Implementación de firma digital para automatizar el proceso de inscripción de protocolo de investigación para la ESCOM

Trabajo Terminal No. 2021-A080

*Alumnos: Bernal Leocadio Josué Eduardo, *Cruz Pérez Raúl Eduardo*

Directores: M. en C. González Albarrán Gisela, M. en C. Peredo Valderrama Rubén.

***email: rcruzp1401@alumno.ipn.mx**

Resumen – Crear una aplicación web responsiva que automatice el proceso de inscripción de protocolos de investigación en la Escuela Superior de Cómputo (ESCOM), haciendo uso del medio de autenticación personal conocido como firma digital[1]. Con dicha aplicación web se buscará acortar los tiempos de respuesta por parte Comisión Académica de Trabajos Terminales (CATT)[2] así como tener una mayor coordinación entre todos los involucrados en dicho proceso administrativo, los cuales son alumnos, directores, sinodales, profesores de seguimiento y jefes de departamentos de la dependencia.

Palabras clave – Aplicación Web, API-REST, CATT, Firma Electrónica, Certificado Digital, Cifrado Asimétrico.

1. Introducción

Hoy en día la implementación de tecnologías para trabajar a distancia se ha vuelto cada vez más recurrente, esto aunado a la situación sanitaria de SARS-CoV-2 por la cual atraviesa nuestro país. La Escuela Superior de Cómputo no ha sido la excepción, sobre todo en la realización y entrega de documentos por parte de los alumnos, la cual incluye entrega de dictámenes, baja de materias, envío de protocolos, entre otros.

Este protocolo tiene como objetivo centrarse en el proceso de inscripción de protocolos, el cual es realizado por la CATT. Este proceso se ha vuelto una problemática para toda la comunidad estudiantil, debido a que al manejarse una modalidad a distancia en las actividades escolares, muchas veces no hay comunicación entre alumnos, profesores y personal administrativo.

Muchos de los procesos administrativos, sino es que todos, se manejan a través de formularios de Google y envío de correos electrónicos. Debido a esto es que buscamos implementar una aplicación web que automatice el registro de alumnos y directores para un protocolo, asignación de sinodales, envío de dictámenes en caso de ser necesario, acuses de recibido, etc; todo esto será desarrollado a través de la implementación de una firma digital [3], la cual nos permitirá validar toda la automatización antes mencionada, sin necesidad de mandar correos electrónicos con el mensaje “Acuse de recibido”, ya que de esta manera se está exponiendo a que tanto el alumno como el profesor no hayan mandado dicho correo y esto sea motivo de falsificación al momento de añadir la prueba al documento final antes de enviarlo directamente a la CATT. Otra de las razones, es la falta de comunicación entre los compañeros de protocolo (alumnos y directores) al momento de validar que ya se recibió el documento, ya que por diversas razones no revisa el correo electrónico, o aparece en la bandeja de “spam”, lo cual dificulta que un director que no está relacionado al área de sistemas desconozca de esta parte; es por eso, que al centrar toda la automatización en esta aplicación, no solo se permitirá el registro de alumnos y directores al protocolo correspondiente, y todo lo antes mencionado, sino también mantener la seguridad al momento de hacer el envío y la recepción de este trabajo, ya que estamos hablando de un trámite para titulación y se requiere un medio de envío seguro y confiable, que no dependa de formularios en dónde no se verifica la identidad del usuario, ni correos electrónicos, que pueden no ser enviados ni recibidos y se está expuesto a algún tipo de falsificación.

La tabla 1 muestra trabajos similares a la propuesta.

Software	Características	Precio en el mercado
HAAP[4]	Registro y asignación de protocolos. Edición de los documentos, así como clasificación y asignación de protocolos a los departamentos académicos correspondientes. Se encarga de gestionar todo el proceso requerido por parte de la CATT para la aprobación de los documentos. Parentesco con la solución propuesta 50% al ser una herramienta enfocada en la clasificación de los protocolos.	No disponible para el público en general
Aplicación Web gestor de protocolos de trabajos terminales con implementación de firma digital para la ESCOM	Será una aplicación web de uso exclusivo para la comunidad de la ESCOM con la cual se hará el trámite de registro de protocolo para los estudiantes que cumplan con los requisitos, la finalidad de esta aplicación es ofrecer los siguientes servicios criptográficos. integridad, no repudio y confidencialidad. Tendrá la funcionalidad de firmar documentos con certificados emitidos por el SAT [6] y certificados generados por la misma aplicación web.	No disponible para el público en general
AutoFirma[5]	Es una aplicación de escritorio diseñada por el Ministerio de Hacienda y Administraciones Públicas de España, cuyo principal objetivo es realizar el firmado de cualquier tipo de documento seleccionándolo desde un fichero, la principal desventaja de esta aplicación de escritorio es que no es posible generar un certificado digital para firmas los documentos por lo que es necesario contar con un certificado emitido por una entidad certificadora. Parentesco con solución propuesta 70%.	No disponible para el público en general
Wondershare PDFelement[6]	Es una aplicación de escritorio muy interesante ya que tiene varias funcionalidades para trabajar con documentos en formato PDF tales como editar, crear, convertir, comentar, extraer datos de formularios, redactar información sensible, agregar firma digital, exportar archivos PDF a Word Excel o PowerPoint, entre otras funciones. Para usar la funcionalidad de firma digital es posible generar un certificado digital emitido por la misma aplicación. El principal inconveniente de esta aplicación de escritorio es que se necesita de una suscripción anual, lo cual es un inconveniente para los usuarios esporádicos que no usen la aplicación de manera constante. Parentesco con la solución propuesta 80%.	Suscripción anual de $49.95 dólares

Tabla 1. Tabla comparativa de productos similares

2. Objetivo

Objetivo general

Desarrollar una aplicación web que sustituya el proceso por el cual un alumno realiza la inscripción de protocolo, dicho proceso está actualmente delegado al departamento CATT (Comisión Académica de Trabajos Terminales).

Esta aplicación web institucional implementará una Firma Digital de documentos, esto mediante el uso de un certificado digital y una llave privada, de este modo será posible iniciar y terminar el proceso de registro de protocolos de investigación.

Se pretende dar la funcionalidad de leer el certificado digital emitido por la dependencia gubernamental SAT [7], ya que esta es una de las dependencias que tienen un estricto control de generación de certificados digitales, con lo cual se pretende homogeneizar el uso de dicho certificado.

Objetivos Específicos

1. Desarrollar interfaces de usuario intuitivas, y que presenten funcionalidades de acuerdo al tipo de usuario con el que se accede a la aplicación web.
2. Crear un modelo de base de datos relacional que satisfaga las reglas de negocio para la aplicación web.
3. Implementar una API web de tipo REST, misma que se comunicará con la aplicación web para dar soporte a todas las funcionalidades requeridas por los distintos tipos de usuarios.
4. Generar funcionalidad para firmar digitalmente a partir de un certificado digital emitido por una entidad generadora de certificados electrónicos válidos en México.
5. En caso de que un usuario no posea un certificado emitido por una entidad certificadora, se buscará que la aplicación web tenga la funcionalidad de generar un certificado auto firmado para así poder hacer uso del sistema.
6. Poner a disposición de la CATT la aplicación web.

3. Justificación

A un año y medio del inicio de la contingencia sanitaria y el inminente cierre temporal [8] de escuelas privadas y públicas, muchos de los trámites que se realizaban en dichas instituciones fueron suspendidos. La Escuela Superior de Cómputo no fue la excepción, poco tiempo después algunos de estos trámites se fueron reanudando con el uso de correos electrónicos o formularios de Google, desde entonces el problema cambió al desconocimiento del estado del trámite realizado, no se le da la difusión adecuada a estos formularios, así como la falta de comunicación entre alumnos, profesores y sinodales con la CATT.

Es importante señalar que la medida adoptada para el registro de un protocolo durante la contingencia actual es aún menos segura que el uso de una firma manuscrita, ya que solo se solicita la impresión de pantalla de la confirmación de enterado del remitente, y al haber demasiados programas dedicados a la edición de imágenes digitales, este método de autenticación puede ser fácilmente replicable y por ende la autoría queda vulnerada. Por otra parte es difícil saber si un documento que fue enviado a un director de trabajo terminal, es el mismo entregado un segundo director de trabajo terminal en un mismo equipo de protocolo, ya que se puede dar el caso de que un equipo de protocolo envie dos versiones de la misma propuesta para cada director de trabajo terminal, así que la integridad del documento se ve vulnerada.

Debido a esto pretendemos implementar el algoritmo de firma digital para firmar y registrar dicho documento a través de la propuesta de una aplicación web y darles a los distintos tipos de usuarios (usuario alumno, usuario jefe de departamento, director de TT, sinodal de TT) las funcionalidades esenciales para el correcto procedimiento de este trámite escolar. Dichas funcionalidades permitirán a los usuarios deslindarse de cualquier

tipo de formulario de Google y correos electrónicos, enfocándose solamente en realizar el trámite de registro, validación, búsqueda y envío de protocolos a través de dicha aplicación.

A través de dicha propuesta pretendemos reducir los tiempos de respuesta para validar un protocolo y de esta manera no esperar hasta mediados de semestre para tener una acta de aprobación de protocolo, así como establecer un canal de comunicación más estrecho entre estudiantes, directores de TT, sinodales de TT y personal de apoyo, por ello es necesario tomar el mayor número de requerimientos funcionales y no funcionales para desarrollar dicha aplicación y que sea de gran utilidad para la dependencia politécnica a la que pertenecemos.

Actualmente en el Instituto Politécnico Nacional se hace el trámite de la cédula profesional con el uso de la firma digital emitida por la dependencia gubernamental SAT(Servicio de Administración Tributaria), es por eso que pretendemos sumar este proceso de inscripción de protocolos a los que ya cuenta el instituto y en un futuro digitalizar más trámites institucionales mediante del uso de este método de autenticación personal llamado firma digital.

4. Productos o resultados esperados

Productos finales del sistema:

- API del sistema web disponible para ser consumida por el sistema web.
- Módulo generador de firmas digitales para usuarios del sistema.
- Módulo de control de usuarios para usuario de tipo administrador.
- Módulo generador de reportes para personal de la CATT.
- Módulo validador de firmas digitales asociados a un protocolo.
- Generación de constancias de protocolo en formato validado por la CATT
- Mecanismo de alerta vía correo electrónico como medida de seguridad para acceder al sistema

El Sistema Web utilizará la arquitectura descrita en la siguiente Imagen 4.1

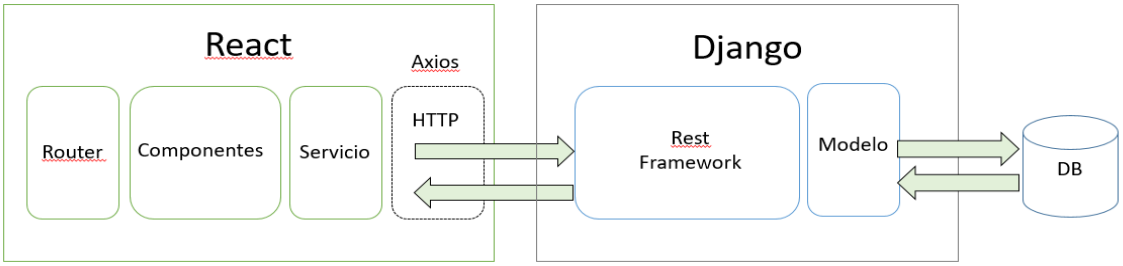


Imagen 4.1. Arquitectura del sistema utilizando el patrón “Modelo Vista Controlador”[9].

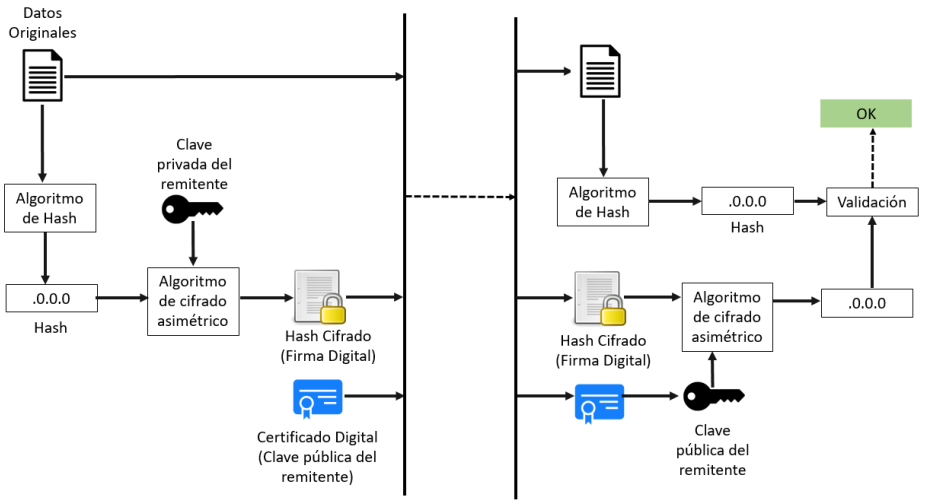


Imagen 4.2 Diagrama de firma electrónica [10].

5. Metodología

Proceso Unificado de Desarrollo (RUP) es una metodología de desarrollo de software que está basado en componentes e interfaces bien definidas, y junto con el Lenguaje Unificado de Modelado (UML), constituye la metodología estándar más utilizada para el análisis, implementación y documentación de sistemas orientados a objetos. Es un proceso que puede especializarse para una gran variedad de sistemas de software, en diferentes áreas de aplicación. La metodología RUP está compuesta de las siguientes fases: inicio, elaboración, construcción, transición[11].

La fase de negocio se caracteriza por obtener todas las reglas del negocio del sistema o en este caso de la aplicación web, así como entrevistar a todos los involucrados (usuarios finales) en la aplicación web.

La fase de elaboración consiste en entender el problema principal que se pretende mitigar así, en esta fase también se pretende establecer una ruta de trabajo para el desarrollo de la aplicación.

Dentro de la fase de construcción iniciaremos con el modelado UML del sistema, diagramas de casos de uso, diagrama de bases de datos relacional, la mayoría de estos diagramas atenderán las reglas de negocio obtenidas en la fase de negocio.

La última fase, la fase de transición será la encargada de hacer la conversión de los diagramas de un estado lógico aun estado físico con el cual ya se podrán hacer las funcionalidades planteadas en los objetivos es aquí donde se visualiza las ventajas de esta metodología de programación, es decir, si se tiene una base sólida de toma de requerimientos, las fases consecuentes tendrán un tiempo menor en el desarrollo del sistema, es por eso que se decidió optar por esta metodología, ya que se contempla atender en un cien por ciento las primeras tres fases en el TT1 y tratar de optimizar al máximo el tiempo en las últimas dos fases que contemplan el TT2.

Herramientas de desarrollo

- Visual Studio Code: Editor de texto de código abierto desarrollado por Microsoft para Windows, Linux y MacOS.
- React: Es una biblioteca de Javascript de código abierto desarrollada por Facebook cuya principal ventaja es el desarrollo de aplicaciones web modulares basada en componentes, también ofrece un flujo claro de datos.

- Django-REST Framework: Es una herramienta que usa el lenguaje de programación python que facilita el desarrollo de API 's para ser consumidas en diferentes entornos ya sea una aplicación web o un dispositivo móvil.
- MySQL: Es un sistema gestor de base de datos relacionales de código abierto que implementa una arquitectura de tipo cliente/servidor.
- DataTable : Plugin de Javascript utilizado en la presentación de información en tablas, capaz de paginar un volumen grande de entradas así como también tener funcionalidades de filtros de búsqueda.
- Azure: Plataforma de Microsoft que ofrece microservicios fácilmente escalables en la nube, con los cuales es posible sacar a producción aplicaciones web desarrolladas con diferentes entornos de programación.

Diseño:

- Bootstrap: Bootstrap es una biblioteca multiplataforma o conjunto de herramientas de código abierto para el diseño de sitios web.
- CSS: Hojas de estilo personalizadas a un sistema institucional.

Repositorio:

- GitHub: GitHub es un servicio web de control de versiones y desarrollo de software colaborativo basado en Git.

6. Cronograma

Nombre del alumno(a): Cruz Pérez Raúl Eduardo TT No.: 2021-A080
Título del TT: Sistema gestor de protocolos de investigación para la Escuela Superior de Cómputo

Cronograma TT 1

Cronograma	Inicio	Fin	Agosto	Septiembre	Octubre	Noviembre	Diciembre
Especificación reglas de negocio	16-ago-21	24-ago-21					
Toma de requerimientos funcionales	22-ago-21	08-sep-21					
Diagrama de casos de uso	09-sep-21	23-sep-21					
Diagrama de clase	23-sep-21	04-oct-21					
Mockups	05-oct-21	15-oct-21					
Creación de la BD	16-oct-21	03-nov-21					
Diseño de la página web	04-nov-21	30-nov-21					
Presentación TT1	01-dic-21	21-dic-21					

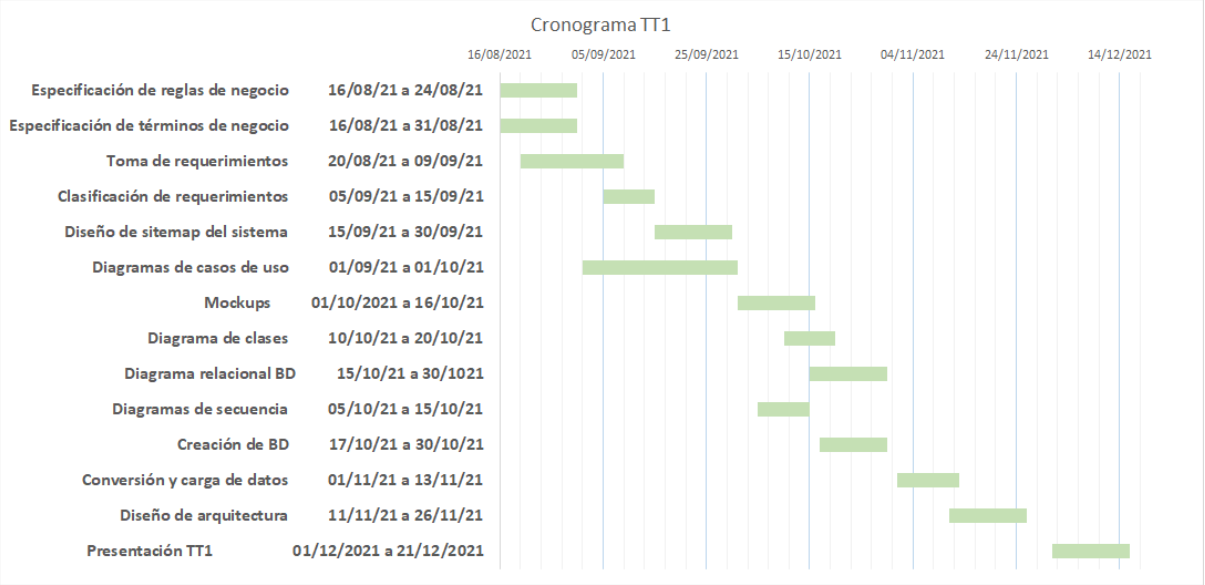
Cronograma Agosto-Diciembre 2021

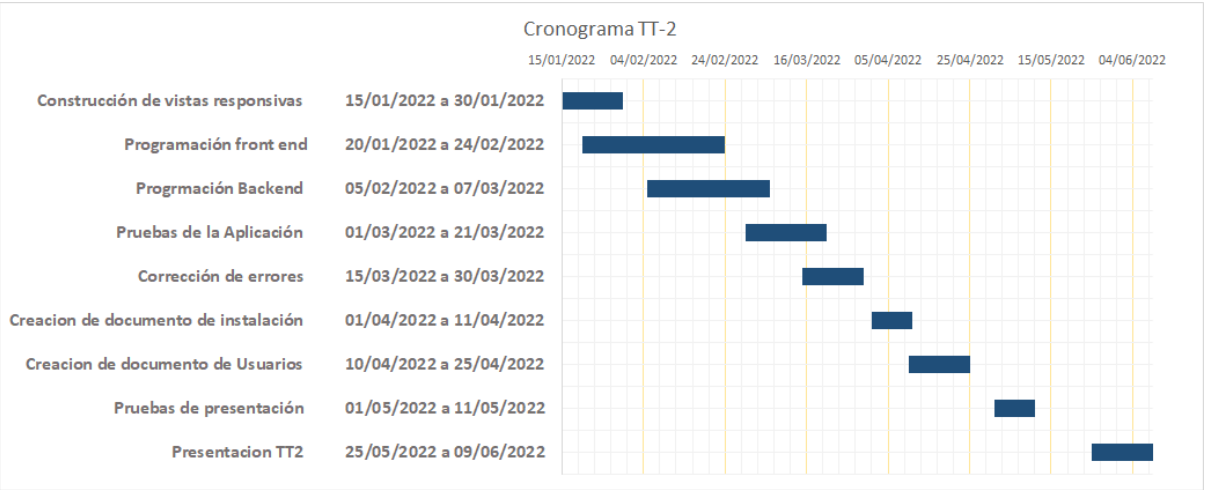
Cronograma TT 2

Cronograma	Inicio	Fin	Enero	Febrero	Marzo	Abril	Mayo	Junio
Programación del Back End	17-ene-22	31-mar-22						
Conexión de la BD	15-mar-22	31-mar-22						
Pruebas	01-abr-22	21-abr-22						
Corrección de errores	22-abr-22	10-may-22						
Alojamiento del servidor	11-may-22	16-may-22						
Manual de usuario	10-may-22	31-may-22						
Presentación TT2	25-may-22	09-jun-22						

Cronograma Enero-Junio 2022

Nombre del alumno(a): Bernal Leocadio Josué Eduardo TT No.: 2021-A080
Título del TT: Sistema gestor de protocolos de investigación para la Escuela Superior de Cómputo





6. Referencias

[1]Universidad Politécnica de Valencia(Área de Sistemas de la Información y las Comunicaciones-Certificados Digitales) https://www.upv.es/contenidos/CD/info/711250normalc.html

[2] Comisión Académica de Trabajos Terminales, ESCOM-IPN[Online]. Recuperado de: https://www.escom.ipn.mx/htmls/escomunidad/catt.php

[3] Benito Carrillo Azahara, abril 2021, viaFirma[Online]. Recuperado de: https://www.viafirma.com/blog-xnoccio/es/diferencias-entre-certificado-digital-y-firma-digital/

[4] Gerónimo Vargas Luis Ángel & Rodríguez Méndez Oscar Eduardo, Herramienta de Apoyo para la asignación de protocolos de TT (Trabajo Terminal TT 2014-A047). Instituto Politécnico Nacional, Escuela Superior de Cómputo 2015, ESCOM-IPN[Online]. Recuperado de: https://tesis.ipn.mx/bitstream/handle/123456789/20433/Reporte%20Tecnico%20Final.pdf?sequence=2&isAllowed=y

[5] Autofirma[Online]. Recuperado de: https://firmaelectronica.gob.es/Home/Descargas.html

[6] Wondershare PDFelement[Online]. Recuperado de: https://pdf.wondershare.net/es/

[7] SAT [Online]. Recuperado de:

Daniel
Hernandez
tel.
hernandez_01@alumno.ipn.mx
Boleta 2019000001

Sello digital

MDSLP/1Ep2t1hUDfTB1athfSFBltzyYiNzGG7G+kL74xxTgkIFmqc4ICv/GKfdCxWf69e9PuD3tLpR2uZb8td0VX+enVr4y2I54H83wvx+Nh0MSPD7QoGhi/PYRqRkBBlrpWVHsyloF6Mqiqt2Ghht9KhXZtwqy6BKpEUW71VG+p7QaccRnbWZIRqnnsD3S7vYE07JmKJdl6kEcYwlBz0eya5G0dulLrP+T0um4l166sRPSpKV8B20q31f5sSEA/cqANvzYJ/JdkwHkGkzImk0AAFc8jdOAgpl1HJj5jhX1bHiz4f22MR5xu5mh5KCve6P2UkMpoFUjAweVRJoZbvA==

Pedro
Goméz
tel.
pedro_gmz700@ipn.mx
Boleta

Sello digital

Az3J3y1DAiw2RZJ17wrLsr4uBOv/0H9/15rmUvQDZEIkyhhP3Y/MIG+iHO5CwP6eN5xKzigJlxv54Gd/WVL4fspRwUuVDMt7OpOZ39wN7ugQaawsae45jyDn/EZ7XA0Azuya6dYBwqhUw1hR27zwiJAFKY68m4WI3UpZIGTrsNct5ha9vxsX7vHSUc5fcfUFQMZXzQ16/3/yqZO1I+HdqKv1gtBVExvrE1a3DK+4Scl33hBC3P7PVzow/7HVT6H3o+DL0D0bK1v2BR4kKA7ZYRQ7GS1ixoKY1NYlKCAVuXHppXlOzcZVJ3nj0AtyhSpBqToh/Z5NRF3CvJeAVxuJmw==