Articulo Original Páginas: 24-29 ISSN
Paradigma Volumen XXII Abril 2021

Sistema De Elaboración, Aprobación, Seguimiento Y Ejecución Del Plan Operativo Anual Implementando Token De Autenticación Digital

JUNIOR
Ing. Luis Fernando Boyan Herrera
Carrera de Ingeniería de Sistemas Escuela Militar de Ingeniería
La Paz, Bolivia
lfboyan@gmail.com

Elaboration, approval, monitoring and implementation system of the annual operational plan implementing digital authentication token

Resumen.- El presente artículo trata sobre el sistema de elaboración, aprobación, seguimiento y ejecución del Plan Operativo Anual, para agilizar los procedimientos e incrementar los niveles de seguridad que requieren mediante un token de autenticación digital implementado en una aplicación móvil que permitirá reguardar la información bajo los criterios de integridad, confidencialidad y disponibilidad. Este sistema se basa en los procedimientos del Plan Operativo Anual del Gobierno Autónomo Municipal de El Alto.

Palabras claves *– token de autenticacion, integridad, confidencialidad, disponibilidad, aplicación móvil*

Abstract - This article deals with the elaboration, approva, monitoring and implementatioin system of the annual operational plan to streamline procedures and increase the levels of security required by means of a digital authentication token implemented in a mobile application that will allow the information to be stored under the integrity, confidentiality and availability criteria. This system is based on the procedures of the Annual Operational Plan of the Municipal Autonomous Government of El Alto

Keywords *– Authentication token, integrity, confidentiality, availability, mobile application*

I. INTRODUCCIÓN

La seguridad de la información engloba un conjunto de técnicas y medidas para controlar todos los datos que se manejan dentro de una institución y hoy en día es uno de los requerimientos más importantes ya que en la mayoría de las aplicaciones y servicios que se brindan a la ciudadanía, no se toman en cuenta medidas de seguridad. La seguridad de la información permite resguardar y proteger la identificación, valoración y gestión de los activos de información en función del impacto que representan para una institución.
Una de las ramas de la seguridad de la información es la criptografía, que estudia los algoritmos utilizados para ocultar o resguardar la información. La criptografía tiene como finalidad autenticar la identidad de los usuarios y proteger el sigilo de comunicaciones personales y de transacciones comerciales y bancarias, entre otras.

La elaboración del Plan Operativo Anual (POA) es una tarea que todos los habitantes en un Municipio deben encarar y del cual todos son Responsables. Para una mejor Planificación, la elaboración del POA permite lograr acuerdos sobre los proyectos en los que se va a invertir los recursos en el año próximo. Por ello, el Gobierno Autónomo Municipal de El Alto y sus distintas Direcciones convocan a participar de cumbres para Planificar el Plan Operativo Anual, es importante la asistencia de cada habitante; es la única manera de lograr que el Plan Operativo Anual represente las demandas de los habitantes del Distrito.

El Plan Operativo Anual (POA) es un instrumento de gestión que permite realizar distintas actividades, como ser:

- Identificar los objetivos y metas de un Municipio o institución.
- Definir las operaciones necesarias para el cumplimiento del Plan Operativo Anual.
- Determinar los recursos y el tiempo de ejecución para cada operación (proyectos y actividades).
- Designar responsables para el desarrollo de las operaciones.

- Establecer indicadores de eficiencia y eficacia.

II. ANTECEDENTES Y JUSTIFICACION TEORICA

La Dirección de Educación del Gobierno Autónomo Municipal de El Alto está encargada de las Unidades de Equipamiento, Infraestructura y Planes Educativos. En base a lo descrito anteriormente referente a la elaboración y aprobación del Plan Operativo Anual, este consta de 3 partes fundamentales que son los programas, proyectos y actividades.

La elaboración de un Plan Operativo Anual en el Gobierno Autónomo Municipal de El Alto se lleva a cabo mediante llaves presupuestarias que están diferenciadas por distintos componentes.

Este procedimiento se realiza independientemente en cada dirección y Unidad. Hoy en día tanto el Gobierno Autónomo Municipal de El Alto tiene mucha demora en la elaboración y aprobación del Plan Operativo Anual por que el procedimiento es manual lo que genera molestia y malestar en los habitantes de los distintos distritos. La Dirección de Educación maneja los procesos de elaboración, aprobación, seguimiento y ejecución del Plan Operativo Anual de manera manual, tanto en el seguimiento y seguridad del mismo. Los procesos para realizar el Plan Operativo Anual emplean herramientas básicas en computación para agilizar la aprobación esto cubre un 30% del proceso en general, sin embargo, el proceso continúa siendo en un 70% manual según las entrevistas realizadas a los Responsables de elaboración, aprobación, seguimiento y ejecución del Plan.

El actual manejo de la información y de los procesos de Planificación del Plan Operativo Anual, tienen niveles bajos de seguridad en la manipulación de la documentación como también pérdida de tiempo en su elaboración. La continuidad del problema no permitirá la integración global de la información, fácil manejo o seguridad de esta, ya que se seguirá trabajando con herramientas básicas como Office Word, Office Excel u hojas manuscritas.

Como problemática principal tenemos que, los actuales procesos de elaboración, aprobación, seguimiento y ejecución del Plan Operativo Anual en la Dirección de Educación del Gobierno Autónomo Municipal de El Alto provocan modificaciones y solicitudes no autorizadas de la información.
Los problemas secundarios que se presentan son

- La gestión de documentos acerca de los programas, proyectos y actividades se presenta de manera desordenada, lo que provoca un mal manejo de información presentada en el proceso de elaboración, posterior aprobación y seguimiento.
- La Planificación y estructura programática del Plan Operativo Anual es parcialmente manuscrita lo que origina retrasos en sus distintas etapas de elaboración.
- Las distintas modificaciones revelan un bajo nivel de seguridad que daña la integridad de la documentación presentada y la malversación del presupuesto de un Distrito.

III. OBJETIVOS Y ALCANCE

Considerando las justificaciones dadas el objetivo principal del artículo es, Desarrollar un sistema de elaboración, aprobación, seguimiento y ejecución del Plan Operativo Anual implementando un token de autenticación digital que permita la modificación y autorización de solicitudes incrementando los niveles de seguridad en la Dirección de Educación del Gobierno Autónomo Municipal de El Alto.
Para apoyar el cumplimiento del objetivo principal nos planteamos objetivos secundarios mencionados a continuación:

- Analizar la situación actual de la gestión de documentos acerca de los programas, proyectos y actividades en la elaboración, aprobación, seguimiento y ejecución del Plan Operativo Anual para determinar los requerimientos del sistema.
- Diseñar el sistema de elaboración, aprobación y seguimiento del Plan Operativo Anual de acuerdo a la Planificación y estructura programática para agilizar los procesos de elaboración, aprobación y seguimiento.
- Diseñar un token de autenticación digital que emplee criterios de encriptación y autenticación para asegurar la integridad en los procesos de aprobación del Plan Operativo Anual
- Realizar pruebas de la integración del sistema de elaboración, aprobación y seguimiento del Plan Operativo Anual con el token de autenticación digital.

El sistema y token de autenticación digital están dirigidos al Gobierno Autónomo municipal de El Alto y todas sus dependencias. Las pruebas que se realizara serán tomadas del plan operativo anual de la gestión 2019.

IV. METODOLOGIA PROPUESTA

Para el desarrollo del token de autenticación digital se plateo el uso de la metodología ágil de desarrollo de Apis (MADA), presentada recientemente para el desarrollo de Apis de autenticación el cual consiste en lo siguiente:

Fase 1 Análisis Abordó las siguientes tareas.

1.1 Estudio de los algoritmos de encriptación.
Para comprender la formulación del problema identificado, es necesario realizar un estudio del ámbito de aplicación del token de autenticación digital, esto también permitirá realizar una identificación inicial de las variables evidénciales o, de entrada y la determinación del algoritmo adecuado para el desarrollo de la Api. Para ello se realizó una entrevista a los responsables de la elaboración del Plan Operativo Anual para identificar los procesos los cuales requieren de mayor nivel de seguridad y en los que se emplearía el token de autenticación para resguardar la disponibilidad, integridad y confidencialidad de la documentación que presenta el POA.
1.2 Análisis del nivel de seguridad actual.
Se realizó un análisis de riesgos para determinar el nivel de seguridad que tiene el sistema manual de elaboración, aprobación, seguimiento y ejecucion del plan Operativo Anual, como se observa en la Tabla 1.

TABLA 1.
ANALISIS DE RIESGOS

Amenazas Sobre la documentación del poa	Determinar	DISPONIBILIDAD	
	Frecuencia	IMPACTO	IMPACTO X FRECUENCIA
Plan operativo anual			
Sistema manual del poa		46.6666667	36.16666667
Aprobacion no autorizada	0.9	50	45
Modificacion no autorizada	0.3	50	15
Almacenamiento de la informacion	0.9	50	45
Copias o reproduccion	0.9	40	36
Acceso a la documentacion	0.9	40	36
Traslado de documentacion	0.8	50	40

Fuente: Elaboración Propia.

Fase 2 Diseño Esta fase abordó los puntos para el diseño del token de autenticación digital:

2.1 Elección del algoritmo de encriptación
Se realizó un análisis comparativo entre los algoritmos de encriptación para realizar la autenticación (simétrica, asimétrica y hibrida), se escogió el algoritmo de encriptación hibrida debido a que es el algoritmo con el cual podemos manejar de manera óptima los procesos de aprobación y ejecución del Plan Operativo Anual.
2.2 Identificación de variables de entrada y salida
Consistió en determinar las variables de entrada del token de autenticación digital, las cuales son las siguientes: id. De usuario, rol de usuario y correo electrónico
La variable de salida es el token de aprobación.
2.3 Selección de variables evidenciales
Se menciona que en esta tarea se debe determinar los atributos de cada variable identificada en el anterior punto, siendo los siguientes, id. de usuario(hash), rol de usuario(string) y correo electrónico(string).
2.4 Definición de la arquitectura del token
Se estableció una serie de condiciones que son parte de la arquitectura del token de autenticación digital que están plasmadas en las siguientes tablas. En la Tabla 2 de realiza una descripción de alto nivel de la Api.

TABLA 2.
DESCRIPCIÓN DE ALTO NIVEL

DATO	DESCRIPCIÓN	TIPO
ID EXTERNO	Identificador del usuario en la API y en otros sistemas	String
CONTRASEÑA	Contraseña del usuario	Hash
USUARIO	Nombre del usuario	String
ROL	Rol del usuario	String
ACESSOS	Acceso restringido del sistema y API	Hash

Fuente: Elaboración Propia.

En la tabla 3 observamos la descripción técnica que tendrá nuestra Api, lo que llega a ser el token de autenticación digital.

TABLA 3.
DESCRIPCIÓN TÉCNICA DE API

CONCEPTO	DEFIINCION
URL	www.Easet-gamea.com
Requiere autenticacion	Authorization
Formato de la peticion	JWT
Formato de respuesta	JWT
Métodos http	POST
Objeto de entrada	Id usuario
Objeto devuelto	Respuesta por token
Documentación	Reporte poa

Publico o privado	Privado
Parámetro de autenticacion	Id usuario
Formato de la API	rest
Seguridad de la api	Hash oauth2
Api manager	apigee

Fase 3 Desarrollo Se realizaron las tareas referentes a la construcción de la red neuronal:

3.1 Determinación de datos de aprendizaje

Se realizaron tablas de valores entradas y salidas deseadas para el desarrollo del token de autenticación digital Estos datos se ingresaron al desarrollo del token de autenticación en sus distintas etapas

3.2 Construcción del token de autenticación digital

Se lo construyo a través del diseño de JASON WEB TOKEN (JWT), en las que podemos observar en la figura 1 sus partes específicas.

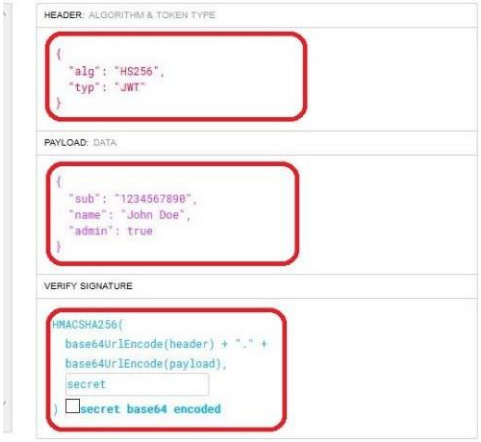

Figura 1. *Partes de JWT*

Una vez construido el token de autenticación digital se procedió a realizar pruebas con el mismo, para verificar los resultados, que s muestra en la siguiente tabla.

TABLA 4.
PRUEBAS DE TOKEN

CASO DE PRUEBA UNITARIA	
NOMBRE:	Prueba del token de autenticacion digital
DESCRIPCIÓN:	Prueba para verificar el registro, visualización y aprobacion de plan operativo anual
CONDICIONES DE EJECUCIÓN:	Estar autenticado como usuario
ENTRADA/PASOS DE EJECUCIÓN:	ingresar al token de autenticacion aprobar plan operativo anual elaborar observacion aprobar ejecucion de programas, proyectos y actividades enviar informe poa presupuesto aprobado a sistema
RESULTADO ESPERADO:	ingreso a la aplicación y envió de informes aprobación de plan operativo anual mediante token aprobar ejecución de plan operativo anual mediante token aprobar y visualizar informes de seguimiento de programas, proyectos y actividades.
OBSERVACIONES:	El módulo continúa en desarrollo y no cumple con todas las especificaciones.
EVALUACIÓN DE LA PRUEBA:	Prueba satisfactoria

Fuente: Elaboración Propia.

V. EXPERIMENTOS Y RESULTADOS

Se realizaron las pruebas del token de autenticación en conjunto con el sistema de elaboración, aprobación, seguimiento y ejecución del plan operativo anual.
Fuente: Elaboración Propia.
Como se puede verificar los resultados del token de autenticación digital son satisfactorias para los procesos de aprobación y ejecución

VI. CONCLUSIONES Y TRABAJO A FUTURO

Una vez desarrollado el sistema y token de autenticación se llegaron a las siguientes conclusiones:

- Se realizó el análisis de la situación bajo la cual trabaja actualmente el GAMEA en el Plan Operativo Anual, identificando los principales procesos que se realiza como se detalla en el Capítulo 4 en su punto 4.2 Análisis de la situación actual.
- El análisis y diseño del sistema se lo realizó trabajando con la metodología SCRUM, lo que permitió llevar un control constante del avance durante todo el proceso de desarrollo del proyecto.
- Se desarrolló el sistema de elaboración, aprobación, seguimiento y ejecución del Plan Operativo Anual permitiendo el acceso de acuerdo a los roles identificados para que los usuarios puedan acceder a la información de dicho procedimiento en el que se encuentra el Plan Operativo Anual
- Se realizó el análisis del token de autenticación y sus métodos de encriptación, escogiendo al

JASON WEB TOKEN, como idónea para su aplicación en el sistema debido a sus características vistas.

- El sistema permite a los usuarios generar reportes de los distintos procesos mencionados de forma inmediata, haciendo que acelere la aprobación y ejecución del Plan Operativo Anual.

Las recomendaciones de acuerdo a lo mostrado son:

- Se recomienda analizar procesos secundarios del Plan Operativo Anual para realizar una documentación más completa e integrarla al sistema
- Se recomienda seguir el manual de usuario del administrador para instalar el sistema en los servidores de la institución y el manual de usuario ante la presencia de dudas o inquietudes que surjan durante el uso del sistema por los diferentes tipos de usuario.
- En la aplicación del token de autenticación se recomienda analizar constantemente las nuevas técnicas, para resguardar mejor la información ante los nuevos ataques informáticos.
- Por seguridad se recomienda realizar copias de respaldo de la base de datos diariamente y reportes de las pruebas realizadas al sistema, por el tipo de información que se almacena

AGRADECIMIENTOS

El presente trabajo fue realizado bajo la supervisión de la Lic. Msc. Claudia Yañiquez Magne, Lic. Cynthia Rodriguez Canaviri, Cnl. Leopoldo Ibañez y Cnl. Julio Cesar Narvaez Tamayo a quienes me gustaría expresar mi más profundo agradecimiento por la colaboraron en el estudio brindando tutela durante todas las fases de desarrollo del sistema y token de autenticación digital.

Referencias

[1] Alvarez, m. A. (2018). Desarrollo web. Obtenido de desarrollo web.

[2] Azaustre, c. (7 de febrero de 2015). Carlosazaustre.es. Obtenido de https://carlosazaustre.es/que-es-la- autenticacion-con-token/

[3] Beekman, g. (2004). Intrroduccion a la informatica. Prentice hall.

[4] Blancarte, o. (8 de junio de 2017). Oscarblancarteblog. Obtenido de https://www.oscarblancarteblog.com/2017/06/08/autenticacion-con-json-web-tokens/

[5] Blog sgsi. (26 de enero de 2017). Obtenido de blog sgsi: https://www.pmg-ssi.com/2017/01/seguridad-de-la- informacion/

[6] Garcia, j. B. (13 de 07 de 2018). Arsys internet. Obtenido de https://www.arsys.es/blog/programacion/autenticacion-api-rest-token/

[7] Garcia, j. M. (7 de julio de 2018). Arsys. Obtenido de https://www.arsys.es/blog/programacion/autenticacion-api-rest-token/

[8] Garzas, j. (2014). Https://blog.conectart.com. Obtenido de https://blog.conectart.com/metodologias-agiles/

[9] Ionos españa. (9 de agosto de 2019). Obtenido de ionos españa: https://www.ionos.es/digitalguide/servidores/seguridad/todo-sobre-los-metodos-de-encriptado/

[10] Menzinsky, a. (2016). Que informaciones son necesarias y utiles para las historias de usuarios.

[11] Nicteja, c. (2019). Fandom. Obtenido de fandom: https://seguridad-priv-y-medidas-de-prevencion-en-la-inf.fandom.com/es/wiki/seguridad,_privaciidad_y_medidas_de_prevenci%c3%93n_de_las_diferentes_tipos_de_amenazas_inform%c3%81ticas

[12] Pressman, r. (2005). Ingenieria de software un enfoque practico. Mexico: mc-graw hill.

[13] Scrum manager. (2016). Obtenido de https://www.scrummanager.net/bok/index.php?title=file:incremento_iterativo_e_incremento_continuo.Jpg

[14] Scrum master. (2016). Obtenido de https://www.scrummanager.net/bok/index.php?title=pila_del_sprint

[15] Sgsi. (16 de enero de 2017). Obtenido de sgsi: https://www.pmgssi.com/2017/01/seguridad-de-la-informacion/

[16] Simmons. (19 de 5 de 2017). Obtenido de https://es.wikipedia.org/wiki/criptograf%c3%ada_asim%c3%a9trica#cite_ref-simmons_1-0

[17] Simmons, g. J. (1992). A survey of information authentication. New york: gj simmons.

[18] Arras vota, a. M. (2010). Comunicación organizacional. Chihuahua, méxico: uach.

[19] Cortés c., m. E., & iglesias l., m. (2004). Generalidades sobre la metodología de la investigación. Ciudad del carmen, campeche, méxico: unicersidad autónoma del carmen.

[20] Firebase. (20 de abril de 2019). Recuperado el 20 de abril de 2019, de firebase (documentación para desarrolladores): https://firebase.google.com/docs/

[21] Fundetic. (2018). Acerca de nosotros. Recuperado el 6 de abril de 2019, de sitio web de fundetic: https://www.fundeticbolivia.org/site/index.php/acerca-de-nosotros/acerca-de-nosotros

[22] Gallego s., a. J. (2019). Manual de introducción a ionic. España.

[23] Lucidchart. (2019). Recuperado el 8 de abril de 2019, de tutorial de diagrama de clases uml: https://www.lucidchart.com/pages/es/tutorial-de-diagrama-de-clases-uml

[24] Menzinsky, a., lopez, g., & palacio, j. (2018). Historias de usuario: ingeniería de requisitos ágil. Scrum manager.

[25] Mobile-d. (2004). Recuperado el 11 de abril de 2019, de moblie-d: http://agile.vtt.fi/mobiled.html

[26] Muradas, y. (23 de marzo de 2018). Recuperado el 11 de abril de 2019, de sqlite para android: la herramienta definitiva: https://openwebinars.net/blog/sqlite- para-android-la-herramienta-definitiva/

[27] Pinelo, d. (2009). Introducción a uml. Recuperado el 11 de abril de 2019, de introducción a uml: https://moodle2.unid.edu.mx/dts_cursos_mdl/pos/ti/is/am/10/introduccion_uml.pdf

[28] Pressman, r. (2010). Ingenieria de software: un enfoque práctico. Mexico, d. F.: mc graw hill.

[29] Ramirez v., r. (2017). Métodos para el desarrollo de aplicaciones móviles. Cataluña: universitat oberta de catalunya.

[30] Rouse, m. (20 de 04 de 2019). Recuperado el 12 de abril de 2019, de base de datos relacional: https://searchdatacenter.techtarget.com/es/definicion/base-de-datos-relacional

[31] Rumbaugh, j., jacobson, i., & booch, g. (2000). El lenguaje unificado de modelado: manual de referencia, spanish edition. Madrid: addison wesley.

[32] Schwaber, k., & sutherland, j. (2016). La guìa de scrum.

[33] Scrum institute. (2019). Recuperado el 9 de abril de 2019, de the scrum product backlog: https://www.scrum-institute.org/the_scrum_product_backlog.php

[34] Scrum manager. (abril de 2019). Obtenido de modelo original de scrum para desarrollo de software: https://www.scrummanager.net/bok/index.php?title=modelo_original_de_scrum_para_desarrollo_de_software

[35] Sommerville, i. (2011). Ingeniería de software, 9na edición.México d.f.: pearson.

[36] Von bertalanffy, l. (1968). General system theory, foundations, development, aplications. New york: george brazilier.

[37] Web1. (2018). Recuperado el 10 de abril de 2019, de diagrama de componentes: https://es.wikipedia.org/wiki/diagrama_de_componentes

[38] Web2. (2015). Recuperado el 11 de abril de 2019, de ¿qué es scrum?: https://queondara.readthedocs.io/en/latest/scrum.html

[39] Web3. (20 de abril de 2019). Recuperado el 12 de abril de 2019, de sistemas operativos móviles: ios: http://eve-ingsistemas-u.blogspot.com/2012/04/sistemas-operativos-moviles-ios.html

Fecha de Envió del Articulo: 29/10/2020
Fecha de Aceptación de artículo: 15/11/2020