente: Propia

2.5. Implementación de la solución

El Software FirmadorSIAD, se diseñó e implementó para que sea utilizado en conjunto con el Sistema Integrado de Actividad Docente (SIAD) de la Carrera de Ingeniería en Sistemas Computacionales (CISIC) y la Carrera de Software (CSOFT), dicho software permite firmar documentos y verificar documentos firmados que pueden ser subidos al repositorio del sistema, mismos, que pueden ser usados como evidencia de algún tipo de tarea que se haya revisado y aprobado por el docente validador.

El FirmadorSIAD ha sido presentado y verificado por docentes de la CISIC/CSOFT (ver Tabla 2.9), ya que, el software será utilizado por los usuarios que puedan acceder al SIAD.

Cabe recalcar que, el software FirmadorSIAD será integrado más adelante al SIAD, bajo una investigación y análisis más profundo de las versiones de las librerías de firmas digitales y Java JDK que se estén usando en ese momento.

2.6. Librerías para firmas digitales

En la siguiente tabla, se puede visualizar las librerías principales que permiten la firma digital en un documento, mismas que fueron utilizadas para el desarrollo del software firmador.

Tabla 2.13: Librerías para firmas digitales

Librería	Función	Versión
Librería Rúbrica	Rúbrica es una librería Java utilizada para aplicaciones de firmas digitales. (Arguello, 2018)	Versión utilizada en el proyecto 0.1.6.
Librería iText Pdf	iText Pdf es una librería capaz de crear, analizar, modificar y mantener documentos en formato pdf, permitiendo también firmar este tipo de documentos.	Versión utilizada en el proyecto 5.5.7.
Librería Bouncy Castle	Proporciona una API criptográfica que permite la generación de certificados, cumpliendo con el estándar X.509. (Inc, 2019)	Versión utilizada en el proyecto jdk15on-164.

Fuente: Propia

CAPÍTULO III

3. VALIDACIÓN DE RESULTADOS

3.1. Análisis e interpretación de resultados

Para el análisis e interpretación de resultados del Firmador SIAD se utilizó Pilar, que es una herramienta que sirve para el análisis y gestión de riesgos implementando la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información), con el fin de analizar amenazas en cuanto a confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.

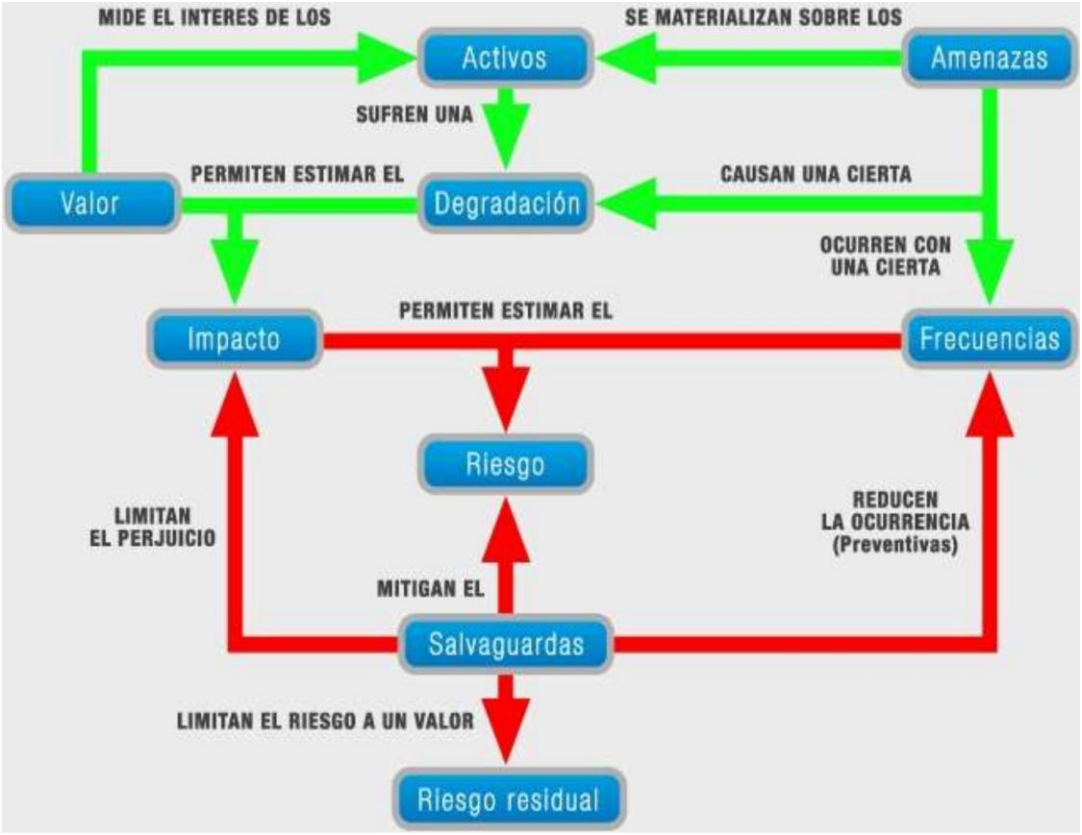


Figura 23: Pilar/EAR

(Gestión, Riesgos, Pilar, Luis, & Villarroya, 2012)

Pilar dispone de una biblioteca estándar que es capaz de realizar calificaciones de seguridad basándose en normas conocidas, como la ISO/IEC 27000 (Código de buenas prácticas para la Gestión de la Seguridad de la Información). (Nacional, 2013)

Para la valoración de resultados se procedió a ingresar los datos del software FirmadorSIAD para realizar un análisis de riesgos de tipo cualitativo, ya que de esta

manera se puede identificar los activos más significativos, identificar las amenazas más relevantes, así como también se puede establecer los activos más críticos, definiéndose como activos a varias de las acciones que realiza el software.

3.1.1. Resultados obtenidos en el Análisis de Riesgos y valoración de activos

En la Figura 24, se puede visualizar los datos con los que fue ingresado el proyecto.

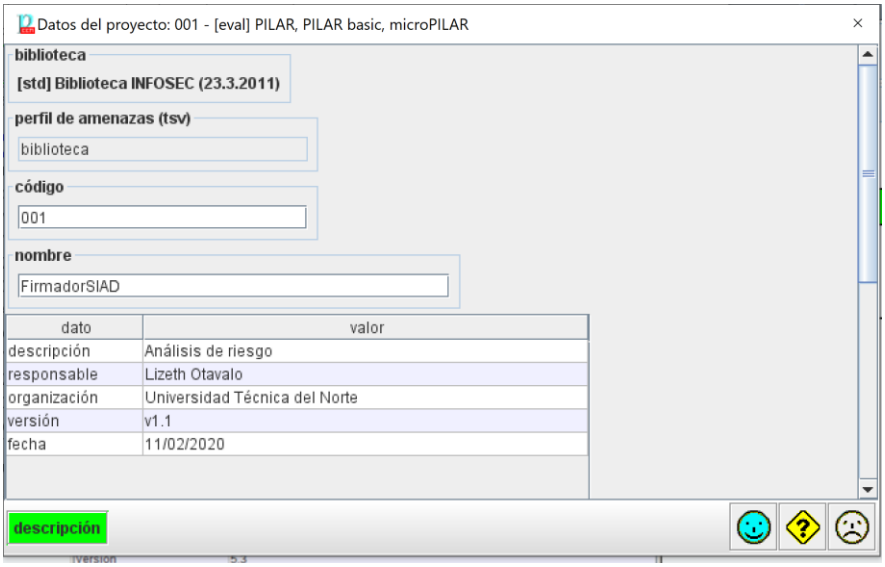


Figura 24: Datos del proyecto

Fuente: Propia

Los dominios de seguridad permiten agrupar a los activos para que sean evaluados con la misma política. Los dominios son los siguientes:

Tabla 3.1: Dominios de seguridad

Código	Dominio
CERT	Certificados digitales
SOFT	SIAD Firmador

Fuente: Propia

Identificación de activos

Los activos hacen referencia a los factores relacionados con el sistema para que pueda funcionar correctamente, y de esta manera alcance los objetivos planteados de seguridad de la información.

Para el tratamiento de estos riesgos se proponen salvaguardas o también conocidos como contramedidas, los activos identificados para la evaluación son los siguientes, teniendo en cuenta que los activos nombrados como *Certificados digitales* y *FirmadorSIAD* son activos esenciales.

Tabla 3.2: Identificación de activos

Código	Activo	Dominio
SEG	Certificados digitales (Esencial como información)	Certificados digitales
APP	FirmadorSIAD (Esencial como servicio)	SIAD Firmador
RED	Red local	Base
CON	Conexión a internet	Base
EDI	Edificio	Base
USU	Usuario validador	Base

Fuente: Propia

Las clases de activos que se relacionaron a *Certificados digitales* (activo), fueron asociados según la necesidad de evaluación de cada uno o según el daño que podría afectar a uno de ellos.

Los activos normalmente están sujetos a amenazas, cuando se indica que un activo no tiene amenazas las propuestas del perfil de amenazas se ignoran, como se puede observar en la Figura 25.

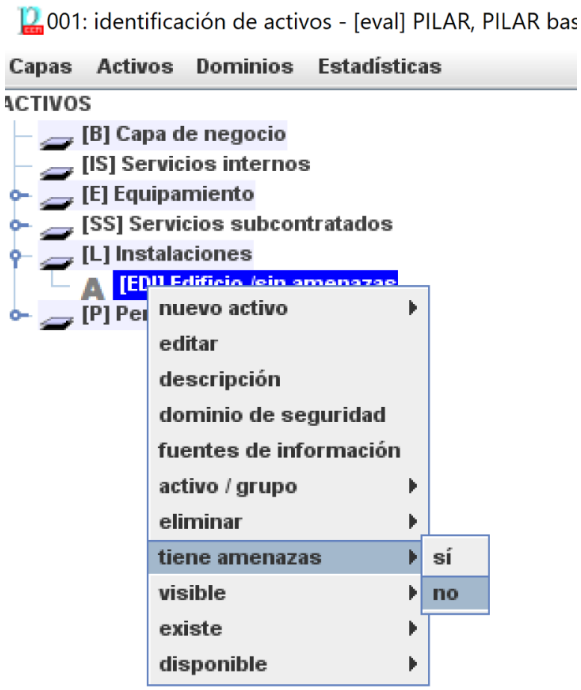


Figura 25: Identificación de activos

Fuente: Propia

En las Figuras 26 y 27 se puede visualizar las clases de activos de los activos esenciales.

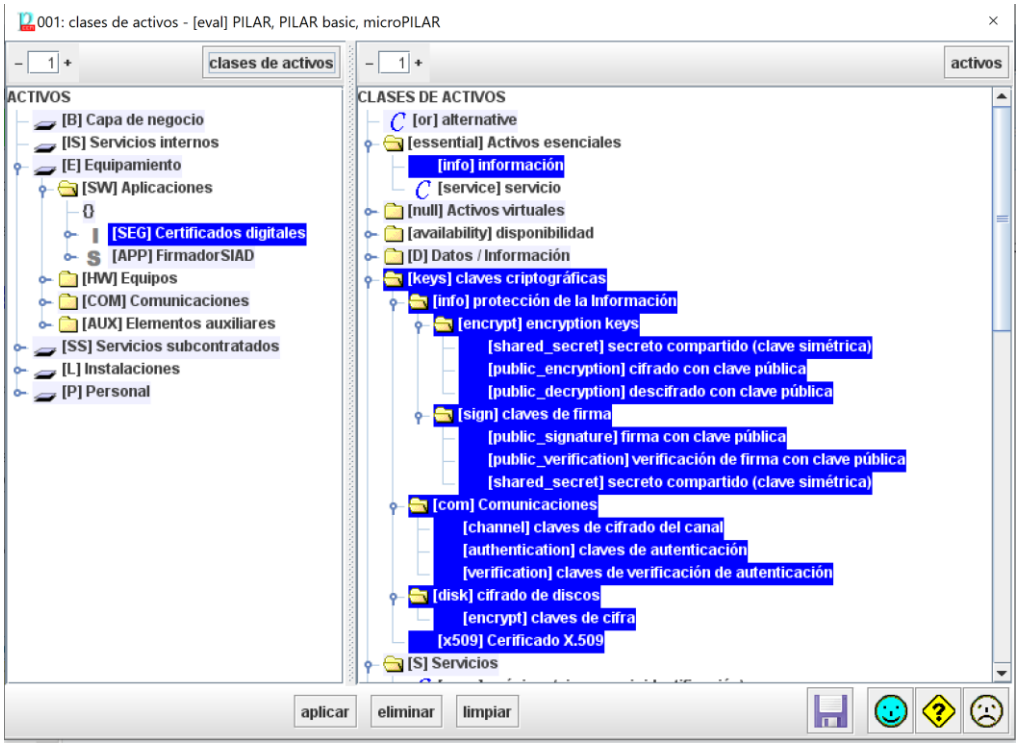


Figura 26: Clases de activos para Certificados digitales

Fuente: Propia

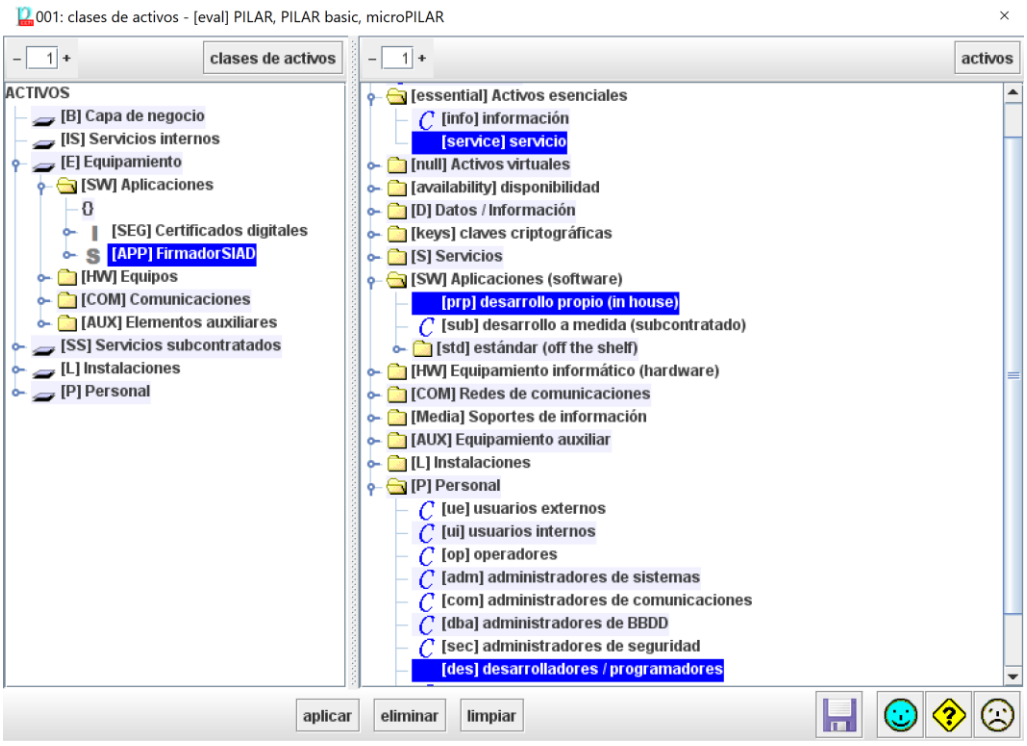


Figura 27: Clases de activos para FirmadorSIAD

Fuente: Propia

Valoración de los activos

Pilar analiza los riesgos en diferentes dimensiones como son: confidencialidad, trazabilidad, autenticidad, integridad y disponibilidad.

Tabla 3.3: Valoración de activos

Disponibilidad	Disponibilidad del activo.
Integridad	Integridad para que el activo no sea modificado.
Confidencialidad	Confidencialidad para que usuarios no autorizados accedan al activo.
Autenticidad	Autenticidad del usuario que accede al activo.
Trazabilidad	Constancia del uso del activo en cada etapa.

Fuente: Propia

La valoración que se asigna a cada activo va según el nivel de importancia que tiene cada uno, teniendo en cuenta que 0 es un criterio de valoración insignificante y 10 es absolutamente crítico.

El activo esencial de evaluación que se tomó en cuenta para la validación de resultados es el de Certificados digitales, ya que, al ser un objeto de valor bastante significativo y confidencial por poseer datos de usuarios en contenedores, podría ser blanco de ataques cibernéticos, lo cual puede hacer que los datos de esta persona estén comprometidos y puedan ser usados para fines malintencionados causando de esta manera problemas legales del propietario.

Por esta razón este activo fue calificado en los niveles de criterio 9 y 6, los cuales indican las afecciones que pueden llegar a causar la exhibición de los datos del certificado digital. En la Figura 28., se puede visualizar la valoración en *Disponibilidad.*

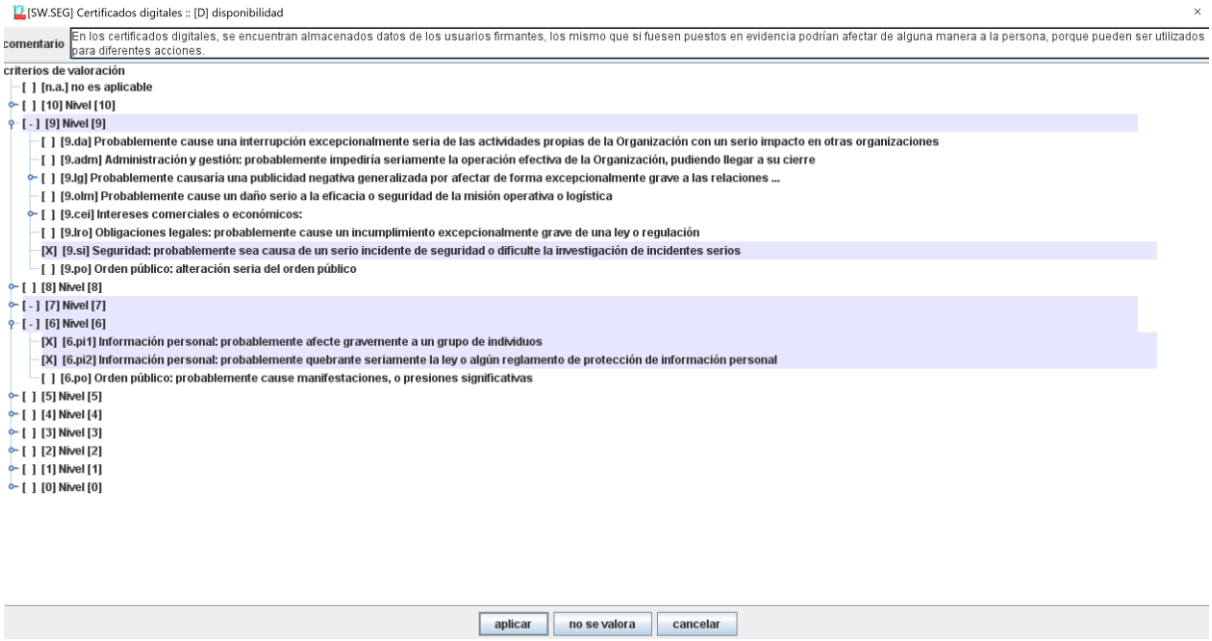
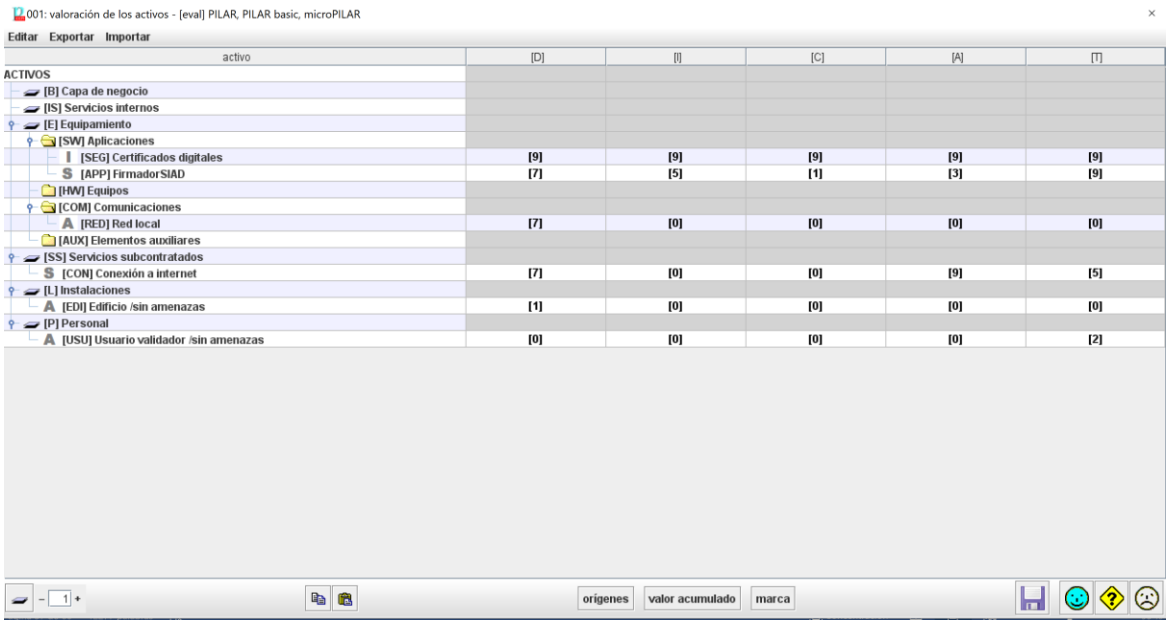


Figura 28: Activo: Certificados Digitales

Fuente: Propia

A continuación, en la Figura 29, se puede evidenciar el valor de criticidad del resto de los activos evaluados.



activo	[D]	[I]	[C]	[A]	[T]
ACTIVOS					
[B] Capa de negocio					
[IS] Servicios internos					
[E] Equipamiento					
[SW] Aplicaciones					
I [SEG] Certificados digitales	[9]	[9]	[9]	[9]	[9]
S [APP] FirmadorSIAD	[7]	[5]	[1]	[3]	[9]
[HW] Equipos					
[COM] Comunicaciones					
A [RED] Red local	[7]	[0]	[0]	[0]	[0]
[AUX] Elementos auxiliares					
[SS] Servicios subcontratados					
S [CON] Conexión a internet	[7]	[0]	[0]	[9]	[5]
[L] Instalaciones					
A [EDI] Edificio /sin amenazas	[1]	[0]	[0]	[0]	[0]
[P] Personal					
A [USU] Usuario validador /sin amenazas	[0]	[0]	[0]	[0]	[2]

Figura 29: Valoración de activos

Fuente: Propia

Amenazas de los activos

En las Figuras 30 y 31 se puede evidenciar las amenazas a las que son expuestas los activos que fueron marcados como esenciales de evaluación.

Estas amenazas fueron seleccionadas según el nivel de riesgo que tiene cada activo por separado.

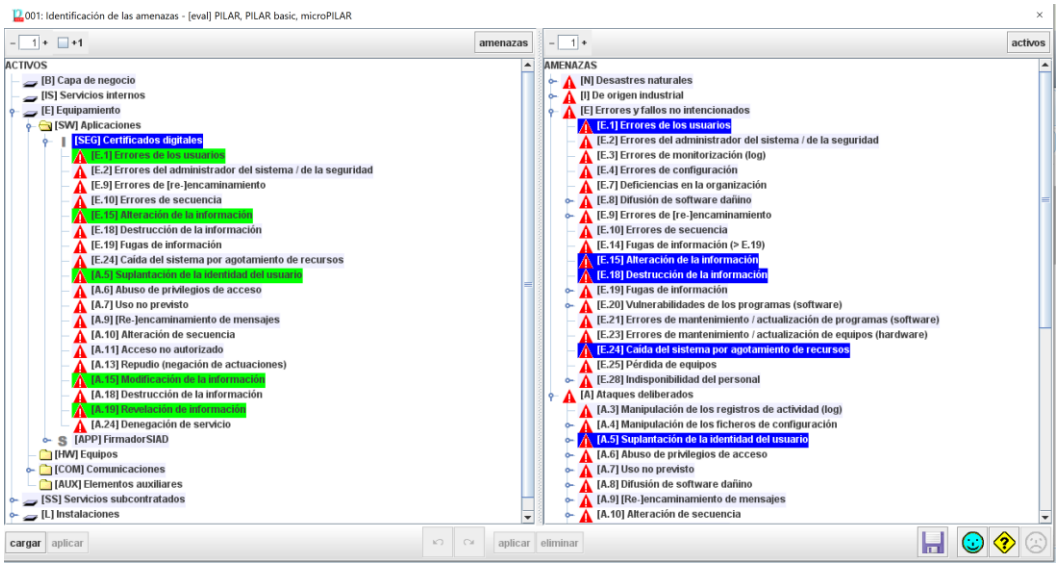


Figura 30: Identificación de amenazas. Certificado digital

Fuente: Propia

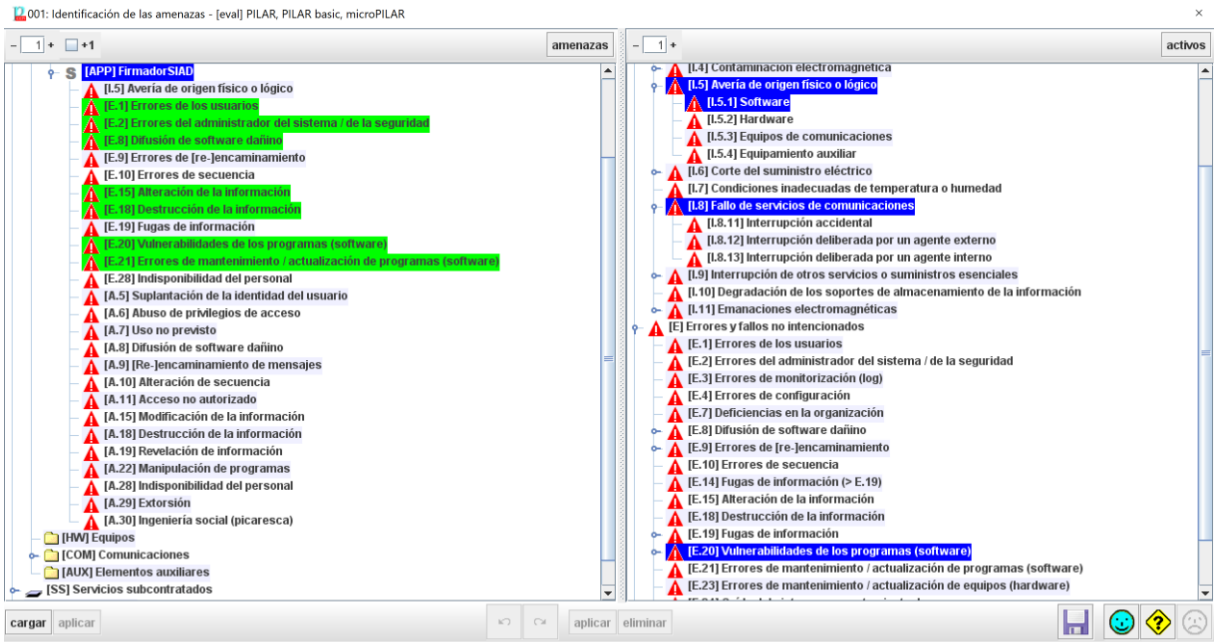


Figura 31: Identificación de amenazas. FirmadorSIAD

Fuente: Propia

Valoración de amenazas

La valoración de amenazas es el resultado de la evaluación en porcentaje de lo que se ingresó anteriormente como valoración de activos.

A continuación, en la Figura 32, se muestra la valoración de amenazas para el activo *Certificado digital* que consideró la herramienta.

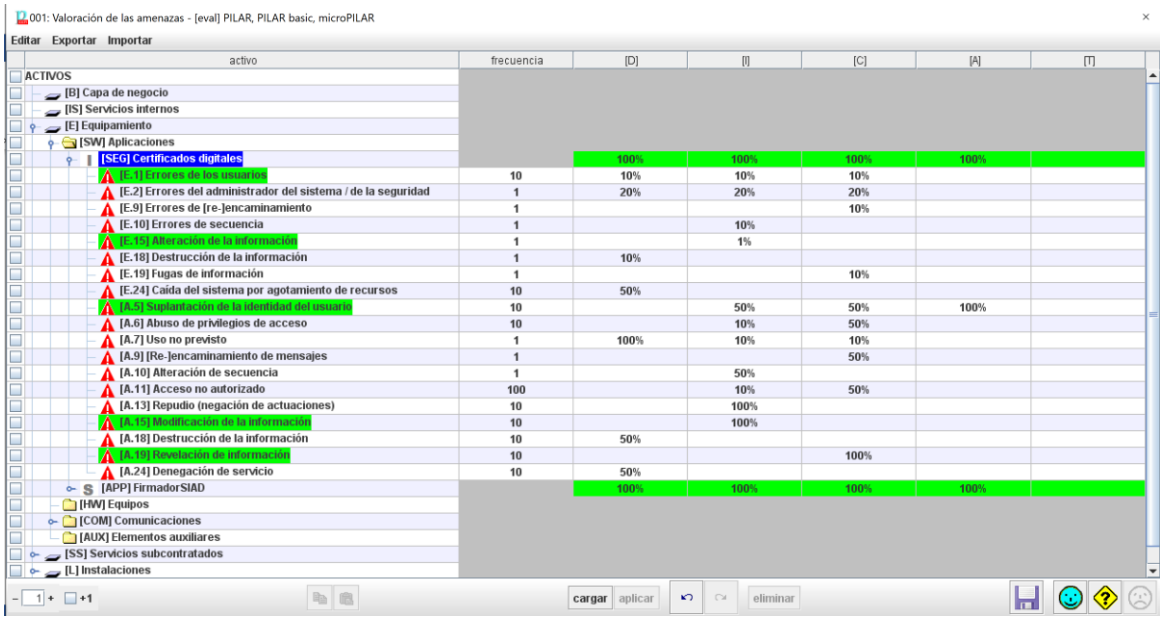


Figura 32: Valoración de amenazas según la herramienta

Fuente: Propia

3.2. Análisis de impactos

El presente análisis de activo, en este caso el *Certificado digital* arrojó buenos resultados en cuanto a la seguridad de la información que se almacena en los contenedores. Evidenciando que el nivel de criticidad de los certificados digitales es bastante riesgoso si se llegara a difundir los datos del usuario, por tal motivo, se demuestra que la firma de documentos con dicho certificado es seguro.

Los factores que demuestran lo dicho son los siguientes:

3	máximo peso	crítica
2	peso alto	muy importante
1	peso normal	importante
0	peso bajo	interesante
✓	aseguramiento: componentes certificados	

Figura 33: Peso relativo de salvaguardas

Fuente: (Gestión et al., 2012)

3.2.1. Salvaguardas

Con la identificación de las salvaguardas se pretende tomar en cuenta las recomendaciones realizadas por la herramienta según el nivel de riesgo que tiene el activo.

En la Figura 34, se muestra las recomendaciones que proporciona la herramienta para el activo *Certificado digital.,* de esta manera se puede reducir el riesgo.

La columna *estrategia* presenta el tipo de protección que proporciona la salvaguarda, los tipos se muestran en la siguiente tabla.

Tabla 3.4: Tipos de protección

PR	Prevención	**AW**	Concienciación
DR	Disuasión	**DC**	Detección
EL	Eliminación	**MN**	Monitorización
IM	Minimización de impacto	**std**	Norma
CR	Corrección	**proc**	Procedimiento
RC	Recuperación	**cert**	Certificación o acreditación
AD	Administrativa		

Fuente: Propia

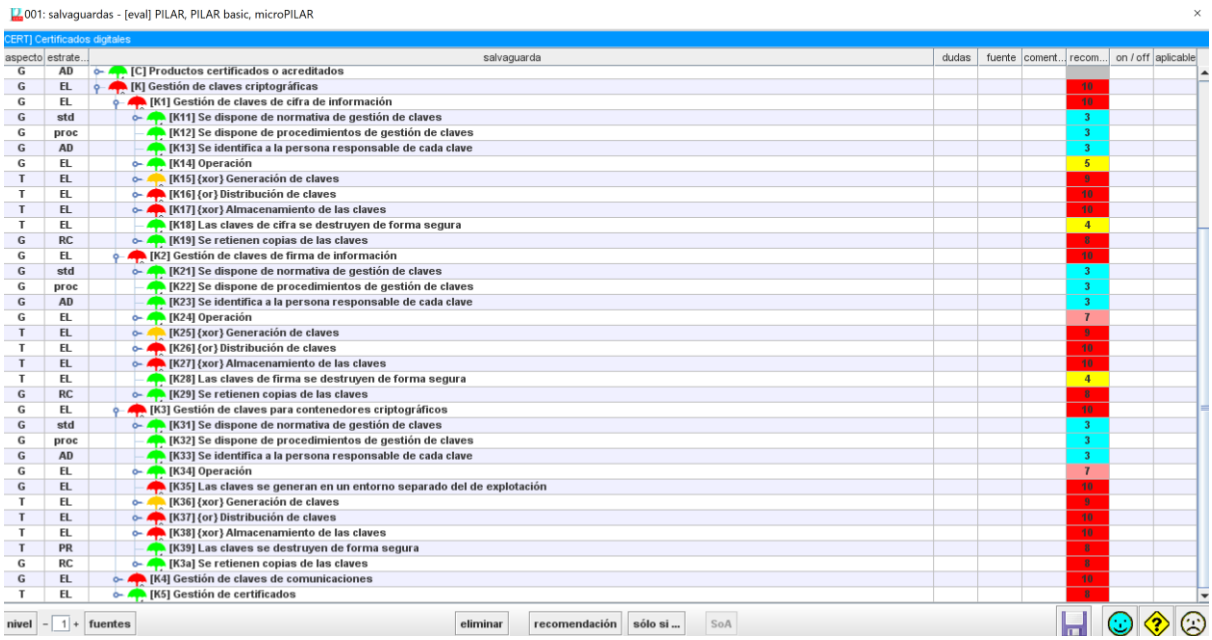


Figura 34: Salvaguardas, certificado digital

Fuente: Propia

Valoración de salvaguardas

Para verificar la eficacia de las salvaguardas, se debe tomar en cuenta la Tabla 3.5:

Tabla 3.5: Eficacia de salvaguardas

NIVEL	SIGNIFICADO	EFICACIA
L0	Inexistente	0%
L1	Inicial	10%
L2	Reproducible pero intuitivo	50%
L3	Proceso definido	90%
L4	Gestionado y mediable	95%
L5	Optimizado	100/

Fuente: Propia

Entre una eficacia del 0% para aquellas que faltan y el 100% para las que se consideran idóneas y eficaces, esta última que combina algunos factores como:

- Capacidad para enfrentar al riesgo que protege.
- Disponibilidad de procedimientos claros de uso normal y en caso de sucesos inesperados.
- Disponibilidad de controles que alerten los posibles fallos.

En la Figura 35, se evidencia la valoración de las salvaguardas a consideración de la herramienta.

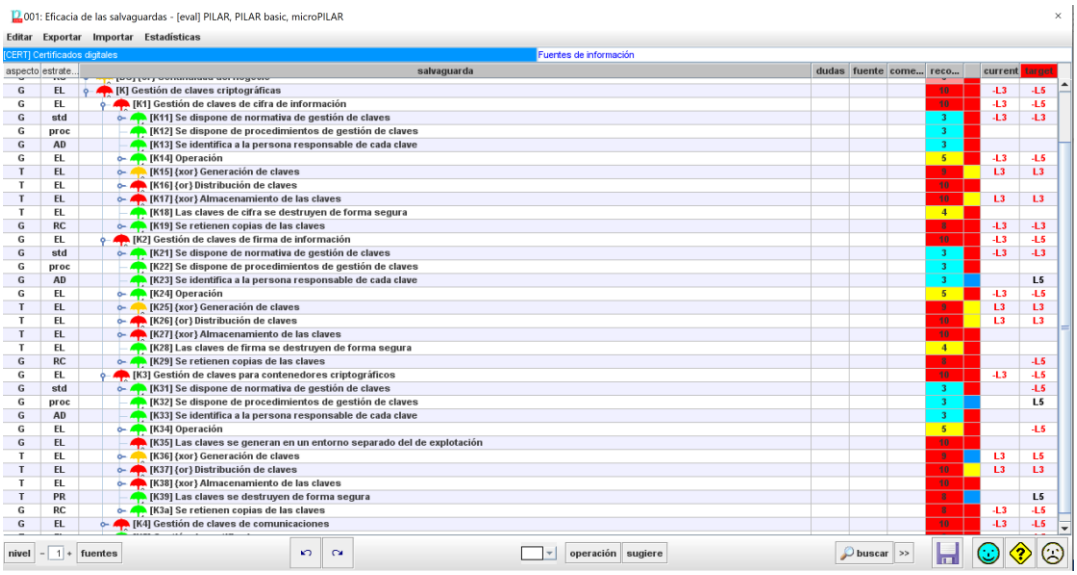


Figura 35: Eficacia de las salvaguardas, certificado digital

Fuente: Propia

En las Figuras 36 y 37 se puede observar la manera en que los activos podrían estar expuestos a impactos y riesgos si estos no estuvieran protegidos en absoluto, las medidas que se tomaron a lo largo del análisis indican lo que podría pasar si se retiran las salvaguardas.

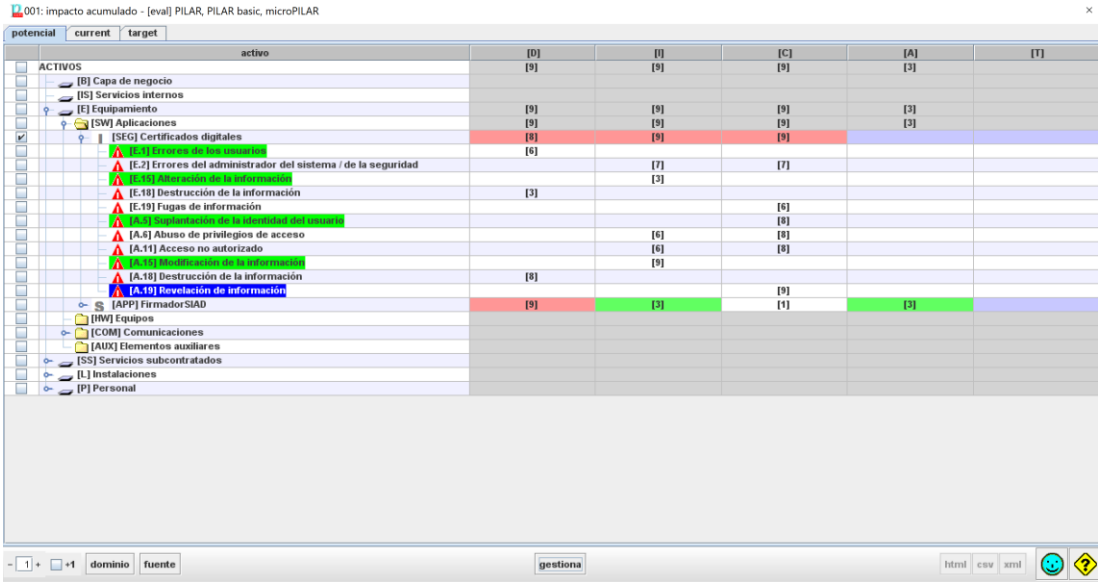


Figura 36: Impacto acumulado

Fuente: Propia

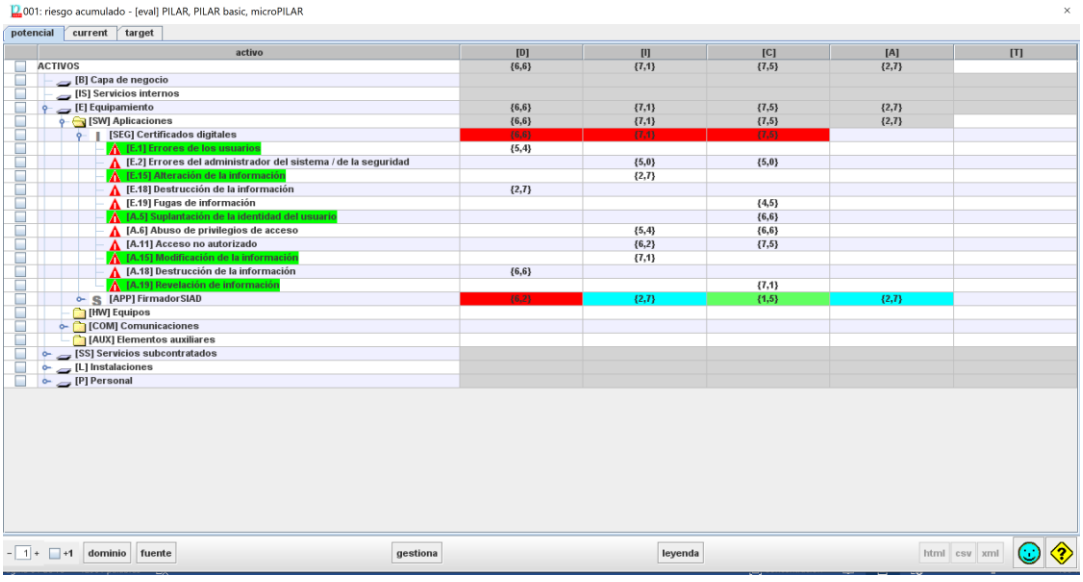


Figura 37: Riesgo acumulado

Fuente: Propia

Frecuentemente los riesgos se caracterizan por tener referencia a sucesos potenciales y sus consecuencias. En la siguiente tabla se observa los colores que se dan según el nivel de riesgo que presente que presente el activo.

Tabla 3.6: Leyenda de nivel de riesgo

5	Crítico
4	Muy alto
3	Alto
2	Medio
1	Bajo
1	Despreciable

Fuente: Propia

Informe gráfico

En la Figura 38, se puede observar gráficamente los resultados que proporcionó la herramienta sobre los riesgos a los que podría ser expuesto el certificado digital, así como también los otros activos que también fueron analizados.

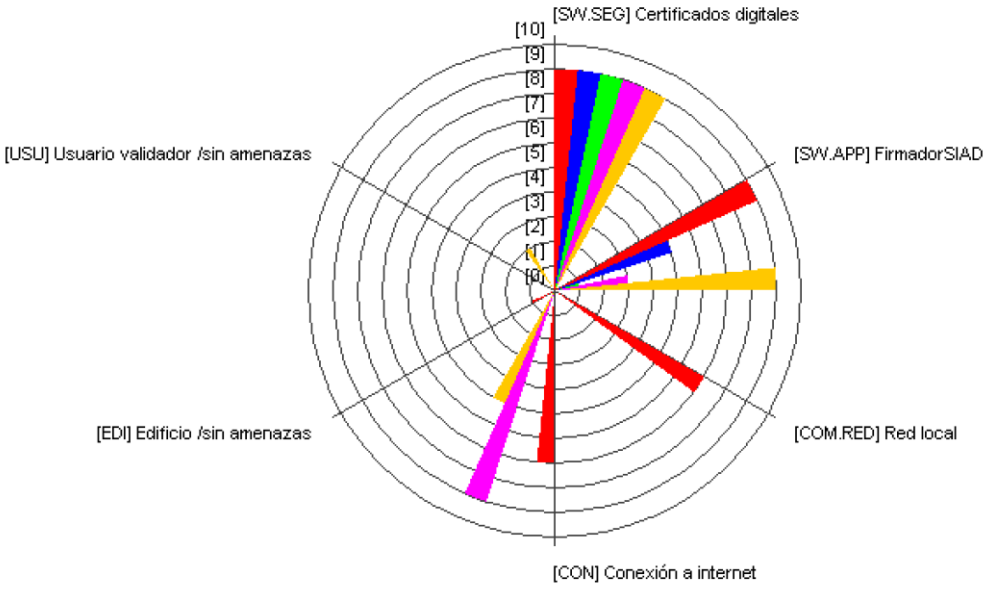


Figura 38: Informe gráfico

Fuente: Propia

CONCLUSIONES

- Entre las librerías que se encontraron para el desarrollo del módulo de firmas digitales se encontraron varias como iText-Pdf, Rúbrica, Mecpy, entre otras, de las que se usaron para este procedimiento iText-Pdf para firmas con certificado tipo archivo y Rúbrica para firmas con certificado tipo token. Estas librerías fueron las que se adaptaron a las necesidades y requerimientos del sistema.

- Esta aplicación exige una gran variedad del cumplimiento de normas y estándares, ya que al ser un proceso que requiere la verificación y validez de una Entidad Certificadora los certificados digitales deben cumplir con el estándar de Infraestructura de Clave Pública X.509, el mismo que proporciona el formato para dicho certificado.

- Tanto la librería Bouncy Castle que provee seguridad generando los certificados X.509 y la librería Rúbrica que entre todas sus funciones posee el poder de firmar, no fueron compatibles con el Sistema SIAD desarrollado en Eclipse.

- La herramienta Pilar permite analizar los riesgos y vulnerabilidades a los que podrían estar expuestos los activos más significativos del software.

RECOMENDACIONES

- Rúbrica fue desarrollada por un equipo de especialistas del Banco Central del Ecuador, por este motivo se debe tener el cuidado necesario para cualquier tipo de actualización que se vaya a realizar en el sistema a futuro, al ser la librería principal por cualquier alteración puede dar errores en su funcionamiento, por eso, es recomendable estudiar y analizar la librería, ya que posee gran parte de las clases que son necesarias para el desarrollo y buen funcionamiento de la aplicación.

- La versión del dispositivo token usado para las pruebas de funcionamiento fue la v5300, misma que al momento de firmar envía un mensaje “Touch sense device”, el cual requiere frotar el dispositivo suavemente en la parte metálica para su buen funcionamiento.

- Para la adquisición del dispositivo Token USB, es recomendable hacerlo con al menos 30 días de anticipación antes de empezar con el desarrollo del software, ya que, por motivos diferentes la solicitud no puede ser aceptada, y el trámite tardaría más de lo planificado.

- La herramienta Pilar permitió evidenciar los riesgos a los que podría ser expuesto un certificado digital si este fuera vulnerado, por lo tanto, por medio del análisis realizado se puede observar las precauciones y medidas que se deberían tomar para protegerlos en el caso de ser necesario.

GLOSARIO DE TERMINOS

- **SIAD:** Sistema Integrado de Actividad Docente.
- **Metodología ágil de trabajo:** Adapta la forma de trabajo a las condiciones del proyecto.
- **SCRUM:** Metodología ágil de trabajo, aplicando un conjunto de buenas prácticas.
- **Sprint:** Ciclo o iteraciones que se tienen dentro de un proyecto Scrum, permite tener un ritmo de trabajo en un tiempo fijo.
- **Product owner:** Transmite la visión de lo que se va a construir a todo el equipo.
- Scrum master: Asesora al equipo para trabajar de una forma organizada.
- **iText-Pdf:** Librería que permite analizar, modificar, crear y mantener documentos en formato pdf.
- **Rúbrica:** Librería que forma parte de una firma.
- **CA:** Autoridad Certificadora que otorga mediante una solicitud un certificado digital.
- **BCE:** Banco Central del Ecuador.
- **SHA:** Función criptográfica, usualmente conocido como hash.
- **HASH:** Algoritmo matemático que transforma bloques arbitrarios de datos en una nueva serie de caracteres con una longitud fija.
- **Criptografía:** Técnica que protege documentos y datos con procedimientos o claves secretas.
- **Kryptós:** Oculto.
- **Gráphein:** Escritura.
- **Simétrico:** En el contexto de la información, hace referencia a que utiliza la misma clave para cifrar y descifrar la información.
- **Asimétrico:** En el contexto de la información, hace referencia a que utiliza diferente clave para cifrar y descifrar la información.
- **SSL:** “Secure Sockets Layer” (en español «capa de conexión segura»), permite establecer conexiones seguras a través de Internet, de forma sencilla y transparente, consiste en interponer una fase de codificación de los mensajes antes de enviarlos por la red.
- **PKI:** Infraestructura de Clave Pública.
- **X.509:** Estándar para Infraestructuras de Claves Públicas.
- **TSA:** Autoridades de Sellado de Tiempo.
- **TSP:** Protocolo de Sellado de Tiempo.
- **Autenticación:** Reconoce unívocamente a un emisor como autor del mensaje.
- **Integridad:** El documento no puede ser alterado de forma alguna durante la transmisión.

- **No repudio:** El emisor y el receptor no pueden negar su vinculación en un documento firmado en ningún caso.
- **Confidencialidad:** Mantiene la información privada.
- **MAGERIT**: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.
- **Pilar:** Herramienta que permite el análisis de riesgos en varias dimensiones.
- **Activos:** Factores más importantes de la aplicación que serán evaluados.

BIBLIOGRAFÍA

Abobeah, R. M., Ezz, M. M., & Harb, H. M. (2015). Public-Key Cryptography Techniques Evaluation. *International Journal of Computer Networks and Applications*, *2*(2). Retrieved from https://www.ijcna.org/Manuscripts/Volume-2/Issue-2/Vol-2-issue-2-M-05.pdf

Aguirre, J. R., & Lucen, M. L. (2019). RSA - EcuRed. Retrieved February 4, 2020, from https://www.ecured.cu/RSA

Albarqi, A., Alzaid, E., Ghamdi, F. Al, Asiri, S., & Kar, J. (2015). Public Key Infrastructure: A Survey. *Journal of Information Security*, *06*(01), 31–37. https://doi.org/10.4236/jis.2015.61004

Alejandro Frechina. (2018). Metodología Scrum ¿Que es? Retrieved May 22, 2019, from https://winred.es/management/metodologia-scrum-que-es/gmx-niv116-con24594.htm

Anónimo. (2019). Metodología SCRUM: ¿qué es y cómo aplicarlo en tu proyecto? Retrieved May 22, 2019, from https://www.sinnaps.com/blog-gestion-proyectos/metodologia-scrum

AprenderCompartiendo. (2016). Firma Digital y Firma Electrónica, diferencias y usos. Retrieved January 8, 2020, from https://aprendercompartiendo.com/firma-digital-firma-electronica-diferencias-usos/

Arguello, R. (2018). Librería rúbrica. Retrieved February 5, 2020, from https://minka.gob.ec/rubrica/rubrica

BCE. (2016). Inicio - Entidad de Certificación BCE. Retrieved May 16, 2019, from https://www.eci.bce.ec/home

BlogNeothek. (2017). Diferencia entre Firmas electrónicas y Firmas digitales – El blog de Neothek. Retrieved January 8, 2020, from https://blog.neothek.com/diferencia-entre-firmas-electronicas-y-firmas-digitales/

Campos, J. (2011). El algoritmo de Diffie-Hellman – Javier Campos .es. Retrieved February 4, 2020, from https://javiercampos.es/blog/2011/07/22/el-algoritmo-de-diffie-hellman/

Carlos De Luca, J. (2015). *La implementación de la firma digital en el sector público: mejoras en la gestión y en los procesos para lograr óptimos resultados*. Retrieved from http://bibliotecadigital.econ.uba.ar/download/tpos/1502-0390_DeLucaJC.pdf

Chulde, A. T. (2016). Contenido del certificado digital y tipo de contenedor que puede almacenarlo - Comunidad de Comercio Exterior. Retrieved January 8, 2020, from http://comunidad.todocomercioexterior.com.ec/profiles/blogs/contenido-del-certificado-digital-y-tipo-de-contenedor-que-puede

DigiCert. (2018). ¿QUÉ SON SSL, TLS Y HTTPS...? Retrieved January 9, 2020, from https://www.digicert.com/es/what-is-ssl-tls-and-https-es/

EcuRed. (2011). SHA - EcuRed. Retrieved February 4, 2020, from https://www.ecured.cu/SHA

García, R. E. C. (2014). *El Impacto Social Y La Incidencia Que Tiene El Uso De La Firma Electrónica (Token), En Los Pequeños Y Medianos Exportadores Ecuatorianos*. UNIVERSIDAD DE LAS FUERZAS ARMADAS.

Gestión, A. Y., Riesgos, D. E., Pilar, H., Luis, J., & Villarroya, Q. (2012). *Dominando los riesgos se compite mejor*.

Gijón. (2014). ¿Cuál es el proceso básico de una firma electrónica? Retrieved May 16, 2019, from https://sedeelectronica.gijon.es/page/12524-cual-es-el-proceso-basico-de-una-firma-electronica

HermesSoft. (2011). Como funciona la firma digital - Procedimientos para su funcionamiento. Retrieved May 16, 2019, from http://www.firma-digital.cr/como funciona/

Holguín García, F. Y. (2018). Análisis de la firma digital con base en la infraestructura de clave pública (Analysis of digital signature based on public key infrastructure). *Hamut'Ay*, p. 95. https://doi.org/10.21503/hamu.v5i2.1622

Hugo David Calderon Vilca. (2011). Firma digital. Retrieved May 16, 2019, from http://hdcalderon.blogspot.com/2011/06/firma-digital.html

IBM. (2017). *Tipos de archivos de certificados*. Retrieved from https://www.ibm.com/support/knowledgecenter/es/SSRMWJ_7.0.1.10/com.ibm.isim.doc/securing/cpt/cpt_ic_security_ssl_oview_ftypes.htm

ICERT-EC Entidad de Certificación. (2017). Contenedores de firma electrónica: Token - archivo - ICERT-EC. Retrieved July 3, 2019, from https://www.icert.fje.gob.ec/productos

Inc, L. of the B. C. (2019). bouncycastle.org. Retrieved February 5, 2020, from https://www.bouncycastle.org/

Informática, S. (2015). Seguridad Informatica: Tipos de Criptografia. Retrieved April 30, 2019, from http://seguinfo-8vo.blogspot.com/p/tipos-de-criptografia.html

iProfesional. (2018). La firma digital, una herramienta para agilizar los trámites. Retrieved May 22, 2019, from https://www.iprofesional.com/legales/15246-La-firma-digital-una-herramienta-para-agilizar-los-tramites

ITU. (2018). X.509 : Tecnología de la información - Interconexión de sistemas abiertos - El directorio: Marcos para certificados de claves públicas y atributos. Retrieved January 8, 2019, from https://www.itu.int/rec/T-REC-X.509/es

José Ortega. (2013). Infraestructura de clave pública (OKI). Retrieved May 16, 2019, from https://es.slideshare.net/junral/actividad-n5-26596212

Judicatura, C. de la. (2017). Sellado de Tiempo - ICERT-EC. Retrieved February 19, 2020,

from https://www.icert.fje.gob.ec/sellado-tiempo

Keitling Daysi Salinas Hinojosa. (2013). Tecnología y Sociedad - TOKENS DE SEGURIDAD. Retrieved May 16, 2019, from http://www.revistasbolivianas.org.bo/scielo.php?pid=S1997-40442013000100025&script=sci_arttext&tlng=es

Kike Torné. (2017). HASH. La función que nos garantiza la autenticidad del archivo – ATIspain TIPS. Retrieved May 7, 2019, from https://www.atispain.com/blog/hash-la-funcion-que-nos-garantiza-la-autenticidad-del-archivo/

Krugman, P., & Wells, R. (2015). *Introducción a la criptografica*. Retrieved from http://www.revista.unam.mx/vol.7/num7/art55/int55.htm

Leones, J. A. J. (2018). *DESARROLLO DE UNA APLICACIÓN DE USO DIDÁCTICO PARA COMUNICACIÓN SEGURA DE DATOS A TRAVÉS DE LA RED*.

Ley de Comercio Electrónico, F. E. y M. de D. (2011). *Ley de comercio electronico, firmas y mensajes de datos norma: publicado:* 1–19. Retrieved from http://www.wipo.int/wipolex/es/text.jsp?file_id=243546

López, M. J. L. (2008). *Criptografía y Seguridad en Computadores on ¿ Quée es la Criptografía ? Objetivo de la Criptografía Historia de la Criptografía*.

López Ruiz, T. R. (2018). *INCIDENCIA DEL USO DEL REPOSITORIO DE FIRMAS DIGITALES EN LA GESTIÓN DE TRÁMITES INSTITUCIONALES DE LA UNIVERSIDAD TÉCNICA DEL NORTE* (Universidad Técnica del Norte). Retrieved from http://repositorio.utn.edu.ec/bitstream/123456789/8295/1/PG 667 TESIS %281%29.pdf

María de los Ángeles Valle C. (2014). *ANÁLISIS DE MÉTODOS CRIPTOGRÁFICOS PARA LA GESTIÓN DE FIRMAS Y CERTIFICADOS DIGITALES DENTRO DE UN CONTEXTO DE SUPERVISIÓN (SBS) PARA ENFRENTAR LOS NUEVOS REQUERIMIENTOS DE SEGURIDAD INFORMÁTICA* (Pontificia Universidad Católica del Ecuador). Retrieved from http://repositorio.puce.edu.ec/bitstream/handle/22000/12017/TESIS CAPITULO I.pdf?sequence=1

María Laura Irigoitia. (2016). *Análisis, Diseño e Implementación de Firma Digital en Documentos Electrónicos*. Retrieved from https://rdu.iua.edu.ar/bitstream/123456789/1144/1/Proyecto de Grado_Maria Laura Irigoitia.pdf

Mike Ashley. (2016). Firmas digitales; guía de “Gnu Privacy Guard.” Retrieved May 14, 2019, from https://www.gnupg.org/gph/es/manual/book1.html

Nacional, C. C. (2013). EAR - Herramientas para el Análisis de Riesgos. Retrieved February 13, 2020, from https://www.ar-tools.com/es/index.html

Naranjo, P. de L. G. (2010). Implementación de firmas digitales para mensajería de datos mendiante la utilización de dispositivos token. (Escuela Superior Politécnica de Chimborazo; Vol. 22). Retrieved from http://dspace.espoch.edu.ec/handle/123456789/546

OBS Business School. (2019). Metodologías agiles: Scrum y kanban y XP | OBS Business School. Retrieved July 12, 2019, from https://www.obs-edu.com/int/blog-project-management/scrum/metodologias-agiles-scrum-y-kanban-y-xp

ODS. (2018). Educación – Desarrollo Sostenible. Retrieved January 8, 2019, from https://www.un.org/sustainabledevelopment/es/education/

Oracle, J. D. (2017). Keytool comands. Retrieved January 29, 2020, from https://docs.oracle.com/javase/8/docs/technotes/tools/unix/keytool.html

P. Sumalatha, & Prof. B. Sathyanarayana. (2015). *Enhanced Identity Based Cryptography for Efficient Group Key Management in WSN*. Retrieved from www.ijaiem.org

Pedro Gutierrez. (2013). ¿Qué son y para qué sirven los hash?: funciones de resumen y firmas digitales. Retrieved May 16, 2019, from https://www.genbeta.com/desarrollo/que-son-y-para-que-sirven-los-hash-funciones-de-resumen-y-firmas-digitales

Quipux. (2015). Quipux - Sistema de Gestión Documental. Retrieved January 8, 2019, from http://quipux.imbabura.gob.ec/

Quonext. (2018). Metodologías ágiles | Scrum, Kanban y XP | Blog Quonext. Retrieved July 12, 2019, from https://www.quonext.com/blog/metodologias-agiles-scrum-kanban-xp/

Rafael Palacios. (2012). *Introducción a la Criptografía: tipos de algoritmos*. Retrieved from http://theory.lcs.mit.edu/~rivest/

Registro Civíl. (2019). Firma Electrónica – Registro Civil. Retrieved January 8, 2019, from https://www.registrocivil.gob.ec/certificado-de-firma-electronica/

Reshma Afshar. (2015). *Digital Certificates PKI*. Retrieved from http://cs.indstate.edu/~rafshar/

Reyes Krafft, A. A., & Preciado Briseño, E. (2009). *Las firmas electrónicas y las entidades de certificación*. Retrieved from http://ebookcentral.proquest.com/lib/utnortesp/detail.action?docID=3178023

Salmón Corp. Blog. (2016). Token de Seguridad. Retrieved May 21, 2019, from https://salmocorpblog.wordpress.com/2016/12/20/token-de-seguridad/

Sanchez, M. (2015). Tipos de Cifrados (SHA1, MD5, RSA). Retrieved May 14, 2019, from http://msmanuelsanchez.blogspot.com/2015/10/tipos-de-cifrados-sha1-md5-rsa.html

Sanjuan, L. (2016). Criptografía I. *Seminario: Seguridad En Desarrollo de Software*, 34. Retrieved from http://manglar.uninorte.edu.co/bitstream/handle/10584/2204/Crip?sequence=1

Santiago Campillo. (2015). La contraseña perfecta. Retrieved May 21, 2019, from https://hipertextual.com/2015/10/contrasena-perfecta

Schwaber, K., & Sutherland, J. (2014). La Guía definitiva de Scrum: Las Reglas de Juego. *Scrum.Org*. Retrieved from https://www.scrumguides.org/docs/scrumguide/v1/scrum-guide-es.pdf%0AScrum.org

Sector, S., & Itu, O. F. (2016). *ITU-T X.509 Corrigendum 3*. *509*(2012).

Signaturit. (2017). El sellado de tiempo y su relación con la firma electrónica. Retrieved January 9, 2020, from https://blog.signaturit.com/es/la-autoridad-de-sellado-de-tiempo-un-cierre-hermetico-para-brindar-mayor-seguridad-a-la-firma-electronica

Sitepro. (2019). Dispositivo criptográfico SafeNet eToken 5300 -. Retrieved January 29, 2020, from https://www.sitepro.com.ar/web/productos/firma-digital/etoken-safenet-5300/

Solidpass. (2013). Token de seguridad sincronizado en el tiempo, OTP. Retrieved May 21, 2019, from http://www.solidpass.com/authentication-methods/time-synchronized-security-token.html

StackOverflow. (2017). cifrado: ¿cuáles son las diferencias entre .pem, .cer y .der? - Desbordamiento de pila. Retrieved January 9, 2020, from https://stackoverflow.com/questions/22743415/what-are-the-differences-between-pem-cer-and-der/22743616

UNAD. (2007). Criptografía | Objetivo. Retrieved May 16, 2019, from http://stadium.unad.edu.co/ovas/10596_10131/criptografa.html

Unión Internacional de Telecomunicaciones. (2016). ITU-T X.509(2012) Cor.3(10/2016). Retrieved February 21, 2019, from https://www.itu.int/itu-t/recommendations/rec.aspx?rec=13032&lang=es

Universidad de Murcia. (2011). La seguridad en informatica. Informatica Aplicada a la Gestion Publica. Curso 2005/06-10. Rafael Barzanallana. Universidad de Murcia (España). Retrieved May 16, 2019, from https://www.um.es/docencia/barzana/IAGP/Iagp10.html

Universidad Politécnica de Valencia. (2012). ¿Qué es un Certificado Digital? : Certificados Digitales : UPV. Retrieved May 21, 2019, from https://www.upv.es/contenidos/CD/info/711545normalc.html

Yofacturo.bo. (2015). ¿Qué es la nueva firma digital y cómo puede ayudar a mi empresa? Retrieved May 17, 2019, from http://yofacturo.bo/2016/09/26/como-puede-ayudar-la-firma-digital-a-mi-empresa.html