FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

DISEÑO E IMPLEMENTACIÓN DE UN PROTOTIPO DE APROBACIÓN ELECTRÓNICA, BASADA EN CLOUD Y SAAS PARA PROCESOS INTERNOS DE LA CARRERA DE TELECOMUNICACIONES DE LA UNIVERSIDAD DE LAS AMÉRICAS

AUTOR

Mauricio Andrés De La Cruz Jácome

AÑO

2018

FACULTAD DE INGENIERÍA Y CIENCIAS APLICADAS

DISEÑO E IMPLEMENTACIÓN DE UN PROTOTIPO DE APROBACIÓN ELECTRÓNICA, BASADA EN CLOUD Y SAAS PARA PROCESOS INTERNOS DE LA CARRERA DE TELECOMUNICACIONES DE LA UNIVERSIDAD DE LAS AMÉRICAS

Trabajo de titulación presentado en conformidad con los requisitos establecidos para optar por el título de Ingeniero en Redes y Telecomunicaciones

Profesor Guía

Msc. Carlos Marcelo Molina Colcha

Autor

Mauricio Andrés de la Cruz Jácome

Año

2018

DECLARACIÓN PROFESOR GUÍA

“Declaro haber dirigido el trabajo, Diseño e implementación de un prototipo de aprobación electrónica, basada en Cloud y SAAS para procedimientos internos de la carrera de Telecomunicaciones de la Universidad de Las Américas, a través de reuniones periódicas con el estudiante Mauricio Andrés De La Cruz Jácome, en el semestre 2018 – 2, orientando sus conocimientos y competencias para un eficiente desarrollo del tema escogido y dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”

_____

Carlos Marcelo Molina Colcha
Magister en Tecnologías de la Información y Comunicación
CI: 170962421-5

DECLARACIÓN DEL PROFESOR CORRECTOR

“Declaro haber revisado este trabajo, Diseño e implementación de un prototipo de aprobación electrónica, basada en Cloud y SAAS para procedimientos internos de la carrera de Telecomunicaciones de la Universidad de Las Américas, a través de reuniones periódicas con el estudiante Mauricio Andrés De La Cruz Jácome, en el semestre 2018 – 2, dando cumplimiento a todas las disposiciones vigentes que regulan los Trabajos de Titulación”.

_____

Milton Neptalí Román Cañizares

Magister en Gerencia de Redes y Telecomunicaciones

CI: 0502163447

DECLARACIÓN DE AUTORÍA DEL ESTUDIANTE

“Declaro que este trabajo es original, de mi autoría, que se han citado las fuentes correspondientes y que en su ejecución se respetaron las disposiciones legales que protegen los derechos de autor vigentes.”

_____

Mauricio Andrés De La Cruz Jácome

CI: 0401179486

AGRADECIMIENTO

Agradezco a Dios y a mi familia quienes me han brindado el apoyo para lograr culminar esta etapa de mi vida.

Particularmente agradezco el apoyo invaluable de mi madre Magdalena Jácome y de mi padre Roberto De La Cruz, que, con su esfuerzo y ejemplo de vida, me enseñaron a luchar para alcanzar los propósitos de vida.

A Elizabeth y a mis hijos, por ser el incentivo de seguir adelante.

DEDICATORIA

Dedico este proyecto a mis hijos y a mis padres quienes fueron artífices de este logro.

RESUMEN

El presente proyecto de titulación, comprende el desarrollo de las fases requeridas para la implementación de un prototipo de aprobación digital, desarrollado en Cloud y SAAS basado en los principios fundamentales de la firma electrónica.

El propósito de esta implementación es automatizar y digitalizar el proceso de aprobación manual para documentos internos utilizados por la Carrera de Telecomunicaciones, para el desarrollo de este proyecto se toma como guía referencial la metodología Top Down de CISCO, cumpliendo con las buenas prácticas técnicas y políticas internas de la Universidad de Las Américas.

El capítulo 1, hace referencia a conceptos técnicos y componentes que intervienen como tal en la operación del sistema de aprobación digital.

El capítulo 2, contempla el desarrollo del proceso de análisis, diseño e implementación de una la solución de “aprobación digital” integrada con office 365 y Document Cloud.

El capítulo 3, presenta la evaluación y resultados extraídos de las pruebas de desempeño de la aplicación implementada. Se demuestra que la implementación cumple con los parámetros técnicos y funcionales de la que requiere la Universidad de Las Américas.

El capítulo 4, muestra las conclusiones y recomendaciones como resultado de la implementación del proceso de aprobación digital. En este capítulo se exponen observaciones que permitan conocer diferentes aspectos para un proceso de mejora contínua.

ABSTRACT

The present project of qualification, includes the development of the phases required for the implementation of a prototype of digital approval, developed in Cloud and SAAS based on the fundamental principles of the electronic signature. The purpose of this implementation is to automate and digitize the manual approval process for internal documents used by the Telecommunications Career. For the development of this project, CISCO's Top Down methodology is used as a reference guide, complying with good technical and political practices. of the University of the Americas.

Chapter 1, refers to technical concepts and components that intervene as such in the operation of the digital approval system.

Chapter 2, contemplates the development of the process of analysis, design and implementation of a "digital approval" solution integrated with office 365 and Document Cloud.

Chapter 3, presents the evaluation and results extracted from the performance tests of the implemented application. It is demonstrated that the implementation complies with the technical and functional parameters required by the University of the Americas.

Chapter 4, shows the conclusions and recommendations as a result of the implementation of the digital approval process. In this chapter, observations are presented that allow knowing different aspects for a process of continuous improvement.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

INTRODUCCIÓN

Antecedentes

Actualmente las Tecnologías de Información y Comunicaciones (TIC), buscan mejorar cada vez mas los campos de la documentación digital y el comercio electrónico desarrollando aplicaciones que permiten automatizar procesos manuales y que se integren a las infraestructuras propias de las organizaciones con el fin de brindar a los usuarios una herramienta que le permita mejorar las labores funcionales y por lo tanto su desempeño laboral. Una de estas aplicaciones es la Aprobación Digital que se basa en los principios básicos de la Firma Electrónica: autenticar, garantizar la identidad de los usuarios, brindar la integridad del mensaje de tal modo que se asegure que el documento “aprobado electrónicamente” no ha sido modificado.

En una organización se transmite información de modo unidereccional o bidireccional, generando una cantidad significativa de información que a su vez se extiende a un manejo burocrático de los documentos físicos propios de los procesos internos de las áreas de la institución, por este motivo se busca establecer una solución para establecer flujos documentales automatizados mediante la implementación de la aprobación digital.

Según una publicación hecha por la Universidad Politécnica de Valencia, en la publicación ¿Qué es una firma electrónica? (2017): “La firma electrónica, es un método criptográfico que asocia la identidad de una persona o de un equipo informático al mensaje o documento. La firma electrónica, puede vincularse a un documento para identificar al autor, para señalar conformidad (o disconformidad) con el contenido, para indicar que se ha leído, o según el tipo de firma, garantizar que no se pueda modificar su contenido.”

En el año 2000, en los Estados Unidos se aprobó la ley de firmas electrónicas en el comercio global y nacional (ESIGN); en Ecuador existe la "Ley de Comercio

Electrónico, Firma Electrónica y Mensajes de Datos vigente desde el año 2002 y su reglamento también redactado y registrado en el mismo año. El uso de la Firma Electrónica en el país es relativamente reciente, puesto que en octubre del 2008 se acreditó al BCE como la primera entidad de certificación. Al comienzo esta tecnología no era muy alta, según las estadísticas proporcionadas por el BCE en el año 2012, se emitieron un total de 24000 certificados electrónicos, actualmente el crecimiento ha sido aproximadamente del 70%.

A nivel empresarial se ha visto la necesidad de implementar nuevas formas de trabajo que contribuyan a reemplazar procesos manuales por procesos automáticos y electrónicos con un respaldo sólido en la seguridad de la información de estos documentos. La Universidad de Las Américas se suma al proceso de implementación del servicio de aprobación digital, cumpliendo con los principios básicos de esta tecnología: integridad, confidencialidad, autenticidad y no repudio a la información.

Alcance

El alcance de este proyecto es dotar de un prototipo de aprobación digital a la Facultad de Ingeniería y Ciencias Aplicadas, que cumpla con los parámetros que se describen a continuación.

Alcance de tipo operativo:

- Enviar documentos de office o pdf para ser aprobados electrónicamente.
- Permitir al usuario (gestor), el envío de un documento electrónico para ser aprobado o rechazado.
- Notificar al usuario aprobador, que tiene un documento pendiente para ser revisado; estos mensajes se notificarán través del correo electrónico institucional.
- Permitir al usuario aprobador, delegar a otra persona para que haga una aprobación digital por ella.

- Permitir descargar una copia de los documentos aprobados.
- Disponer del estatus actual del documento dentro del flujo.

Gestión automática

La aplicación ejecuta el flujo del documento electrónico de manera automática, una vez que el documento haya sido enviado por el gestor documental a los usuarios aprobadores.

Integridad del documento

Esta característica se basa en una estructura de seguridad de una clave pública (PKI) para certificar los documentos con una aprobación digital. La aprobación digital crea con un algoritmo hash que toma información única específica en el documento aprobado, generando una cadena de números y letras de longitud fija, criptográficamente sonora y codificada en hexadecimal.

Confidencialidad y Seguridad

Haciendo uso de claves de correo electrónico identificado (DKIM), Autenticación de mensajes basada en el dominio, Informes y Conformidad (DMARC), y Marco de políticas del remitente (SPF). La seguridad de la información se basa en certificaciones de cumplimiento, como SOC 2-Type 2 e ISO 27001.

Validación de autenticidad de la aprobación digital

A través de una funcionalidad que permita realizar la verificación del ID de transacción electrónica (encriptada).

Auditoría

Registrar y preservar un registro de auditoría para información relevante perteneciente a cada usuario y documento en cada paso del proceso de flujo de trabajo.

Encriptación

Los documentos y activos en reposo se encriptan mediante el cifrado AES (Standard Avanzado de Encriptación) de 256 bits y es compatible con HTTPS TLS v1.2 (más otras versiones heredadas) para ayudar a garantizar que los datos en tránsito también estén protegidos, este tipo de encripción se caracteriza por ser segura contra los ataques de fuerza bruta.

Key Size	Possible combinations
1-bit	2
2-bit	4
4-bit	16
8-bit	256
16-bit	65536
32-bit	4.2×10^{9}
56-bit (DES)	7.2×10^{16}
64-bit	1.8×10^{19}
128-bit (AES)	3.4×10^{38}
192-bit (AES)	6.2×10^{57}
256-bit (AES)	1.1×10^{77}

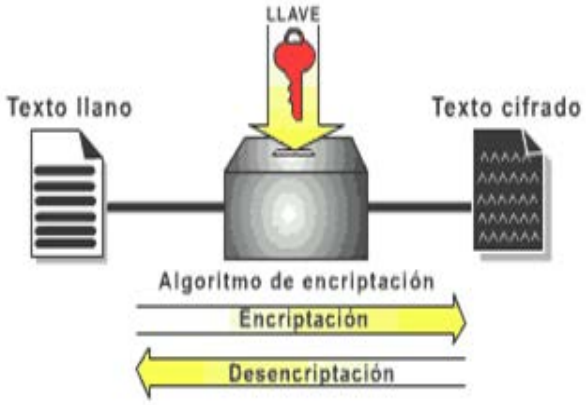


Figura 1. Definición de encriptación.
Adaptado de (DataQUBO Backup, 2013)

Justificación

La justificación del desarrollo de este proyecto se basa en los beneficios esperados con la implementación de este proyecto, que son los siguientes:

- Generar documentos electrónicos “aprobados”, que tengan validez.
  Con la implementación del sistema de aprobación digital la institución podrá generar documentos digitales que cumplan con las características de autenticidad, integridad y no repudio a la información.

- Aumentar la productividad de los usuarios. El coste de oportunidad del tiempo invertido por los empleados en tareas administrativas es un punto importante que analizar, pues la implementación del proyecto de aprobación digital permitirá ahorrar el tiempo utilizado en actividades de tipo manual.

Este tiempo puede ser utilizado por los usuarios para realizar otras actividades laborales que aporten más valor que contribuyan a mejorar la productividad de la institución.

- Simplificar y automatizar la gestión documental.
  Optimizando los procesos manuales (recolección de aprobaciones en papel), reduciendo y agilitando el envío y recepción de documentos, a través de notificaciones del correo electrónico institucional.

- Reducción de costes asociados a la impresión de documentos.
  El uso del sistema de aprobación digital busca ser un factor que colabore con el ahorro en gasto administrativos que hacen referencia a menor consumo de tinta, de papel, gastos de mantenimiento de las impresora y menor gasto en material para archivar de manera adecuada la documentación.

- Un beneficio derivado de disminuir el consumo de papel, es la contribución de UDLA para preservar el medio ambiente.

- Disponer de forma instantánea del servicio de aprobación digital, para brindar la facilidad de acceder a la aplicación por medio de un navegador web a través de un dispositivo móvil, desktop o laptop.

- Brindar la seguridad con gestión documental en la nube.
  El sistema de aprobación digital emplea prácticas de seguridad estándar para proteger sus documentos, datos e información personal basado en la nube.

Objetivos

Objetivo general

Diseñar e implementar un prototipo de aprobación electrónica (digital), basada

en Cloud y SAAS para procesos internos de la carrera de Redes y Telecomunicaciones de la Universidad de Las Américas.

Objetivos específicos

- Identificar las características técnicas y la operación de la firma digital.

- Diseñar e implementar una solución que permita realizar aprobaciones digitales, basada en la funcionalidad de la firma digital e integrado con office 365 y document Cloud; tomando como referencia la metodología Top-Down de Cisco.

- Evaluar que la solución implementada cumpla con los parámetros técnicos, legales y funcionales de la institución.

- Concluir y sugerir.

Metodología Top-Down

El desarrollo de este proyecto de titulación toma como marco de referencia la metodología Top-Down la cual se basa en el Ciclo de vida de un servicio de Cisco.

La metodología Top-Down parte desde el análisis de los requerimientos del usuario para determinar las metas de negocio, con el fin de obtener una macro organización y una estructura del proceso del diseño e implementación.

El empleo de la metodología Top Down propone:

- Mejorar la calidad, ya que permite encontrar errores en etapas tempranas del diseño.
- Reorganizar labores del diseño de la integración.
- Reducir la necesidad de una extensiva verificación del estado final del diseño.

Para la ejecución de este proyecto se toma como referencia esta metodología adaptando el desarrollo de sus fases según los requerimientos propios de esta implementación que se describen en la siguiente figura.

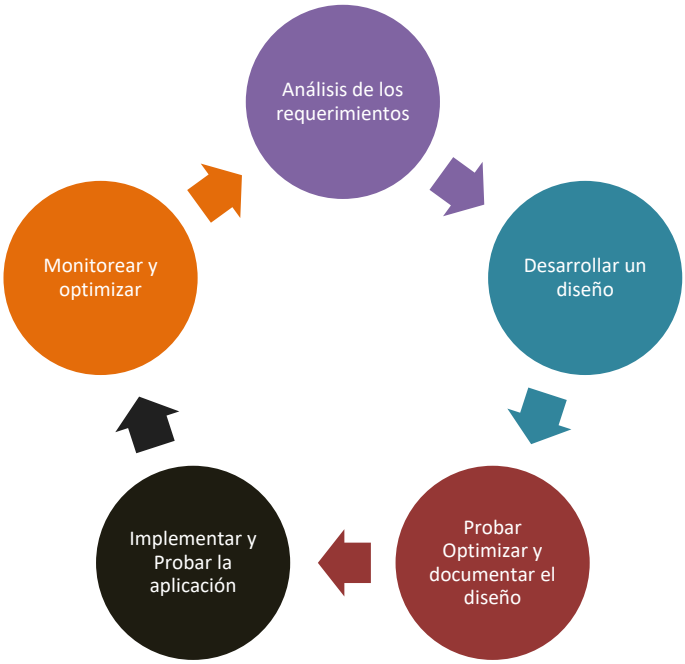


Figura 2. Etapas de la Metodología Top down.

La metodología Top Down se basa en el ciclo de vida PPDIOO de Cisco, que significa: “Preparar, Planear, Diseñar, Implementar, Operar y Optimizar”.

Preparar: En esta etapa se toman desiciones importantes para identificar los requerimientos técnicos del negocio; en base a esto se genera la propuesta de la solución a implementarse.

Planear: Esta fase hace referencia al análisis de la problemática actual para determinar la funcionalidad que debe cubrir la solución a implementarse.

Diseñar: En este paso se diseña la integración (solución). Se decide sobre la tecnología que se va autilizar, aplicaciones o servicios; esta desición se hace en base a las fases anteriormente mencionadas.

Implementar: En el desarrollo de esta fase se ejecutan las configuraciones del servicio, tanto a nivel de administración como a nivel del usuario final. Para ejecutar este paso, se prepara con anterioridad el orden, las actividades y responsables de la implementación de la solución.

Operar: La implementación y la verificación consiste en las pruebas de rendimiento de la aplicación integrada.

Optimizar: Durante la ejecución de las pruebas y uso de la aplicación implementada se comprueba si hay errores, si estos son frecuentes o imposibles de manejar, podría ser necesario rediseñar la solución implementada; esto se evita si los pasos anteriores se han desarrollado correctamente.

De manera adicional esta fase, permite hacer ajustes no previstos en la etapa de diseño.

1. MARCO TEÓRICO

Este capítulo trata sobre los conceptos teóricos a ser aplicados en el proceso de diseño e implementación del prototipo de aprobación digital, haciendo referencia a los elementos que participan a nivel técnico, funcional y metodológico.

Finalmente se revisan los criterios técnicos, los cuales establecen parámetros para el diseño e implementación de la aplicación que se va a integrar.

1.1. Criptografía

1.1.1. Definición de criptografía

Este término proviene de las raíces griegas “cryptos” que significa “oculto” y “grafe” que significa “escritura”.

Es el conjunto de técnicas, métodos y algoritmos que tienen como objetivo cifrar mensajes para resguardarlos, protegerlos y hacerlos incomprensibles para quien no debe tener acceso a ellos.

1.1.2. Objetivo de la criptografía

El objetivo de la criptografía es estudiar algoritmos, sistemas y protocolos que se utilizan para dotar de seguridad a la información, las comunicaciones y los involucrados (emisor y receptor).

La criptografía diseña, implementa y utiliza sistemas criptográficos para brindar algún tipo de seguridad. Por lo tanto, debe referir su estudio a las siguientes propiedades: integridad, confidencialidad, autenticidad y vinculación

1.1.3. Tipos de criptografía

La criptografía consta de varios métodos modernos como la criptografía simétrica, asimétrica, híbrida (que consiste en la combinación de las dos anteriores), teniendo en cuenta las funciones hash (o de resumen).

Criptografía simétrica

Este tipo de criptografía utiliza la misma clave para cifrar y descifrar un documento. La criptografía simétrica, también llamada criptografía de clave secreta o criptografía de una clave (en inglés single-key cryptography), es un método criptográfico en el cual se usa una misma clave para cifrar y descifrar mensajes por parte del emisor y del receptor. En la figura no. 3 se representa de manera gráfica la descripción de la criptografía simétrica. (ADC Telecommunications, Inc, 2008).

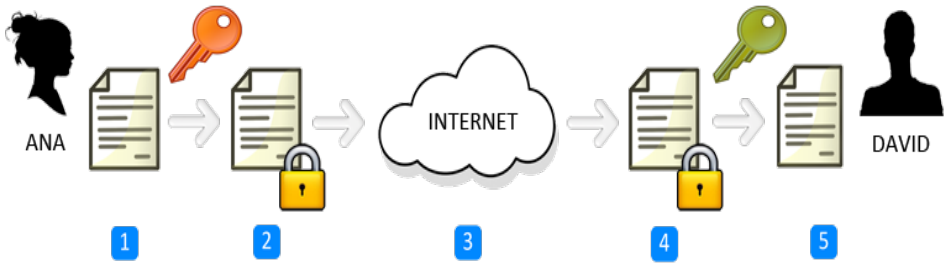


Figura 3. Criptografía simétrica.
Tomado de (ADC Telecommunications, 2009)

Criptografía asimétrica

La criptografía asimétrica se basa en el uso de dos claves: la pública y la clave privada (que no se debe revelar).

La criptografía asimétrica utiliza dos claves complementarias llamadas clave privada y clave pública, estas claves se generan de manera simultánea y están ligadas la una de la otra; los algoritmos asimétricos se basan en funciones matemáticas fáciles de resolver en un sentido, pero muy complicadas de realizarlo en sentido inverso, a menor que se conozca la llave. (ADC Telecommunications, 2009).

A continuación, visualizamos un ejemplo de cómo funciona la criptografía asimétrica, el cual se evidencia en la figura 4.

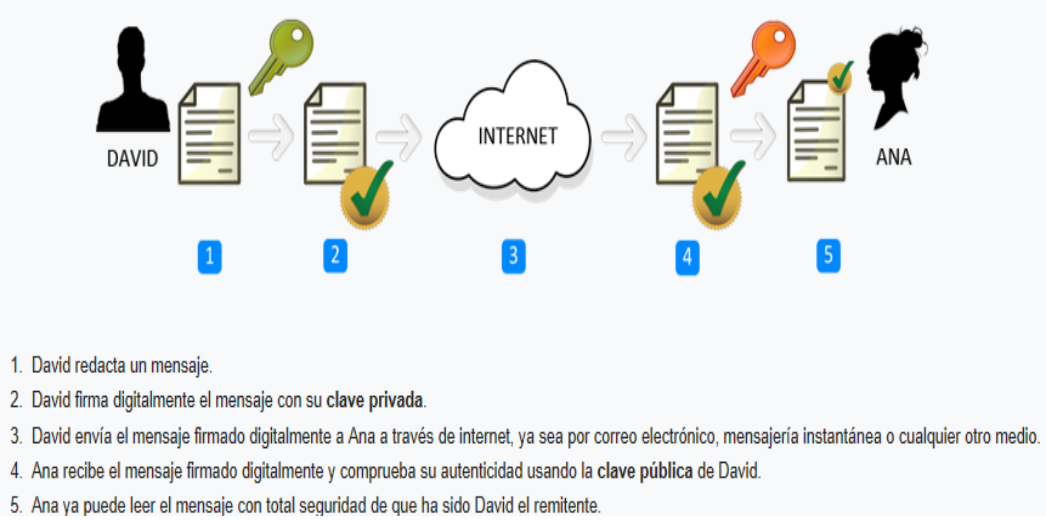


Figura 4. Criptografía asimétrica.
Adaptado de (ADC Telecommunications, 2009)

Criptografía híbrida

Es un método criptográfico que utiliza el cifrado simétrico y también el cifrado asimétrico; el uso de cifrado simétrico para solventar los problemas de privacidad y el tiempo de procesado del uso del cifrado asimétrico

El proceso para usar un sistema criptográfico híbrido es el siguiente (para enviar un archivo):

- Generar una clave pública y otra privada (en el receptor).
- Cifrar un archivo de forma síncrona.
- El receptor envía su clave pública.
- Se cifra la clave utilizada para encriptar el archivo con la clave pública del receptor.
- Se envía el archivo cifrado (síncronamente) y la clave del archivo cifrada (asíncronamente y solo puede ver el receptor).

En la siguiente figura, se demuestra a nivel global el funcionamiento de la criptografía híbrida.

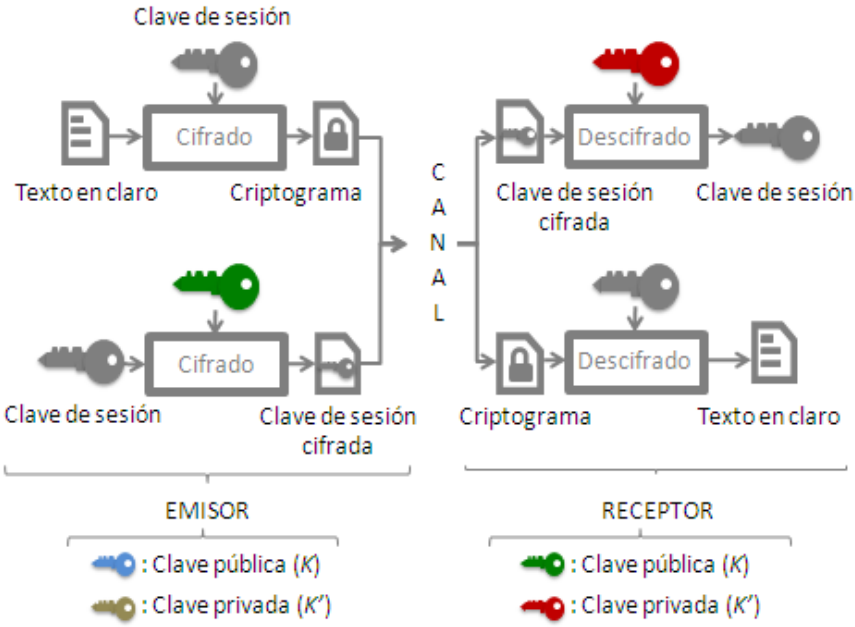


Figura 5. Criptografía híbrida.
Adaptado de (ADC Telecommunications, 2009)

1.2. Aprobación digital

1.2.1. Definición de aprobación digital

La Aprobación digital permite automatizar el flujo que se requiere para cumplir con el proceso de la "aprobación de documentos electrónicos", permite manejar de manera óptima la gestión documental. La "Aprobación Digital" satisface los parámetros fundamentales de seguridad de la "Firma Electrónica", que son los siguientes: autenticación, integridad, no repudio a la información y confidencialidad de los documentos electrónicos.

Según Gonzalo, et al. (2012), cuando citan a Moreno Blesa (2008): "La firma electrónica pretende ser el instrumento que permita garantizar la seguridad en las comunicaciones telemáticas, aportando a los medios de comunicación empleados, autenticidad que es fundamental acreditar que las partes son realmente quienes dicen ser, integridad que se tendrá que demostrar que la información no ha sido alterada desde el momento en el que ha sido transmitida." (Pág. 322).

Cabe mencionar el desarrollo de este proyecto, la Aprobación Digital se fundamenta en los principios funcionales y técnicos de la Firma Electrónica.

1.2.2. Características de la aprobación digital

Integridad

Asegura que la información almacenada no esté contaminada o sea alterada de una manera que no sea apropiada, es decir, consiste en asegurar que la información no haya sufrido cambios no autorizados, de manera accidental o intencional, una vez haya sido aprobado.

Autenticación

Es un servicio de seguridad que permite verificar la identidad; consiste en identificar al emisor de mensaje y sus atributos principales, asegurando que es la persona que figura como firmante.

No repudio a la información

Esta característica está ligada a la autenticación, pues garantiza que el emisor no pueda negar que haya firmado y enviado un mensaje hacia un destinatario porque para enviar el documento digital.

Es un servicio de seguridad que permite probar la participación de las partes en una comunicación. Por lo tanto, existen dos posibilidades:

- No repudio en origen: El emisor no puede negar que envió el mensaje porque el destinatario tiene pruebas del envío.
- No repudio en el destino: El receptor no puede negar que recibió el mensaje.

La posesión de un documento y su firma digital asociada será prueba efectiva del contenido y del autor del documento.

Confidencialidad

La confidencialidad mantiene la información protegida de las personas que no tienen autorización para leerla. El objetivo requiere que aquellos que están protegiendo los datos y quiénes deben tener acceso a ella, tengan acceso a los mecanismos de protección para los datos mientras se almacenan y al mismo tiempo estén siendo transferidos a través de los canales correspondientes.

Infraestructura de la clave pública

Una infraestructura de clave pública (Public Key Infrastructure), es la combinación de productos de hardware, software, políticas y procedimientos para proveer un nivel adecuado de seguridad en transacciones electrónicas a través de redes públicas, como el Internet.

Generalmente, una estructura PKI consiste en:

- Una política de seguridad que establece y define la dirección que debería seguir la organización respecto de la seguridad de su información considerando también los procesos y principios establecidos para el uso de medios criptográficos.

- Una Autoridad Certificante. Es el componente clave de una estructura PKI y es la encargada de realizar la emisión y administración de los certificados durante todo el ciclo de vida de los mismos.

- Un sistema de administración de certificados. Establece el tratamiento que recibirán los certificados generados, desde el procedimiento de generación hasta su revocación o recertificación.

- Un conjunto de aplicaciones que hacen uso de la tecnología PKI. Aplicaciones como un servidor web, navegadores, correo electrónico y VPN.

Función Hash

Una función hash es un método para generar claves o llaves que representen de manera unívoca a un documento o conjunto de datos. Es una operación matemática que se realiza sobre este conjunto de datos de cualquier longitud, y su salida es una huella digital, de tamaño fijo e independiente de la dimensión del documento original.

Las funciones hash son algoritmos que consiguen crear a partir de una entrada (ya sea un texto, contraseña o un archivo) una salida alfanumérica de longitud normalmente fija que representa un resumen de toda la información que se le ha dado, es decir, a partir de los datos de la entrada crea una cadena que solo puede volverse a crear con esos mismos datos.

1.3. Adobe Document Cloud

Es un servicio de Adobe Systems el cual provee a los usuarios el acceso a las aplicaciones de diseño gráfico, de video, de diseño web y de servicios en la nube. Adobe Documento Cloud, trabaja haciendo uso del modelo de software como servicio (SAAS).

Es una plataforma que engloba varias herramientas, entre ellas Adobe Acrobat CC, y que se centra en la capacidad de acceder a los documentos PDF en cualquier parte directamente a través de la nube con nuestra cuenta de Adobe. Trabaja con archivos que estén almacenados tanto en Creative Cloud, como Document Cloud y Microsoft Office 365. Actualmente permite conectar esta solución con otras herramientas como Dropbox o Google Drive.

El acceso a la plataforma de Adobe Document Cloud se hace desde el siguiente URL: https://documents.adobe.com.

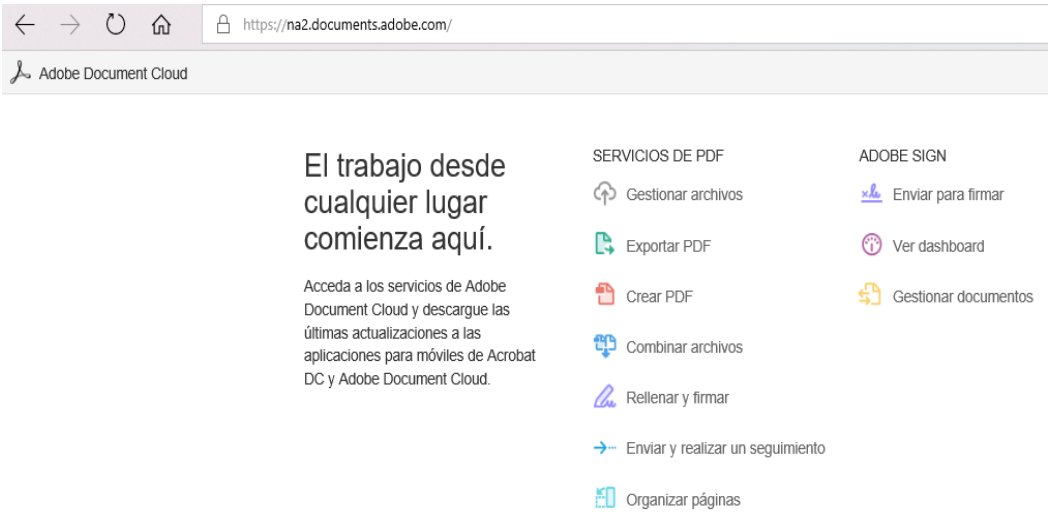


Figura 6. Portal de Adobe Document Cloud
Adaptado de (Adobe, 2018)

1.4. Tecnología de la nube

La tecnología de la nube no es una entidad física, sino una red enorme de servidores remotos de todo el mundo que están conectados para funcionar como un único ecosistema. Estos servidores están diseñados para almacenar y administrar datos, ejecutar aplicaciones o entregar contenido o servicios, como streaming de vídeos, correo web, software de ofimática o medios sociales. En lugar de acceder a archivos y datos desde un equipo personal o local, accede a ellos en línea desde cualquier dispositivo conectado a Internet, de tal modo que la información está disponible desde cualquier ubicación.

Las empresas utilizan cuatro modelos diferentes para implementar recursos en la nube.

- Nube pública, que comparte recursos y ofrece servicios al público a través de Internet. En este modelo se las organizaciones que hacen uso de la Nube pública, comparten el mismo hardware, almacenamiento y recursos de red. Una nube privada, está compuesta de recursos tecnológicos que son exclusivos de una empresa y organización. Usualmente los centros de datos

se hospedan en el entorno local. Las nubes privadas son utilizadas en organizaciones gubernamentales o instituciones financieras. Este modelo provee a sus administradores de más flexibilidad para personalizar su entorno.

- Una nube híbrida, que comparte servicios entre nubes públicas y privadas, según su finalidad. Los datos y las aplicaciones pueden moverse entre nubes privadas y públicas, es decir, se utiliza cada una de ellas según las opciones de implementación, por ejemplo: en la nube pública se puede alojar un servicio requiera de gran volumen con menor seguridad y en la nube privada alojar un servicio que maneje operaciones confidenciales.

En la siguiente tabla (Tabla 1.) se describe las características de la nube pública, privada e híbrida.

Tabla 1

Características de la Nube pública, privada e híbrida.

Categoría de Usos	Nube Pública	Nube Privada	Nube Híbrida
Tenencia	Se almacenan datos de múltiples organizaciones en un entorno compartido.	Se almacenan datos de una sola organización en la Nube.	Los datos de las múltiples organizaciones se almacenan en un entorno compartido. Sinembargo los datos almacenados en la Nube privada se mantienen

			privados por la organización.
Exposición al público	Cualquier usuario puede hacer uso de los servicios alojado en la Nube pública.	Sólo los usuarios de la organización, pueden utilizar los servicios de la Nube privada.	Cualquier usuario puede acceder a los servicios de la Nube pública, pero solo los usuarios de la organización pueden acceder a los servicios en la Nube privada.
Ubicación del centro de Datos	En cualquier lugar donde se encuentren alojados los servicios que pone a disposición el proveedor.	Dentro de la red de la organización.	En cualquier lugar de Internet para servicios de Nube pública, así también como dentro de la red de la organización de la Nube privada.
Gestión de servicio en la Nube	El proveedor de servicios en la nube administra y da mantenimiento a los servicios, en este caso la organización	La organización debe tener sus propios administradores de los servicios que están alojados	En este modelo, la organización debe administrar la Nube privada, mientras que la Nube pública la

	simplemente los usa.	en la Nube privada.	administra el proveedor de soluciones en (CSP) - Políticas de Seguridad de Contenido.
Componentes de Hardware	El proveedor de soluciones (CSP) en la Nube pública proporciona todo el hardware y garantiza que funcione en todo momento.	En este caso, debe ser provisto por la propia organización, que tienen que comprar servidores físicos para construir la Nube privada.	La organización debe proporcionar el hardware para la nube privada, mientras que el hardware del CSP, se usa para servicios de Nube pública.
Gastos	Costo inferior: no es necesario adquirir hardware o software, de tal modo que solo se para por el servicio que se usa.	En este modelo, resulta costoso, ya que la organización debe proporcionar y gestionar el hardware, las aplicaciones y la red.	Los servicios de la Nube privada deben ser proporcionados por la organización, incluido el hardware, las aplicaciones y la red, mientras que el CSP administra los servicios de Nube pública.

1.5 Servicio de SaaS, IaaS, PaaS

Software as a Service, es un modelo que tiene como propósito distribuir aplicaciones o sistemas de cómputo usando el internet.
Se caracteriza por lo siguiente:

- Actualizaciones automáticas.
- Acceso Global.
- Pago según el uso.
- Bajo costo de adquisición.
- Rápida implementación.
- Disponibilidad más rápida que el software tradicional.

Actualmente existen servicios que forman parte del desarrollo de la tecnología del Cloud Computing, entre los cuales se definen los siguientes:

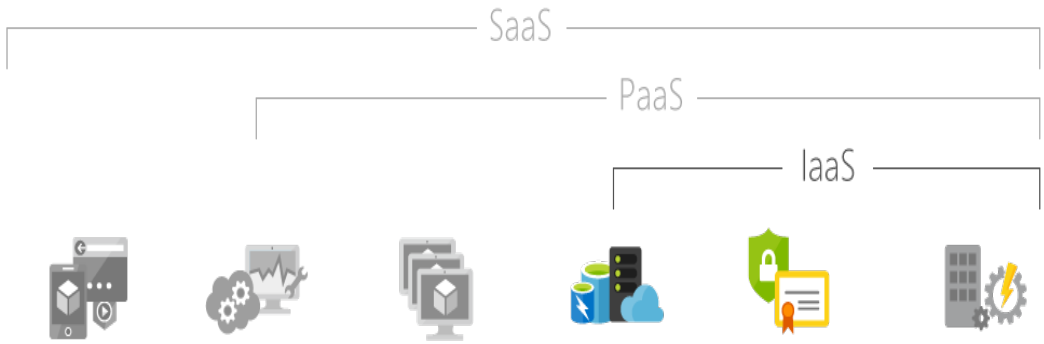


Figura 7. Cloud Computing - SaaS

Adaptado de (Microsoft, 2018)

a) Microsoft Azure. Infraestructura como servicio.

- **Servicio IaaS** (Infraestructura como Servicio)

Se define como la infraestructura informática que se administra y aprovisiona a través de internet; evita el costo y complejidad de la compra y administración de servidores físicos y otra infraestructura de centro de datos. Microsoft. (2018). (Micosoft Azure. Infraestructura como servicio). Es considerado un modelo

fundamental utilizado por Cloud computing, junto con la plataforma como servicio (PaaS) y el Software como Servicio (SaaS).

Ventajas del uso de IaaS:

- Mejora el factor de recuperación anti desastres.
- Permite responder más rápido a una situación variable del negocio.
- Brinda el acceso a las aplicaciones con más rapidez.

- **Servicio PaaS** (Plataform as a Service).

Esta categoría de servicios cloud, consta de un entorno que brinda a los desarrolladores las herramientas necesarias para crear aplicaciones y servicios que funcoionen a través de internet.

Este servicio incluye infraestructura (servidores, almacenamiento y redes), pero de manera adicional incluye middleware, herramientas de desarrollo, servicios de inteligencia empresarial (BI), sistemas de administración de base de datos, entre otras. Su funcionalidad es sustentar el ciclo de vida de las aplicaciones web. Microsoft. (2018). (Plataforma como servicio).

En la figura 8, hace referencia Cloud Computing – PaaS, en la que se puede observar que forma parte de la estructura del Softwae como servicio – SAAS.

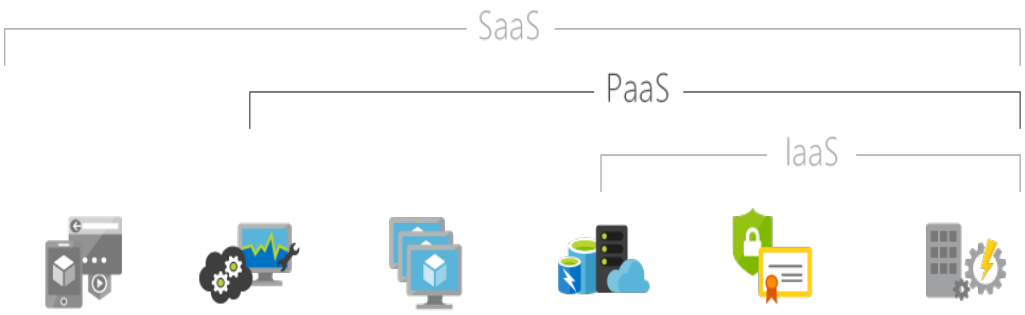


Figura 8. Cloud Computing - PaaS.
Adaptado de (Microsoft, 2018)

Beneficios de SAAS

Determina el acceso al software sin necesidad de comprar hardware, software, sistemas operativos, únicamente conectándose a través de un navegador. El uso de este servicio permite tener externamente los sistemas.

SAAS, permite tener mayor disponibilidad y seguridad de los datos, por ejemplo: la disponibilidad de procedimientos de backup, restore y en general de planes de contingencia en caso de pérdida de información o de fallo del hardware (servidores).

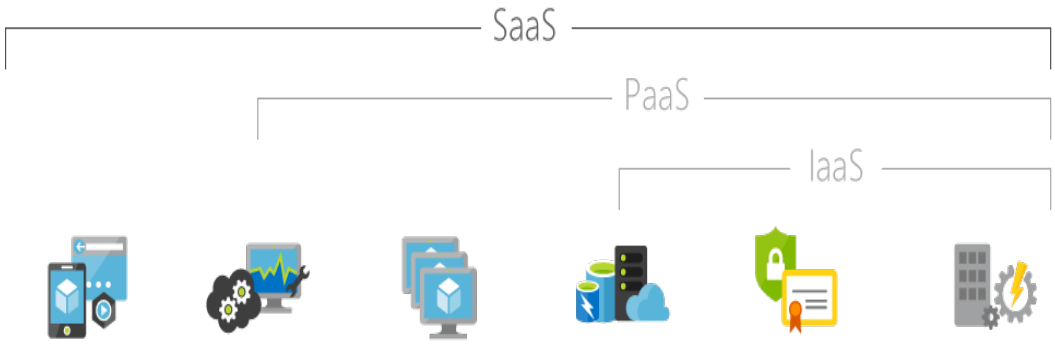


Figura 9. Cloud Computing - IaaS

Adaptado de (Microsoft, 2018)

a) Micosoft Azure. Infraestructura como servicio.

1.5. Office 365

1.5.1. Definición de Microsoft office 365

Office 365 es la plataforma de productividad, comunicación y colaboración alojada en la nube. Según Microsoft, Office 365 es capaz de editar documentos en cualquier explorador con Web Apps, revisar correo electrónico en cualquier dispositivo, realizar reuniones en línea para ver y escuchar a socios y clientes, además de que se pueden editar documentos de manera simultánea, para así tener un negocio más eficiente y productivo y lo mejor, todo esto desde la nube.

1.5.2. Características de Microsoft office 365

Microsoft Office 365, integra el sistema Office de siempre con las herramientas necesarias para trabajar en equipo, colaborar en tiempo real y acceder a los documentos de su empresa siempre que lo necesite. En general office 365 permite el uso de las siguientes herramientas:

Skype for bussines. A través de ella se llevan a cabo reuniones mediante videoconferencias, compartiendo contenido en tiempo real, accediendo desde cualquier dispositivo móvil.

OneDrive. Que actualmente tiene 1 TB de almacenamiento en la nube para guardar archivos y compartirlos. Permite el uso de aplicaciones de Office tanto online como offline.

Outlook de Office 365. Con el dominio corporativo. Tiene hasta 50 GB de capacidad en buzón. Esta aplicación cuenta con un Centro de administración, a través del cual se puede administrar los servicios configurados.

1.6. Centro de datos

Un centro de datos, es un espacio donde se almacena y se procesan datos; un centro de datos consta de Network, security, Computing, Storage, Cloud computing y virtualización.

“Un centro de datos es un espacio exclusivo donde las empresas mantienen y operan las infraestructuras TIC que utilizan para gestionar su actividad empresarial. Es el espacio donde alojar los servidores y sistemas de almacenamiento donde se ejecutan las aplicaciones y se procesan y almacenan los datos y el contenido. Para algunas empresas se trata de una simple jaula o bastidor, mientras para otras puede ser una sala privada donde alojar un

determinado número de bastidores, dependiendo del tamaño de la empresa." (Interxion, 2017).

Un centro de datos contiene 3 componentes a nivel general: Sitio, infraestructura y gestión; cada una de ellas con sus correspondientes subcomponenetes que se describen la siguiente figura.

Figura 10. Componentes de un centro de datos.

1.7. Virtualización

La virtualización es el medio a través del cual se crea una versión virtual de un recurso o de un dispositivo físico. La virtualización de un centro de datos es la consolidación de servidores físicos en servidores virtuales, con el objetivo de ofrecer mayor almacenamiento y mayor potencia de procesamiento.

El uso de la virtualización en una empresa puede alcanzar un ahorro desde el 30% al 70% en gastos que hagan referencia a software, hardware, almacenamiento, mantenimiento y operación. A continuación, se menciona algunos de los beneficios que brinda la virtualización:

- Permite hacer uso eficiente de los recursos de hardware, facilitando la creación y administración centralizada de todas las máquinas virtuales.
- Brinda medios adecuados para hacer uso de técnicas de Disaster Recovery.
- Permite migrar esquemas de múltiples aplicaciones a sistemas integrados.

- Mejorar el procedimiento de pruebas de test, por ejemplo: revirtiendo los datos de un estado anterior previo a un snapshot.
- La virtualización es rentable si se requiere separar servicios en diferentes servidores. El uso de servidores virtuales, permite crear una infraestructura dinámica en la nube y por lo tanto a un sistema Cloud Computing.
- Gestión automatizada y mejor uso del factor de almacenamiento.
- Reduce errores de los datos y por lo tanto la carga de trabajo.

La virtualización tiene diferentes tipos de virtualización, que se utilizan para mejorar y optimizar cloud computing, entre ellos tenemos: virtualización de hardware o de servidor, virtualización de red, virtualización de almacenamiento, virtualización de memoria, virtualización de software, virtualización de datos, virtualización de escritorio.

1.8. Diferencia entre firma electrónica y firma digital

Firma electrónica

Se define como datos electrónicos que acompañan la información (en formato electrónico), que identifican al firmante; este tipo de firma tiene el mismo objetivo que la firma manuscrita: dar fe de un acto de voluntad e identificar al firmante. Una firma electrónica puede ser una contraseña, frase, líneas dibujadas con el ratón, una imagen jpg con la imagen de una firma manuscrita, etc.

Firma digital

Es un proceso de cifrado matemático que permite comprobar la autenticidad de los datos cifrados. Se trata de un sistema de cifrado asimétrico y emplea por lo tanto una llave privada y una llave púbilca; es decir, a través de un certificado digital emitido por entidad de certificación acreditada, que incorpore datos

electrónicos que identifiquen y autentiquen al firmante (o aprobador) utilizando una llave pública y otra privada basada en la criptografía asimétrica.

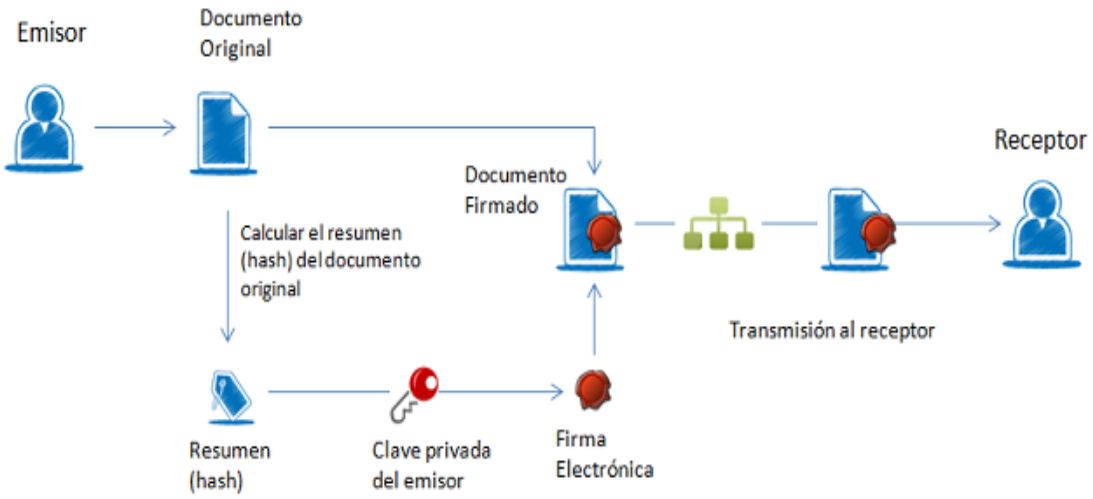


Figura 11. Proceso básico de firma digital.
Adaptado de (PAe, 2017)

La firma digital es un concepto que nace con la criptografía de llave pública (Menezes et al., 1996). Con la firma digital, se busca la provisión de seguridad informática de autenticación, verificación y no repudio a la información; técnicamente se hace uso de la teoría de los números del álgebra abstracta, refiriéndose específicamente a la teoría de grupos y campos finitos (LidI and Niederreiter, 1986).

El propósito de la firma digital es reemplazar la firma autógrafa, en la tabla 2, se muestra la comparativa entre la firma autógrafa y la firma digital.

Tabla 2

Diferencias entre la firma digital y la firma autógrafa.

Propiedad	Firma autógrafa	Firma digital
Tiene presunción jurídica ante un juez.	NO	SI
Permite detectar alteraciones en el documento.	NO	SI
Se aplica a documentos electrónicos y transacciones.	NO	SI
Tiene que ser considerada como evidencia en juicio.	SI	SI
Asegura la integridad del documento.	NO	SI
La mayoría de las personas cuentan con ella.	SI	NO

Actualmente existen diferentes tecnologías de autenticación, las cuales determinan la seguridad que brindan, entre ellas tenemos: fallas en la autenticación, tasa de falsos rechazos, tasa de falsos aceptados, fácil de usar, altamente seguro; en la siguiente tabla se puede aprecia las métricas determinadas por el mecanismo de autenticación. Esta información está basada en un estudio realizado por la empresa Adobe Inc., y se presenta en la tabla 3.

Tabla 3

Análisis comparativo de tecnologías de autenticación.

Medio de autenticación	Fallas en la autenticación	Fallas de falsos rechazos	Tasa de falsos aceptados	Fácil de usar	Seguro
Firma digital	●●●●●	●●●●●	●●●●●	●●●●○	●●●●●
Tarjeta inteligente	●●●●○	●●●●○	●●●●○	●●●●●	●●○○○
Passwords	●●●●●	●●●●●	●●●●●	●●●●●	●○○○○
Firma Autógrafa	●●●○○	●●●○○	●●●○○	●●●●●	●●●○○
Voz	●○○○○	●●●○○	●●●○○	●●●●○	●●○○○
Huella dactilar	●●●●○	●●●●○	●●●●○	●●●●○	●●●○○
Reconocimiento de rostro	●●○○○	●●○○○	●●○○○	●●●●○	●●○○○
Patrón de retina	●●●●○	●●●●○	●●●●○	●●●○○	●●●●○
Escaneo de Iris	●●●●○	●●●●○	●●●●○	●●●○○	●●●●○

Adaptado de (Instituto Politécnico Nacional, 2013).

Parte de este estudio hace referencia al panorama de la aplicación de la firma digital, en el siguiente gráfico se detalla el grado de reconocimiento según la ley en cada uno de los países, donde es considerada como igual la firma autógrafa con la firma digital. A continuación, se ilustra esta información (Figura 12. Panorama mundial de la aplicación digital).

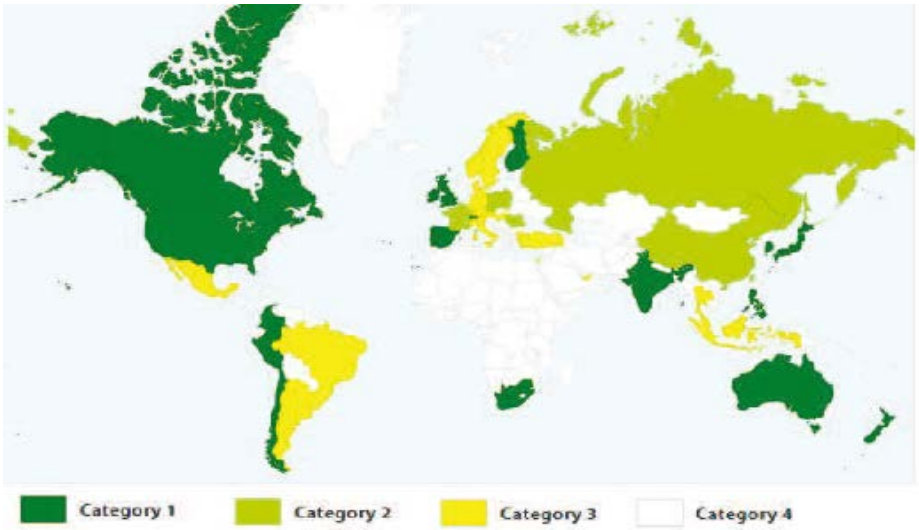


Figura 12. Panorama mundial de la aplicación digital
Adaptado de (Instituto Politécnico Nacional, 2013).

El estudio realizado por Adobe, segmenta por categorías divididas de la siguiente manera:

Categoría 1. Países donde bajo la ley, la firma electrónica en los negocios es considerada como igual a la firma autógrafa. Países: Australia, Canada, Chile, Colombia, Finlandia, India, Irlanda, Japón, Nueva Zelanda, Perú, Filipinas, Portugal, Singapur, Sudáfrica, Corea del Sur, España, Suiza, Inglaterra, Estados Unidos.

Categoría 2. Países donde la firma electrónica para las empresas se considera aplicable, pero no necesariamente igual a la firma autógrafa. Países: Bélgica, China, República Checa, Francia, Polonia, Rumania, Rusia, Taiwán.

Categoría 3. Países donde la firma electrónica, se considera aplicable en empresas, pero no necesariamente igual a la firma autógrafa. Argentina, Austria, Brasil, Dinamarca, Alemania, Hungría, Hong Kong, Indonesia, Israel, Italia, Macao, Malasia, México, Noruega, Suecia, Tailandia, Turquía, EAU, Uruguay.

Categoría 4. Países no considerados en el estudio.

2. DISEÑO E IMPLEMENTACIÓN

El capítulo dos, inicia con la descripción técnica del sistema que será implementado e integrado Adobe Sign a la infraestructura de la UDLA, contempla el desarrollo del proceso de análisis, diseño e implementación del proyecto, basado en la operación de firma electrónica e integrado con office 365 y Document Cloud.
Se desarrollan las fases requeridas desde el análisis hasta la implementación del sistema de aprobación digital tomando como guía referencial la metodología Top Down.

2.1. Descripción de la metodología Top Down

La metodología Top Down fue promovida por los investigadores de IBM Harlan Mills y Niklaus Wirth, que utilizaron esta metodología para usos prácticos y desarrollo de proyectos de tecnología.

La metodología Top Down también es conocida como de arriba a abajo y depende en establecer una serie de niveles de mayor a menor complejidad las cuales brinden una solución al problema, consiste en efectuar una relación entre las etapas de la estructuración de forma que una etapa jerárquica y su inmediato inferior se relacionen mediante entradas y salidas de información.

Este diseño consiste en una serie de descomposiciones sucesivas del problema inicial, que recibe el refinamiento progresivo de las instrucciones que van a formar parte del programa. La utilización de la técnica de diseño Top Down permite la simplificación del problema y de los subprogramas de cada descomposición. Las diferentes partes del problema pueden ser programadas de modo independiente e incluso por diferentes personas. El programa final queda estructurado en forma de bloque o módulos lo que hace más sencilla su lectura y mantenimiento.

Según Huerta (2010, Ed. 3). Los objetivos y limitaciones incluyen la capacidad de correr las aplicaciones en red que reúne los objetivos comerciales corporativos, y la necesidad de trabajar dentro de restricciones comerciales, como paquete, personal limitado que está conectado a una red, y márgenes de tiempo cortos.

Según Fonseca (2010, Ed. 1) la metodología Top Down es de tipo iterativo, ya que permite realizar cambios cuando más información es recopilada. Esta metodología se basa en el procedimiento de división y estructura de grupo, determinando el propósito del servicio que estos usuarios van a recibir.

Para el desarrollo de este proyecto se toma como guía referencial la metodología Top Down, la cual adaptamos a las siguientes fases:

FASE 1. Análisis de requerimientos.

- Levantamiento de línea base.
- Realidad problemática.
- Definición del problema.
- Análisis de los requerimientos.

FASE 2. Desarrollo de un diseño de integración.

- Selección de tecnología y aplicación a implementarse.
- Identificar las características técnicas de Adobe Sign.
- Modelo de operación de la aprobación digital.

FASE 3. Implementación y pruebas de la aplicación.

- Implementar e integrar la aplicación Adobe Sign.
- Realizar pila de pruebas.

FASE 4. Monitorear y optimizar.

- Operar la aplicación de aprobación digital.
- Monitoreo del rendimiento de la aplicación.

- Optimización de la implementación.

2.2. Fase 1. Análisis de requerimientos

2.2.1. Levantamiento de la línea base

Se describe la situación del proceso actual de la parte documental en la carrera de Ingeniería de Telecomunicaciones de la UDLA, los problemas detectados que proporcionarán los requerimientos necesarios y que componentes tecnológicos existe actualmente.

2.2.2. Realidad de la problemática

La Facultad de Ingeniería y Ciencias Aplicadas actualmente trabaja con procedimientos internos que requieren de firmas de aprobación las cuales se manejan de manera manual, esto incluye impresión de documentos, movilización por parte de los usuarios responsables de conseguir las aprobaciones manuales, archivar los documentos impresos y firmados, mantener organizado y disponible esta información recopilada.

El problema existente se origina porque el procedimiento de recolección de aprobaciones es de tipo “manual”, motivo por el cual se presentan varias desventajas que afectan de manera general al desarrollo y mejoramiento en el aspecto tecnológico y documental, pues como toda institución busca el mejoramiento en calidad de trabajo haciendo uso de la tecnología.

Por lo anterior la Facultad de Ingeniería y Ciencias Aplicadas, generó la necesidad de buscar un medio tecnológico que contribuya a solventar estas necesidades identificadas, haciendo uso de una aplicación electrónica, políticas de seguridad de la información, así también estandarizar las políticas de uso de la aplicación a implementarse.

2.2.3. Definición de la problemática

Basado en el análisis de las encuestas realizadas en FICA (Tabla 1), se definen los siguientes puntos que hacen referencia a las condiciones actuales con que se maneja este proceso

SITUACION ACTUAL	MÉTODO MANUAL
	Este gráfico describe de manera práctica como una persona (encargada de recolectar las aprobaciones) se ve obligada a realizar una planificación tipo método manual, la cual incluye movilizarse hasta el lugar donde se encuentran lo usuaros aprobadores, este procedimiento consume tiempo no planificado, retrasa los procesos que dependen de estas aprobaciones y en conclusión se torna confusa.

Figura 13. Procedimiento de recolección de aprobaciones autógrafas.

A continuación, se describen los puntos, sobre la problemática actual referenciada en el procedimiento de recolección de aprobaciones de documentación; para esto se procedió a realizar una encuesta en Facultad de Ingeniería y Ciencias Agropecuarias con la persona responsable de realizar la recolección de las firmas autógrafas, ver el Anexo 1. (Encuesta – definición de problemática).

Tabla 4

Resumen de la situación actual en FICA.

Tabla de resumen de la situación actual, recolección de aprobaciones autógrafas en FICA	
1	El tiempo utilizado para movilizarse y conseguir una aprobación excede del tiempo planificado para realizar esta tarea.
2	Uso innecesario del servicio de impresión.
3	Disponer de un lugar donde almacenar y custodiar la documentación, teniendo en cuenta que esta necesidad va a ser creciente.
4	La frecuencia de envío de documentos para firmar es diaria o semanal según el caso, lo cual genera problemas de calidad, cuello de botella o problemas de coordinación entre el gestor del documento y los usuarios aprobadores.
5	No se dispone de un medio formal de la función de delegar
6	No se dispone de un log o histórico del flujo del documento, que describa con exactitud el tiempo que tardan en aprobar un documento, motivo por el cual no hay un medio de medición para mejora un proceso si así se requiere.
7	El procedimiento manual que actualmente se utiliza, no asegura la integridad, autenticación, confidencialidad y no repudio a la información del documento.
8	Actualmente no se dispone de ninguna herramienta tecnológica que permita automatizar este proceso manual.

2.2.4. Análisis de los requerimientos

En base a los puntos identificados en la definición de la problemática, se realiza el análisis y definición de los requerimientos técnicos que la aplicación debe

cumplir. El análisis de los requerimientos de tipo técnico y de tpo funcinal que se resumen en la tabla 2. Análisis de requerimientos técnicos y funcionales.

Tabla 5

Análisis de requerimientos técnicos y funcionales.

Tabla de análisis de requerimientos técnicos	
1	Control de identidades de usuarios validado a través de una autenticación con office 365.
2	Certificación de la integridad de un documento.
3	Permitir el acceso a rastros para auditoría.
4	El proceso de notificación debe hacerse utilizando un medio seguro, se sugiere el mail corporativo.
5	Se requiere que el almacenamiento de la documentación sea en la nube.
6	El acceso a la aplicación debe ser desde cualquier dispositivo que esté conectado al internet.
7	Simplificar y automatizar la gestión documental.
8	Brindar seguridad a la gestión documental en la nube.
9	Reducción de costes asociados al servicio de impresión de documentos.
10	La aplicación debe asegurar la integridad, autenticación, confidencialidad y no repudio a la información del documento.

Componentes tecnológicos

Para el desarrollo de este proyecto, se realizó un análisis de los elementos tecnológicos que UDLA dispone actualmente y que hace referencia tanto a nivel de infraestructura tecnológica como a nivel de software (aplicativos). Este análisis se realiza en base al objetivo general de esta implementación, es decir, lo requerido para la implementación de la “aprobación digital.

A continuación, se describe los componentes tecnológicos requeridos para esta implementación.

Adobe Sign

Es una aplicación para realizar el proceso de firmas electrónicas basado en la nube a nivel corporativo que permite automatizar los procesos de firma en papel por flujos de trabajo de firma electrónica completamente automatizados. UDLA dispone actualmente del licenciamiento, que permite el uso de esta aplicación propia de Document cloud de Adobe.

A continuación, se describe los requisitos del sistema (Requisitos del sistema de Adobe Sign, 2018).

Requisitos del Sistema Adobe Sign

Los requisitos del sistema que Adobe Sign solicita que el usuario final disponga para que esta aplicación funcine correctamente.

Navegador

La aplicación de Adobe Sign, para que su funcinamiento sea óptimo requiere que el usuario final trabaje con los siguientes navegadores:

- Microsoft Windos 10 con Microsoft Edge, Firefox o Chrome.
- Microsoft Widows 8 con Internet Explorer 11 o posterios, Firefox o Chrome.
- Mac OS X 10.9 o versiones posteriores con Safari 7, Firefox o Chrome.

Aplicación móvil

La aplicación de Adobe Sign, requiere que los dispositivos móviles tengan acceso al internet y que dispongan de sistemas operativos de windows, iOS y Android.

Formatos compatibles con Adobe Sign

Adobe Sign, es una aplicación que permite trabajar directamente con documentos que tengan las siguientes extenciones:

- Adobe PDF (.pdf)
- Microsoft Word (.doc y .docx)
- Microsoft Excel (.xls y .xlsx)
- Microsoft PowerPoint (.ppt y .pptx)
- Texto (.txt)
- Texto enriquecido (.rtf)
- Gráficos (.tif, .jpg, .jpeg,.gif, .bmp y .png)
- Web (.htm o .html)

Requisitos de aplicación / protocolo

Se requiere usar la versión de Java 8 o una versión posterior.

También se puede utilizar Java 7, pero TLS 1.2 debe ser habilitado para el uso explícito por la aplicación.

Requisito de TLS 1.2

TLS (Transport layer Security), es el protocolo de seguridad utilizado en los navegadores web requerida por aplicaciones que requieren de intercambio de datos seguros a través de una red.

El TLS 1.2, necesita de Java 8 o superior. Tambien de NET 4.6 o posterior y para aplicaciones que usan OpenSSL: OpenSSL 1.01 o posterior.

Software requerido para visualizar un documento electrónico de Adobe Sign

Para visualizar los documentos electrónicos, es necesario hacerlo desde Adobe Reader 9.0 o versiones porteriores para documentos asegurados mediante el cifrado AES de 128 bits o inferior. Si se utiliza Adobe Reader 10 o versiones porteriores para documentos asegurados mediante el cifrado AES de 256 bits.

Infraestructura de Red

Intervalos de IP en la lista de elementos permitidos. Se incluye de forma explícita direcciones IP en la lista de elementos permitidos en la red, se solicita añadir los siguientes intervalos de IP en su cortafuego:

52.71.63.224/27
52.35.253.64/27
40.67.155.147/32
40.67.154.249/32

Rangos de Ip para retransmisines de correo saliente. Hay organizaciones que emplean listas blancas de direcciones IP para controlar la conexión de los servidores de correo entrantes, por tal motivo es necesario añadir las siguientes direcciones IP a dicha lista blanca:

40.67.157.141/32
40.67.154.24/32
40.67.158.131/32
52.205.63.172/30
52.41.255.236/30
52.208.255.252/30
52.208.255.252/30
52.197.127.252/30

Office 365

Es una aplicación que proporciona un servicio basado en la nube con herramientas web que permiten acceso a correo, documentos, contactos y calendarios desde casi cualquier lugar y con cualquier dispositivo. Tiene las siguientes herramientas: correo electrónico y calendario, Office Web Apps, sitios web y colaboración, mensajería instantánea y conferencias en línea. Permitiendo un acceso a la información desde cualquier sitio cuando se lo requiera, lo que

permite responder de manera oportuna peticiones importantes a nivel corporativo. UDLA, es un cliente de Microsoft y como tal dispone del licenciamiento que le permte utilizar esta herramienta.

Microsoft Azure

Es la plataforma de administración de computación basada en la nube pública de Microsoft. Azure proporciona el acceso a diferentes servicios incluidos los de analítica, almacenamiento, redes y administración de aplicaciones en una red centro de datos. UDLA, es un cliente de Microsoft y como tal dispone del licenciamiento que le permte utilizar esta herramienta.

2.3. Fase 2. Desarrollo de un diseño de integración

2.3.1. Selección de tecnología a implementarse

En base al levantamiento de línea base y el análisis de requerimientos se establece que la solución que se va a implementar es Adobe Sign por cuanto es un activo de software licenciado que la UDLA posee. Adobe Sign, una solución de Adobe Document Cloud, es un servicio para firmar electrónicamente basado en la nube de nivel empresarial que se adapta para este proyecto de aprobación digital.

La infraestructura de Adobe Sign reside en data centers de primer nivel operados por proveedores de servicios de nube Rackspace y Amazon Web Services que proporciona seguridad para este proceso en la UDLA, considerando que solo personal autorizado y aprobado por la compañía Adobe, empleados y contratistas con una función legítima tienen acceso a los sitios seguros de los servidores.

2.3.2. Características técnicas de Adobe Sign

Adobe Sign es una solución de Adobe Document Cloud, que permite enviar, firmar, dar seguimiento y administrar procesos de firma y firmar digitalmente

documentos desde cualquier dispositivo en cualquier lugar. Adobe Sign cumple o puede ser configurado para cumplir con las normas reguladoras de muchas industrias. Al ser un servicio robusto basado en la nube, Adobe Sign de forma segura maneja grandes volúmenes de procesos de firma electrónica incluyendo: manejo de identidades, certificación de integridad, mantenimiento de rastros de auditoría, validación de la aprobación digital.

2.3.3. Arquitectura de Adobe Sign

La arquitectura de Adobe Sign está diseñada para ser escalable y que permita ejecutar un gran volumen de transacciones sin degradación en el rendimiento. Con el fin de ofrecer un servicio de alto nivel de escalabilidad y disponibilidad del servicio en la nube, Adobe Sign almacena en diversos clusters, con redundancia de base de datos con recuperación automática.

Adobe Sign costa de capas lógicas; cada una de ellas con una función específica y que esta monitoreada por una suite que permite el registro de indicadores principales, por ejemplo, alertas en tiempo real, si ocurriera unincidente, registros de diagnósticos y forenses para solucinar un problema raíz o el tiempo que tome la aplicación para connvertir documentos en PDF´s o uso de sus recursos.

Cada capa lógica en la aplicación de Adobe Sign esta monitoreada por una suite de herramientas que mantiene un registro de los indicadores principales, como el tiempo para convertir documentos en PDF’s o el uso de recursos. El panel de monitoreo permite a los responsables de Operaciones de Adobe Sign ver fácilmente la calidad del servicio. Las alertas en tiempo real alertan a los Ingenieros si ocurre algún incidente o si ocurre un proceso fuera de lugar.

Si la situación no puede ser remediada, Adobe Sign mantiene registros de diagnóstico y forenses para que se pueda resolver el incidente rápidamente y atiendan el problema de raíz para evitar que vuelva a ocurrir. A continuación, se

presenta el diagrama describe la división de las capas lógicas de la arquitectura de la aplicación de Adobe sign, ver la figura 14.

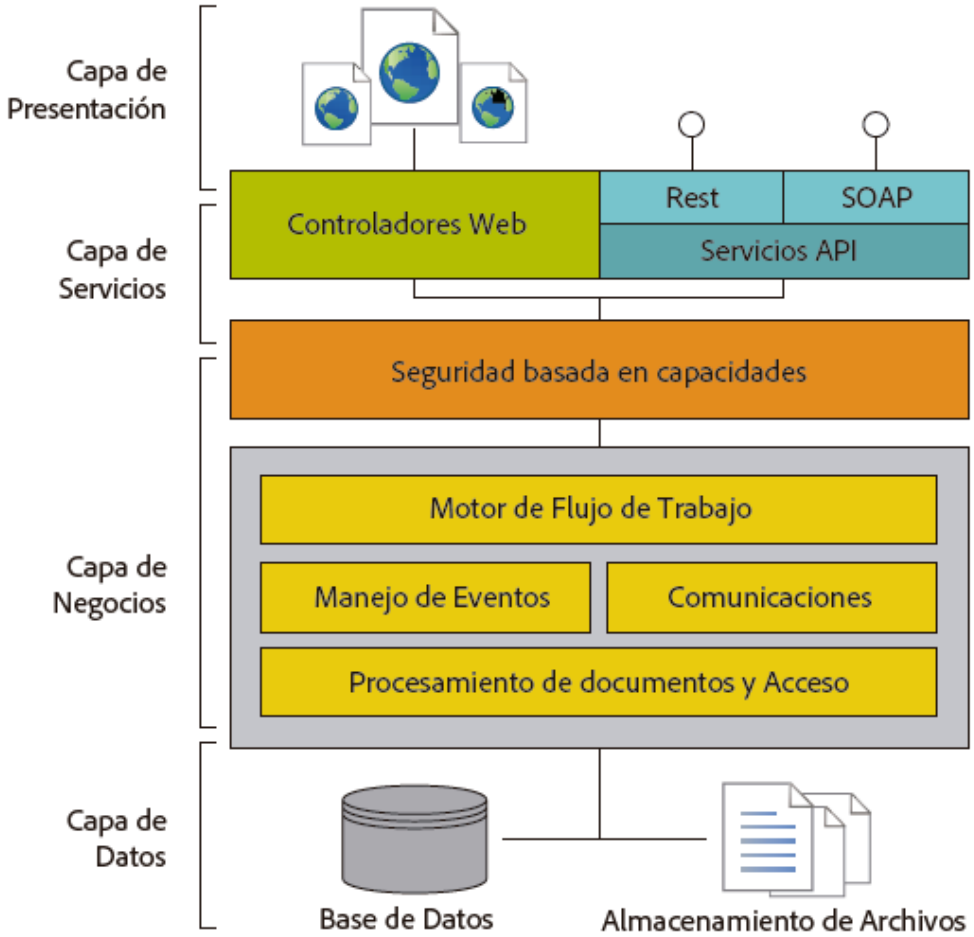


Figura 14. Arquitectura de las capas lógicas de Adobe Sign.
Adaptado de (Adobe Sign, junio, 2018)

Capa de Presentación

La capa de presentación hace referencia a la interface de usuario web (UI), así como la generación y muestra de documentos a ser aprobados electrónicamente, archivos PDF finales certificados y componentes del flujo de trabajo.

Capa de Servicios

La capa de servicios usa las funciones necesarias para los servicios del usuario, servicios web, interfaces API, como el Gateway REST y el API SOAP. Los servidores web exteriores manejan las solicitudes de navegadores, también los API y los servidores de correo manejan el tráfico de comunicaciones interno y externo. Los servidores web distribuyen las solicitudes dinámicas complejas a los servidores de aplicación de Adobe Sign en la capa de negocio, a través de balanceadores de carga en hardware.

Los servidores de la capa de servicios también incorporan reglas de filtrado de seguridad para prevenir ataques comunes y protección de firewall para fortalecer el control de acceso.

Capa de Negocios

Esta capa maneja el flujo de trabajo, la seguridad basada en capacidades, conversión de documentos y servicios de imagen, manejo de eventos, registro y monitoreo, acceso de archivos y manipulación y funciones de comunicación.

Motor de flujo de Trabajo. El motor del flujo de trabajo ejecuta y maneja todos los procesos de negocio y pasos que requiere un documento a través del proceso de firma. El motor de flujo de trabajo utiliza un lenguaje declarativo basado en XML para describir las pre-condiciones para ejecutar flujos de trabajo específicos del usuario y la secuencia de eventos requerida para completar un proceso de aprobación.

Seguridad basada en capacidades. La seguridad basada en capacidades define, controla y audita los recursos disponibles y las operaciones permitidas para un usuario autenticado o aplicación. Los recursos incluyen cualquier información en forma de documentos, datos, metadata, información de usuario, reportes y API´s.

Manejo de Eventos. El manejo de eventos guarda y conserva un trazo de auditoría relacionada con cada usuario y documento en cada paso del flujo de

trabajo. Al momento que ocurre cada paso del flujo de trabajo, Adobe Sign genera un evento y distribuye mensajes a través de un sistema asíncrono de mensajería a los recursos apropiados del sistema.

Comunicaciones. Adobe Sign utiliza el correo electrónico para notificaciones de eventos de firma y la entrega opcional de los documentos firmados y certificados al final del proceso. Para minimizar el spam y el phishing, Adobe Sign permite el correo autenticado con Domain Keys Identified Mail (DKIM), Autenticación vía mensaje basado en domino, Reporte y Conformación (DMARC) y Sender Policy Framework (SPF).

Procesamiento de documentos y acceso. Adobe Sign proporciona funcionalidad libre de estado para convertir distintos formatos de archivo a PDF, encriptando y desencriptando archivos y rasterizando imágenes para ser vistas en un navegador web. Para las acciones de procesamiento de documentos lo hace a través de un sistema de mensajería asíncrono basado en colas para comunicarse entre los recursos del sistema. De manera adicional, todo el procesamiento de documentos de acceso al Network Attached Storage (NAS) sucede en segundo plano, permitiendo que el procesamiento de Adobe Sign parezca instantáneo para los usuarios en cada paso del flujo de trabajo.

Capa de Datos. Esta capa es la encargada de dar acceso a la base de datos transaccional, la base de datos del sistema asíncrono de mensajería y el almacén de documentos. Los datos transaccionales almacenados en la capa de datos incluyen el documento original del cliente, versiones intermedias de documentos generados durante el proceso de firma, metadata de documentos, usuarios, eventos y el PDF final firmado procesado por Adobe Sign.

Seguridad en Adobe Sign. Adobe Sign utiliza prácticas de seguridad estándar en la Industria: para manejo de identidad, confidencialidad de datos e integridad de documentos: para ayudar a proteger sus documentos, datos e información personal.

Manejo de Identidad. Esta aplicación utiliza un modelo basado en roles para el manejo de identidades, que se encarga de la autenticación, autorización y control de acceso en el sistema de Adobe Sign. La seguridad basada en capacidades y los procesos de autenticación están definidos y habilitados para una organización por un administrador de Adobe Sign. Adobe Sign define roles generales de usuario para:

- **Remitente:** Usuario licenciado con permisos específicos, otorgados por el administrador para crear flujos de trabajo y enviar documentos para ser aprobados.

- **Destinatarios.** Usuario verificado a quien se da acceso por el remitente para aprobar un documento. Por defecto, Adobe Sign envía un correo al destinatario que incluye una dirección para aprobar el documento que contiene identificadores específicos de cada transacción.

- **Autorizador.** Usuario verificado a quien se da permisos por parte del parte del remitente para aprobar un documento.

Autenticación de Usuario. Adobe Sign soporta los siguientes tipos de autenticación:

- Adobe Sign ID. Una dirección de correo verificada y una contraseña que combinadas se utilizan por un usuario para ingresar de forma segura a una cuenta de Adobe Sign.

- Adobe ID. Puede utilizarse un Adobe ID para ingresar a los servicios licenciados de Adobe incluyendo Adobe Sign. Adobe monitorea de forma constante todas las ID de Adobe para detectar actividad anormal para poder mitigar de forma rápida amenazas potenciales de seguridad.

- Google ID. Identificación de usuario autenticada por Google, como Google Mail o Google Apps.

- Single sign-on (SSO). Este tipo de autenticación se basa en Security Assertion Markup (SAML). Es un estándar XML con el que los dominios web seguros pueden intercambiar datos de autenticación y autorización de los usuarios de tal modo que les permite acceder a aplicaciones que utilizan sus recursos en la nube.

Certificación de Documentos. En cada paso en el flujo de trabajo, Adobe Sign mantiene un checksum seguro del documento para asegurar la integridad y confidencialidad del documento. Adobe Sign utiliza la infraestructura de llave pública (PKI) para certificar los archivos finales firmados con una firma digital antes de distribuirlos a los participantes.

La firma digital se crea con un algoritmo hashing que toma información específica del archivo PDF firmado para mostrar una línea de tamaño fijo codificada en hexadecimal de forma criptográfica con números y letras.

Esto se muestra como la barra azul y la certificación en el encabezado del documento PDF final firmado, la firma digital verifica la integridad del documento (ver la siguiente imagen) y ofrece la certeza de que el documento no ha sido alterado desde que el certificado fue aplicado. El PDF final certificado puede ser asegurado con una contraseña adicional en caso de ser necesario.

Para generar las llaves utilizadas para bloquear y certificar el documento final en PDF, Adobe Sign utiliza certificados específicos emitidos por autoridades de certificación (CAs) y Autoridades de Timestamp (TSAs). En algunos casos, Adobe Sign puede ser configurado para generar documentos certificados utilizando CAs. Las llaves PKI utilizadas para certificar los documentos PDF finales están almacenadas en un módulo de seguridad en hardware para prevenir ataques en línea y modificaciones.

Encriptación. Adobe Sign encripta los documentos y activos en reposo usando encriptación AES 256-bit y soporta HTTPS TLS v1.0 (o mayor) para ayudar a asegurar que los datos en tránsito también se encuentran protegidos.

Los documentos en reposo tienen permisos establecidos en la seguridad basada en capacidades a través de la capa de acceso de datos. Todas las llaves de encriptación de los documentos se encuentran almacenadas en un entorno seguro con acceso restringido y son rotadas como sea necesario. Adicionalmente, los remitentes tienen la opción de asegurar un documento con una contraseña privada adicional.

Compliance. Adobe Sign está diseñada para que los destinatarios verificados interactúen con documentos en cualquier lugar y dispositivo, Adobe Sign cumple o puede ser configurado para observar los requisitos regulatorio. Los usuarios mantienen control sobre sus documentos, datos y flujos de trabajo y pueden escoger como dar cumplimiento a las regulaciones locales o nacionales.

- ISO 27001, Adobe Sign está certificado en ISO 27001: 2013. El standard ISO 27001 fue publicado por la International Organization for Standardization (ISO). La ISO 27001 contiene los requerimientos para sistemas de administración de seguridad de la información (ISMS) que pueden ser auditados para una autoridad certificadora independiente y acreditada.

- SSAE 16 SOC 2. El Statement on Standards for Attestation Engagements (SSAE), hace referencia a los controles de TI para seguridad, disponibilidad, integridad de proceso y confidencialidad (Tipo 2).

- PCI DSS. El Payment Card Industry Data Security Standard (PCI DSS) es un estándar de seguridad de datos para empresas que manejan tarjetas de crédito, que necesitan incrementar el control sobre los datos de los

usuarios de las tarjetas de crédito y de reducir los fraudes electrónicos. Adobe Sign está calificado como observante del PCI DSS 3.0 como proveedor de servicios mercantiles.

- HIPAA. El Health Insurance Portability and Accountability Act (HIPAA), asegura la información, brindando confidencialidad a los datos que involucran a usuarios del servicio de salud. Adobe Sign puede ser configurado para ser utilizado de forma que cumpla con las normas HIPAA.

- GLBA. El U.S. Gramm-Leach-Bliley Act (GLBA) ofrece regulaciones para instituciones financieras para garantizar la información personal de los clientes. Adobe Sign puede ser configurado para que las entidades financieras observen los requerimientos de GLBA.

- FERPA. El U.S. Family Educational Rights and Privacy Act (FERPA) está diseñado para preservar la confidencialidad de los registros de estudiantes en los E.U. y su información. Adobe Sign puede configurarse para manejar datos regulados de estudiantes de forma que observen los requerimientos de FERPA.

Integración Adobe Sign con otras plataformas

Adobe Sign, permite la integración con múltiples aplicacione, por ejemplo, Salesforce, Apttus, Workday, Ariba y productos Microsoft. De manera adicional Adobe Sign cuenta con una gama amplia de APIs que permiten la integración con sistemas de negocio propietarios o páginas web vía HTTPS seguro o servicios SOAP o REST.

2.3.4. Modelo de operación de la aprobación digital

Definición de Firma Electrónica.

La firma electrónica abarca una amplia gama de tecnologías y metodologías, pueden ser utilizados para los procesos internos de una empresa tales como la aprobación para las solicitudes, la documentación más formal y aceptación de los términos de un documento digitalizado, para la protección de la reputación de los documentos electrónicos e incluso para realizar transacciones comerciales electrónicas.

Según Skoog (2008), “La firma electrónica es un medio único, que no está escrito a mano, que sirve para identificar a una persona y que nadie más puede usar.” (Pág. 129)

Según Gonzalo, et al. (2012), cuando cita a Moreno Blesa (2008): La firma electrónica pretende ser el instrumento que permita garantizar la seguridad en las comunicaciones telemáticas, aportando a los medios de comunicación empleados, autenticidad que es fundamental acreditar que las partes son realmente quienes dicen ser, integridad que se tendrá que demostrar que la información no ha sido alterada desde el momento en el que ha sido transmitida. (pág. 322).

Operación de la Aprobación Digital

Generación de la Aprobación digital

El funcionamiento de la aprobación digital está basado en una clave pública y una clave privada, cada parte tiene un par de claves, una para cifrar y otra para descifrar.

El procedimiento se divide en dos partes:

- Procedimiento de Aprobación digital.
- Procedimiento de Verificación de la Aprobación digital.

Aplicación de Aprobación digital

Este procedimiento se resume en los siguientes pasos:
Cuando se "aprueba" un documento electrónico, una huella digital única (llamada hash) del documento se crea utilizando un algoritmo matemático. Este hash es único para este documento en particular; en caso que se haga el más mínimo cambio resultará en un hash diferente.

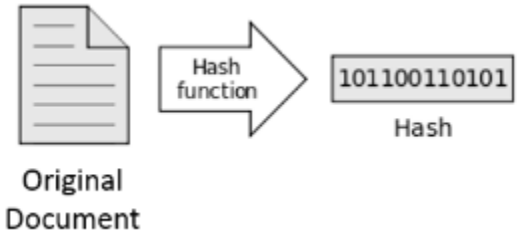


Figura 15. Huella digital única hash
Adaptado de (Seguridad América, 2018).

El Hash es encriptado utilizando la llave privada del usuario aprobador. Por tal motivo el hash encriptado y la llave pública del usuario aprobador son combinadas en una aprobación digital la cual se agrega al documento. Este procedimiento se visualiza en la siguiente figura.

Figura 16. Encriptación y la llave pública
Adaptado de (Seguridad América, 2018).

El documento aprobado electrónicamente está listo para ser distribuido o archivado.

El procedimiento de aplicación de aprobación digital de modo completo se observa en el siguiente gráfico.

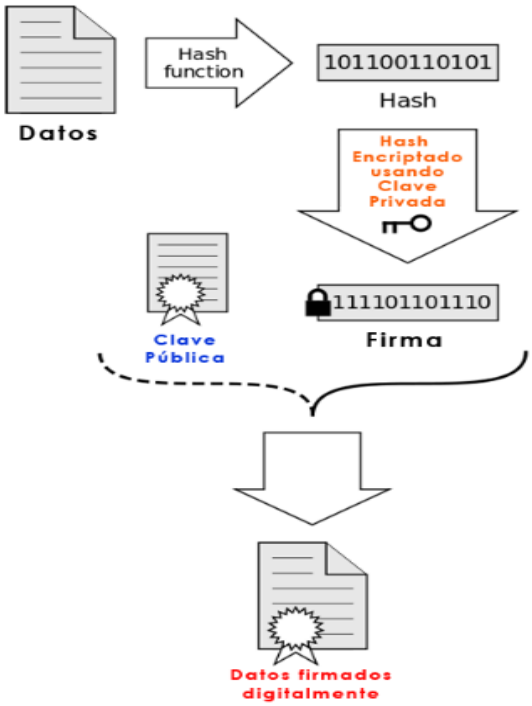


Figura 17. Procedimiento de la aprobación digital.
Adaptado de (Seguridad América, 2018).

Verificación de la Aprobación digital

La validación de una aprobación digital, consiste en la verificación de:

- La identidad del firmante.
- La integridad del documento firmado.
- La validez del certificado utilizado.

El procedimiento es el siguiente:

- El receptor recibe una notificación en su correo electrónico, documento digital que espera ser aprobado.

- Descifrar el certificado digital del gestor del documento, mediante la clave pública de la entidad certificadora.

- El usuario aprobador puede acceder a la clave pública del usuario gestor y a los datos de identificación del mismo el cual contiene el certificado.

- El receptor usa la clave pública del emisor para descifrar el Resumen del mensaje cifrado creado por el emisor del documento.

- Si el contenido del mensaje recibido ha sido cifrado por emisor, el receptor debe utilizar su clave privada para descifrar el contenido del mensaje.

- El receptor o usuario aprobador, obtiene su propio resumen del mensaje usando la misma función Hash que uso el emisor o gestor documental, sobre el contenido del mensaje sin cifrar.

- El receptor compara el resumen recibido del emisor con el resumen suyo, y si ambos son iguales significa los siguiente:

- El mensaje ha llegado sin sufrir ninguna alteración desde que fue enviado por el gestor del documento o emisor.

- El resumen descifrado por el receptor con la clave pública del emisor ha sido necesariamente cifrado por el emisor con su clave privada, por lo que podemos estar seguros que el mensaje proviene inequívocamente del emisor original.

- Si la comparación del resumen no coincide, quiere decir que el mensaje ha sido alterado por terceros durante la transmisión, o que el mensaje ha sido firmado por otra persona.

En la figura 18, se visualiza un ejemplo en el cual, los códigos del Hash coinciden de tal modo que la “aprobación digital” es válida.

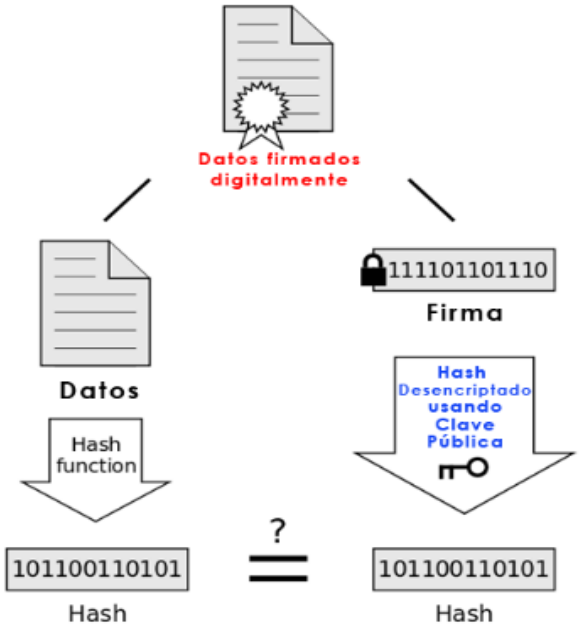


Figura 18. Verificación de un documento aprobado digitalmente
Tomado de (Seguridad América, 2018).

2.4. Fase 3. Integración y pruebas de la aplicación

El software como servicio (SaaS) tiene la capacidad de desarrollar aplicaciones de línea de negocio o servicios comerciales en la nube que se pueden integrar con Azure Active Directory (Azure AD) para ofrecer inicio de sesión seguro y autorización para los servicios. Para integrar una aplicación o un servicio con Azure AD, se debe registrar primero la aplicación en Azure AD.

La integración de esta solución se hace haciendo uso del AWS Single Sign-On (AWS SSO), en adelante se explica a detalle el procedimiento de la configuración y la integración de Adobe Sign, haciendo uso de AWS SSO.

2.4.1. Implementación e integración de Adobe Sign

Concepto de AWS Single Sign – ON (AWS SSO)

AWS SSO es un servicio de AWS que le permite ejecutar la autenticación haciendo uso de las credenciales existentes en Microsoft Active Directory para obtener acceso a aplicaciones basadas en la nube, como aplicaciones empresariales y cuentas de AWS (Office 365, Salesforce, Box), mediante el uso del inicio de sesión único (SSO).

AWS SSO está diseñado para administrar varias aplicaciones empresariales y cuentas de AWS, que desean centralizar la administración del acceso de los usuarios a dichos servicios de la nube y que quieran conceder a los empleados una única ubicación para obtener acceso a las cuentas y aplicaciones sin necesidad de tener que recordar una contraseña más. En la siguiente figura se visualiza la integración del AWS SSO con la infraestructura de UDLA.

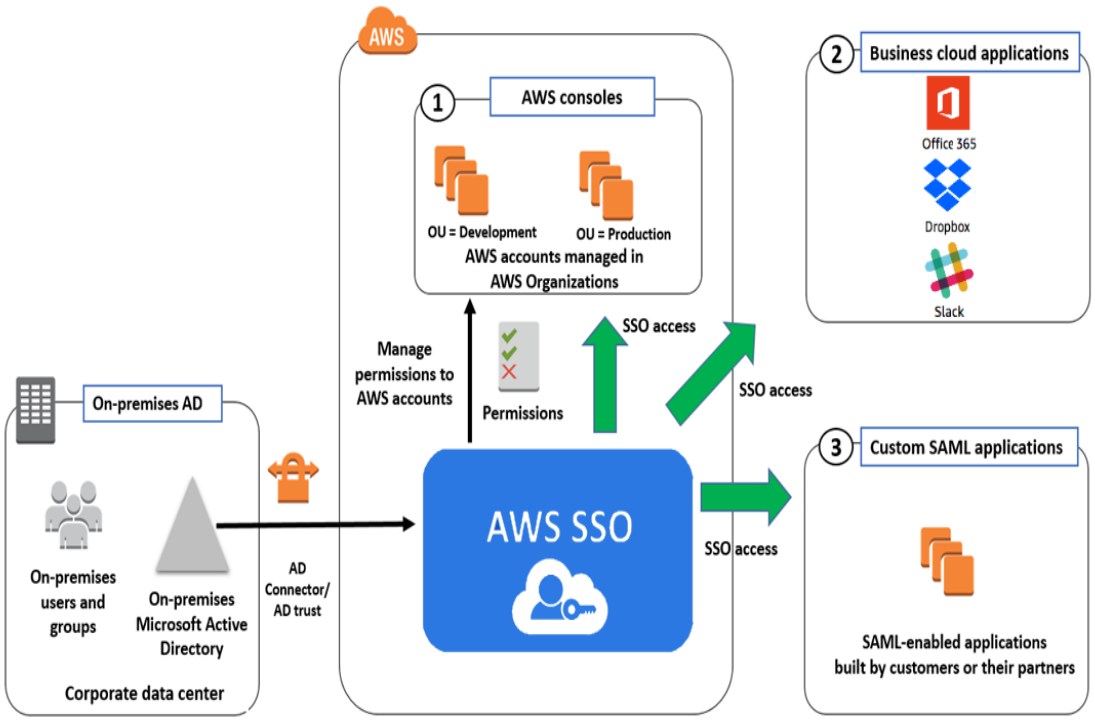


Figura 19. Modelo del AWS - Single On

Tomado de (AWS Security, 2018).

Caraterísticas de AWS SSO

AWS SSO permite asignar y administrar de manera rápida y sencilla el acceso de los usuarios a varias cuentas de AWS, aplicaciones en la nube que admitan SAML (como Salesforce, Office 365 y Box) y aplicaciones internas personalizadas, desde una ubicación centralizada.

A través de esta herramienta, se puede iniciar sesión con los nombres de usuario y contraseñas de Active Directory corporativos existentes para obtener acceso a las aplicaciones a partir del portal de usuario personalizado. Los usuarios no necesitarán recordar varios grupos de credenciales ni URL de acceso a aplicaciones en la nube. Una vez que haya añadido usuarios al grupo de Active Directory correspondiente, obtendrán automáticamente acceso a cuentas y aplicaciones activadas para los miembros de dicho grupo, de este modo se obtendrá una mejor visibilidad del uso de las aplicaciones en la nube porque podrá monitorear y auditar actividad de inicio de sesión de manera centralizada desde AWS CloudTrail.

AWS SSO elimina la complejidad administrativa de las soluciones de SSO personalizadas que utiliza para conceder y administrar identidades en aplicaciones empresariales y cuentas de AWS. Como utiliza varias cuentas de AWS y añade cuentas con frecuencia, la configuración de SSO con los servicios federados de Active Directory (AD FS) para obtener acceso a estas cuentas implica aprender el lenguaje de programación de notificaciones de AD FS personalizado.

Procedimiento de uso de AWS SSO

AWS SSO permite asignar y administrar de manera rápida y sencilla el acceso de los usuarios a varias cuentas de AWS, aplicaciones en la nube que admitan SAML (como Salesforce, Office 365 y Box) y aplicaciones internas personalizadas, desde una ubicación centralizada.

A través de esta herramienta, se puede iniciar sesión con los nombres de usuario y contraseñas de Active Directory corporativos existentes para obtener acceso a las aplicaciones a partir del portal de usuario personalizado. Los usuarios no necesitarán recordar varios grupos de credenciales ni URL de acceso a aplicaciones en la nube.

Una vez que haya añadido usuarios al grupo de Active Directory correspondiente, obtendrán automáticamente acceso a cuentas y aplicaciones activadas para los miembros de dicho grupo, de este modo se obtendrá una mejor visibilidad del uso de las aplicaciones en la nube porque podrá monitorear y auditar actividad de inicio de sesión de manera centralizada desde AWS CloudTrail.

2.4.2. Configuración de Microsoft Azure con SSO

Descripción

La Consola de Administración de Adobe permite que un administrador del sistema configure los dominios y los directorios que se utilizarán para el acceso a través de Federated ID para inicio de sesión único (SSO). Tras acreditar la propiedad de un dominio mediante un token de DNS y su vinculación con un directorio de Federated ID, los usuarios que tienen direcciones de correo electrónico en el dominio notificado pueden iniciar sesión en Creative Cloud mediante un sistema IdP después de que las cuentas correspondientes se hayan creado en la Consola de administración de Adobe relevante. El proceso se suministra como servicio de software que se ejecuta en la red de la empresa y se accede a él desde Internet o desde un servicio en la nube alojado por terceros que permite la verificación de los detalles de inicio de sesión del usuario a través de la comunicación segura usando el protocolo SAML.

Cuando un usuario se autentica en la aplicación, Azure AD emite un token de SAML para la aplicación que contiene o reclama información de los usuarios que

los identifica de manera exclusiva. De forma predeterminada, la información incluye un nombre de usuario, una dirección de correo electrónico, un nombre y un apellido. Puede ver o editar las reclamaciones enviadas en el token de SAML a la aplicación en la ficha de atributos y liberar el atributo del nombre de usuario.

Requisitos previos

Los requisitos previos para configurar un dominio para el inicio de sesión único utilizando Microsoft Azure como IdP, debe cumplir lo siguiente:

Un dominio aprobado en un directorio de su Consola de administración de Adobe. El estado del directorio en la Consola de administración de Adobe debe presentar la opción de: se requiere configuración o que un directorio ya se hubiera configurado antes.
Se puede acceder al panel de Microsoft Azure iniciando sesión como administrador el cual permita crear una aplicación empresarial.

Creación de aplicación SSO en Azure para Adobe

Para realizar la configuración SSO en Azure, realice los siguientes pasos:
En Azure Active Directory > Azure Active Directory > Aplicaciones empresariales > Todas las aplicaciones y haga clic en Nueva aplicación.

En Agregar una aplicación de la galería, indicar "Adobe Creative Cloud" en el campo de búsqueda.
Seleccionar Adobe Creative Cloud; a continuación, asigne un nombre al conector, haga clic en "Añadir" y espere a que finalice el proceso.

En Azure Active Directory > Aplicaciones empresariales > Todas las aplicaciones > seleccionar la nueva aplicación del conector de Adobe Creative Cloud.
En un navegador web adicional, iniciar sesión en la Consola de administración de Adobe y acceda a Configuración -> Identidad haciendo clic en el nombre de

dominio y, a continuación, en el botón Configurar SSO. En el portal de Azure, dar clic en Inicio de sesión único y seleccione el modo de esta aplicación de conector como "Inicio de sesión único basado en SAML".

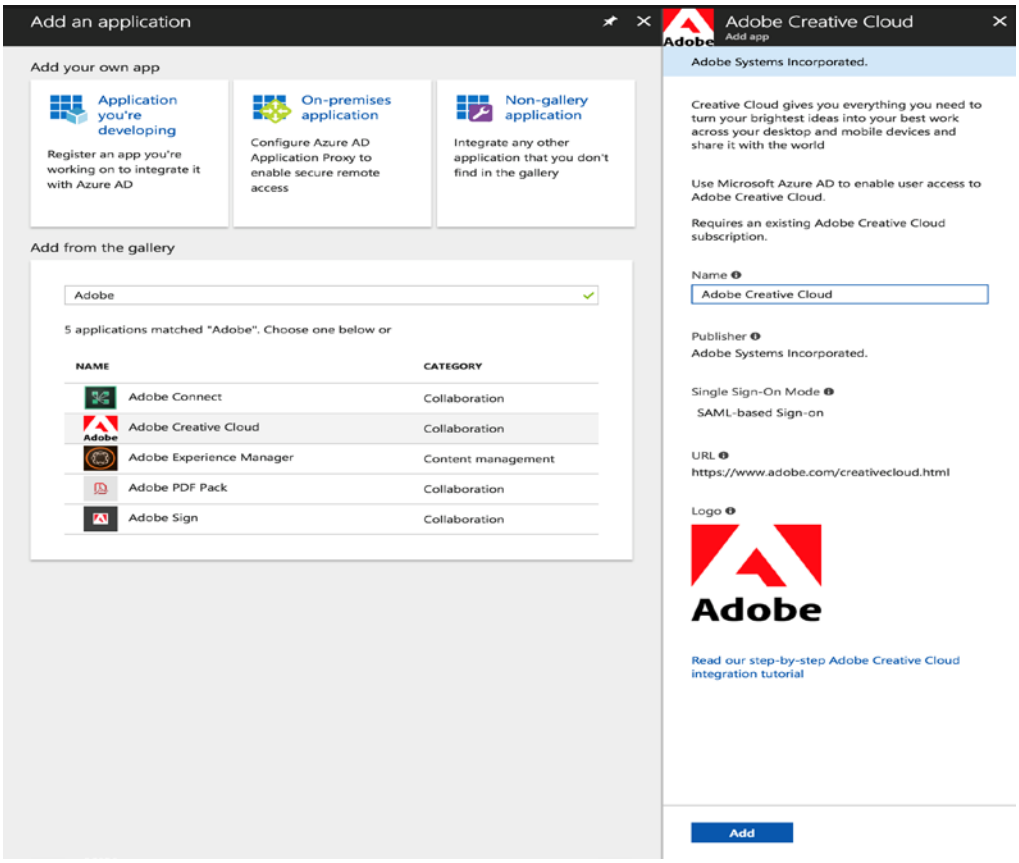


Figura 20. Configuración del SSO
Tomado de (Adobe SSO, 2018).

Haga clic en la casilla para Ver y editar todos los demás atributos de usuario. Editar los atributos del token de SAML.

Dar clic en el vínculo en la base de la página donde se encuentra el nombre del conector de inicio de sesión único de Azure para que aparezca la documentación de Microsoft sobre el inicio de sesión único de Adobe.

Copiar el ID de entidad SAML de Azure AD del portal de Azure y péguelo en el campo Emisor de IdP en la página Configuración de identidad del dominio en la Consola de administración de Adobe.

Copiar la URL del servicio de inicio de sesión único de Azure AD del portal de Azure y péguela en el campo URL de inicio de sesión de IdP en la página Configuración de identidad del dominio en la Consola de administración de Adobe.

Haga clic en 'X' para cerrar la página de documentación del portal de Azure y volver a la ventana de configuración de la aplicación empresarial del conector de inicio de sesión único de Adobe. En la sección Certificado de firma de SAML, hacer clic en Certificado (base 64).

Cargar el certificado obtenido en el paso anterior en la Consola de administración de Adobe como certificado IdP y guardar los datos haciendo clic en Completar configuración.

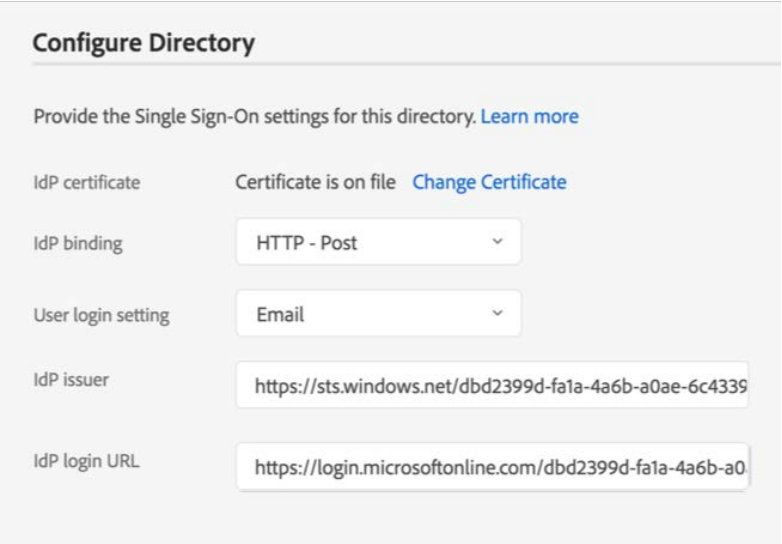


Figura 21. Configuración de Adobe como certificado idP.
Tomado de Tomado de (Adobe SSO, 2018).

Guardar la configuración de este directorio en la Consola de administración de Adobe; para ello, haga clic en el botón Descargar metadatos.

Este archivo se utilizará para obtener determinados atributos de la configuración.

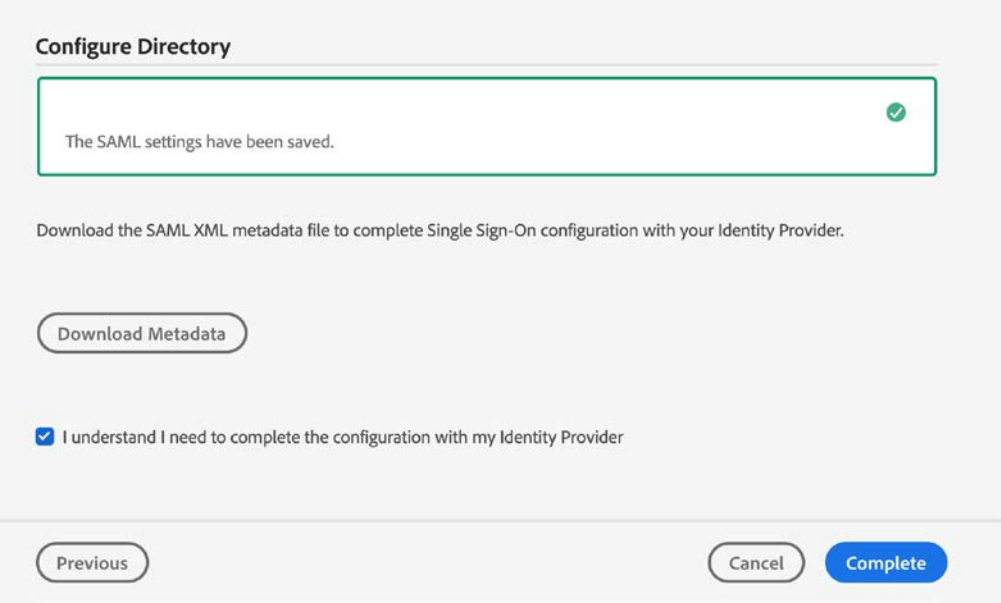


Figura 22. Proceso de configuración del SAML XML.
Adaptado de (Adobe SSO, 2018).

Abrir los metadatos en un editor de texto o un navegador web; a continuación, copie lo valores de EntityID y AssertionConsumerService en el portal de Azure en los campos Identificador y URL de respuesta respectivamente, como se muestra en la captura de pantalla a continuación.

Utilice la URL de EntityID en los metadatos del campo Identificador de la configuración de Azure:
https://www.okta.com/saml2/serviceprovider/spi1t5qdd3rI7onSl0x78

Utilice la URL de AssertionConsumerService en la URL de respuesta de la configuración de Azure:
https://adobe-examp,e-dot-com-a8bd-prd.okta.com/auth/saml2/accaouthl

Guarde esta configuración en el portal de Azure mediante el vínculo Guardar situado en la parte superior de la página.

Figura 23. Entity ID, campo identificador de configuración de Adobe. Adaptado de (Adobe SSO, 2018).

Asignación de usuarios a través de Azure

Para asignar usuarios a través de Microsoft Azure a fin de permitirles iniciar sesión con el conector de Adobe Creative Cloud, efectúe los pasos que se indican a continuación. Hay que tener en cuenta que aún deberá asignar licencias a través de la Consola de administración de Adobe.

En Azure Active Directory > Aplicaciones empresariales > Todas las aplicaciones y seleccione la nueva aplicación del conector de Adobe Creative Cloud.
Haga clic en Usuarios y Grupos.
Haga clic en Añadir usuario para seleccionar usuarios que asignar a este conector que les permitirá iniciar sesión mediante el inicio de sesión único.
Haga clic en Usuarios o en Grupos; a continuación, seleccione uno o más usuarios o grupos a los que se permita iniciar sesión en Creative Cloud, y haga clic en Seleccionar seguido de Asignar.

Figura 24. Azure Active Directory, módulo de User Access
Adaptado de (Adobe SSO, 2018).

Prueba de acceso del usuario a la aplicación Adobe Sign

Para probar el acceso del usuario, se ejecuta el siguiente procedimiento: Asegurarse, de añadir usuarios dentro de la Consola de administración de Adobe como Federated ID y asignarlos a un grupo para la asignación de derechos.

Escribir la dirección de correo electrónico (corporativo) en el formulario de inicio de sesión de Adobe y debería recibir la federación en Azure AD.

3. EVALUACIÓN

Este capítulo, hace referencia a las pruebas que validan al proceso de aprobación digital implementado, adicionalmente se presentarán los resultados. Este capítulo involucra la descripción de la prueba, el protocolo, la evaluación de los resultados. De igual manera se procede a presentar pantallas que evidencian el funcionamiento de la aplicación.

3.1. Estrategia de las pruebas

El objetivo global de la estrategia de pruebas es demostrar el funcionamiento de la aplicación integrada, tanto a nivel de eficiencia y de funcionalidad. Para el cumplimiento de lo descrito, se ejecuta un plan de pruebas cuyo contenido se describe a continuación:

- Recopilar, diseñar y documentar casos de prueba, estos casos deben cubrir más de un requerimiento funcional.

- Pruebas de aceptación. Las cuales se realizan para comprobar que la aplicación cumpla con las expectativas de los usuarios finales. Este tipo de prueba integra las pruebas funcionales, pruebas de carga y pruebas de estrés.

- La ejecución de la prueba contará con la participación de los usuarios finales, en este caso: un usuario que hará el rol de gestor documental y los usuarios aprobadores en este caso los Directores y Decano de la Facultad de Ingeniería y Ciencias Aplicadas de UDLA.

- El documento que se utilizará para las pruebas es el siguiente: Minuta de reunión de concejo de FICA.

- El detallo de las pruebas se basará en el “Catálogo de pruebas del Sistema”.

- Para el monitoreo del desarrollo de la prueba se realizará utilizando el portal Web propio de Adobe, en el cual se detalla el flujo que tiene el documento, así también como el seguimiento que se hace a las notificaciones que se reciben en el buzón del correo corporativo.

- Una vez se haya completado el flujo aprobado por el usuario, se anexarán actas de aceptación, en las cuales conste que los requerimientos funcionales estén completos.

Tabla 6

Catálogo de pruebas.

ID Test	Módulo	Descripción
01	**Acceso**	Verificar que el usuario tenga acceso web a la url http://www.adobe.com/la. Proceder al iniciar la sesión utilizando las credenciales solicitadas, en este caso: Usuario. Correo electrónico corporativo. Clave. Correspondiente a cada usuario.
02	**Acceso**	Verificar que el usuario acceda a la aplicación Adobe Sign.
03	**Aplicación**	Verificar que los módulos Tablero, Enviar, Gestionar y Cuenta estén activos y funcionando.

04	**Funcionalidad**	Realizar una prueba de la función enviar y aprobar un documento para ser aprobado electrónicamente, para ellos se debe contar con un usuario con rol de Gestor documental y usuarios aprobadores en este caso los Directores de FICA.
05	**Revisión**	El monitoreo del flujo del documento sea a través del acceso web al portal de Adobe – Menú Gestionar. También se verificará las notificaciones recibidas en el buzón del correo corporativo con la información correspondiente a cada salto del flujo. Esta prueba se hará con la aceptación del documento.
06	**Funcionalidad**	Realizar una prueba de la función enviar y cancelar un documento, para ello se debe contar con un usuario con rol de Gestor documental y un usuario aprobador que ejecute la función de cancelar.
07	**Revisión**	El monitoreo del flujo del documento sea a través del acceso web al portal de Adobe – Menú Gestionar. También se verificará las notificaciones recibidas en el buzón del correo corporativo con la información correspondiente a cada salto del flujo.
08	**Funcionalidad**	Realizar una prueba de la función enviar y delegar un documento, para ello se debe contar

		con un usuario con rol de Gestor documental y un usuario aprobador que ejecute la función de cancelar.
09	**Revisión**	El monitoreo del flujo del documento sea a través del acceso web al portal de Adobe – Menú Gestionar. También se verificará las notificaciones recibidas en el buzón del correo corporativo con la información correspondiente a cada salto del flujo.

3.2. Ejecución de las pruebas

La ejecución de pruebas se hace en base a las funcionalidades que tiene la aplicación, resumida en los siguientes casos de uso:

Tabla 7

Ejecución de pruebas.

No	Tipo de Prueba	Observación
01	El Gestor documental envía un archivo para ser revisado y aprobado.	La prueba es exitosa. El flujo se competa, se reciben las notificaciones en el correo electrónico corporativo y se registran en la plataforma de adobe.

02	El Gestor documental envío un archivo para ser revisado pero es cancelado, es decir este documento sea denegado.	La prueba es exitosa. El flujo se competa, se reciben las notificaciones en el correo electrónico corporativo y se registran en la plataforma de adobe.
03	El Gestor documental envía un archivo para ser revisado y aprobado, pero el usuario aprobador “delega” a otro usuario para que revise y apruebe el documento.	La prueba es exitosa. El flujo se competa, se reciben las notificaciones en el correo electrónico corporativo y se registran en la plataforma de adobe.
04	El Gestor documental envía un archivo para ser revisado y aprobado, pero el usuario aprobador “delega” a otro usuario para que revise y deniegue el documento.	La prueba es exitosa. El flujo se competa, se reciben las notificaciones en el correo electrónico corporativo y se registran en la plataforma de adobe.

3.3. Procedimiento de las pruebas

A continuación, se detalla la prueba No. 01. La cual se detalla a continuación y se describe desde el acceso a la aplicación.

Tabla 8

Prueba del gestor documental.

No	Tipo de Prueba	Observación
01	El Gestor documental envía un archivo para ser revisado y aprobado.	La prueba es exitosa. El flujo se competa, se reciben las notificaciones en el correo electrónico corporativo y se registran en la plataforma de adobe.

3.4. Acceso a la aplicación

Para el ingreso a la aplicación de Adobe Sign, realizar los siguientes pasos:
Ingresar al sistema tecleando el siguiente link: http://www.adobe.com/la
Para iniciar sesión, se da clic en iniciar sesión.

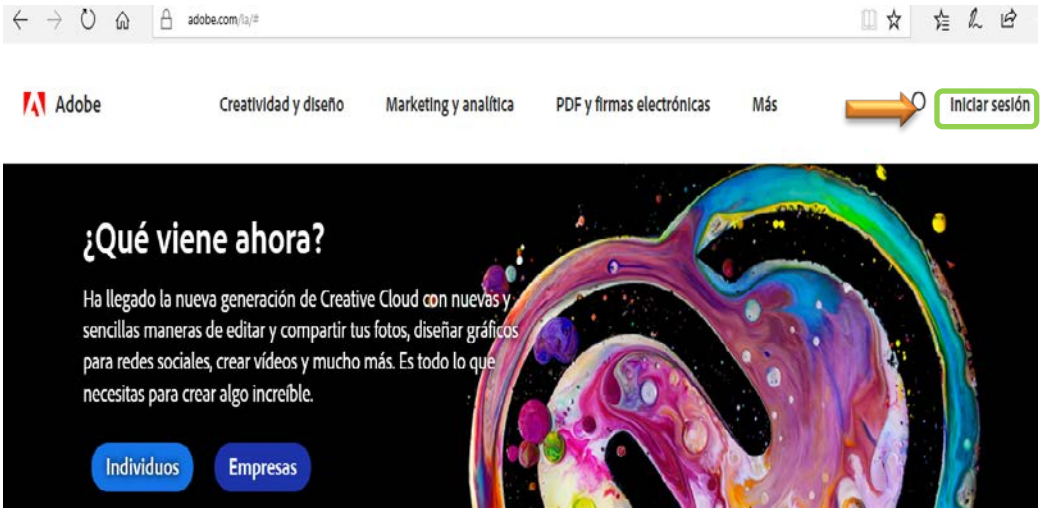
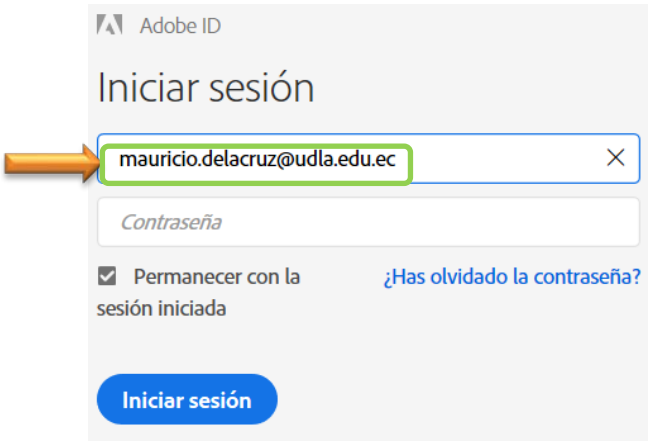


Figura 25. Inicio de sesión de Adobe Sign
Tomado de (Adobe, 2018).

a. Ingresar el usuario y contraseña

El usuario es la dirección electrónica corporativa, en nuestro caso nombre@mail.com y la contraseña la que utilizamos para hacer uso de la cuenta de office 365.



Se elige la opción de la aplicación “ADOBE SIGN”. Como se visualiza en la figura 26.

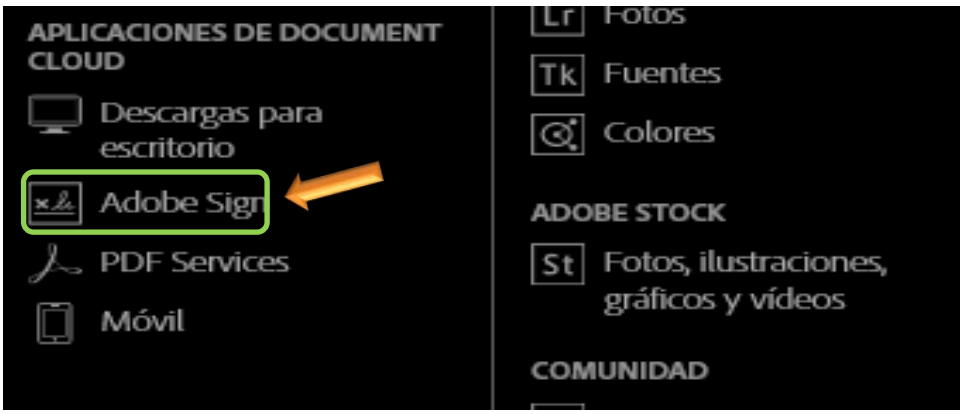


Figura 26. Selección y acceso a la aplicación de Adobe Sign.
Tomado de (Adobe, 2018).

3.5. Procedimiento de envío de un documento digital

Esta opción es utilizada para iniciar el proceso del flujo del documento, para lo cual procederemos de la siguiente manera.

a. En destinatarios tenemos dos opciones:

1. **Completar en Orden.** Esta opción se utiliza cuando se requiere que el documento tenga un orden específico en el orden de su flujo; el orden que el documento transite en el flujo, depende del orden en el que ingresemos los correos electrónicos, al momento que queremos enviar un documento.

2. **Completar en cualquier orden.** Esta opción envía las notificaciones para aprobar el documento al mismo tiempo a los usuarios que forman parte del flujo del proceso.

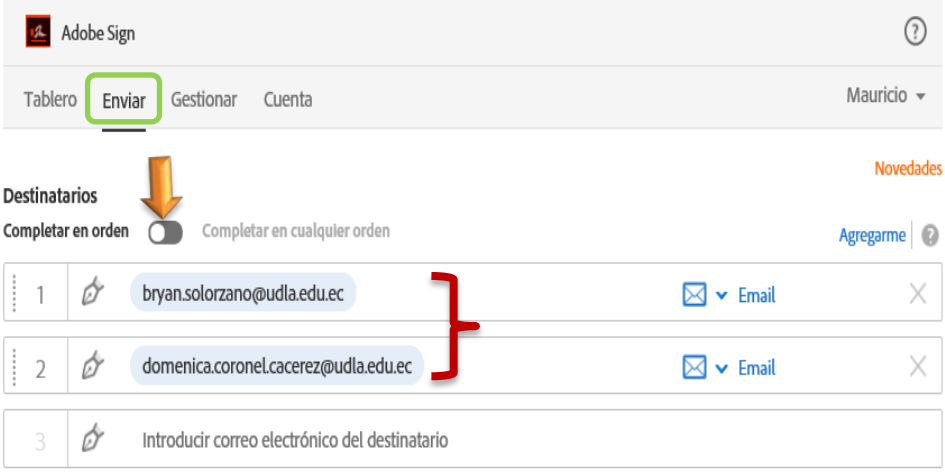


Figura 27. Procedimiento de envío del documento digital, ingreso direcciones electrónicas de usuarios aprobadores.
Adaptado de (Adobe, 2018).

b. A continuación, tenemos el campo “Mensaje”, aquí procedemos a ingresar el título que corresponda al documento enviado, se sugiere que se tenga un estándar definido por cada usuario para mantener un orden, de ese modo el “gestor del documento” pueda llevar un mejor control al momento de controlar el flujo del documento.

c. En el campo “Archivos”, dar clic al botón “Agregar archivos” y seleccionar el documento que va a ser enviado para la aprobación digital. El campo archivo permite agregar directamente archivos de office o archivos pdfs, la aplicación adobe sign los une y genera un solo archivo pdf. Es decir, no hay necesidad de convertir un archivo de office en pdf.

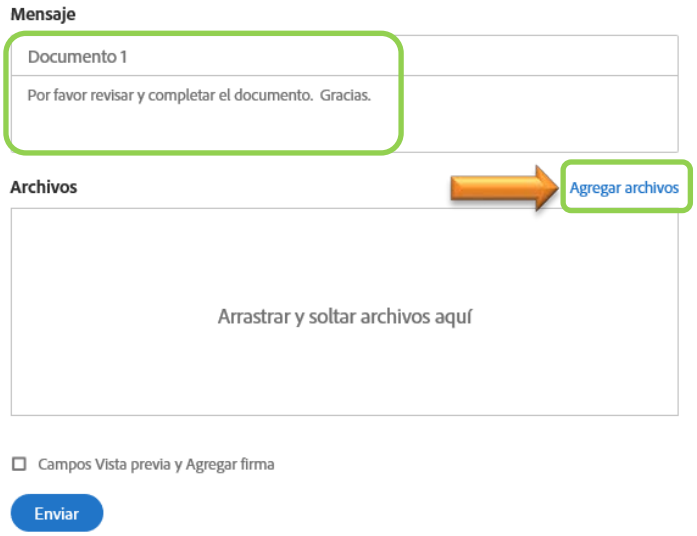


Figura 28. Procedimiento para adjuntar archivos.
Adaptado de (Adobe, 2018).

d. Adjuntamos el archivo que requiere ser aprobado. Podemos obtenerlo de la PC, de la nube (Box, Dropbox o Google Drive). Una vez identificado el archivo, se da clic en el botón “Adjuntar”.

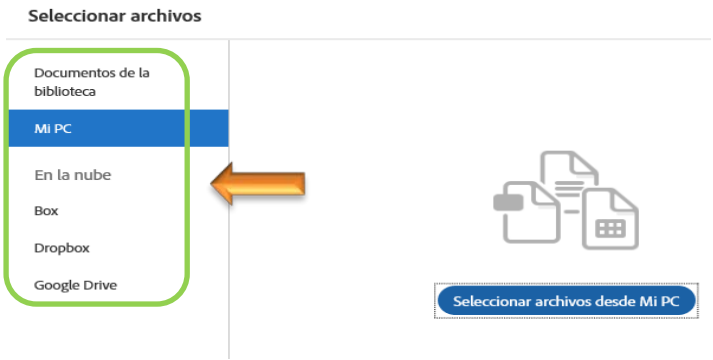


Figura 29. Procedimiento para adjuntar archivos desde una ubicación determinada.

e. Una vez que el gestor, ha adjuntado el archivo, se procede a marcar la opción “Campos Vista previa y Agregar firma” y ha continuación clic en el botón “Siguiente”.

f. En esta pantalla se despliega el documento a ser revisado. Al lado derecho superior aparecen los destinatarios que van a recibir el documento a ser revisado y el orden que seguirá el flujo del documento. Escogemos al primero y nos dirigimos a “Campos de Firma”, seleccionamos “Firma” y lo arrastramos hasta el espacio que corresponde la aprobación del primer usuario, el mismo procedimiento utilizamos para arrastrar el campo firma para los otros destinatarios ingresados. Una vez completado este proceso se da clic en el botón “Enviar”.

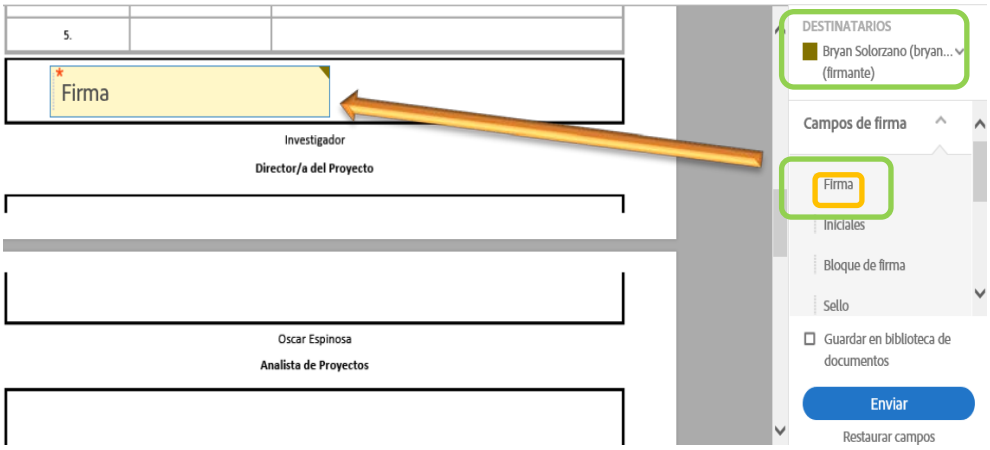


Figura 30. Selección del campo firma.
Adaptado de (Adobe, 2018).

g. La siguiente pantalla indica que el documento ha sido enviado exitosamente. En ese momento el sistema envía una notificación al “gestor del documento” y al primer “destinatario”, indicando que tiene un documento para su revisión.

Figura 31. Notificación de envío del documento.
Adaptado de (Adobe, 2018)

3.6. Procedimiento de la aprobación digital

Este procedimiento detalla los pasos ejecutados por los usuarios aprobadores, desde que reciben la notificación que han recibido un documento para ser revisado, hasta el momento que aprueban, deniegan o delegan esta función a otro usuario.

A continuación, se describen los pasos para el procedimiento de aprobación digital.

a. El destinatario recibe un mail de notificación, el cual le informa que ha recibido un documento para ser revisado. Para abrir el documento, revisarlo y aprobarlo debe dar un clic en el link "Haga clic aquí para revisar y aprobar convocatoria."

Figura 32. Notificación para revisar y aprobar un documento.
Adaptado de (Adobe, 2018)

b. A continuación, se despliega el documento y automáticamente aparece un cursor el cual le indica al usuario aprobador donde dar un clic para aparezca la imagen de su aprobación.

Figura 33. Campo de aprobación del documento.
Adaptado de (Adobe, 2018)

Cabe recalcar que el usuario aprobador tiene las siguientes opciones con respecto a su gestión; estas opciones se despliegan al dar un clic en **"Otras acciones".** Las opciones que se presentan son las siguientes:

- Debe aprobar otra persona (si requiere reenviar para que otra persona lo apruebe).

- No aprobaré electrónicamente (en caso de denegar o no autorizar).
- Borrar datos de documento (si solicita que editen algo del documento).

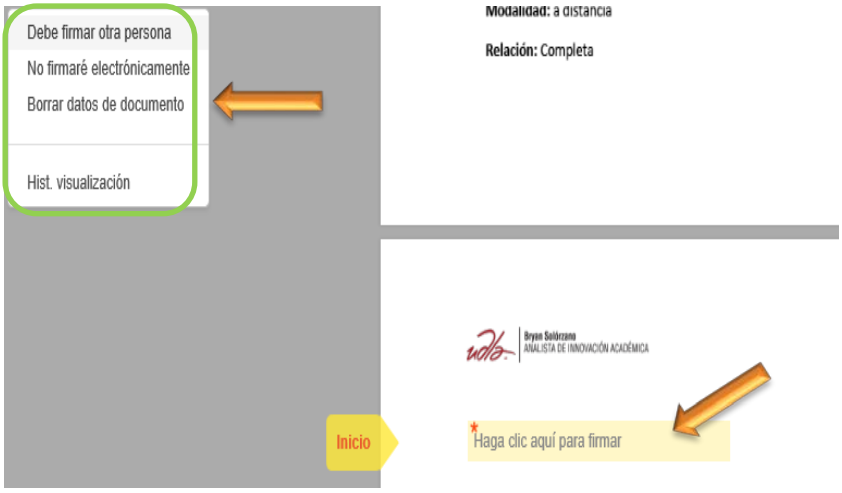


Figura 34. Opciones de gestión del documento.
Adaptado de (Adobe, 2018)

c. Al momento de dar un clic en el campo firma, automáticamente aparece la rúbrica electrónica del usuario aprobador. La aplicación señala el siguiente paso, dar clic en el botón **"Clic aprobar".**

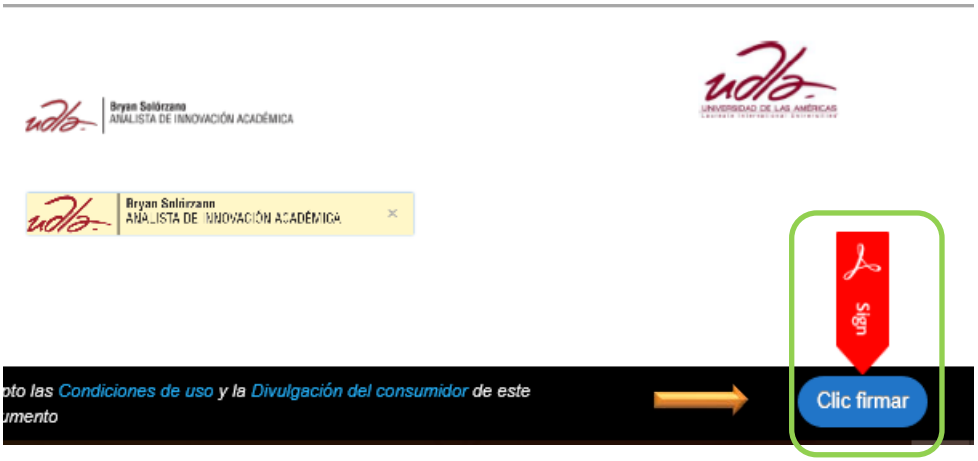


Figura 35. Aprobación del documento digital.
Tomado de (Adobe, 2018)

d. La siguiente pantalla aparece indicando que el documento ha sido aprobado correctamente, para seguridad se sugiere que el usuario aprobador de un clic en el botón “Descargar una copia”, la misma que debe guardar en la carpeta con el nombre “Aprobación digital”, alojada en la ubicación del OneDrive propio del perfil del usuario.

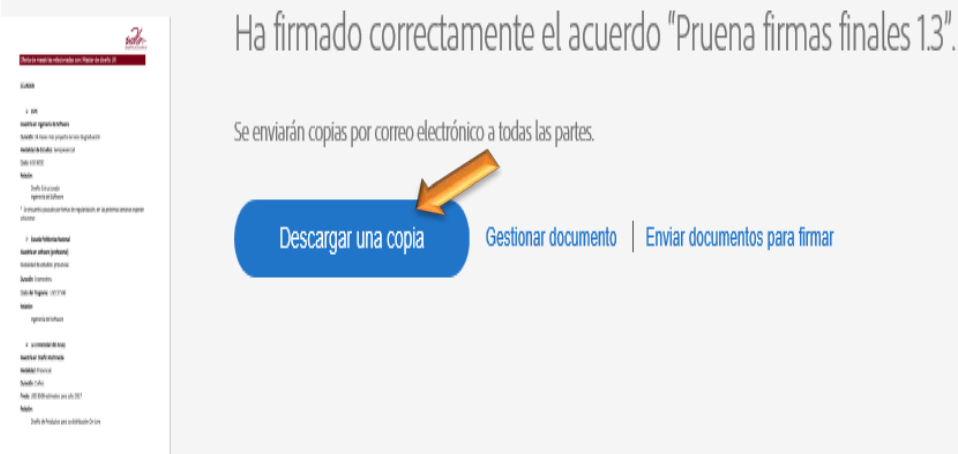


Figura 36. Copia de un documento aprobado.
Adaptado de (Adobe, 2018)

3.7. Procedimiento para archivar documentos aprobados

Una vez que el documento ha completado el flujo de aprobación digital, el “gestor del documento” recibe un mail donde se notifica que el documento ha sido aprobado y el flujo del documento ha finalizado. Esta notificación se visualiza acompañada de un archivo adjunto (en formato PDF). Por política de seguridad es requerido que el “documento aprobado” debe ser archivado por el usuario denominado gestor documental, dado que Él es el responsable de almacenar y preservar los “documentos aprobados”.

En la siguiente figura, se ilustra como llega la notificación al buzón de correo electrónico del usuario (gestor documental).

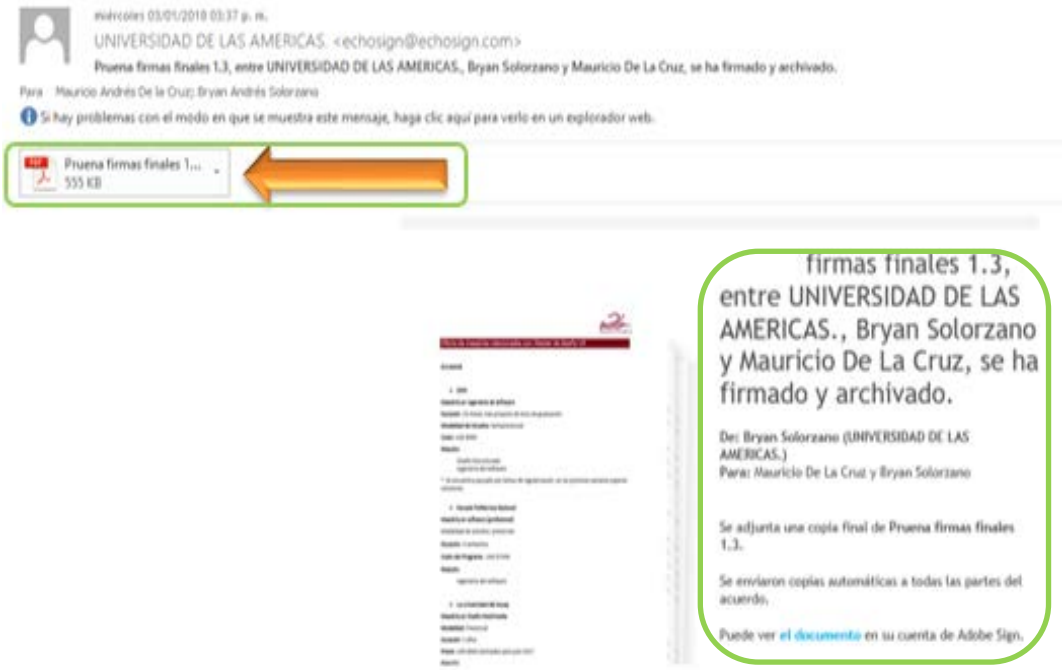


Figura 37. Notificación de un documento aprobado.
Adaptado de (Adobe, 2018)

3.8. Reporte de pruebas

Tras la ejecución de las pruebas según el Plan de Pruebas se presenta en esta sección los resultados obtenidos. Se determina de manera general que se obtuvieron porcentajes superiores al 90% de efectividad, la estrategia de pruebas y el seguimiento de las misma fueron necesarias para lograr los resultados esperados, cumpliendo con los requerimientos técnicos, funcionales y legales (basados en la política de uso en la Universidad).

A continuación, se presenta las pantallas de la prueba realizada en FICA, para este caso un usuario cumple el rol de Gestor Documental y los usuarios aprobadores son los Directores, el documento utilizado para esta prueba está alineado con la política de uso de la aplicación.

Tabla 9

Reporte de prueba del gestor documental.

No	Tipo de Prueba	Observación
01	El Gestor documental envía un archivo para ser revisado y aprobado.	La prueba es exitosa. El workflow se competa, se reciben las notificaciones en el correo electrónico corporativo y se registran en la plataforma de adobe.

Una vez gestor documental envía un documento para iniciar el flujo que el documento enviado finalice con todas las aprobaciones, esta prueba consiste en recoger las aprobaciones de cada uno de los Directores de FICA. En las siguientes pantallas se visualiza el orden en el cual se completa el flujo.

Figura 38. Prueba de aprobación. Primera aprobación

Adaptado de (Adobe, 2018)

En las imágenes se visualiza el certificado de Adobe Sign, la cual certifica que el documento aprobado es único y original. Este certificado se presenta con una banda celeste en la parte superior del documento. Las aprobacines digitales utilizan un ID digital baado en un certificado que emite una autoridad de certificación (CA) acreditada o un proveedor de servicios de confianza (TSP).

El certificado de Adobe Sign se visualiza de la siguiente manera:

Figura 39. Certificado de Adobe Sign
Adaptado de (Adobe, 2018)

Continuando con el flujo del archivo, se presenta en las siguientes imágenes, la cual ilustra el orden en el cual los usuarios aprobadores fueron completando el flujo del documento.

La siguiente figura ilustra las dos primeras aprobaciones electrónicas, lo cual implica que los usuarios aprobadores recibieron el documento digital (a través de una notificación en su mail), lo revizaron y lo aprobaron. Según este caso el flujo del documento sigue su curso, es decir, está a espera que el resto de usuarios aprobadores revicen, aprueben, deleguen o denieguen el documento.

Figura 40. Prueba de aprobación. Dos aprobaciones.
Adaptado de (Adobe, 2018)

La siguiente figura, indica que ya se procedió con la ejecucipón de la tercera aprobación digital. Luego de esta aprobación el documento continúa con su flujo.

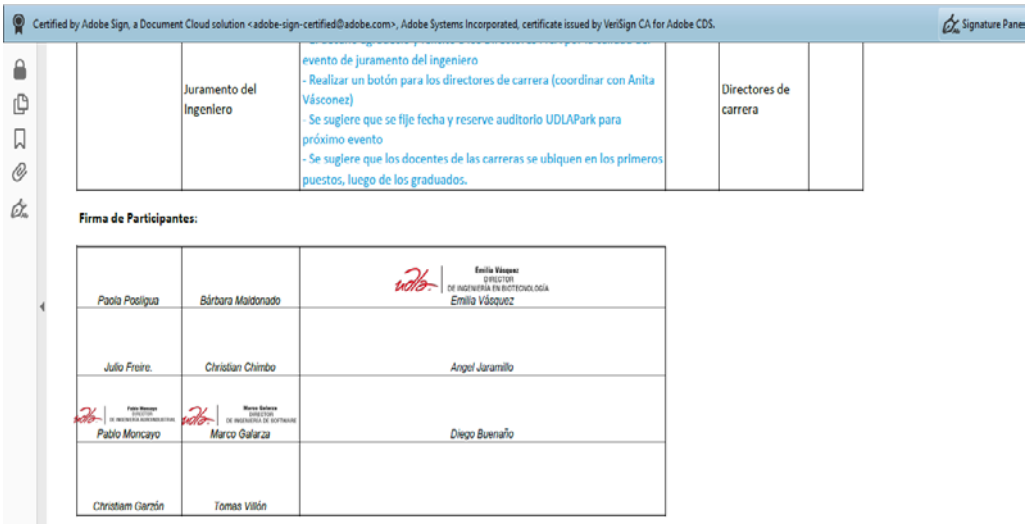


Figura 41. Prueba de aprobación. Tercera aprobación.
Adaptado de (Adobe, 2018)

Esta figura ilustra la cuarta y quinta aprobación digital.

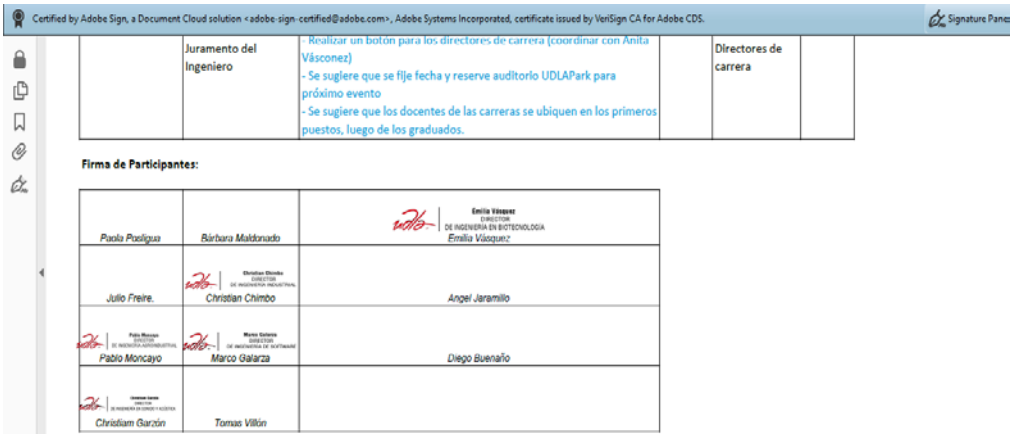


Figura 42. Prueba de aprobación. Cuarta y quinta aprobación.
Adaptado de (Adobe, 2018)

En esta figura se observa que el flujo ya ha completado la sexta aprobación digital.

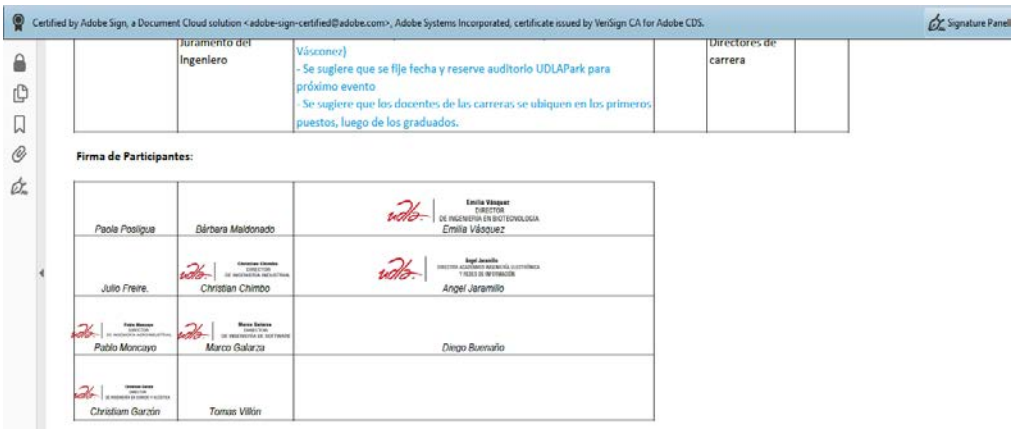


Figura 43. Prueba de aprobación. Sexta aprobación.
Adaptado de (Adobe, 2018)

En esta figura se observa que el flujo ya ha completado la séptima aprobación digital.

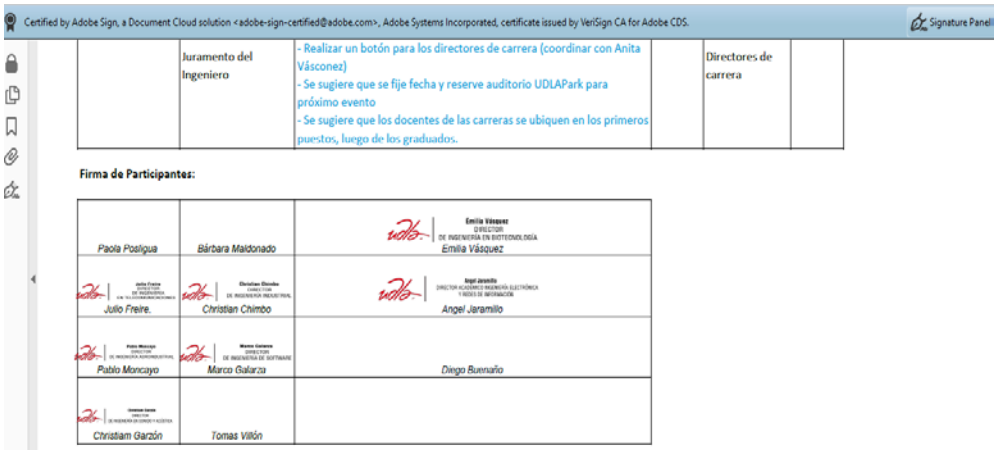


Figura 44. Prueba de aprobación. Séptima aprobación.
Adaptado de (Adobe, 2018)

La siguiente figura ilustra la octava, novena y décima aprobación digital, con las cuales finaliza el flujo del documento de manera exitosa. Visualizar la figura 45.

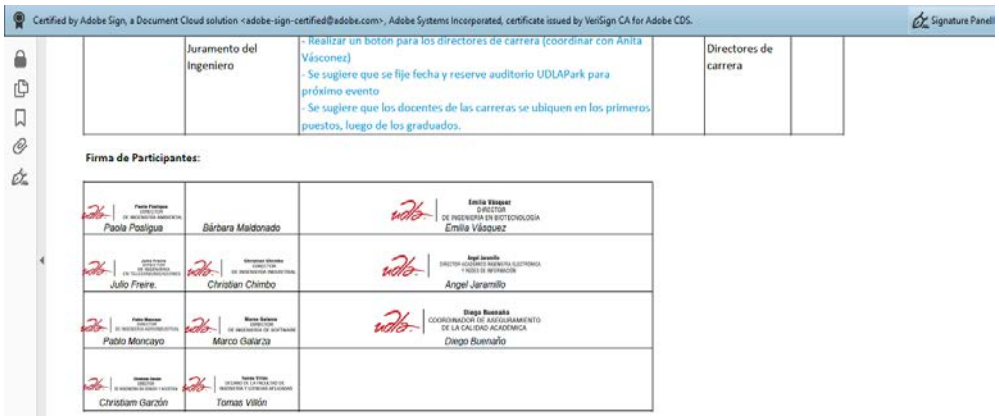


Figura 45. Final del flujo del documento aprobado.
Adaptado de (Adobe, 2018)

3.9. Historial e informe de auditoría

Esta es una opción que Adobe Sign utiliza para evidenciar el paso a paso que el documento tuvo desde que el gestor documental inició el flujo, hasta que el documento digital haya finalizado el flujo programado. Gracias a esta opción, esta aplicación, permite a los usuarios tomar desiciones, incluso sobre el orden

en que se ejecuta la aprobación de un documento digital, el cual representa un procedimiento definido por una o mas áreas.

Una vez finalizado el flujo, el documento genera un historial correspondiente al flujo del documento, esto incluye la siguiente información:

- Título del documento.
- Fecha de creación del documento.
- Nombre y dirección electrónica del usuario gestor.
- El estatus del documento, en este caso “Aprobado”.
- Transaction ID. Que hace referencia al ID de la transacción el cual está encriptado y por medio de este se valida la autenticidad del documento aprobado.

A continuación, se presenta la primera parte de la información del historial del flujo, en la cual se visualiza los datos antes mencionados.

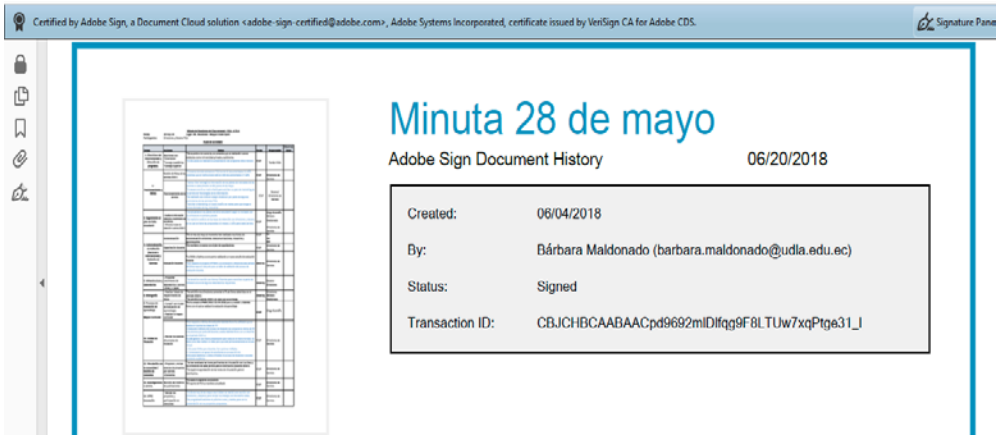


Figura 46. ID de la transacción electrónica del documento aprobado.
Adaptado de (Adobe, 2018)

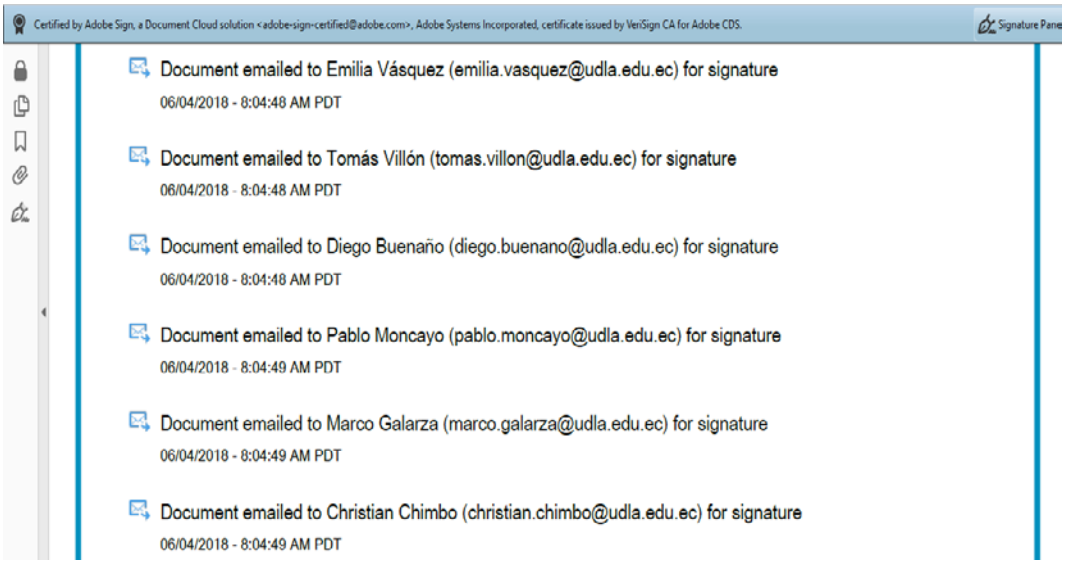


Figura 47. Historial de flujo del documento electrónico aprobado.
Adaptado de (Adobe, 2018)

La siguiente información que presenta el historial del documento es, la fecha y hora de cuando visualizó el documento el usuario aprobador. Como dato adicional se visualiza la dirección IP pública de la red a la cual se encuentra conectado el dispositivo a través del cual se aprobó el documento.

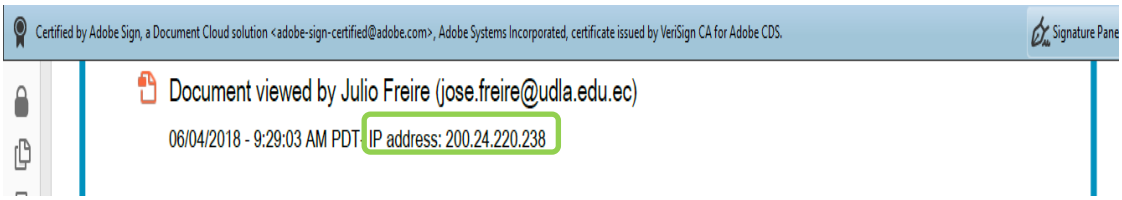


Figura 48. Historial del flujo del documento, ip del equipo del usuario aprobador.
Adaptado de (Adobe, 2018)

Luego presenta los datos del momento en que el documento fue aprobado; los datos que se presentan son los siguientes: fecha y hora del momento en que se aprobó el documento. También la dirección IP pública de la red a la cual se encuentra conectado el dispositivo a través del cual se aprobó el documento.

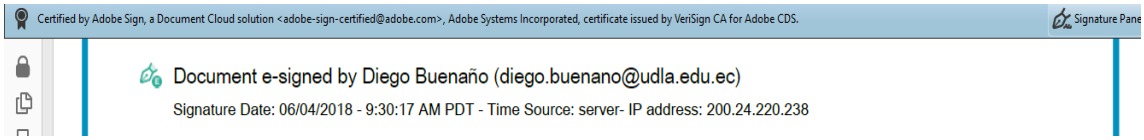


Figura 49. Historial del flujo del documento, hora, fecha, ip de equipo de donde se aprobó el documento.
Adaptado de (Adobe, 2018)

Finalmente, los datos en los cuales se notifica al usuario gestor del documento que todos los usuarios aprobadores han completado el flujo de aprobaciones. Se visualiza la fecha, la hora y los correos electrónicos de los usurios aprobadores.

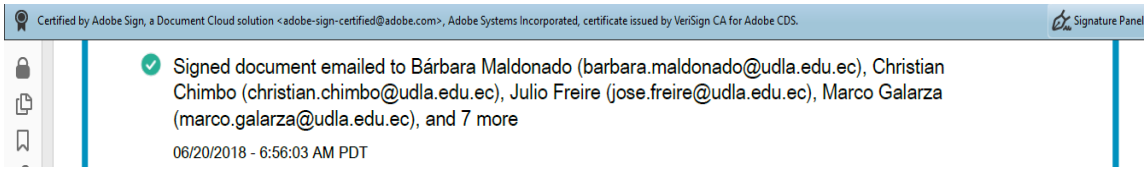


Figura 50. Historial del flujo del documento, visualización de todos los usuarios aprobadores.
Adaptado de (Adobe, 2018)

De esta manera se verifica que el funcionamiento de la aplicación, es óptima y cumple con el análisis de requerimientos, los cuales se dieron origen al desarrollo de este proyecto.

3.10. Verificación de integridad y autenticidad del documento

La verificación de la autenticidad confirma que el certificado del aprobador existe en la lista de identidades de confianza del validador; también confirma si el certificado de firma es válido según la configuración de Adobe Sign. La verificación de integridad del documento confirma si el contenido del documento aprobado ha cambiado después de que ha sido aprobado.

La aplicación implementada tiene la funcionalidad de verificación, la cual permite revisar la autenticidad y la integridad del archivo, el procedimiento es ejecuta, dando un clic en una de las aprobaciones, y automáticamente se redirecciona a un URL propio de Adobe el cual analiza, verifica y notifica con un mensaje la veracidad del documento aprobado.

En la siguiente imagen se visualiza, cuando un documento aprobado cumple con la autenticidad y la integridad.

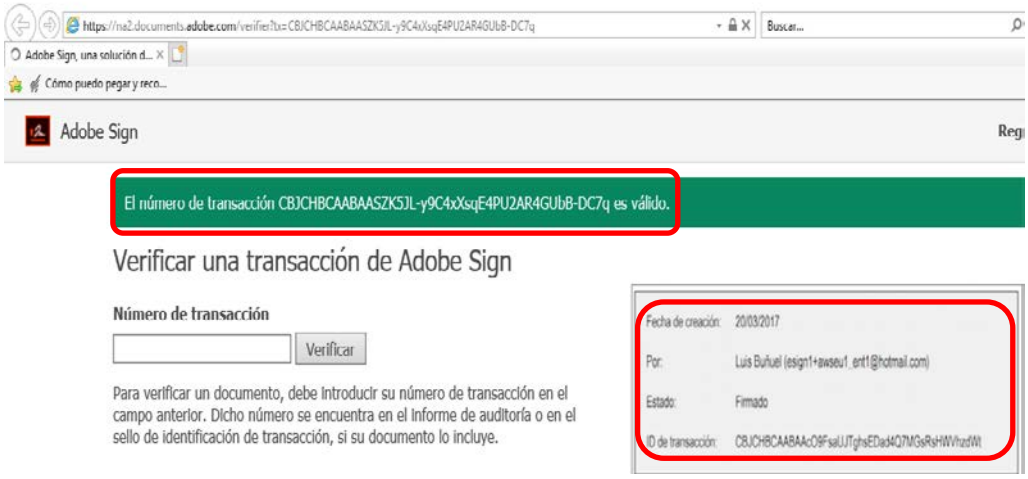


Figura 51. Verificación del número del ID de la transacción electrónica. Adaptado de (Adobe, 2018)

3.11. Fase 4. Monitorear y optimizar

En esta fase se realiza el monitoreo del rendimiento y funcionalidad de la aplicación implementada, se comprueba si hay errores y si estos son frecuentes o imposibles de manejar, podría ser necesario rediseñar la solución implementada; esto se evita si los pasos anteriores se han desarrollado correctamente.

De manera adicional esta fase, permite hacer ajustes no previstos en la etapa de diseño.

Para realizar el monitoreo del desempeño Adobe Sign, se procedió a realizar el seguimiento del uso de la herramienta y una encuesta realizada a algunos usuarios aprobadores y al usurio cuyo rol es de gestor documental, las mismas que se evidencian en el (Anexo 2. Encuesta: Pruebas de aceptación). Esta encuesta dejó los siguientes resultados:

Pregunta 1.

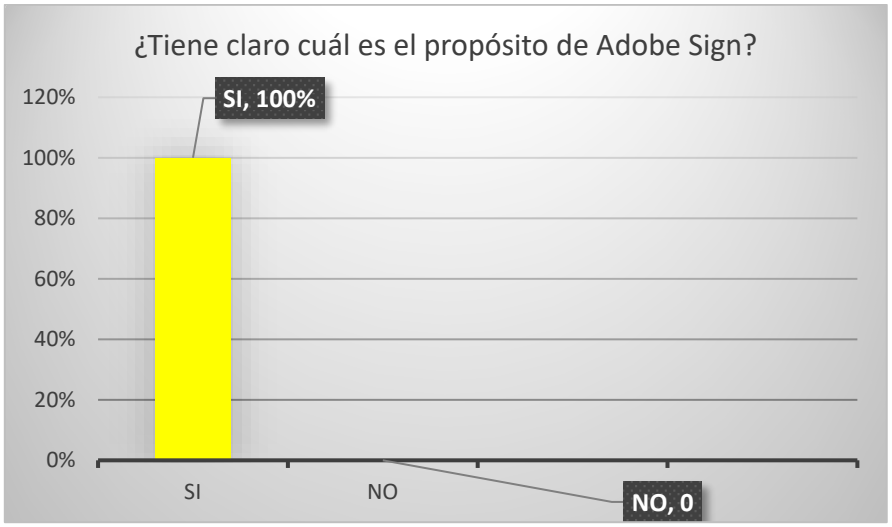


Figura 52. Resultados de la encuesta de satisfacción, pregunta 1.

Pregunta 2.

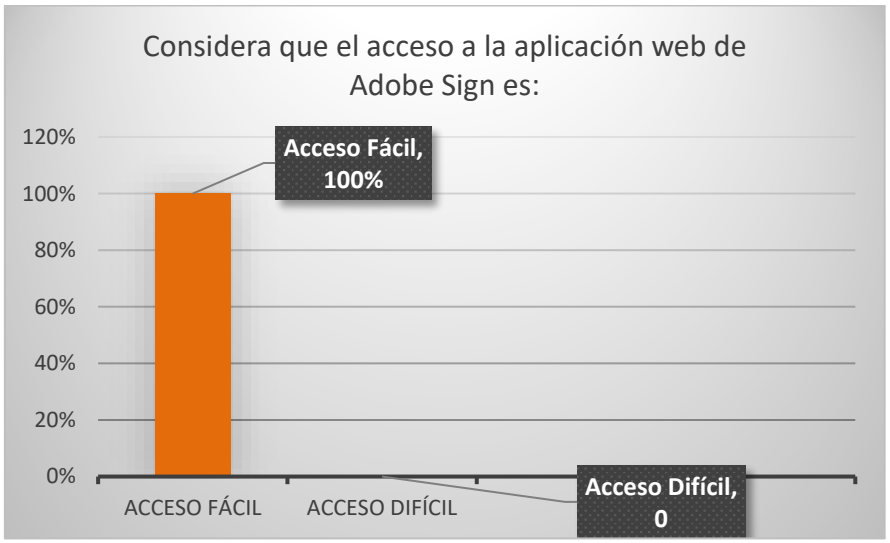


Figura 53. Resultados de la encuesta de satisfacción, pregunta 2.

Pregunta 3.

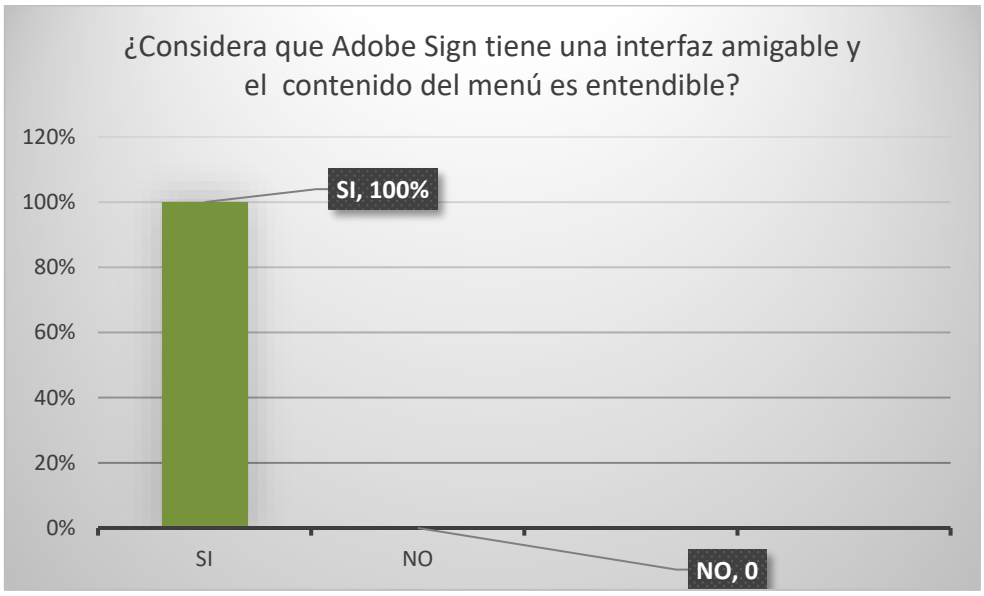


Figura 54. Resultados de la encuesta de satisfacción, pregunta 3.

Pregunta 4.

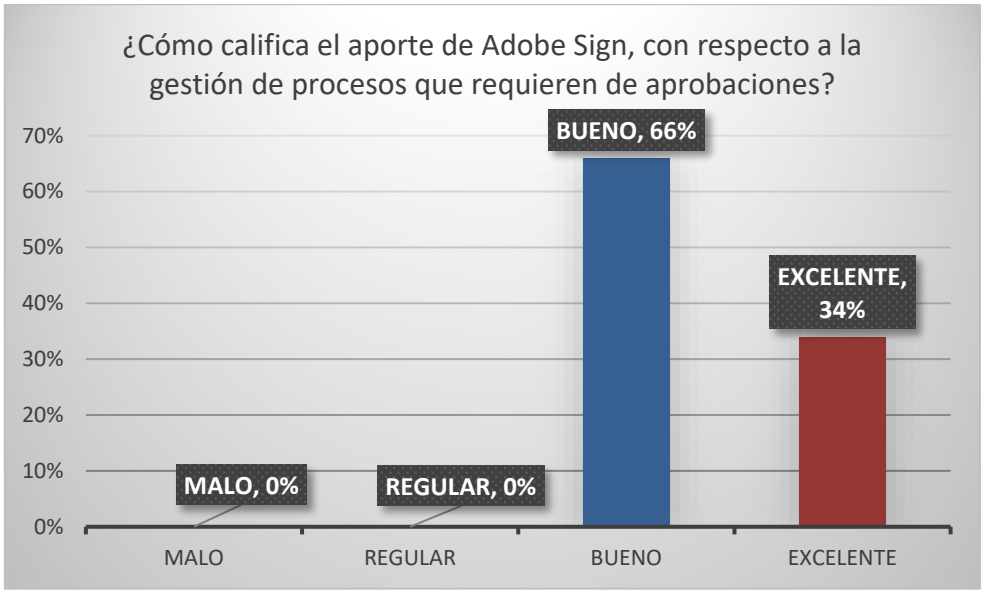


Figura 55. Resultados de la encuesta de satisfacción, pregunta 4.

Pregunta 5.

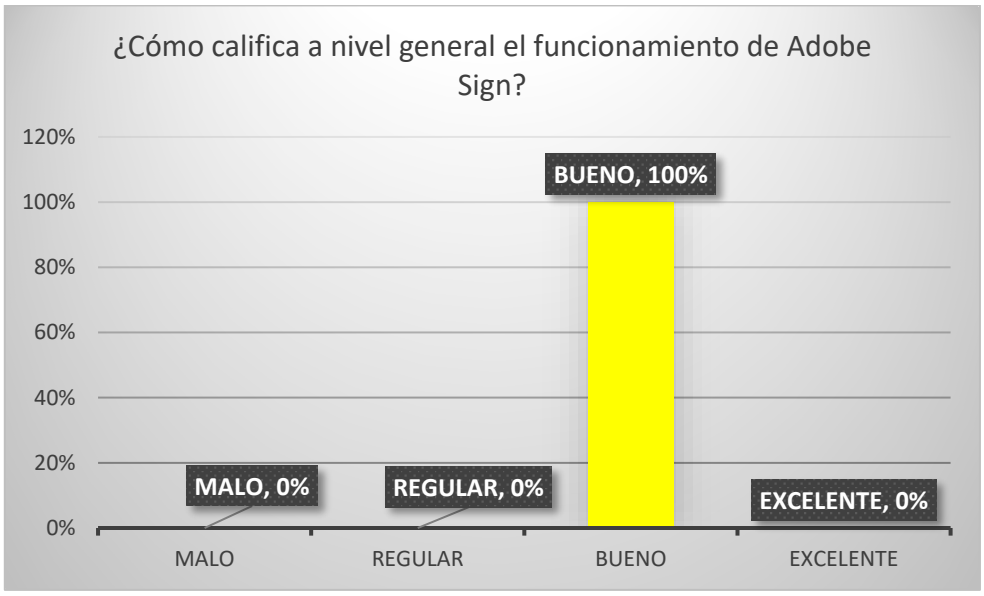


Figura 56. Resultados de la encuesta de satisfacción, pregunta 5.

Pregunta 6.

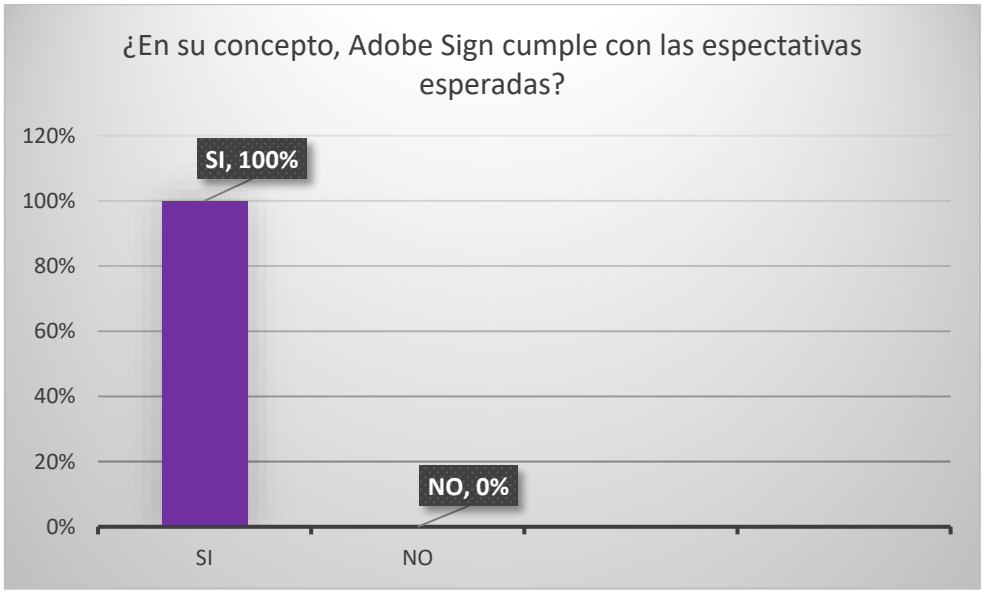


Figura 57. Resultados de la encuesta de satisfacción, pregunta 6.

Pregunta 7.

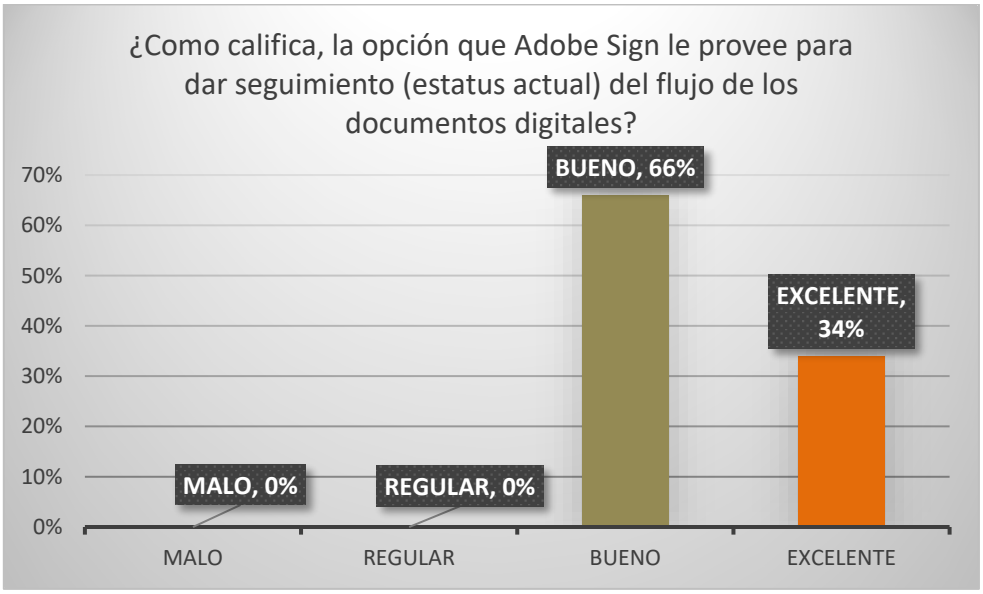


Figura 58. Resultados de la encuesta de satisfacción, pregunta 7.

Pregunta 8.

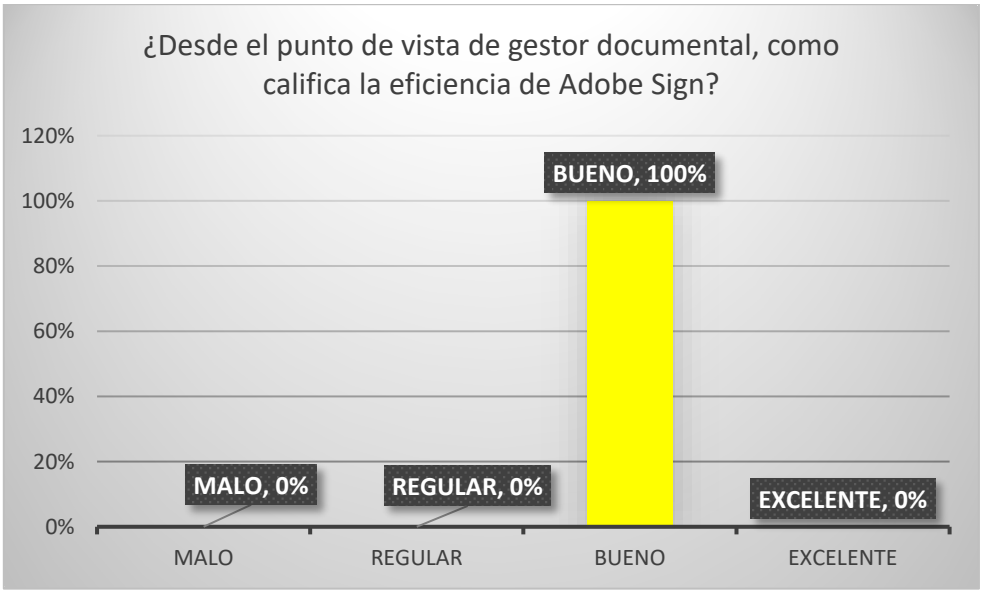


Figura 59. Resultados de la encuesta de satisfacción, pregunta 8.

Pregunta 9.

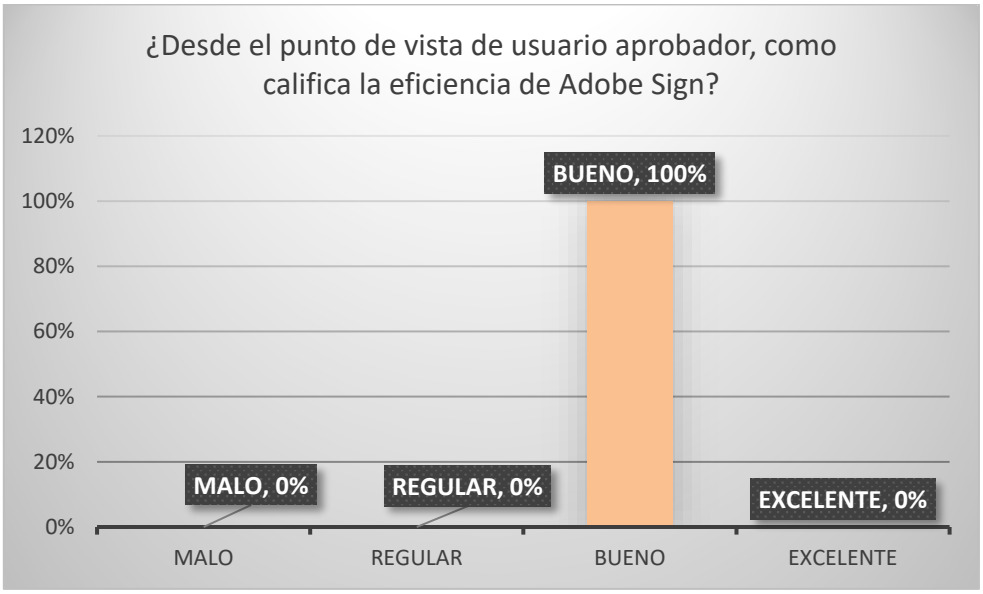


Figura 60. Resultados de la encuesta de satisfacción, pregunta 9.

En base al análisis de las ilustraciones presentadas, se concluye que la solución de Adobe Sign, funciona de manera óptima y cumple a cabalidad con los requerimientos que dieron origen al desarrollo del proyecto de implementación de la “Aprobación Digital” en la Facultad de Ingeniería y Ciencias Aplicadas de UDLA.

4. CONCLUSIONES Y RECOMENDACIONES

Este segmento del documento, muestra las conclusiones y recomendaciones como resultado del proceso de implementación de aprobación digital.

4.1. CONCLUSIONES

Se ha Diseñado e Implementado un prototipo de aprobación digital, basada en Cloud y SAAS para procesos internos de la carrera de la Facultad de Ingenierías y Ciencias Aplicadas de la Universidad de Las Américas.

Se identificó el proceso y operación de la aprobación digital en sus características técnicas y las aplicaciones para su implementación como son office 365 y document Cloud.

Se realizó el control de la solución implementada, evaluando el cumplimiento de los parámetros técnicos, legales y funcionales de la institución.

Esta tecnología mediante la aplicación Adobe permiten automatizar procesos de tipo manual a electrónicos, obteniendo seguridad en la información y optimización en la gestión documental y reducción de los tiempos.

El uso de la tecnología de aprobación digital, permite certificar la autoría, integridad y veracidad de los documentos digitales; también el impulsar la generación de documentos electrónicos con características de: integridad, confiabilidad y conformidad.

El desarrollo de este proyecto, obligó a establecer y promulgar políticas, procedimientos y prácticas de gestión documental de archivos electrónicos, basado en la política de uso propio de la Universidad.

Para la Universidad un punto importante del uso de la aplicación de aprobación digital, es el cuidado del medio ambiente producto de la reducción del uso de papel y energía eléctrica.

El uso de nuevas Tecnologías de Información y Comunicaciones, abren la posibilidad de cambios continuos generando un impulso innovador, que contribuya al impulso de integrar soluciones que permitan automatizar de manera segura procedimientos institucionales.

4.2. RECOMENDACIONES

Analizar opciones futuras de depósitos de documentos (metadatos), generados por las transacciones electrónicas.

Es importante concientizar a los usuarios de la aprobación digital la conciencia de asumir con responsabilidad del uso de esta tecnología.

Estudiar las opciones tecnológicas que se pueden integrar con la aprobación digital, lo cual permita explotar de mejor manera la información generada por las transacciones electrónicas a través de la aplicación de la minería de datos.

Se sugiere realizar periódicamente una auditoría del proceso de aprobación digital, tanto a nivel funcional como a nivel técnico.

Se recomienda a los usuarios de la aprobación electrónica: custodiar adecuadamente su clave de acceso a la aplicación, de igual manera al recibir una comunicación aprobada digitalmente: verificar que sea válida.

El momento que se requiera hacer uso de esta aplicación se recomienda utilizar una conexión segura de internet.

El uso del sistema de aprobación digital es un sistema transaccional electrónico, por tal motivo es importante disponer de un plan de contingencia ante riesgos de pérdida de información o en caso que no se disponga del servicio.

REFERENCIAS

Adobe, (2018). Adobe Analytics, procesamiento de métricas. Recuperado el 12 de febrero de 2018 de https://helpx.adobe.com/es/analytics/kb/average-time-spent-on-site.html

Adobe, (2018). Adobe Sign, conceptos básicos. Recuperado el 23 de marzo de 2018 de https://helpx.adobe.com/es/analytics/kb/average-time-spent-on-site.html

Adobe, (2018). Adobe Sign technical overview. Recuperado el 27 de abril de 2018 de https://www.adobe.com/content/dam/acom/en/security/pdfs/adobe-sign-technical-overview-ue.pdf

Alcatel, en las nubes Net: El Medio de las Telecomunicaciones. 5.125 (Apr. 16, 2001): p13. From Informe Académico. Copyright: COPYRIGHT 2001 Servicios Editoriales Sayrols S.A. de C.V. Recuperado de https://www.globalsign.com/es/blog/como-funcionan-las-firmas-digitales/

AWS Security, (2018). *Introducing AWS Single SIgn - On.* Recuperado el 22 de abril de 2018 de https://aws.amazon.com/es/blogs/security/introducing-aws-single-sign-on/

Beasley, J., & Nilkaew, P. (2014). *Networking Essentials (4a ed.).* Pearson College Div. January 16, 2014. New Mexico State University.

DataQUBO Backup, (2013). Encriptaión: ¿qué tan seguro es AES?. Recuperado el 19 de enero de 2013 de http://www.dataqubo.com/encriptacion-que-tan-seguro-es-aes/

Instituto Politécnico Nacional, (2013). *Firma Electrónica: concepto y requerimientos para su puesta en práctica.* Recuperado el 14 de junio de 2013 de https://www.tamps.cinvestav.mx/~mmorales/documents/dsMexico.pdf

Interxion, (2017). *Centro de Datos.* Recuperado 2 de febrero de 2017 de http://www.interxion.com/es/centros-de-datos/

LidI and Niederreiter, (1986) LidI, R. and Niederreiter, H. (1986). *Introduction to finite fields and their applications.* Cambridge University Press, New York, NY, USA

Menezes et al., (1996) Menezes, A. J., Vanstone, S.A., and Oorschot, P.C.V. (1996). *Handbook oj Applied Cryptography.* CRC Press, Inc., Boca Raton, FL, USA, 1st edition

Microsoft, (2018). *Microsoft Azure, definición de Nube.* Recuperado el 11 de marzo de 2018 de https://azure.microsoft.com/es-es/overview/what-is-the-cloud/

Microsoft, (2018). *Infraestructura como servicio.* Recuperado el 30 de abril de 2018 de https://azure.microsoft.com/es-es/overview/what-is-iaas/

Microsoft, (2018). *Microsoft Azure. Pataforma como servicio.* Recuperado el 10 de mayo de 2018 de https://azure.microsoft.com/es-es/overview/what-is-paas/

Microsoft, (2018). *Microsoft Azure. Cloud Computing - SaaS*. Recuperado el 22 de abril de 2018 de https://azure.microsoft.com/es-es/overview/what-is-saas/

Microsoft, (2018). *Configurar Microsoft Azure para uso con Adobe SSO.* Recuperado el 15 de marzo de 2018 de https://helpx.adobe.com/la/enterprise/kb/configure-microsoft-azure-with-adobe-sso.html

Microsoft, (2018). *Azure AD Single Sign-Out .* Recuperado el 28 de enero de 2018 de https://docs.microsoft.com/en-us/azure/active-directory/active-directory-saas-custom-apps

Microsoft, (2018). *Azure AD SAML Entity ID.* Recuperado el 05 de marzo de 2018 de https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-federation-saml-idp

PAe, (2017). *La Firma Electrónica. Portal de Administración Electrónica Ministerio de Política Territorial y Función Pública Secretaría General de Administración Digital.* Recuperado el 9 abril de 2017 de http://firmaelectronica.gob.es/Home/Ciudadanos/Firma-electronica.html

SaaS *what is it, and why should*, Eric Hunter and Donald R. Barthel GP From Academic OneFile. Copyright: COPYRIGHT 2011 American Bar Associatio. 24 of June, 2011 de http://www.abanet.org/genpractice/magazine/index.html

Seguridad América, (2018). *Aplicación de aprobación electrónica. ¿Qué es una Firma Digital ATTL?* Recuperado el 20 de julio, 2018 de https://seguridadamerica.com/en/que-es-una-firma-digital-aatl/

Skoog, D., Crouch, S., & Holler, F. J. (2008). Principios de Análisis Instrumental. México, D.F.: Cengage Learning Editores. STI. (2013). Subsecretaría de Tecnologías de la información. Recuperado el 18 de mayo de 2013 de http://www.informatica.gob.ec/sistemas/transversales/firma-electronica

Universidad Politécnica de Valéncia, (2017). *Área de Sistemas de Información y comunicaciones Certificados digitales. ¿Qué es una Firma electrónica?, definición de Firma Electrónica.* Recuperado el 15 de agosto, 2017, de https://www.upv.es/contenidos/CD/info/711250normalc.html

ANEXOS

Anexo 1

Encuesta: Definición de problemática

Encuesta sobre la definición de la problemática

	Proyecto de Implementación de Adobe Sign
udla	Encuesta de Definición de problemática

PREGUNTA	CRITERIOS DE EVALUACION	
1. El tiempo utilizado para movilizarse y conseguir una aprobación excede del tiempo planificado para realizar esta tarea.	SI ✓	NO
2. El desarrollo de la actividad de recoger aprobaciones manuales, es causante de generar problemas de coordinación entre los aprobadores y el gestor documental.	SI ✓	NO
3. Considera que en ocaciones se ha utilizado innecesariamente reimpresiones de los documentos que se utilizan para se probadas. (En caso de alguna equivocación en el texto, por ejemplo).	SI ✓	NO
4. Considera que sería de ayuda para el desarrollo de esta actividad, la implementación de un sistema que automatice el procedimiento de aprobación documental?	SI ✓	NO
5. Actualmente la FICA cuenta con un log o histórico que informe con exactitud el flujo (con fecha y hora) del momento que fue aprobado?	SI	NO ✓
6. De 1 a 5, siendo 5 el valor mas alto; Como calificaría la importancia de tener una herramienta tecnológica que permita automatizar procedimientos manuales con una aplicación que permita hacer uso de la aprobación electrónica?	5	

Observaciones

Por que considera importante hacer uso de una herramienta tecnológica, que permita automatizar el procedimiento de aprobaciones manuales?

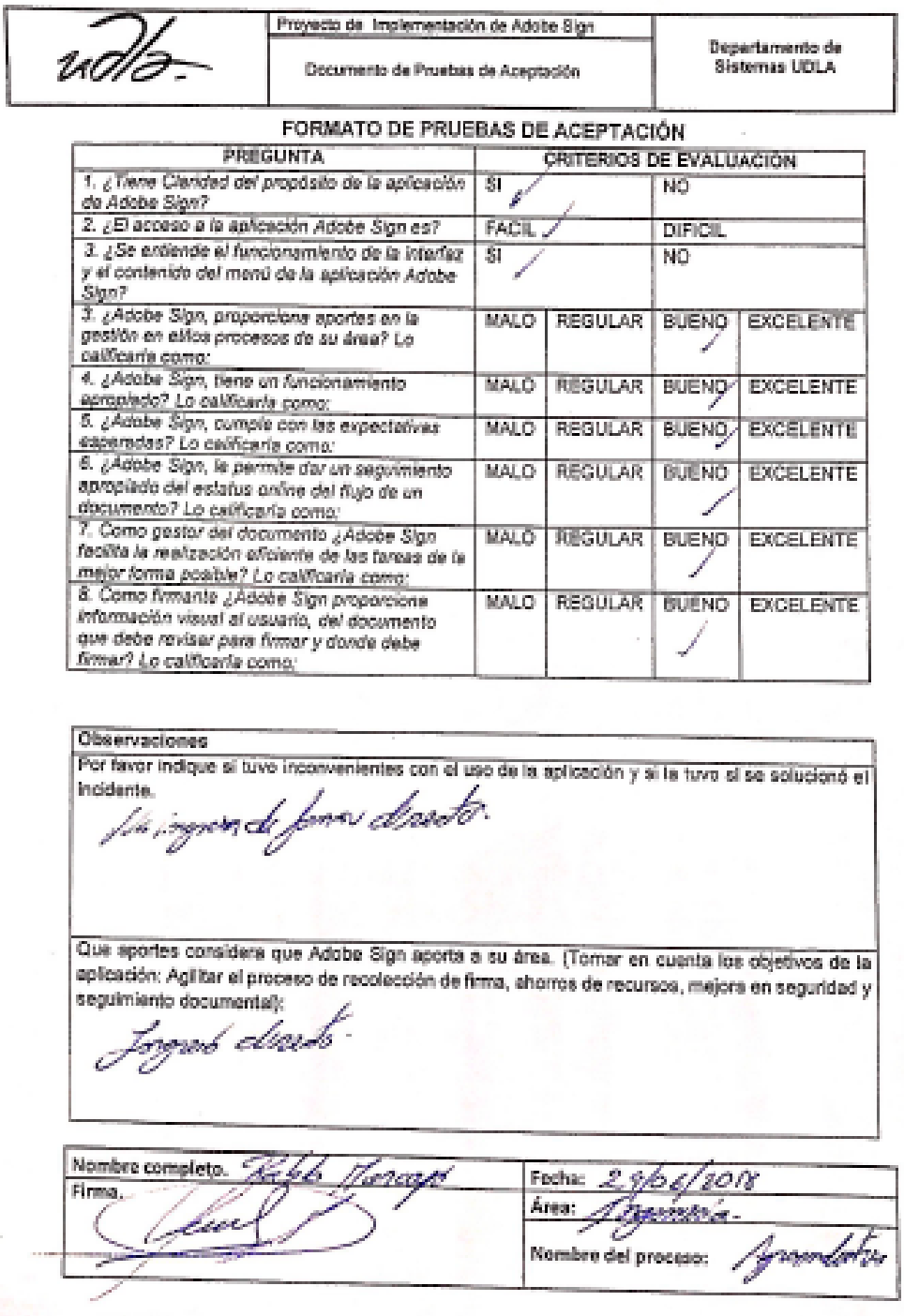
Evita el uso de papel innecesario, permitiendo el cuidado del planeta.

Nombre completo: Barbara Maldonado Chamorro	Fecha:
Firma: Barbara M.	Area: Facultad de Ingeniería y Ciencias Aplicadas

Anexo 2

Encuesta de las pruebas de aceptación

Encuesta de las pruebas de aceptación



	Proyecto de Implementación de Adobe Sign	Departamento de Sistemas UDLA
udla	Documento de Pruebas de Aceptación	

FORMATO DE PRUEBAS DE ACEPTACIÓN

PREGUNTA	CRITERIOS DE EVALUACIÓN			
1. ¿Tiene Claridad del propósito de la aplicación de Adobe Sign?	SI ✓		NO	
2. ¿El acceso a la aplicación Adobe Sign es?	FACIL ✓		DIFICIL	
3. ¿Se entiende el funcionamiento de la interfaz y el contenido del menú de la aplicación Adobe Sign?	SI ✓		NO	
3. ¿Adobe Sign, proporciona aportes en la gestión en ellos procesos de su área? Lo calificaría como:	MALO	REGULAR	BUENO ✓	EXCELENTE
4. ¿Adobe Sign, tiene un funcionamiento apropiado? Lo calificaría como:	MALO	REGULAR	BUENO ✓	EXCELENTE
5. ¿Adobe Sign, cumple con las expectativas esperadas? Lo calificaría como:	MALO	REGULAR	BUENO ✓	EXCELENTE
6. ¿Adobe Sign, le permite dar un seguimiento apropiado del estatus online del flujo de un documento? Lo calificaría como:	MALO	REGULAR	BUENO ✓	EXCELENTE
7. Como gestor del documento ¿Adobe Sign facilita la realización eficiente de las tareas de la mejor forma posible? Lo calificaría como:	MALO	REGULAR	BUENO ✓	EXCELENTE
8. Como firmante ¿Adobe Sign proporciona información visual al usuario, del documento que debe revisar para firmar y donde debe firmar? Lo calificaría como:	MALO	REGULAR	BUENO ✓	EXCELENTE

Observaciones

Por favor indique si tuvo inconvenientes con el uso de la aplicación y si la tuvo si se solucionó el incidente.

No, ninguno de forma directa.

Que aportes considera que Adobe Sign aporta a su área. (Tomar en cuenta los objetivos de la aplicación: Agilitar el proceso de recolección de firma, ahorros de recursos, mejora en seguridad y seguimiento documental):

Seguridad directa.

Nombre completo: [illegible]	Fecha: 2/06/2018
Firma:	Área: [illegible]
	Nombre del proceso: [illegible]

	Proyecto de Implementación de Adobe Sign	Departamento de Sistemas UDLA
udla	Documento de Pruebas de Aceptación	

FORMATO DE PRUEBAS DE ACEPTACIÓN

PREGUNTA	CRITERIOS DE EVALUACIÓN			
1. ¿Tiene Claridad del propósito de la aplicación de Adobe Sign?	SI X		NO	
2. ¿El acceso a la aplicación Adobe Sign es?	FACIL ✓		DIFICIL	
3. ¿Se entiende el funcionamiento de la interfaz y el contenido del menú de la aplicación Adobe Sign?	SI X		NO	
3. ¿Adobe Sign, proporciona aportes en la gestión en ellos procesos de su área? Lo calificaría como:	MALO	REGULAR	BUENO ✓	EXCELENTE
4. ¿Adobe Sign, tiene un funcionamiento apropiado? Lo calificaría como:	MALO	REGULAR	BUENO ✓	EXCELENTE
5. ¿Adobe Sign, cumple con las expectativas esperadas? Lo calificaría como:	MALO	REGULAR	BUENO ✓	EXCELENTE
6. ¿Adobe Sign, le permite dar un seguimiento apropiado del estatus online del flujo de un documento? Lo calificaría como:	MALO	REGULAR	BUENO ✓	EXCELENTE
7. Como gestor del documento ¿Adobe Sign facilita la realización eficiente de las tareas de la mejor forma posible? Lo calificaría como:	MALO	REGULAR	BUENO ✓	EXCELENTE
8. Como firmante ¿Adobe Sign proporciona información visual al usuario, del documento que debe revisar para firmar y donde debe firmar? Lo calificaría como:	MALO	REGULAR	BUENO	EXCELENTE

Observaciones
Por favor indique si tuvo inconvenientes con el uso de la aplicación y si la tuvo si se solucionó el incidente. Al inicio no podía ingresar por el link de outlook, luego se configuró ya se pudo. Antes tocaba ingresar en la página de adobe
Que aportes considera que Adobe Sign aporta a su área. (Tomar en cuenta los objetivos de la aplicación: Agilitar el proceso de revalidación de firma, ahorros de recursos, mejora en seguridad y seguimiento documental): eficiente al solicitar firma, en menor tiempo se tiene un documento completo, evita estar buscando a las personas.

Nombre completo: Bárbara Maldonado Chamorro	Fecha: 28/06/2018
Firma: Bárbara Mal	Área: Facultad de Ingeniería y Ciencias Ap Nombre del proceso:

udla	Proyecto de Implementación de Adobe Sign Documento de Pruebas de Aceptación	Departamento de Sistemas UDLA

FORMATO DE PRUEBAS DE ACEPTACIÓN

PREGUNTA	CRITERIOS DE EVALUACIÓN			
1. ¿Tiene Claridad del propósito de la aplicación de Adobe Sign?	SI X		NO	
2. ¿El acceso a la aplicación Adobe Sign es?	FACIL X		DIFICIL	
3. ¿Se entiende el funcionamiento de la interfaz y el contenido del menú de la aplicación Adobe Sign?	SI X		NO	
3. ¿Adobe Sign, proporciona aportes en la gestión en estos procesos de su área? Lo calificaría como:	MALO	REGULAR	BUENO	EXCELENTE X
4. ¿Adobe Sign, tiene un funcionamiento apropiado? Lo calificaría como:	MALO	REGULAR	BUENO X	EXCELENTE
5. ¿Adobe Sign, cumple con las expectativas esperadas? Lo calificaría como:	MALO	REGULAR	BUENO X	EXCELENTE
6. ¿Adobe Sign, le permite dar un seguimiento apropiado del estatus online del flujo de un documento? Lo calificaría como:	MALO	REGULAR	BUENO	EXCELENTE X
7. Como gestor del documento ¿Adobe Sign facilita la realización eficiente de las tareas de la mejor forma posible? Lo calificaría como:	MALO	REGULAR	BUENO X	EXCELENTE
8. Como firmante ¿Adobe Sign proporciona información visual al usuario, del documento que debe revisar para firmar y donde debe firmar? Lo calificaría como:	MALO	REGULAR	BUENO X	EXCELENTE

Observaciones
Por favor indique si tuvo inconvenientes con el uso de la aplicación y si le tuvo si se solucionó el incidente.
Que aportes considera que Adobe Sign aporta a su área. (Tomar en cuenta los objetivos de la aplicación: Agilitar el proceso de recolección de firma, ahorros de recursos, mejora en seguridad y seguimiento documental):

Nombre completo. DIEGO BUENAÑO T.	Fecha: 28/06/2018
Firma. 	Área: TICA
	Nombre del proceso: