



UNIVERSIDAD TÉCNICA DEL NORTE

INSTITUTO DE POSTGRADO

MAESTRÍA EN INGENIERÍA DE SOFTWARE

**“INCIDENCIA DEL USO DEL REPOSITORIO DE FIRMAS DIGITALES EN LA
GESTIÓN DE TRÁMITES INSTITUCIONALES DE LA UNIVERSIDAD
TÉCNICA DEL NORTE”**

Trabajo de Investigación previo a la obtención del Título de Magíster en Ingeniería de Software

Autor: Ing. Tobías Ramiro López Ruiz

Tutor: Msc. Diego Trejo

IBARRA, ECUADOR. 2018

APROBACIÓN DEL TUTOR

“En calidad de Tutor del Trabajo de Grado presentado por el ingeniero Tobías Ramiro López Ruiz, para optar por el grado de Magíster en Ingeniería de Software, doy fe de que dicho trabajo reúne los requisitos y méritos suficientes para ser sometido a presentación (pública o privada) y evaluación por parte del jurado calificador que se designe”.

MSC. DIEGO TREJO

A handwritten signature in blue ink, appearing to be 'D. Trejo', is written over a light blue rectangular background. The signature is fluid and cursive.

IBARRA, 31 DE MAYO DE 2018

FIRMA

Aprobación del Jurado

“INCIDENCIA DEL USO DEL REPOSITORIO DE FIRMAS DIGITALES EN
LA GESTIÓN DE TRÁMITES INSTITUCIONALES DE LA UNIVERSIDAD
TÉCNICA DEL NORTE”

Por: Ing. Tobías Ramiro López Ruiz

Trabajo de Grado de Maestría aprobado en nombre de la Universidad Técnica del Norte,
por el siguiente jurado, a 31 de mayo de 2018.



MSc. Alexander Guevara



MSc. Mauricio Rea



MSc. Daysi Imbaquingo

DEDICATORIA

A mi familia: Dayanara, Piedad, Ismael, Efrén, Aimee.

Por su amor y paciencia en esta etapa de mi vida.

AGRADECIMIENTO

A todos, quienes me apoyaron en la consecución de esta meta. A los docentes que compartieron sus experiencias y enseñanzas. Especialmente al Msc. Diego Trejo, tutor de este trabajo, por su ayuda y seguimiento del mismo. Al Ing. Juan Carlos García, Director de Desarrollo Tecnológico e Informática de la U.T.N. por su aporte a la parte práctica y principal beneficiario institucional. De forma especial a: Msc. Daysi Imbaquingo, Msc. Alexander Guevara y Msc. Mauricio Rea por su especial interés en la revisión del documento.

A los funcionarios de la DDTI en especial a Gabriela Cardenas y María Fernanda Rivera quienes facilitaron la implementación del software y las pruebas prácticas; a Lic. Samia Bedon y Ab. Angélica Espinosa por concederme audiencia para entrevistas sobre uso del QUIPUX en la UTN.

A mi familia por su infinito amor y paciencia, a la Msc. Carolina Torres por su comprensión respecto al uso del tiempo para la redacción de este documento.

BIBLIOTECA UNIVERSITARIA

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

La Universidad Técnica del Norte, dentro del proyecto Repositorio Digital Institucional, determinó la necesidad de disponer de textos completos en formato digital con la finalidad de apoyar los procesos de investigación, docencia y extensión de la Universidad.

Por medio del presente documento dejo sentada mi voluntad de participar en este proyecto, para lo cual pongo a disposición la siguiente información:

1. IDENTIFICACIÓN DE LA OBRA

DATOS DE CONTACTO	
CEDULA DE IDENTIDAD:	1002176905
APELLIDOS Y NOMBRES:	López Ruiz Tobías Ramiro
DIRECCIÓN:	La Esperanza, carrera Galo Plaza 17-28
EMAIL:	ingtobiaslopez@gmail.com
TELÉFONOS:	Fijo: 2660236 Móvil: 0986508155

DATOS DE LA OBRA	
TÍTULO:	Incidencia del uso del repositorio de firmas digitales en la gestión de trámites institucionales de la Universidad Técnica del Norte
AUTORES:	López Ruiz Tobías Ramiro
FECHA:	31 de mayo de 2018
PROGRAMA:	POSTGRADO
SOLO PARA TRABAJOS DE GRADO	
TÍTULO POR EL QUE OPTA:	Magíster en Ingeniería de Software
ASESOR:	Msc. Diego Trejo

2. AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD

Yo, Tobías Ramiro López Ruiz, con cédula de ciudadanía número 100276905, en calidad de autor y titular de los derechos patrimoniales de la obra o trabajo de grado descrito anteriormente, hago entrega del ejemplar respectivo en formato digital y autorizo a la Universidad Técnica del Norte, la publicación de esta obra en el Repositorio Digital Institucional y uso del archivo electrónico en la Biblioteca Universitaria con fines académicos, para ampliar la disponibilidad del material y como apoyo a la educación, investigación y extensión; en concordancia con la Ley de Educación Superior Art. 144

3. CONSTANCIAS

El autor manifiesta que esta obra es original, se respetaron derechos de autor a terceros, por lo tanto es el titular de los derechos patrimoniales, por lo que asume la responsabilidad sobre el contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a 31 de mayo de 2018.

.....

Tobías Ramiro López Ruiz

CI 1002176905



CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE GRADO A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

Yo, Tobías Ramiro López Ruiz, con cédula de ciudadanía número 100276905 manifiesto mi voluntad de Ceder a la Universidad Técnica del Norte los derechos patrimoniales consagrados en la Ley de Propiedad intelectual del Ecuador vigente, artículos 4,5 y 6, en calidad de autor del trabajo de grado denominado INCIDENCIA DEL USO DEL REPOSITORIO DE FIRMAS DIGITALES EN LA GESTIÓN DE TRÁMITES INSTITUCIONALES DE LA UNIVERSIDAD TÉCNICA DEL NORTE que ha sido desarrollado para optar por el título de Magíster en Ingeniería de Software, en la Universidad Técnica del Norte, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente sobre esta obra.

.....

Ingeniero Tobías Ramiro López Ruiz

CI 1002176905

UNIVERSIDAD TÉCNICA DEL NORTE

INSTITUTO DE POSGRADO

PROGRAMA DE MAESTRÍA

*“INCIDENCIA DEL USO DEL REPOSITORIO DE FIRMAS DIGITALES EN LA
GESTIÓN DE TRÁMITES INSTITUCIONALES DE LA UNIVERSIDAD TÉCNICA DEL
NORTE”*

Autor: Ing. Tobías Ramiro López Ruiz

Tutor: Msc. Diego Trejo

Año: 2018

RESUMEN

Con la existencia del Habeas Data en la Constitución ecuatoriana y la Ley de Comercio Electrónico, el Banco Central del Ecuador es responsable de emitir y validar Firmas Electrónicas para realizar cualquier intercambio de datos en que se requiera que haya validez legal. La Universidad Técnica del Norte, en adelante UTN, se encuentra implementando nuevas tecnologías de comunicación e información mediante la evolución de sus procesos institucionales para atender adecuadamente a sus estudiantes. QUIPUX es un software para la gestión documental que no cumple con los requisitos para integrarlo al Sistema Integrado de Información Universitaria de la UTN, cuyo acrónimo es SIIU. Implementar un software de servicios de firmas digitales para incidir positivamente en al menos un proceso de la gestión de trámites institucionales: EMISIÓN DE CERTIFICADOS DE MATRÍCULA FIRMADOS DIGITALMENTE EN LA UTN. Documentar la SRS según el estándar ISO / IEC 29148. Diseñar una arquitectura de software y un conjunto de algoritmos para firmar o validar certificados mediante X.509, usar SOAP o JDBC para relacionar servicios del repositorio de firmas digitales con el SIIU, cumpliendo algunas normas de usabilidad y seguridad aplicables según ISO 9126. Existe: Un documento SRS acorde con ISO 29148, una interface para firmar y validar certificados, respuestas estudiantiles de aceptación del software implementado, certificados de matrícula con validez legal nacional. Al reducir tiempos de respuesta y consumo de papel, automatizando con software algunas tareas repetitivas de certificación entonces el uso del repositorio de firmas digitales incide positivamente en la gestión de trámites institucionales.

PALABRAS CLAVE: Habeas Data, Repositorio de firmas digitales, Sistema Integrado de Información Universitaria, Certificados de Matrícula, ISO 29148, ISO 9126, X.509, SOAP, JDBC, XML, Incidencia del Software, Gestión de Trámites Institucionales, BPM, UTN.

UNIVERSIDAD TÉCNICA DEL NORTE

INSTITUTO DE POSGRADO

PROGRAMA DE MAESTRÍA

*“INCIDENCE OF THE USE OF THE DIGITAL SIGNATURES REPOSITORY IN THE
MANAGEMENT OF INSTITUTIONAL PROCEDURES OF THE NORTH TECHNICAL
UNIVERSITY.”*

Author: Engineer Tobias Ramiro Lopez Ruiz

Tutor: MSc. Diego Trejo

Año: 2018

ABSTRACT

With the existence of Habeas Data in the Ecuadorian Constitution and the Electronic Commerce Law, the Central Bank of Ecuador is responsible for issuing and validating Electronic Signatures to perform any data exchange in which it is required to have legal validity. Universidad Técnica del Norte, hereinafter UTN, is implementing new communication and information technologies through the evolution of its institutional processes to adequately serve its students. QUIPUX is a software for document management that does not meet the requirements to integrate it into the University Information Integrated System of the UTN, whose acronym is SIIU. Implement a digital signature services software to positively impact at least one process of the management of institutional procedures: ISSUANCE OF CERTIFICATES OF REGISTRATION SIGNED DIGITALLY IN THE UTN. Document the SRS according to the ISO / IEC 29148 standard. Design a software architecture and a set of algorithms to sign or validate certificates through X.509, use SOAP or JDBC to relate services from the digital signature repository to the SIIU, complying with some applicable usability and security standards according to ISO 9126. There is: An SRS document in

accordance with ISO 29148, an interface to sign and validate certificates, student responses to acceptance of the software implemented, registration certificates with national legal validity. By reducing response times and paper consumption, automating some repetitive certification tasks with software, the use of the repository of digital signatures positively affects the management of institutional procedures.

KEYWORDS: Habeas Data, Repository of digital signatures, Integrated System of University Information, Certificates of Enrollment, ISO / IEC 29148, ISO 9126, X.509, SOAP, XML, Advocacy of the Software, Management of Institutional Procedures, BPM, UTN.

Contenidos

1. ANTEPROYECTO	1
1.1. TEMA	1
1.2. Contextualización del problema	1
1.3. Planteamiento del Problema	3
1.4. Justificación	4
1.5. Formulación del problema	5
1.6. Alcance de los objetivos y lineamientos de valoración de su cumplimiento .	5
1.7. Objetivos	7
1.7.1. Objetivo General	7
1.7.2. Objetivos Específicos	8
2. MARCO REFERENCIAL	9
2.1. CONCEPTUALIZACIÓN	9
2.1.1. Software orientado a servicios de certificación electrónica	9
2.1.2. Firma electrónica y certificado de firma electrónica	10
2.1.3. Gestión de trámites institucionales con firma electrónica	10
2.1.4. Flujos de trabajo de trámites institucionales	11

2.1.5.	Levantamiento de requerimientos de trámites de estudiantes, empleados y Secretario Abogado	12
2.1.6.	Software de servicios del repositorio de firmas digitales de la UTN .	15
2.1.7.	Creación, almacenamiento y uso de las firmas digitales	16
2.1.8.	Peticiones de documentos legales en la UTN	17
2.1.9.	Actividades legales del Secretario Abogado que requieran emitir documentos firmados	17
2.1.10.	Incidencia del uso del Software de certificación electrónica en la Gestión del trámite institucional	18
2.1.11.	Métricas de Impacto del uso de Software en la gestión del trámite institucional de la UTN	22
2.2.	COMPETENCIAS Y LÍNEA DE INVESTIGACIÓN	24
2.3.	FUNDAMENTACIÓN FILOSÓFICA	25
2.4.	ESTADO DEL ARTE	39
2.4.1.	FUNDAMENTACIÓN TEORICA Y CONCEPTUAL DE LA METODOLOGÍA UTILIZADA EN CADA FASE DEL PROYECTO	39
2.4.2.	Requisitos de software. Una revisión sistemática de literatura	42
2.4.3.	Arquitectura de servicios del repositorio de firma digital	42
2.4.4.	Incidencia: Influencia del Software en la comunicación institucional	46
2.4.5.	Métricas de incidencia en aplicaciones orientadas a servicios en la gestión del trámite institucional en la UTN	48
2.5.	PROPOSICIÓN	51
3.	METODOLOGÍA	52
3.1.	Tipo de investigación	52

3.2.	Método de investigación	52
3.3.	Diseño de la investigación	52
3.4.	Modalidad de Investigación	52
3.4.1.	Investigación de campo	52
3.4.2.	Investigación documental bibliográfica	53
3.4.3.	Exploratorio	53
3.4.4.	Descriptivo	53
3.5.	Esquema para el cumplimiento de objetivos	54
3.6.	Variables e indicadores	54
3.6.1.	Técnicas	55
3.6.2.	Instrumentos	56
3.7.	Población	57
3.8.	Fase 1: Determinar los requerimientos del Software para la gestión de servicios de mensajes de datos firmados en la UTN	57
3.9.	Fase 2: Valorar usabilidad y seguridad de alternativas de software para la gestión de servicios de mensajes de datos firmados	58
3.9.1.	Consideraciones de los estudiantes sobre la usabilidad	58
3.10.	Fase 3: Diseñar la Arquitectura del Software para gestión de servicios de mensajes de datos firmados en las dependencias de la UTN considerando su factibilidad de implementación	60
3.10.1.	Descripción del proceso de selección y adaptación de estilos arquitecturales aplicables	60
3.10.2.	DISEÑO MACRO	60
3.10.3.	DISEÑO MICRO	60

3.10.4. EVALUACIÓN	60
3.10.5. IMPLEMENTACIÓN	61
3.11. Fase 4: Desarrollo del conjunto de algoritmos de servicio de firmas digitales dentro de los límites de la infraestructura física y lógica del SIIU (ERP de la UTN)	62
3.12. Fase 5: Relacionar el software de servicios del repositorio de firmas digitales con el ERP institucional integrando componentes más pertinentes según sea el caso	62
4. RESULTADOS Y DISCUSIÓN	64
4.1. RESULTADOS	64
4.1.1. R1: Requerimientos del Software para la gestión de servicios de mensajes de datos firmados en la UTN	64
4.1.2. R2: Valoración de Usabilidad y seguridad del software para la gestión de servicios de mensajes de datos firmados. Atributos de calidad basados en el ISO 9126.	69
4.1.3. R3: Arquitectura del Software de Gestión de Trámites institucionales de la UTN	76
4.1.4. R4: Desarrollo del conjunto de algoritmos del repositorio de firmas digitales	90
4.1.5. R5: Relacionar el software de gestión basado en el ERP con la base de datos de la UTN	94
4.2. DISCUSIÓN	100
4.2.1. Influencia tecnológica	100
4.2.2. Influencia legal	102

5. CONCLUSIONES Y RECOMENDACIONES	103
Bibliografía	108
Anexos	116

Índice de figuras

1.	Una aproximación al documento de SRS segun ISO/IEC 29148	15
2.	Taxonomía de investigación en tecnologías IoT	29
3.	husr	41
4.	9126-3	45
1.	Operacionalización VD	55
2.	Operacionalización VI	55
1.	CU1	66
2.	IMSOAP	67
3.	DISEÑO MACRO	79
4.	Arquitectura BPM GDTUTN	83
5.	ServicioWebUTN	85
6.	FirmasDigitales	85
7.	DocumentosXML	85
8.	WS	89
9.	DEV CLOUDUTN	91
10.	AlgORCL	92
11.	docxml	94

12.	GDTUTN	97
13.	SUBIRFD	98
14.	NROE	99

Índice de cuadros

1.	Actividades del Secretario Jurídico susceptibles de automatización.	21
2.	Métricas de Impacto del uso de Software en la gestión del trámite de la UTN.	23
1.	Verificadores de trazabilidad del software basado en objetivos del proyecto.	53
1.	Resultados encuesta estudiantil. Elaborado por: Autor	74
2.	E6.1.2 Integridad, confidencialidad y no repudio SOAP	74
3.	E6.1.3 ingresa XML y sale XML firmado con X.509	75
4.	USO DEL REPOSITORIO DE FIRMAS DIGITALES EN LA UTN	97

Capítulo 1

ANTEPROYECTO

1.1. TEMA

INCIDENCIA DEL USO DEL REPOSITORIO DE FIRMAS DIGITALES EN LA GESTIÓN DE TRÁMITES INSTITUCIONALES DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1.2. Contextualización del problema

La automatización de tareas es una necesidad de las empresas. La gestión documental está pasando de ser impresa a digital alrededor del mundo. En el sector público grandes volúmenes de información escrita se mueven usando papel autografiado por sus autores, cuyo objetivo es mejorar la atención al ciudadano desde los archivos, según lo expuesto por (Casas-De-Barran, Griffin, Millar, y Roper, 2015; Hernandez, 2016).

En Ecuador, el SRI ha liderado el uso de la firma electrónica, la cual, según un informe trimestral de Amoroso (2015) tenía 12681 contribuyentes que pueden emitir comprobantes con validez legal. La certificación electrónica es de preferencia usada para la recepción de facturas en la recaudación de impuestos y otra documentación legal. Las instituciones

gubernamentales ecuatorianas aprovechan la firma electrónica para gestión de documentos con QUIPUX, de acuerdo a (UTN, 2016).

Con este entorno, la firma digital y el Reglamento Interno de la Universidad Técnica del Norte, en adelante denominada UTN, se considera factible gestionar los trámites internos de la UTN sin usar papel con la ayuda de un software para el efecto.

El uso del papel conlleva consecuencias negativas entre otras: de-forestación, ralentización excesiva del tiempo de atención en cualquier oficina, costo en efectivo por consumo de papel, mantenimiento de impresoras, reparación de equipos y suministros de impresión. Las alternativas al uso del papel no son nuevas, la digitalización de documentos legales que al inicio son una copia del papel autografiado es una alternativa válida a ser tomada en cuenta. “La automatización de los procesos claves representa resultados de impacto en la satisfacción de los clientes internos y externos, a través de ventajas como la disminución de costos, tiempos de espera y papel, y un mejor aprovechamiento de la información”(Jimenez, Salamanca, y Garavito, 2007). Otro avance significativo que ha dado Ecuador hacia el buen vivir, es la sustentación legal con la Ley de Comercio Electrónico, Firmas electrónicas y Mensajes de Datos, que según la Asamblea Nacional (2014), facilita la mensajería de datos con validez legal; tanto en afirmación de autenticidad como en seguridad de transporte; sobre la base de protocolos seguros.

La acción de comunicar información mediante documentos legales al interior y exterior de la UTN es un tanto caótica, está basada en el uso del papel y es operada a mano, existe un deterioro de la imagen institucional e inadecuado proceso de gestión documental, el protocolo interno que la UTN utiliza para gestionar el trámite requiere una enmienda que facilite aprovechar la certificación electrónica como único instrumento válido de comunicación con

validez legal.

El reglamento interno para uso del sistema de gestión documental aprobado por el Honorable Consejo Universitario de la UTN en su Art. 30, según Naranjo y Chiliquinga (2014) dice:

Aplicación Web para firmar electrónicamente.- La Dirección de Desarrollo Tecnológico e Informático será el encargado de la adquisición, instalación, configuración y renovación de los certificados de firmas electrónicas (tokens).

Toda la documentación debe ser enviada única y exclusivamente por el sistema de gestión institucional QUIPUX, debidamente firmada electrónicamente.

En caso extremo de impresión de documentos se deberá imprimir en ambas caras de las hojas.

En la práctica, el QUIPUX de la UTN adolece algunas falencias de Software que deben superarse para servir efectivamente a la gestión del trámite institucional en todas las dependencias universitarias.

1.3. Planteamiento del Problema

La gestión de trámites institucionales en la UTN al ser un proceso manual, esta subordinado a la rapidez de cada funcionario para servir las peticiones de los interesados, quien a su vez responde en un tiempo determinado que considerado lento según una encuesta realizada a una muestra significativa de estudiantes. Este proceso descrito es susceptible de generar errores, causando molestias a los interesados en su mayoría estudiantes; se ralentiza la agilidad con que se responden las peticiones documentales. Por su parte los interesados en obtener un documento o certificado deben viajar una o más veces a obtener respuestas de los funcionarios o dependencias de la UTN, en consecuencia hay

un tiempo perdido tanto para el funcionario que realiza el proceso de emisión como para el interesado que necesita el documento. Los efectos colaterales son de alto impacto puesto que se muestra una imagen institucional deteriorada o caducada de eficiencia en la UTN.

El QUIPUX en la UTN sirve para la gestión documental; pero este, no cumple a cabalidad ciertos requisitos de integración, seguridad y utilidad para el SIIU que requiere la Institución; por lo que **existe la necesidad de automatizar la gestión de trámites institucionales usando un repositorio de firmas electrónicas integrado al ERP que satisfaga los requerimientos de Software establecidos por la Dirección de Desarrollo Tecnológico e Informático de la UTN.**

1.4. Justificación

Con los avances en Tecnología y cambios Legales en nuestro país, se observan oportunidades de mejora en los servicios que la UTN puede ofrecer cada día tanto a clientes internos (empleados, autoridades, secretarios abogados y otros funcionarios) como clientes externos (estudiantes, empresas y otros interesados).

La presente investigación es importante porque facilita el servicio de mensajería de datos firmados que tienen validez legal desde y hacia el interior de la UTN; evitando colas de personas en las oficinas solicitando documentos, evitando la falta de atención oportuna, entre otras situaciones caóticas que se resuelven por efecto colateral directo o indirecto derivado de usar el repositorio de firmas digitales en la UTN.

La utilidad básica del presente trabajo radica en la automatización de tareas que se realizan en forma manual, en el caso de gestionar trámites institucionales en la UTN. Este trabajo beneficiará a 7993 estudiantes, sin considerar el número de empleados y empresas vinculadas con la UTN que pueden realizar sus trámites documentales con más prontitud y

agilidad, evitándose las molestias de viajar una o más veces para solicitar un certificado u otro documento con validez legal.

El impacto esperado es del tipo organizacional y ambiental ya que se transformará la forma de realizar trámites legales institucionales siendo este proceso un referente local para otras instituciones públicas y privadas inclusive.

La factibilidad de desarrollo es positiva debido a que existe el interés tanto de funcionarios, estudiantes y empresas en optimizar o mejorar los procesos de gestión de trámites institucionales; es decir, se trata de una necesidad básica de resolver la situación caótica actual de la gestión de procesos usando documentos firmados digitalmente ya que existen los recursos tecnológicos, económicos y humanos para llevar a efecto la solución que se investigará.

1.5. Formulación del problema

Como incide uso del repositorio de firmas digitales disponibles en la base de datos de la UTN en la gestión de trámites institucionales con firma electrónica?

1.6. Alcance de los objetivos y lineamientos de valoración de su cumplimiento

Según la DDTI: En la UTN se han documentado 11 procesos administrativos institucionales usando BPM de Aura Portal, uno de estos es el proceso denominado Trámites Estudiantiles; existen más de 7 trámites estudiantiles de tipo jurídico diferentes entre los cuales existe el proceso de EMISIÓN DE CERTIFICADOS DE MATRÍCULA FIRMADOS DIGITALMENTE EN LA UTN. Debido al número de trámites se hace obligatorio limitar el alcance de esta investigación al estudio de este caso; por lo que se implementa

un software de propósito general que cubra aspectos clave considerados importantes para la DDTI, para validar el cumplimiento de este objetivo se anexa dos verificadores tangibles: (1) El acta firmada del Director de la DTI indicando que recibe el software y este se encuentra en funcionamiento (2) El conjunto de algoritmos entregados en CD que forman parte del acta correspondiente.

Para determinar los requerimientos del software para gestión de servicios de mensajes de datos firmados se describe mediante la adopción parcial del estándar ISO / IEC 29148, considerando los requisitos clave cuya selección se basa en un checklist de cumplimiento de las necesidades de la DDTI. Para conocer las necesidades operativas de gestión de mensajes de datos firmados se establece una entrevista y la recopilación de las características tecnológicas de los equipos sobre los que funciona el SIIU.

Para obtener los verificadores de cumplimiento tangibles de la valoración de usabilidad y seguridad de las alternativas de software para la gestión de servicios de mensajes de datos firmados se valoran las alternativas mediante un checklist sobre la lista de estándares establecidos por el gobierno para la emisión de firmas digitales y certificados electrónicos.

El diseño de la arquitectura sobre la que se basa el desarrollo de algoritmos de servicios de firmas digitales y mensajería de datos debe cubrir las necesidades de integración del SIIU con los servicios de firma electrónica y gestión documental institucional de la UTN basado en X.509 que es el estándar usado por el gobierno ecuatoriano para la emisión y certificación de firmas electrónicas.

Para relacionar el software de gestión de servicios de mensajería de datos existentes en la Base de datos de la UTN con el ERP institucional se verifica la integración de los componentes considerados más pertinentes, con el uso de SOAP o JDBC es una necesidad actual de la UTN por lo que se busca adaptar esta arquitectura en los procesos de comunicación

interna.

Lineamientos de valoración en que se considera un objetivo específico cumplido

Para determinar los requerimientos de software basta con especificar un documento de SRS en un estándar de desarrollo aceptado. Para valorar la usabilidad se establecen los parámetros del estándar 9126 como aceptables. En cuestiones de seguridad se necesita usar https para comunicación de datos del SIIU, mediante uso de firma electrónica con infraestructura X.509. El diseño de la arquitectura del servicio del repositorio de firmas digitales se acepta que sea orientado a SOAP o JDBC. Los algoritmos de servicio de firmas digitales deben atender dos servicios: firmar y validar; tomando como datos archivos en formato XML y respondiendo con certificados firmados usando infraestructura X.509 que sean depositados en la base de datos Oracle 12c compatible con el SIIU de la UTN. Para relacionar el software de gestión de servicios de mensajería de datos mediante el uso de firmas digitales se adopta SOAP o JDBC como método de intercambio de mensajes debido a que esta Arquitectura permite integrar componentes de software entre el SIIU, Aura Portal y el Servicio de Firmas Digitales.

1.7. Objetivos

1.7.1. Objetivo General

OG1. Implementar un software de servicios de gestión de trámites institucionales firmados electrónicamente mediante el repositorio de firmas digitales de la Universidad Técnica del Norte.

1.7.2. Objetivos Específicos

- OE1. Determinar los requerimientos del software para gestión de servicios de mensajes de datos firmados en la UTN.
- OE2. Valorar usabilidad y seguridad de alternativas de software para la gestión de servicios de mensajes de datos firmados.
- OE3. Diseñar una arquitectura de software para apoyar la gestión de servicios de mensajes de datos firmados en las dependencias de la UTN considerando su factibilidad de implementación.
- OE4. Desarrollar un conjunto de algoritmos de servicio de firmas digitales y mensajería de datos aplicando el proceso de software más adecuado que facilite la usabilidad y seguridad del software dentro de los límites de la infraestructura física y lógica del ERP de la UTN.
- OE5. Relacionar el software de gestión de servicios de mensajería de datos mediante el uso de firmas digitales existentes en la Base de Datos de la UTN con el ERP institucional, integrando los componentes más pertinentes según sea el caso.

Capítulo 2

MARCO REFERENCIAL

2.1. CONCEPTUALIZACIÓN

Las variables que se consideran en el desarrollo del presente trabajo de investigación se definen considerando la literatura existente en los aspectos Lingüístico, Literario, Legal, Institucional en el Sector de educación superior, Técnico y Tecnológico en el ámbito del Software y Gestión del trámite institucional. Las definiciones y perspectivas desde distintos puntos de vista son fundamentales para establecer con claridad y precisión las variables que son objeto de estudio.

2.1.1. Software orientado a servicios de certificación electrónica

Es un Conjunto de algoritmos instalados en un servidor Web, con propiedades de SOAP como describe el W3C (2007) para emitir documentos con firma digital y validez legal ecuatoriana de uso interno o externo en una institución o persona natural, sobre plantillas de archivos en formato XML desarrollado por el W3C (2007), que tienen un emisor y receptor humanos. Según el Servicio de Información Comunitario Sobre Investigación y Desarrollo de la Unión Europea en su publicación No. 95250 del C.O.R.D.I.S. (2016), el término “certificación” tiene varios significados diferentes en las Tecnologías de Información y Co-

municación, TIC. Esta definición presentada, tiene validez en el ámbito de la gestión documental y de trámites institucionales para la UTN como estudio de la incidencia del Software descrito.

2.1.2. Firma electrónica y certificado de firma electrónica

Existe una diferencia entre firma electrónica y certificado de firma digital que se aclara:

Certificado de firma electrónica

Según la Asamblea Nacional: “El certificado de firma electrónica es un archivo electrónico, que certifica la vinculación de la firma electrónica con una persona determinada, a través de un proceso de comprobación que confirma su identidad”(B.C.E., 2009).

Firma electrónica

Según el Diccionario de la Real Academia Española, DRAE, firma digital:“Información cifrada que identifica al autor de un documento electrónico.”(Española, 2017)

2.1.3. Gestión de trámites institucionales con firma electrónica

La gestión del trámite es considerada como un cambio en el proceso de negocios, Andersen (2015) menciona que los empleados deben participar en la gestión, sin embargo no se observa que este autor haya considerado el uso de la firma electrónica como elemento de comunicación que tenga algún valor legal.

Según Cruz y Ramón López Paz (2014), en representación de Oracle Corp. consideran que:

La Gestión de Procesos de Negocios (BPM., siglas en inglés) abarca el conjunto de conceptos, métodos, técnicas así como herramientas de software que brindan soporte

al ciclo de vida de los procesos de una organización: ciclo BPM. Su propósito consiste en facilitar la creación de valor para obtener mayor rendimiento y eficiencia.

Se puede afirmar que la Gestión del trámite institucional es un equivalente análogo del proceso de negocio, con la diferencia que el trámite institucional en la UTN es un proceso de negocio sin fines de lucro al estar inmerso dentro de los fines institucionales y por creación de acuerdo a CEAACES (2011).

El uso de la firma electrónica para dar validez legal al trámite institucional automatizado mediante BPM. queda definido como una gestión del proceso de negocio mediante intercambio de documentos certificados con firma electrónica cuya información se caracteriza por haber sido emitida por su autor identificado en la firma electrónica y tener valor legal para el receptor.

La gestión del trámite institucional al interior de la UTN, puede realizarse mediante emisión e intercambio de documentos certificados con firma digital, esta se emite para uso interno. En cambio, la gestión del trámite institucional hacia fuera de la institución, es decir, el trámite entre instituciones puede realizarse mediante emisión e intercambio de documentos certificados, cuya firma electrónica se emite por la entidad gubernamental autorizada para el efecto; esta firma electrónica tiene validez en el ámbito ecuatoriano. Para el trámite internacional deben revisarse los convenios de firma electrónica con los respectivos países

2.1.4. Flujos de trabajo de trámites institucionales

Los flujos de trabajo del proceso de los trámites institucionales consisten en un conjunto de actividades que se realizan en forma manual o automática. Esta definición es análoga al

B.P.M.(Gestión del Proceso de Negocio). Para el caso de la UTN, esto se realiza en cada dependencia, departamento, facultad o asociación de empleados y estudiantes. Es de interés el valor legal de la documentación solicitada y emitida por cada dependencia. “Estas comunicaciones deben llevarse a cabo de manera segura, ya que pueden participar en aplicaciones tales como pagos y sistemas de acceso”(León-Coca, Reina, Toral, Barrero, y Bessis, 2013). Los flujos de trabajo automatizados basados en servicios Web tienen ciertas deficiencias que se deben superar para la implantación exitosa de un Servicio Web; esto según (Tsamoura, Gounaris, y Manolopoulos, 2011). El principal reto para el ingeniero de Software es el cumplimiento de la Ley según expone Wilk (2016), en este caso, la Protección de Datos que está amparada en el Art. 92 de la Constitución ecuatoriana vigente.

2.1.5. Levantamiento de requerimientos de trámites de estudiantes, empleados y Secretario Abogado

En el ámbito del Software, la elicitación de requerimientos es parte del SWEBOK(Cuerpo de conocimientos en la ingeniería de software), según (Usman, Britto, Börstler, y Mendes, 2017), establecerlos forma parte de las áreas en ingeniería de Software que le competen al desarrollador y a los Stakeholders (interesados/as). Los requerimientos de calidad del Software para la gestión del trámite de estudiantes, empleados y Secretario Abogado se describen en el documento (López, 2016). Este es un proceso de software para establecer con la mayor precisión posible los requisitos funcionales y los atributos de calidad que debe cumplir el Producto de Software según las necesidades de los interesados. Algunos atributos de calidad que debería tener un software de cualquier índole deben conceptualizarse y posteriormente definirse en relación a la métrica de calidad establecida en el estándar que se adopte para el ciclo de vida del Software construido, cada atributo se define como una cualidad según el Diccionario de la Real Academia Española de la Lengua así:

- Rendimiento.-“Proporción entre el producto o el resultado obtenido y los medios utilizados”(DRAE, 2017a)
- Disponibilidad.-“Conjunto de fondos o bienes disponibles en un momento dado”(DRAE, 2017b)
- Accesibilidad.-“De fácil comprensión, inteligible”(DRAE, 2017c)
- Utilidad.- “Que trae o produce provecho, comodidad, fruto o interés”(DRAE, 2017d).
La palabra usabilidad no está definida en el diccionario de la lengua española. Facilidad para usar el software es un atributo de calidad que se asocia en este documento a la definición de utilidad explicada según el DRAE (2017d),por cuanto usar el software trae consigo beneficios para las personas naturales o jurídicas.
- Estabilidad.-“Que se mantiene sin peligro de cambiar, caer o desaparecer”(DRAE, 2017e)
- Portabilidad.-“Movable y fácil de transportar”(DRAE, 2017f)
- Interoperabilidad.- El DLE no contempla esta palabra en su diccionario. El IEEE la utiliza para referirse a la habilidad de dos o más sistemas y/o componentes para intercambiar información y utilizar esta luego de ser intercambiada. Los autores Cuenca, Gómez, y Scotti (2012) han acuñado el término inglés “interoperability between information systems, software or medical device” en un artículo publicado.
- Escalabilidad.-Se usa para decir que es propiedad deseable de un sistema, una red o un proceso, que indica su habilidad para reaccionar y adaptarse sin perder calidad, o bien manejar el crecimiento continuo de trabajo en forma fluida. El DLE define adaptable así: “Capaz de ser adaptado”(DRAE, 2017g)

- Concurrencia.-“Coincidencia, concurso simultáneo de varias circunstancias”(DRAE, 2017h)
- Mantenimiento.-“Conjunto de operaciones y cuidados necesarios para que instalaciones, edificios, industrias, etc., puedan seguir funcionando adecuadamente”(DRAE, 2017i) Esta definición puede aplicarse a la dificultad para realizar tareas de mantenimiento al Software como un atributo de calidad tangible.
- Interfaz.-“Conexión, física o lógica, entre una computadora y el usuario, un dispositivo periférico o un enlace de comunicaciones”(DRAE, 2017j)
- Seguridad.-“Que no falla o que ofrece confianza”(DRAE, 2017k)

Es recomendable adoptar o diseñar un estándar para medir la calidad del Software que se desarrolla y entrega al DDTI-UTN. Por experiencia del autor en los procesos de compras públicas ecuatorianas se muestra que en el desarrollo de Software para el sector público, existen tres etapas o fases bien definidas:

- Fase 1.- para elicitación de requerimientos contractuales y especificaciones de software entre los que constan: Convenio de pago, contrato, selección de proveedor, tiempo de desarrollo, asignación de recursos, entrega, recepción, garantías, mantenimiento, soporte técnico.
- Fase 2.- Ciclo de vida para desarrollo del Software en el que consta fecha límite de entrega y en caso de aceptación: implantación, pruebas de operación, puesta en marcha, recepción parcial y total; en caso de rechazo: multas por entrega tardía, renuncias y cancelación del contrato.
- Fase 3.- Producción en que está vigente el tiempo de garantía del fabricante de Software y el soporte técnico.

Antúnez Javier (2013), propone desarrollar el documento de requerimientos de la siguiente forma según la figura 2.1, el cual es una aproximación al uso del estándar ISO/IEC 29148.

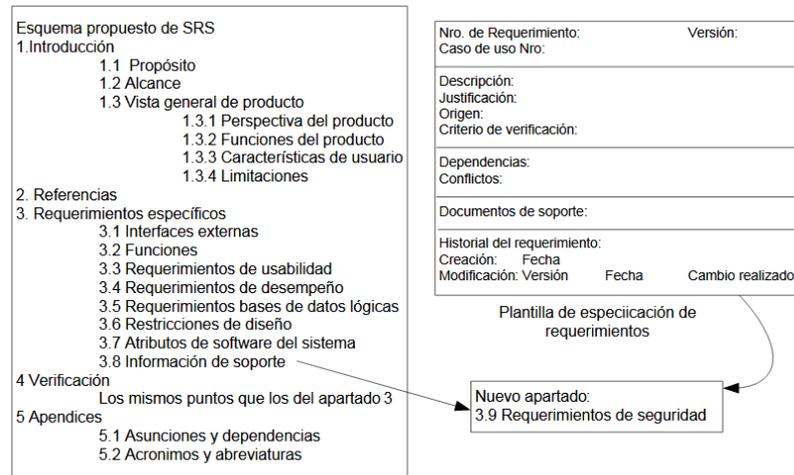


Figura 1: Una aproximación al documento de especificación de requerimientos de software según el estándar ISO/IEC 29148

Un estándar de calidad exclusivo para la fase de desarrollo del Software sugerido por la ISO es el 9126, este puede ser usado como material para desarrollo de Software. El INEN (2014) propone adoptar ISO/IEC 25010:2011, IDT en el desarrollo y evaluación de la calidad del Software.

Un enfoque por resultados en el tiempo permite medir el avance del proyecto de software mediante métricas más precisas.

2.1.6. Software de servicios del repositorio de firmas digitales de la UTN

Cada empleado de la UTN puede disponer de una firma electrónica almacenada en un archivo digital según la Ley de Comercio Electrónico ecuatoriana. El software de servicios del repositorio de firmas digitales en la UTN es un programa de ordenador que firma certi-

ficados electrónicos usando la firma digital del empleado responsable de la emisión documental con validez legal. El Software de servicios debe satisfacer las condiciones mínimas exigidas en la Ley para garantizar:

- (1) Integridad
- (2) Confidencialidad
- (3) No repudio
- (4) Pertinencia de la Información Certificada

sin perjuicio de cumplir con los demás atributos generales de calidad del Software.

2.1.7. Creación, almacenamiento y uso de las firmas digitales

La creación de una firma digital tiene dos orígenes según el propósito:

(1) Banco Central del Ecuador a través del Registro Civil en las oficinas designadas para el efecto en algunas ciudades, la persona natural en este caso el empleado o funcionario de la UTN deberá disponer de una firma electrónica vigente en el formato requerido, a saber p12 (PKCS12). Esta firma tiene validez legal en todo el territorio ecuatoriano.

(2) El DDTI-UTN que podría emitir un archivo de firma digital en formato p12, asociado al empleado que vaya a emitir certificación electrónica. Esta firma tiene validez legal al interior de la UTN y no podrá ser usada para uso externo o en comunicación con otras instituciones o empresas. El DDTI-UTN se constituye en garante de la calidad y uso de la firma electrónica, así creada.

El almacenamiento de la firma digital debe satisfacer las condiciones de seguridad más óptimas requeridas en forma general para el proceso de software. El responsable de custodiar el almacenamiento del repositorio debe garantizar al menos las condiciones exigidas

en el Habeas Data vigente en Ecuador de acuerdo a la Ley, en amparo del Artículo 92 de la Constitución según (Constituyente, 2008).

El uso de las firmas digitales puede ser manual o automático. En cualquier caso debe establecerse con claridad que, el uso de la firma digital sea responsabilidad de su propietario y sea este, quien autorice y controle la emisión automática de certificados con firma electrónica. Por principio ético, la firma digital debe usarse tomando en cuenta el riesgo del uso indebido, mal uso, abuso, negligencia y otros aspectos agravantes que podrían perjudicar a la Institución y al Emisor de documentos certificados con firma electrónica.

2.1.8. Peticiones de documentos legales en la UTN

En el reglamento interno de la UTN se establece los lineamientos para gestión documental mediante el software QUIPUX. Es necesario realizar adaptaciones al reglamento interno de la UTN para que considere las definiciones establecidas ibídem, que permitan aprovechar los beneficios de usar este software de firma electrónica para gestionar la petición documental en forma legal de la UTN con respuesta a los pedidos semiautomática en cada dependencia interna.

2.1.9. Actividades legales del Secretario Abogado que requieran emitir documentos firmados

El Secretario Abogado es el responsable de tramitar asuntos académicos de todo tipo, Jimenez, Salamanca, y Garavito (2007) explican que se manejan los siguientes temas:

- Solicitudes estudiantiles de pregrado y posgrado al Consejo de Facultad (traslados, reserva de cupo, reintegro, reingreso, cancelación de asignaturas, inscripción de asig-

naturas, homologaciones, etc.).

- Gestión de asuntos de personal docente (contratación, comisión de estudios, comisión de servicios o disfrute de vacaciones, etc.).
- Certificados (estudios, notas, plan de estudios, etc.).
- Asuntos jurídicos de estudiantes y docentes.
- Concursos de convocatoria de docentes
- Graduación de posgrados y pregrado
- Archivo
- Matrículas.

2.1.10. Incidencia del uso del Software de certificación electrónica en la Gestión del trámite institucional

En forma general un Software tiene uno o varios propósitos:

1. Automatizar tareas repetitivas
2. Resolver problemas
3. Entretenimiento
4. Facilitar misiones complejas
5. Comunicar a las personas

Según el propósito del Software puede especificarse y medirse la incidencia de su uso en las actividades personales o institucionales.

¿Como incide el Software de certificación electrónica en la gestión del trámite institucional en la UTN?

Cada dependencia universitaria tiene sus características que definen la factibilidad de automatizar por software según el propósito que se tenga y el respaldo legal para hacerlo, esto incide directamente sobre ciertos aspectos del proceso de gestión, algunos de estos son: *eficiencia en el servicio, costo de oportunidad, reducción al consumo de papel, organización de la información, cumplimiento legal, disminución de los errores administrativos y atascos en el servicio, etc.* En cada dependencia se puede establecer las actividades que son factibles de automatizar, según son los beneficios esperados y que pueden requerir certificación electrónica, tanto para los documentos recibidos como para los emitidos, luego de su procesamiento.

Secretario Jurídico

El cuadro 2.1 muestra algunas actividades del Secretario Jurídico que podrían ser susceptibles de automatización. Se muestra el tipo de actividad, una descripción breve del concepto sobre lo especificado, se caracteriza el requerimiento de firma digital y se indica si la firma electrónica sobre el documento es a la entrada o salida del proceso legal en la oficina del Secretario Abogado. Se puede observar los tiempos de servicio estimados empíricamente para cada petición documental mediante Software con certificación electrónica ejecutada en forma manual por el Secretario Abogado siempre que no haya nada que se oponga a

la emisión del certificado o documento pedido. Este cuadro muestra la información que es susceptible de ser automatizada mediante un software de gestión documental. FD REQ indica si el requerimiento es firmado digitalmente. EF Y SF indica si la entrada o salida es firmada. En la última columna se muestra un estimado de tiempo de espera del servicio en caso de ser automatizado por software.

Empleado

El empleado como funcionario público y autoridad:

Un cambio en la cultura organizacional es necesario fomentar entre los empleados, al amparo de un reglamento interno que facilita la transición entre el proceso manual de certificación documental hacia uno semiautomático en que algunas decisiones son tomadas con ayuda del Software y este emite documentos válidos y otras aún esperan del funcionario para su emisión.

El empleado como receptor documental:

Al igual que un estudiante, el empleado que requiere un certificado procede a pedirlo mediante el servicio Web al funcionario competente para emitirlo. Esta gestión puede demorar un tiempo en ser tramitada según el caso.

Estudiante

En la asociación estudiantil:

Cualquier certificado que sea susceptible de automatizar puede incorporarse al flujo de trabajo del Software GDTUTN, esto implica la necesidad de implementar un servicio Web para la Asociación de Estudiantes, con la incorporación de una firma digital del represen-

Cuadro 1: Actividades del Secretario Jurídico susceptibles de automatización.

TIPO	ACTIVIDAD	FD REQ.	EF	SF	t(min)
Solicitudes estudiantiles	Presentar plantillas de peticiones	NO		v	1
	Identificar al Solicitante	Cédula	v		1
	Organizar la documentación	Archivo			1
	Dar Validez legal al documento	SI	v	v	1
Asuntos personal docente	Comisión de estudios	SI	v	v	5
	Comisión de servicios	SI	v	v	5
	Vacaciones	Cédula		v	5
Certificados	Estudios	Cédula		v	1
	Notas	Cédula		v	1
	Plan de Estudios	Cédula		v	1
Asuntos Jurídicos	De estudiantes	SI		v	30
	De docentes	SI		v	30
	De trabajadores	SI		v	30
Concursos	Docentes	Cédula	v	v	1
	Estudiantiles	Cédula		v	1
	Públicos	Cédula		v	5
	Institucionales	RUC		v	5
	Escalafón	Cédula		v	5
Graduación	Pregrado	Cédula		v	20
	Posgrado	Cédula		v	20
Archivo	Certificados Históricos	CI/RUC		v	30
	Actualización de Certificados	CI/RUC		v	30
Matrículas	Inscripción	Cédula		v	1
	Admisión	Cédula		v	1
	Promoción	Cédula		v	1

tante legal de los estudiantes en el repositorio de datos en la UTN. En forma personal:

Los 7993 estudiantes registrados durante el 2016 en la UTN, pueden solicitar documentos o certificados electrónicos con validez legal tanto para uso en la UTN como para uso personal con la misma validez legal amparado en la Ley de Comercio Electrónico vigente en Ecuador. El impacto esperado de uso del repositorio de firmas digitales es alto, implica reducción de gastos, ahorro de tiempo y papel. El valor del transporte podría ser invertido en otra necesidad personal que puede ser entre otras cosas alimentación o vestimenta; el tiempo ahorrado puede ser utilizado por el estudiante para otra actividad académica, recreativa o alimentación lo que incidirá indirectamente en mejorar la calidad de vida; el ahorro de papel implica menos consumo de los recursos naturales, mejor organización personal y orden. Estas son incidencias lógicas, deducidas de la relación causa efecto de los cambios en la organización institucional y personal.

Por principio, el hecho de automatizar tareas repetitivas deja en libertad a la persona para dedicar su tiempo actividades mas humanas y propias del intelecto, que ciertas tareas sean de misión crítica como emitir certificados digitales es un proceso que requiere alta confiabilidad, seguridad de hardware, software y un entorno legal apropiado.

2.1.11. Métricas de Impacto del uso de Software en la gestión del trámite institucional de la UTN

Para medir el impacto del software en la gestión del trámite se ideó una tabla con la que se describe un conjunto básico de métricas para medir incidencia que pueden ser obtenidas o calculadas, por el mismo Software según los casos de consumo del servicio Web orientado a SOA, para emisión de certificados digitales válidos en las dependencias de la UTN. El cuadro 2.2 muestra indicadores de impacto del uso de Software en la gestión del trámite

institucional de la UTN.

Cuadro 2: Métricas de Impacto del uso de Software en la gestión del trámite de la UTN.

Actividad	Métrica	Calidad	Cantidad	Esp.	Obs.
Solicitud	XML	Solicitudes por unidad de tiempo	#XML/min	17	
Respuesta	PKCS12	Certificados por unidad de tiempo	#P12/min	17	
Emision FD	FD-P12	Firmas digitales P12 en repositorio	#FD-P12	2000	
Servicio1	TS	Tiempo de servicio del Secretario-Ab.	minutos	3.4	
Cola1	TC	Tiempo de espera de la Solicitud	minutos	30	
Cola2	TL	Tiempo de llegada entre Solicitud	minutos	2	
Cola3	TR	Tiempo de respuestas sin Leer	minutos	30	
Transporte	Ahorro	Ahorro por transporte/c. Solicitud	USD	0.6	
Impresión	Ahorro	Ahorro por papel A4 75gr/c. Certificado	USD	0.01	
Oportunidad	Ahorro	Tiempo de gestión/c. Solicitud-Certificado	minutos	120	

Descripción de la métricas de incidencia de uso del Software de servicios de certificación electrónica en la UTN

Solicitudes por unidad de tiempo

Este indicador es aceptado si se incrementa significativamente la capacidad de receptor solicitudes identificando al sujeto que pide, por unidad de tiempo.

Certificados por unidad de tiempo

Este indicador es aceptado si se incrementa significativamente la capacidad de emitir certificados firmados digitalmente al sujeto que pide, por unidad de tiempo.

Firmas digitales P12 en repositorio

Este indicador muestra la cantidad de firmas digitales almacenadas en el repositorio y su estado. Además es posible mostrar el consumo de recursos mediante un contador que muestra

las veces que han sido usadas.

Tiempo de servicio del Secretario Abogado

Este indicador muestra la cantidad de tiempo que cada Secretario Abogado ha usado para firmar digitalmente documentos en formato PDF o XML cuya certificación sea manual.

Tiempo de espera de la Solicitud

Tiempo que se demora una solicitud antes de ser atendida.

Tiempo de llegada entre Solicitud

La demora o inactividad en el servicio Web entre solicitudes.

Tiempo de respuestas sin Leer

La cantidad de tiempo transcurrido entre la emisión del certificado electrónico y el indicador de que ha sido leído

Ahorro

Algunos indicadores son calculados tomando en cuenta una situación análoga típica de consumo del servicio usando transporte, papel y firma autografiada. Esto permite observar la incidencia de uso del software en la gestión del trámite institucional y verificar el impacto directo sobre la imagen empresarial y acondicionamiento tecnológico.

2.2. COMPETENCIAS Y LÍNEA DE INVESTIGACIÓN

El presente trabajo en concordancia con TICAL (2016), está enmarcado en el Eje temático: Soluciones TIC para la Gestión. Líneas de investigación: Firma digital aplicada a los procesos.

¿ Cuáles competencias ha desarrollado o aplicado en su proyecto o trabajo de grado?

Se desarrollaron competencias en ingeniería de software. Líneas de investigación: Inge-

nería de Requisitos, Proceso de Software, Uso de Estándares en Calidad, Arquitectura, SOA, Aplicaciones Web y Cloud Computing.

¿Sobre que línea o sublínea de investigación trabajó? En concordancia con (UTN, 2014), se trabajaron principalmente las siguientes competencias:

- “Adquirir habilidades para especificar requisitos, ..” En ingeniería de requisitos sobre la recopilación de requerimientos del software documentados según la norma ISO / IEC 29148.
- “Capacidad de manejo de herramientas de desarrollo asistido por software..” Para el proceso de desarrollo del software se estableció de mejora continua con metodología de desarrollo RUP de software.
- “.. SOA, Lenguajes de Descripción de Arquitectura de Software.”
- “.. Confiabilidad y seguridad.”
-

2.3. FUNDAMENTACIÓN FILOSÓFICA

Comunicaciones personales e institucionales, pasado, presente y futuro

Internet de las Cosas

Los datos personales pueden ser generados desde casi cualquier cosa. Con los avances de la tecnología el Hardware está más ligado al servicio ergonómico. En una taxonomía de conceptos presentada por Sethi y Sarangi (2017), se muestra cual es la conexión de IoT, cuales son los protocolos y la arquitectura orientada al Cloud que existe. Ellos enfatizan que “La computación ubicua es el núcleo de la Internet de las cosas”.

Computación Ubicua

Con el surgimiento del Internet nuevos paradigmas aparecen, entre otros la Computación Ubicua(Sethi y Sarangi, 2017), con la que una persona puede comunicarse y estar omnipresente mediante el proveedor de servicios. En ética, la comunicación personal de dos interlocutores cambia cuando el medio deja de ser el aire y lo reemplaza el ciberespacio. La comunicación entre pares u homólogos puede verse afectada cuando se trata de la comunicación entre el hombre y la máquina, ya que esta no posee todas las cualidades humanas que le caracterizan a la persona.

Comunicación e integración entre sistemas heterogéneos

Comunicar datos es mágico según (López y Rosero, 1999), ya que podría poseer características para desencadenar procesos incontrolables, algunos ejemplos muestran esta incidencia: (1) Un mensaje escrito y publicado en una Red Social podría insinuar a la violencia cuyo efecto colateral concurrente es incontrolable. (2) Una serie de comandos enviados desde la Tierra al Software para mover el Pathfinder lo dejaron varado en Marte, ha resultado imposible volverlo a controlar adecuadamente. Cada proceso del software una vez que ha sido instalado sobre el hardware y activado, debe constituirse en célula auto protegida y autorregulada subordinada al ser humano en cuanto a los principios éticos de un ente robot, cuya ética de construcción recae en el ingeniero de software. Desarrollar aplicaciones de computadora implica responsabilidad social(Spinellis, 2017). El entendimiento de los mensajes en lenguaje español es ambiguo por construcción semántica cuya interpretación es inexacta o imprecisa, esto se elimina cuando los interlocutores son: hombre con máquina o una computadora con otra, debido al alto grado de formalismo del lenguaje y la notación matemática(Takacs, Richter, Csizinszky, Mazzei, y Simon, 2015) con la que se traduce un algoritmo comunicado desde la persona al procesador y la precisión semántica con que la computadora responde peticiones personales. Las personas comunican información me-

diante:

- Palabras (Audio,Digital)
- Expresión corporal (Visual)
- Movimientos de los dedos (Táctil)
- Otras partes sensibles a dispositivos biométricos (Digital)

Las computadoras comunican información mediante:

- Pantalla (Visual)
- Puertos seriales y paralelos (Bits)
- Dispositivos Entrada y Salida (Bits)
- Adaptadores de Interfaz (Analógico y Digital)
- Parlantes (Audio)

Una descripción empírica basada en la experiencia

El **Audio** es la forma física de los sonidos que pueden ser ambientales o palabras expresadas mediante la boca en un idioma particular. Es posible la transducción del Audio en señal eléctrica digital que es procesada por la Computadora y transformada en datos. ¿Puede un Software distinguir las palabras de tal forma que se identifique la persona relacionándola con su número de identidad del registro civil?

Las personas podemos distinguir a otras al escuchar el timbre de voz. Se puede afirmar por vivencia que: si una persona sana X escucha a otra Y, con quien haya charlado anteriormente, X reconoce a Y al escuchar sus palabras, con tal precisión que casi inmediatamente la trata por su nombre con un mínimo margen de error. Este reconocimiento esta siendo

investigado para ser replicado por la interacción VL/HCC.

La **Expresión corporal** es la esencia del ser humano, muestra la forma física de la persona en estado activo. Cualquier humano sano reconoce a otro con solo mirarlo, siempre que lo haya visto y dialogado antes. Además, decide si le gusta o no; las redes sociales aplican este concepto para mantener conectada a la gente. Una persona reconoce visualmente a otra por su expresión corporal incluido su rostro y la trata por su nombre con un margen de error mínimo. El elemento clave del reconocimiento es el rostro humano, el iris de los ojos, la huella dactilar; aunque la expresión corporal aporta pistas adicionales sobre la identidad de una persona, incluso sobre la personalidad pero este es tema que sale del alcance de este trabajo.

¿Puede un Software distinguir la expresión corporal de tal forma que se identifique la persona relacionándola con su número de identidad del registro civil? Los avances tecnológicos nos muestran que es posible identificar una persona en base a la transducción de pistas visuales capturadas por los dispositivos biométricos; incluso se distingue el rostro de las personas cuya imagen ha sido capturada en una fotografía, facebook es un ejemplo de esto. La huella dactilar ha demostrado en la práctica, de administración del talento humano, ser la mejor opción para identificar la presencia de una persona en un lugar e instante de tiempo. Las tasas de error en el reconocimiento basado en rostro son muy altas y a menudo se recurre al voto para decidir sobre la identidad de una persona. La complejidad de reconocer mediante el iris del ojo lo hace menos viable.

El Internet de las cosas es la tendencia actual de manejar el flujo de información y comunicar datos a interlocutores personales o máquinas. Se está construyendo Hardware/Software que facilite la comunicación personal y ergonomía al capturar información sensorial para enviar al servicio de tratamiento más adecuado. Esto cambia la perspectiva humana

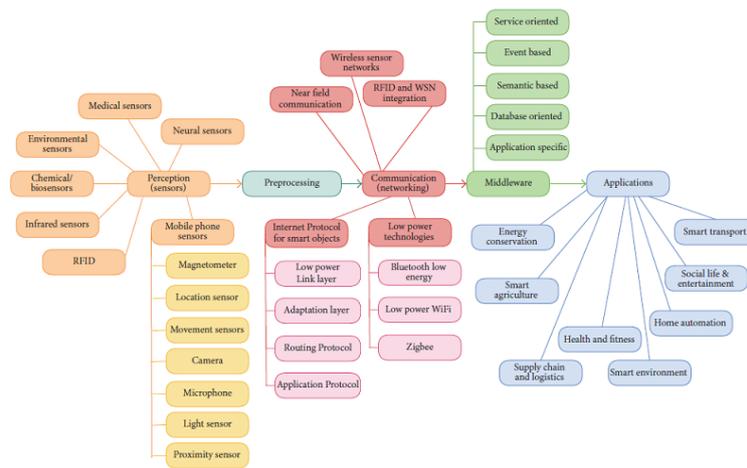


Figura 2: Taxonomía de investigación en tecnologías IoT (Sethi y Sarangi, 2017)

hacia una Web con un entorno de mayor riesgo en la protección de datos. De acuerdo a (Giuliani y cols., 2016), se deben cumplir estándares de seguridad de Hardware y Software para comunicar datos. La base de una comunicación segura no debe afectar la Libertad ni Integridad personal.

El trámite institucional es un proceso en la estructura de las relaciones humanas; al principio la humanidad estaba acostumbrada a que el medio de enlace y transporte de información sea uno bastante privado(aire) y seguro(hasta una distancia audible por el oído humano); posteriormente se utilizó el papel escrito en un lenguaje simbólico para comunicar y guardar información. La solicitud verbal de documentos institucionales ha cambiado su formalidad al ser escrita y en papel, este proceso consume papel el cual desencadena en efectos primarios ambientales negativos y otros secundarios indeseados y nocivos. El uso de Internet para solicitar documentos cambia el entorno de comunicación a uno público en el ciberespacio que podría ser vulnerado por atacantes ávidos de información ultra secreta y personal. Este riesgo en el cambio de entorno para transporte de mensajes, es parte del trabajo que el ingeniero de software debe minimizar para satisfacer una demanda creciente de peticiones documentales con validez legal en el caso de la UTN.

Cualquier entorno de seguridad construido por el hombre ha resultado inseguro comparado con la evolución en materia de seguridad vital que el mundo natural muestra, por ejemplo, hasta el momento ha sido imposible detectar lo que un individuo está pensando con una precisión tal que se pueda redactar o reproducir todos y cada uno de los pensamientos generados en unidad de tiempo discreto. El pensamiento humano ha evolucionado sobre la base biológica de la estructura celular del cerebro humano, el secreto mejor guardado hasta ahora es la idea que se forma en el cerebro que hasta el momento ha permanecido invulnerable por la neurociencia. Esto significa que incluso así guardado y con toda su evolución, los delincuentes comunes y sin mucha ciencia pueden descubrir sus secretos mediante técnicas empíricas basadas en amedrantar al sujeto o la violación de sus derechos humanos; en estos casos la idea fluye desde el pensamiento en forma de mensaje expresado por la voz o por señas y gestos.

El momento que la idea se comunica, esta pasa de un entorno más seguro hacia otro de menor seguridad, en el ambiente lo constituyen las palabras expresadas en forma oral, escrita o digital y pueden escucharse, leerse o decodificarse para ser entendidas por alguien o una computadora mediante Software. Pero ¿Qué significado tiene? y ¿Cuál es la importancia de las ideas en la gestión del trámite?: Para responder la primera, se hace referencia a la Constitución ecuatoriana en el Artículo 92, esta idea comunicada se transforma en datos o es atendida por el receptor o interlocutor humano, quien por principio legal debe proteger esos datos o mensaje en la intervención de terceros desautorizados. Por las características de este trabajo, solo se considera dos tipos de interlocutores: humano y computadora. En este estudio se descarta a los receptores humanos, es responsabilidad de Todos acatar la Ley, y, eso va mas allá del alcance de este trabajo. La computadora que recibe el mensaje o dato del humano debe proporcionar un Software que cubra las necesidades de Protección a

sus Datos en un ambiente considerado Útil y Seguro.

La Protección de Datos según el tipo de interacción Humano Computadora:

FODA de la interacción Humano Computadora para la gestión documental

Es necesario describir las Fortalezas, Oportunidades, Debilidades y Amenazas que representa la interacción entre el Hombre y la Computadora para gestión documental y trámite institucional; el principio en que se basa esta descripción es: En un sistema de comunicación orientado a personas, el mensaje emitido debe protegerse de:(1) Acceso desautorizado, (2) Tergiversación, (3) Plagio y cualquier otra acción u omisión que perjudique al emisor del mensaje; el receptor debe recibir mensajes: (1) Originales, (2) Íntegros, (3) Confidenciales y que tengan todas las características necesarias para cumplir el objetivo deseado para ambos: emisor y receptor. El medio de comunicación debe garantizar las propiedades de los mensajes y ejecutar el proceso de transporte adecuado. Estos principios son conocidos por todos en forma implícita, están ligados a la esencia del ser y pensar expresada mediante el lenguaje.

Comunicación Humano Computadora mediante Palabras

Esta comunicación es conocida como Verbal.

FORTALEZAS. La palabra es rápida y directa de expresar las ideas en lengua española para el caso ecuatoriano en su mayoría de la población.

OPORTUNIDADES. Actualmente existe software para traducir la voz humana en mensajes de texto que pudieran entenderse en forma semántica mayoritariamente para Inglés y Español, por ejemplo, la arquitectura de Software HMI (Cavaliere, Bastos-Filho, Palazuelos-Cagigas, y Sarcinelli-Filho, 2015).

DEBILIDADES. Esta forma de comunicación está muy limitada y a menudo existen errores de traducción o compilado que tergiversan la expresión del pensamiento. La lista de idiomas soportados por el software falta cubrir lenguas nativas de la región. Existe un grupo significativo de población ecuatoriana que habla otras lenguas nativas.

AMENAZAS. La protección de datos pasa por un espacio y tiempo vulnerable debido a la existencia de micrófonos y sensores de ultrasonido que terceros podrían utilizar para acceder al mensaje sin autorización.

Comunicación Humano Computadora mediante Expresión corporal

Esta comunicación es conocida como No verbal.

FORTALEZAS. Se puede expresar sentimientos.

DEBILIDADES. Poco apto para comunicar ideas concretas.

AMENAZAS. Al interpretar la expresión corporal podría ocasionar tergiversación de la idea.

OPORTUNIDADES. Actualmente la discapacidad humana es motivo de estudio para tratamiento y la máquina es ideal para traducir imágenes o movimientos en palabra escrita siguiendo algún patrón sensorial adecuado, por ejemplo: redes neuronales.

Comunicación Humano Computadora mediante Movimientos de los dedos

Es la más común, de hecho, las computadoras personales disponen de teclado.

FORTALEZAS. El pulso de las teclas es la forma y el medio tradicional de comunicación entre humano y computadora. DEBILIDADES. La comunicación del teclado puede ser interceptada por software e intervenida por terceros para actividades delictivas.

AMENAZAS. El síndrome del túnel carpiano es una enfermedad que se desarrolla con el exceso de trabajo por mala posición del teclado. Siempre existirá errores al presionar las teclas debido a la naturaleza humana.

OPORTUNIDADES. En la actualidad se poseen teclados con analizador predictivo y embebidos en el hardware para garantizar un nivel mínimo de errores por presionar inadecuadamente las teclas.

Comunicación Humano Computadora mediante datos biométricos

FORTALEZAS. Detectan con un nivel de certeza superior al 99% a la persona que lo posee.

DEBILIDADES. Debido a su falibilidad es imposible garantizar solo por este método la autenticidad de la persona que registra su información.

AMENAZAS. Siempre existe el responsable de relacionar la data recuperada que podría errar manualmente el proceso por falla humana.

OPORTUNIDADES. Es una buena forma de incrementar el nivel de seguridad y confiabilidad de la autenticidad de la persona en el proceso de certificación electrónica.

Comunicación Computadora Computadora mediante Protocolos

Es útil definir las características de Protección de Datos en el proceso de comunicación de Computadora Computadora, es la base de Hardware sobre la que el Software trabaja:

FORTALEZAS. Existen protocolos de comunicación hasta el momento, 100% seguros en cuanto a cifrado de información e infraestructura de intercambio, uno de estos es el Protocolo X.509 utilizado legalmente en el Ecuador para comunicar datos firmados digitalmente

sobre HTTPS con claves de seguridad tipo TOKEN o archivo P12.

DEBILIDADES. Existen instantes de tiempo en el proceso de cifrado y almacenamiento del certificado electrónico en que el nivel de seguridad disminuye y se restringe al entorno del Sistema Operativo en el Equipo o Computadora emisora. La seguridad en comunicación Computadora Computadora pese al esfuerzo e innovación en tecnología de protección a datos, esta subordinada a la condición humana que es susceptible de errores.

AMENAZAS. Generalmente la infraestructura física es en cierta medida vulnerable a ataques delictivos que podrían destruir la información almacenada. Ecuador es considerado un país con alto nivel de corrupción personal y de funcionarios públicos.

OPORTUNIDADES. El nivel de seguridad es un aspecto militar que para el sector público depende de la fortaleza bélica de un país para cumplir la Constitución y obedecer la Ley, y de la ética del personal responsable en el conjunto servidor de datos. La infraestructura de las instalaciones en servicio y los cuartos de máquina cumplen normas de Seguridad y Protección Ambiental.

Reseña histórica de las comunicaciones en el Ecuador

Antes de ser República, el territorio donde hoy ocupa Ecuador fue dominado por el Imperio Inca que corresponde al Tahuantinsuyo. En esa época las comunicaciones de datos llevaban los Chasquis¹(CIESPAL, 1972), quienes eran nativos que comunicaban las disposiciones del Inca² y otros mensajes desde la sede del Tahuantinsuyo en Quito hasta los límites sureños en Antofagasta al Sur de Chile. La información se comunicaba mediante

¹Chasqui. De origen quechua. En el Imperio incaico, mensajero que transmitía órdenes y noticias.

²Inca. Monarca que gobernaba el Imperio incaico

un sistema de nudos en cuerdas denominado Quipu³(Urton y Brezine, 2009) y se recorría por senderos que unían todo el territorio imperial a través de la cordillera de los Andes. La distancia diaria que se recorría era de aproximadamente 400Km. Se cubría el territorio en un tiempo estimado de 5 días.

Con la llegada de los Españoles, la época Colonial, fue dominada por el caballo que era traído de Europa y con este las comunicaciones fueron mas rápidas, además los mensajes eran escritos en castellano y por lo general eran redactados por gente más ilustrada denominados Patricios. Las rutas de los Chasquis siguieron utilizándose. Los mensajes que se generaban en Quito podían llegar a Europa a través del Atlántico pero estos demoraban mucho tiempo por la travesía del Océano que podría demorar meses o nunca llegaba debido a los naufragios o asaltos piratas que eran muy comunes en esa época, entre 1532 y 1830 en que inicia la etapa republicana constitucional del Ecuador (Ayala, 2008). El ocultamiento de información en la comunicación adquirió importancia para las luchas patrióticas en contra del colonialismo español y la formación de republicana y democrática del Ecuador. En la época republicana ecuatoriana, antes del telégrafo, la comunicación de información era transmitida junto con otra carga útil por los arrieros; el abuelo de quien redacta este documento fue uno de ellos, y se llamaba Leonardo Ruiz, quien se jubiló cuando fue presidente José María Velasco Ibarra, al cerrarse la fábrica de textiles Imbabura en Atuntaqui y vivió lo suficiente para ver la instalación de telefonía fija con sus 98 años de existencia. Según El contaba sus anécdotas, uno de los mayores problemas del transporte tanto de mercadería, información y dinero era la seguridad e integridad personal, a menudo se organizaban asaltos por robo en el camino a los viajeros. Las emboscadas a los viajeros eran

³Quipu. Los Khipu(del inglés=Quipu) son dispositivos textiles anudados para el mantenimiento de registros utilizados por los Inkas(del inglés=Incas). El imperio inca se extendió a lo largo de los Andes y duró desde alrededor de 1400 dC hasta la conquista española del Perú en 1532.

frecuentes y este problema aún persiste en la actualidad por las vías. Los arrieros ecuatorianos transportaban información junto con mercadería y víveres de norte a sur y cubrían las rutas de los Chasquis, usando carruajes de madera jalados por caballos, llevaba 2 días recorrer la ruta Ipiales Quito por estos senderos. A principios del siglo XIX aun trabajaban los arrieros cuando llego el automóvil y con este el transporte de información escrita se redujo a una oficina de correos nacionales que cubría los servicios de mensajería escrita y transporte de carga usando vehículos motorizados lo que ocasionó la desaparición de los arrieros, pero la vialidad no estaba aún al nivel de las exigencias.

El correo nacional ecuatoriano a menudo se perdía, por ineptitud del personal que laboraba o por error humano en la especificación del destinatario o por cualquier otra causa. La privacidad de información enviada por correo se veía afectada por falta de Ética del personal que transportaba. Las demoras en los juicios fueron siempre un calvario para los litigantes si el caso era civil y peor si el caso era penal la información a menudo se desvanecía en el camino o se tergiversaba por el transportista, o se demoraba demasiado en llegar, o el mensaje original era cambiado.

El Virreinato de Lima era la única sede Judicial en la época colonial para emitir los Juicios de casos Civiles y Penales, las comunicaciones casi nunca llegaban intactas el correo era intervenido a voluntad de los encargados, al no haber una tecnología adecuada de ocultamiento de información sensible, pese a todo algunas técnicas de cifrado ya se utilizaban para proteger en algo el contenido de la información legal que se transportaba.

Con el aparecimiento del correo postal ecuatoriano apareció también el sobre, membrete y sello que de alguna manera permitía proteger y ocultar la información transportada. El dinero y otras formas de información impresa fueron mejorando su técnica para protección de datos. La tecnología nacional después del imperio Incaico en el Tahuantinsuyo sufrió

un retroceso por la inobservancia Ética y Moral de la gente que conquistó y dominó esta región.

Al llegar la telefonía fija y el desarrollo de las Telecomunicaciones en el Ecuador, se mejoró el intercambio de información. A finales del siglo XX, llegó al Ecuador el Internet y con este el correo electrónico y la Web. Pronto el sector público posicionó su estrategia de gobierno en la Web. Es necesario destacar el hecho que la Ciencia y Tecnología ha llegado al país por influencia extranjera y muy poco se avanzó en Investigación hasta la llegada de Internet y las Redes Sociales.

El correo nacional inició sus operaciones en 1831, la empresa pública a tecnificado su sistema operativo según se publica en el portal ANDES (2015), en la actualidad esta encargada del soporte al Software QUIPUX que es el sistema de gestión documental estatal.

La influencia de los Países del norte global sobre América Latina es notoria; en el Ecuador se ha transformado la visión general sobre la cultura, ciencia y comunicación científica. Según CIESPAL (2016), las plataformas tecnológicas sobre las que se divulga el conocimiento científico valora un tipo de rentabilidad ajeno a nuestra realidad. Las nuevas tecnologías de comunicaciones y la adopción de estándares internacionales que son parte del Software, como el protocolo X.509 que es la norma actual para comunicar información al SRI, los algoritmos de cifrado RSA en que se basa el fichero de formato P12 donde se almacena la firma digital personal; además de existir un entorno Legal apropiado, constituye una oportunidad para emprender en innovación y desarrollo ecuatoriano hacia procesos de negocios y trámites institucionales tecnificados. Un reciente artículo que narra la influencia de los Chasquis en Quito, menciona la existencia de Chasquis motorizados, como narra Ernesto Terán: “Un chasqui en la calle es un auto menos haciendo trámites”(Terán, 2016). El muestra la necesidad de optimizar la gestión de trámites ciudadanos.

Para Ocampo (2015), el reto latinoamericano es:

“..el desarrollo de un aparato administrativo capaz de ayudar a la sociedad a cumplir las funciones de provisión de bienes y servicios de interés colectivo, dentro de la particular combinación entre Estado y mercado que cada sociedad defina con base en sus propios procesos democráticos”.

En historia de la administración y gobierno universitario, la comunicación es fundamental para proveer servicios de interés colectivo, con el surgimiento de las TIC, existe una oportunidad de mejora al proceso de trámites institucionales con efectos positivos para el ahorro de tiempo y dinero en este contexto.

Entorno legal para priorizar los productos de origen nacional frente al producto extranjero

La oportunidad para desarrollar y proveer al Estado ecuatoriano software de origen nacional, pese a la existencia de las grandes corporaciones internacionales como Microsoft, Oracle, etc. que lideran el mercado del software mundial, esta consagrado en la Ley.

El Artículo 339 de la Constitución ecuatoriana, según la Constituyente (2008) establece que:

El Estado promoverá las inversiones nacionales y extranjeras, y establecerá regulaciones específicas de acuerdo a sus tipos, otorgando prioridad a la inversión nacional.

Las inversiones se orientarán con criterios de diversificación productiva, innovación tecnológica, y generación de equilibrios regionales y sectoriales.

La UTN al ser una entidad gubernamental debe propiciar el desarrollo de la Empresa Nacional, dando las facilidades respectivas para que el producto desarrollado en Ecuador tenga

valor sobre el extranjero. Este precepto, aunque no es exclusiva responsabilidad de la Institución, debería ser aplicado al proceso de investigación en desarrollo Software productivo para consumo nacional y exportación. La calidad puede medirse con los estándares internacionales, sin embargo algunos son certificables solo por empresas extranjeras; esto dificulta la adopción del estándar a una empresa nacional. En esta investigación se elige los estándares para desarrollo de software actuales que son de libre acceso y no son privativos de adaptarse.

Manejo de procedimientos institucionales, algunos casos de estudio análogos

Para desarrollar la aplicación se optó por utilizar Oracle GlassFish Server cuya notación la describen Jendrock y cols. (2017). Se comienza automatizando un departamento semilla para hacer evolucionar el software en toda la Universidad (Runeson y Höst, 2008). En el desarrollo del software se opta por usar la metodología de desarrollo RUP, según lo que describen Alejandro y Raúl Martínez Martínez y Martínez (2011).

2.4. ESTADO DEL ARTE

2.4.1. FUNDAMENTACIÓN TEORICA Y CONCEPTUAL DE LA METODOLOGÍA UTILIZADA EN CADA FASE DEL PROYECTO

Los objetivos de este trabajo de investigación se relacionan con el cuerpo de conocimientos de la ingeniería de software, describiéndose cualitativamente las características del producto entregable y su incidencia sobre los procesos de gestión documental de la DDTI en la UTN. Para cumplir cada objetivo se establece la relación que este tiene con el SEW-

BOK y se seleccionan criterios de ingeniería de software existentes más específicos para definir, construir y valorar las características del software que satisfagan las necesidades indicadas por la DDTI.

Criterios para valorar software de gestión documental

De acuerdo a (GETDSA, 2017) los criterios para valorar son: ALMACENAMIENTO, NAVEGACIÓN Y CONSULTA como se describe a continuación:

CRITERIO	PREGUNTAS	INDICADOR	MEDIDA
ALMACENAMIENTO	Lógico,	Repositorios	TAMAÑO,
	Físico	Dependencias	LUGAR
NAVEGACIÓN	Credenciales,	Seguridad de acceso	CAPAS DE SEGURIDAD,
	Orden	Disponibilidad	RAPIDEZ DE CONSULTA
CONSULTA	Búsqueda,	Rastreabilidad,	LOCALIZACION,
	Formato	Archivos	XML, PDF

Elicitación de Requerimientos

“Un proceso de desarrollo de software es un conjunto de personas, estructuras de organización, reglas, políticas, actividades y sus procedimientos, componentes de software, metodologías, y herramientas utilizadas o creadas específicamente para definir, desarrollar, ofrecer un servicio, innovar y extender un producto de software” (Mara, 2006) Un resultado clave de la elicitación de requerimientos es la “Trazabilidad de Requerimientos de Software en Entornos Ágiles de gran escala” (Paula-Izaurre, 2018), por pequeño que sea el producto en número de requerimientos funcionales basado en la experiencia de Paula-Izaurre (2018) para determinar los principales atributos y características que debe cumplir un requerimiento, se puede simplificar la elicitación de requerimientos mediante una entrevista

que contenga lo siguiente:

Los resultados verificables del proceso de elicitación son cuadros con mnemotécnicos de

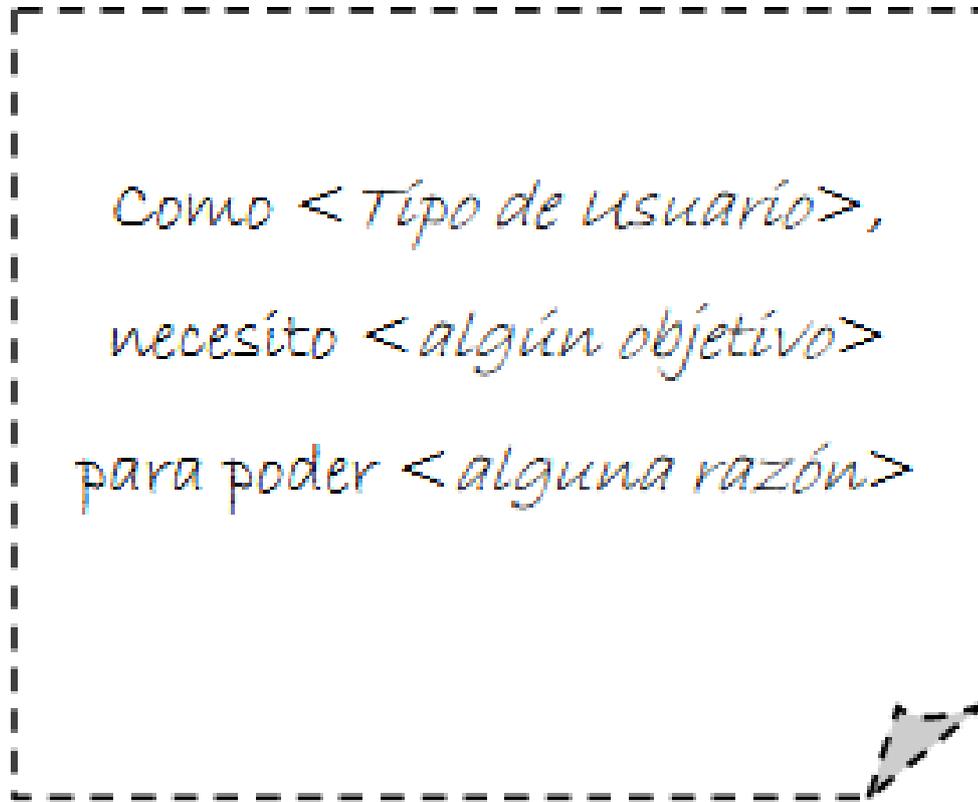


Figura 3: Historias de usuario.(Paula-Izaurre, 2018)

diálogo informales enfatizando la participación del cliente y la entrega del producto de software en respuesta a la evolución de requerimientos.

Trazabilidad de requerimientos de software aplicada al proyecto

Se encontraron al menos dos criterios para definir la trazabilidad de requerimientos del software: RUP descrito por Sandoval (2008) y Ágil ya descrito anteriormente, el primero un criterio formal y el segundo informal.

2.4.2. Requisitos de software. Una revisión sistemática de literatura

Según Abad, Noaen, y Ruhe (2016), se han sintetizado al menos 18 patrones de uso codificando los documentos SRS. Otros autores exponen que: “La industria y la sociedad en su conjunto se enfrentan a cambios radicales debido al rápido crecimiento de las tecnologías digitales ya su penetración en prácticamente todas las áreas”(Ebert y Duarte, 2016). Un estándar actual en la industria utilizado para documentar especificaciones de requisitos del Software es el Estándar ISO/iec 29148. Debido a que el Estándar ISO / IEC 29148 es más conocido en la UTN, se lo adopta para describir los requisitos de software. Hacer las preguntas correctas y capturar información precisa sobre los requisitos es una característica que describen Juristo, Moreno, y Sanchez-Segura (2007) acerca del proceso de especificación. Para probar el software bajo las especificaciones correspondientes se recomienda adaptar el estándar ISO 9126 por su simplicidad frente al ISO 29119 que propone “Software and systems engineering Software testing Part 1:Concepts and definitions” (2013), que contiene normas para verificación formal, control del proceso y pruebas de software.

2.4.3. Arquitectura de servicios del repositorio de firma digital

REGLAS DE NEGOCIO. Acuerdo de nivel de servicio

Cuando se trata de la aplicación para computadora, orientada a servicios sobre la Web, el SLA es una característica clave; de acuerdo a “Research on Cloud Resource Optimization Model Based on Users’ Satisfaction” (2016), la calidad del servicio requiere métricas e indicadores específicos basados en tiempo de respuesta y satisfacción del cliente. Para el caso de la certificación electrónica es fundamental establecer un proceso de ejecución del servicio que consuma el menor tiempo de respuesta posible y sea de preferencia infalible. Es necesario considerar el acuerdo de nivel de servicio en vista que la organización que

desarrolla el BPM mantiene este tipo de documento para el desarrollo de los procesos de gestión automatizados al interior de la UTN. Para el caso del servicio del repositorio de firmas digitales solo se debe considerar la disponibilidad de la base de datos del SIIU y la interoperación mediante SOA.

Seguridad de Acceso en la computación ubicua

Uno de los principales retos de la certificación electrónica sobre la Web es su seguridad. Fraley y Cannady (2016) exponen sobre el ritmo de crecimiento del malware polimórfico y metamórfico que han podido evitar infraestructuras de protección y atacar su objetivo. En el desarrollo de la aplicación se toma en cuenta la seguridad como un factor clave para la infalibilidad del servicio de certificación electrónica en factores como: determinación de autenticidad del sujeto solicitante, integridad del documento cifrado y firmado, transporte sobre la Internet y aseguramiento de la infraestructura física del servidor Web de la UTN. Hasta el momento se aprovecha los beneficios de las investigaciones sobre Seguridad conocidas y la aplicación de las mejores estrategias adoptadas por el DDTI-UTN.

Determinación de la autenticidad del sujeto solicitante

Un servicio Web del registro civil entrega información confidencial mediante convenio entre las partes.

Integridad del documento cifrado y firmado

El protocolo adoptado para firmar el archivo digital que representa un documento en formato XML es el X.509. Jacobs (2016) explica que la autenticación es un servicio básico de seguridad, según este protocolo, existen varios enfoques para asegurar la autenticidad del documento cifrado: KDC,PKI(sobre el que están los certificados digitales en base al estándar X.509), RADIUS, Diameter y Set.

La adopción y adaptación de X.509 al protocolo de certificación electrónica mediante una

aplicación tipo SOA alojada en un Cloud es una decisión tomada sobre la base del uso que se le da en el Ecuador a la firma digital y cuya implementación opera mejor sobre infraestructuras compatibles para integración de sistemas y aplicaciones de computadora en . Se prevé que el SIIU de la UTN emitirá documentación legal desde procesos tales como: facturación electrónica, declaración de impuestos, certificados de diversa índole, matriculación, promociones, graduación, administración de talento humano, comunicaciones legales con diversas instituciones públicas o privadas y personas nacionales o extranjeras, sistemas de pago y acceso a datos. En estos casos y por lo expuesto en el Reglamento a Ley de Comercio electrónico deberá usarse los estándares adoptados por el gobierno para que exista compatibilidad al integrar procesos de software heterogéneos. **Transporte sobre Internet**

Https es el protocolo de comunicación más utilizado por los navegadores Web. Su funcionamiento se basa en algoritmos SSL/TLS que son utilizados, según Suga (2014), por la Agencia de Seguridad Nacional en EEUU. Este protocolo permite comunicación cifrada de un extremo a otro basado en archivos de llave para cifrar y descifrar datos. Uno de los principales problemas recurrentes es la ralentización del servicio, este detalle ha sido considerado en la especificación de requerimientos para el Software orientado a servicios de certificación electrónica.

Protección de datos. Aspecto legal de la certificación electrónica en el Ecuador.

El Art. 92 de la Constitución ecuatoriana establece la Acción de Habeas Data (Constituyente, 2008), según esta, toda persona tiene derecho a la protección de datos; esto implica que el responsable de Software debe garantizar la seguridad informática y la atención al pedido ciudadano.

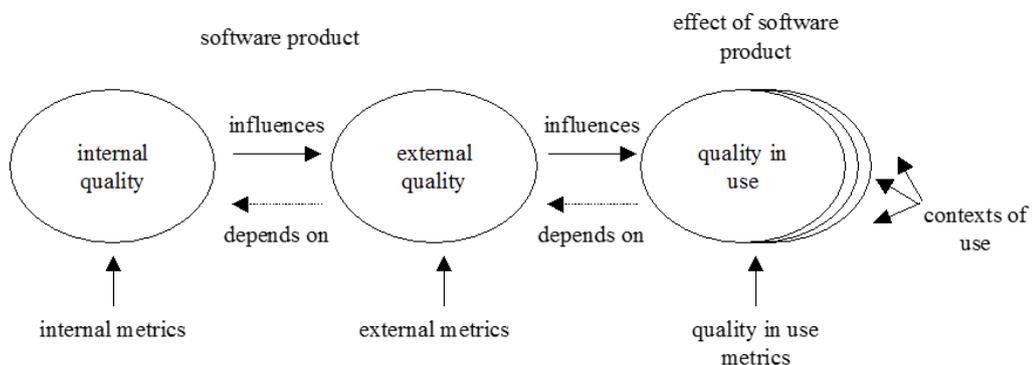
Acción de hábeas data Art. 92.- Toda persona, por sus propios derechos o como representante legitimado para el efecto, tendrá derecho a conocer de la existencia y a acceder

a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico. Asimismo tendrá derecho a conocer el uso que se haga de ellos, su finalidad, el origen y destino de información personal y el tiempo de vigencia del archivo o banco de datos. Las personas responsables de los bancos o archivos de datos personales podrán difundir la información archivada con autorización de su titular o de la ley. La persona titular de los datos podrá solicitar al responsable el acceso sin costo al archivo, así como la actualización de los datos, su rectificación, eliminación o anulación. En el caso de datos sensibles, cuyo archivo deberá estar autorizado por la ley o por la persona titular, se exigirá la adopción de las medidas de seguridad necesarias. Si no se atendiera su solicitud, ésta podrá acudir a la jueza o juez. La persona afectada podrá demandar por los perjuicios ocasionados.

Aspecto tecnológico

La organización (ISO/IEC-JTC1-/SC-7/WG-6, 2002) proporciona identificación de métricas de calidad del Software en Utilización como se observa en la figura: Aunque el cumpli-

Figura 4: Influencia de la calidad de software en uso según la ISO / IEC 9126-3



miento total de la norma es un proceso extenso que involucra diferentes factores entre los más relevantes: (1) La tecnología de hardware y software de base sobre la que se sustenta

la aplicación, (2) la administración del sistema informático integrado y (3) la calidad de las reglas de negocio sobre las que se pretende aplicar: Leyes internas y externas de la UTN, en este caso es indispensable marcar lineamientos para el cambio de reglamentación con la finalidad de adoptar la implementación del servicio basado en normas claras que permitan solucionar incidentes que pudieran suscitarse basados en causas específicas: humanas, tecnológicas o ambientales. La descripción de todos estos factores no es parte del presente trabajo de investigación.

Bajo esta norma el contexto de utilización del servicio de firma digital es el SIIU, sobre la base de datos ORACLE 12c con aplicación web sobre APACHE en ORACLE LINUX 6.9.

2.4.4. Incidencia: Influencia del Software en la comunicación institucional

¿Cuál es la incidencia real del Software para servicios de certificación electrónica sobre la comunicación institucional? En el caso GDTUTN, se considera un cambio en estado de la comunicación documental que puede ser observado mediante las métricas establecidas para medir el impacto del mismo y que han sido definidas en este acápite.

El proceso que se sigue para determinar la influencia real del software en la comunicación institucional responde a las especificaciones de requerimientos del DDTI-UTN. Las ERS han sido documentadas, su influencia esta prevista y esperada según el LSA (Acuerdo de Nivel de Servicio según ITIL, aunque ITIL (2000) considera incidencia a: “Cualquier evento que no forma parte del desarrollo habitual del servicio y que causa, o puede causar una interrupción del mismo o una reducción de la calidad de dicho servicio. El objetivo de ITIL es reiniciar el funcionamiento normal tan rápido como sea posible con el menor impacto para el negocio y el usuario con el menor coste posible.”). Al inicio de la puesta en marcha

y operación del Software, existen muy pocos datos para decidir lo que ocurrirá pero si es posible blindar y armar el Software, adoptando estándares que le permitan crecer y evolucionar durante el ciclo de vida productivo. La gente medirá su impacto personal y decidirá si usarlo o no, según haya mayores beneficios que obstáculos o amenazas según se hayan ejecutado en firme, incidir positivamente en la gestión del trámite es lo esperado.

Durante el ciclo de servicio, este Software aporta beneficios tangibles que pueden ser medidos según las métricas establecidas para medir su impacto, y otros intangibles que se guardan en la memoria de los consumidores humanos. Estos últimos son determinantes para seguir usando el Software o no. Un indicador esperado positivo es que, la aplicación de computadora entregada a la DDTI-UTN, se siga usando muchos años después de haber sido firmado el acta de entrega y recepción. Otro indicador indirecto es la visión de gente sobre el sistema de gestión documental, que sale del ámbito de la presente investigación.

Evidencia se recoge mediante una ejecución del Software, con recolección de datos sobre el modelo de colas, aplicado al caso de estudio del Servicio de Firmas digitales para certificación documental y flujos de trabajo del trámite institucional.

Aclaración: Gestionar la incidencia es diferente a incidir la gestión. En el primer caso se trata de hacer algo para solucionar una incidencia u ocurrencia de un evento indeseado o inesperado y que afecta negativamente sobre el proceso empresarial, en este caso una normativa aplicable es la ISO/IEC 20000, pero esto no es el objetivo ni esta dentro del alcance de este trabajo. En el segundo caso se trata de influir positivamente sobre el proceso empresarial a fin de obtener una mejoría en algún indicador de evaluación respecto a la gestión, en el caso ingeniería de software, se trata de utilizarlo con la esperanza que influya positivamente sobre la gestión del trámite institucional en el caso UTN, por lo menos en dos indicadores de evaluación: **eficiencia del trámite y disminución del consumo de papel** en

al menos un proceso de gestión: **solicitud de certificados de matrícula.**

2.4.5. Métricas de incidencia en aplicaciones orientadas a servicios en la gestión del trámite institucional en la UTN

La tendencia del Internet de las Cosas, IoT, sobre la Web, consiste en integrar las Aplicaciones Web, WebApps, en servicios del tipo: Protocolo de Aplicaciones Orientadas a Servicio, SOAP, que como se ha visto, se alojan en una nube, Cloud, pública o privada, sobre Internet. La Calidad del Servicio, QoS, definida sobre características de la arquitectura del SOAP, dispone de métricas para medir el cumplimiento sobre Acuerdo del Nivel de Servicio, SLA, establecido para el uso del Cloud o servidor de WebApps y Bases de Datos. Algunos autores proponen aplicar la teoría de juegos para asegurar QoS en entornos Cloud, como por ejemplo, Chejerla y Madria (2017), que nos muestran un entorno resiliente al ataque. Una aplicación tipo WebApp orientada a SOAP debe satisfacer los requisitos establecidos y garantizar la seguridad, que para el caso de la UTN, debe integrar los requisitos establecidos en el documento contractual producto de la elicitación de requerimientos y las condiciones legales establecidas por el Honorable Consejo Universitario para Utilizar el Repositorio de firmas digitales en la gestión del trámite institucional. Los Sistemas de Seguridad Crítica (SCS) requieren enfoques de ingeniería de requisitos (RE) más sofisticados, esto según Vilela, Castro, Martins, y Gorschek (2017), muestran una taxonomía en que se han utilizado técnicas de:

- (1) análisis de riesgos
- (2) análisis de seguridad
- (3) información relacionada con la seguridad

- (4) un conjunto detallado de información sobre la especificación de peligros

El consumo de una aplicación SOAP en la gestión del trámite institucional es del tipo SCS porque el uso del Software debe cumplir estrictamente con la Ley en forma infalible, esto implica establecer métricas de consumo SOAP con un SLA muy estricto en características de Seguridad y Utilidad para el SIIU como requerimientos no funcionales mínimos.

Sobre el diseño de Cyber-Physical-Systems, CPS, según (Ashibani y Mahmoud, 2017), los problemas de seguridad en esta área se han convertido en un tema global. El indicador de seguridad sobre métricas de consumo aceptable para la UTN es, que el número de errores en el servicio sea cero o localizable hasta el origen, con un nivel de certeza del 100%. Esto significa que todos los documentos firmados deben: archivarse y registrarse en forma adecuada inmediatamente se hayan generado, asegurarse la identidad del sujeto solicitante y del firmante, el proceso de certificación debe ser legalmente correcto, el orden de los pasos del algoritmo de certificación electrónica debe seguirse en forma estricta, debe ocultarse la información respecto a terceros, acceso a datos oportuno y sin errores, distinguir humano robot, entorno del servicio libre de virus informáticos y otras amenazas. Algunas de estas características pueden medirse directamente a través del Software y su resumen mostrarse como un informe sobre métricas de consumo del Webservice. Tres características que un Cloud debe satisfacer y son consideradas importantes de acuerdo a Alonso, Escalante, y Orue-Echevarria (2016): **portabilidad de datos, la privacidad de los datos y la interoperabilidad.**

Modelo de colas aplicable al Servicio de certificación digital del caso UTN

Para evaluar un servicio Web tipo SOA, la aplicación se expone al riesgo de incumplir por lo menos uno de tres requisitos no funcionales sugeridos por Costa, Pires, Delicato,

y Merson (2016): seguridad, fiabilidad y rendimiento durante la ejecución del servicio. El Software de certificación digital debe responder a un modelo de múltiple servidor para atender múltiples clientes, considerando que en la mayoría de las veces existirá mas clientes solicitando documentos que servidores atendiendo pedidos. Dada la naturaleza del Servicio, un modelo de colas resulta aplicable para medir la QoS en los tres requisitos no funcionales mencionados. Un elemento clave es la determinación del modelo de servicio aplicable, en concordancia con Jafer, Liu, y Wainer (2013), emula la sincronía de eventos discretos en servicios paralelos de certificación digital que opera sobre una plataforma heterogénea de servicios integrados mediante ESB, WebServices, Cloud y SOAP. Un enfoque adecuado en la selección del tipo de arquitectura SOAP, de acuerdo a Reeve (2013): “minimiza el impacto en el sistema de origen y el tamaño de los mensajes enviados entre instancias”.

Breve resumen de la teoría de colas

Debido a la naturaleza de las métricas de calidad del servicio de firmas digitales y su incidencia sobre gestión documental es necesario establecer un modelo matemático para fundamentar las líneas de espera y definir el tipo de colas y su respectivo indicador. Las fórmulas no son nuevas y sus definiciones se adaptan para valorar y fundamentar esta investigación, un resumen válido se refiere Lillo (2018), aquí un extracto:

- Cliente se considera una solicitud de documento firmado. Estas solicitudes pueden auto numerarse a medida que el software captura la solicitud en línea. El tiempo que se demora una solicitud en llegar despues de otra se considera tiempo entre llegadas. Un cliente tardara un total de tiempo entre llegada, en la cola y en ser servido. Esta demora puede ocasionar molestias y en algunos casos
- Servicio se considera la aplicación de software que ejecuta el proceso de negocio ma-

nual o automatizadamente. El servicio puede demorarse mas o menos tiempo según la naturaleza del trámite y la disponibilidad de tiempo del firmante sea este personal o electrónico. Este tiempo se denomina tiempo de servicio.

- Cola o canal de espera. Puede ser de uno o vario canales y tiene una disciplina que puede ser FIFO, LIFO, aleatorio, orden de prioridad, etc. La longitud de la cola se mide por el número de clientes en línea de espera. El tiempo en la cola es el tiempo que tarda un cliente entre el tiempo de llegada y el tiempo que comienza a ser atendido.

Para modelar el comportamiento complejo de sistemas de software con muchos servidores y colas es conveniente usar simuladores, en concordancia con (Lillo, 2018). Los indicadores esperados de incidencia del uso del repositorio de firmas digitales sobre la gestión de trámites institucionales pueden ser obtenidos mediante simulación de la teoría de colas.

Estos valores pueden ser comparados con los obtenidos experimentalmente mediante la implementación y pruebas de los servicios.

El comportamiento variable de un servicio se puede estandarizar por medio de técnicas estadísticas que facilitan la tarea de estimación en tiempos y costos.

2.5. PROPOSICIÓN

El uso del repositorio de firmas digitales incide positivamente sobre la gestión documental interna y externa de la UTN en el ámbito legal y tecnológico.

Capítulo 3

METODOLOGÍA

3.1. Tipo de investigación

Tipo de Investigación Aplicada. Descriptiva y Correlacional.

3.2. Método de investigación

Se usó principalmente el Inductivo Deductivo.

3.3. Diseño de la investigación

Es descriptiva y correlacional.

3.4. Modalidad de Investigación

3.4.1. Investigación de campo

Esta investigación se realiza directamente en las dependencias de la UTN que representan las unidades de observación descritas. Para obtener resultados tangibles a corto plazo que faciliten la obtención de verificadores de cumplimiento se elige el proceso MATRICU-

LACIÓN y la obtención de certificados de matrícula firmados digitalmente como evidencia del cumplimiento.

3.4.2. Investigación documental bibliográfica

Con el propósito de fortalecer la investigación, se recurre a obtener la información teórica de diferentes autores obtenidas en fuentes secundaria (libros, revistas especializadas, publicaciones, internet, etc.), también en fuentes de información primaria a través de documentos válidos y confiables.

3.4.3. Exploratorio

Se exploran y valoran las alternativas de solución automatizadas para gestionar el trámite institucional mediante el uso del repositorio de firmas digitales de la UTN, Específicamente se describe la relación que debe existir entre el servicio de firma electrónica y la emisión de certificados obtenidos mediante el SIIU en la UTN.

3.4.4. Descriptivo

Se describe cualitativamente los estándares de calidad aplicables: ISO / IEC 29148 para elicitación de requerimientos y el 9126 para control de calidad del software de servicios del repositorio de firmas digitales.

Cuadro 1: Verificadores de trazabilidad del software basado en objetivos del proyecto.

PROCESOS	RUP	AGIL	OBJ.	PRODUCTOS
REQUERIMIENTOS	CONCEPCION	HISTORIAS	OE1	DOC-ISO / IEC 29148
VALORACION	CONCEPCION	HISTORIAS	OE2	DOC-ISO / IEC 9126
ARQUITECTURA	ELABORACIÓN		OE3	ARQ-OMGSYSMLv1.4
DESARROLLO	CONSTRUCCIÓN	SCRUM	OE4	ALG-GDTUTNv1.0
RELACION SIIU	TRANSICION		OE5	IMPL-GDTUTNv1.0

3.5. Esquema para el cumplimiento de objetivos

CONCEPCION. OE1 Y OE2

OBJETIVOS	INDICADORES	VERIFICADORES
OE1	Número de RQ establecidos por la DDTI	ISO / IEC 29148
OE2	Atributos de calidad	ISO / IEC 9126-3

ELABORACIÓN. OE3

OBJETIVOS	INDICADORES	VERIFICADORES
OE3	Estilos arquitecturales	X.509, SOAP, JDBC, PL/SQL

CONSTRUCCIÓN. OE4

OBJETIVO	INDICADORES	VERIFICADORES
OE4	Conjunto de algoritmos	RESULTADOS DE LAS PRUEBAS

TRANSICION. OE5

OBJETIVO	INDICADORES	VERIFICADORES
OE5	Número de XML firmados	XML FIRMADOS EN LA UTN

3.6. Variables e indicadores

El proceso de gestión de trámite institucional es considerado variable dependiente con respecto al uso del repositorio de firmas digitales.

La incidencia del uso del repositorio de firmas digitales en la gestión de trámites institucionales es la relación que se establece cualitativa y cuantitativamente en esta investigación.

CONCEPTUALIZACION	DIMENSIONES	INDICADORES	ITEMS BASICOS	TECNICAS E INSTRUMENTOS	
VD: Gestión de trámites institucionales de la Universidad Técnica Del Norte.	Flujo de trabajo para solicitudes de documentación legal en la UTN	Mapas de ruta de solicitudes de documentación requerida por:	¿Cómo se genera la documentación legal requerida por estudiantes, empleados y secretario abogado?	Entrevista	
			1. Estudiantes	Guía de Entrevista	
Es el recorrido que sigue un documento legal solicitado por alguien en la UTN y que se analiza, firma y/o devuelve al interesado en un tiempo determinado.	Levantamiento de tramites:	2. Empleados			
					1. Estudiantes
	2. Empleados	Numero de documentos autorizados, rechazados, firmados manualmente, firmados automáticamente,			Muestras obtenidas de documentos en proceso
	3. Secretario Abogado				

Figura 1: Operacionalización de la Variable Dependiente

CONCEPTUALIZACION	DIMENSIONES	INDICADORES	ITEMS BASICOS	TECNICAS E INSTRUMENTOS
VI: Uso del repositorio de firmas digitales disponibles en la base de datos de la UTN	Creación de Firmas digitales	Nro. De firmas digitales existentes	¿Cuántas firmas se crean o modifican en el repositorio?	Observación
				Muestras obtenidas de firmas digitales
Es el servicio que se pretende dar al repositorio de firmas digitales para emitir y archivar digitalmente documentos firmados de forma automática.	Servicios del Repositorio	Operaciones de firmado: solicitud, validación (aceptación o negación), firma, entrega o devolución de documento firmado digitalmente	¿Cuántas operaciones de firmado se realizan?	
	Acceso a la Base de Datos de la UTN	Servicios del repositorio de firmas digitales disponibles en la base de datos de la UTN		Observación
				Muestras obtenidas de documentos firmados
	Peticiones de documentos legales de estudiantes y otros interesados			
	Acciones legales documentadas de los funcionarios			
	Actividades legales documentadas del secretario abogado			

Figura 2: Operacionalización de la Variable Independiente

3.6.1. Técnicas

Para describir cualitativa y cuantitativamente las variables del problema se utilizan las siguientes técnicas: Obtención de muestras del campo, Entrevista, Observación.

Obtención de muestras de campo

Para definir elementos cuantitativos y su crecimiento con el tiempo, por ejemplo, el número de peticiones de documentos en un departamento de prueba en este caso DDTI-UTN.

Entrevista

Se entrevista a la Abogada del Instituto de Postgrado para obtener información cuantitativa del uso de las firmas digitales y la relación con los trámites legales del IP-UTN, como departamento escogido para semilla por su similitud con otras dependencias universitarias.

Observación

Se observa los procesos de gestión de trámites institucionales automatizados tanto con el uso del Sistema Documental institucional denominado Quipux así como el BPM que el DDTI-UTN implementa en Aura Portal para usarse en toda la Universidad.

Se sintetiza la obtención del certificado de matrícula en formato XML basado en la observación de las muestras de certificados firmados manualmente y la entrevista la Ing. María Fernanda Rivera funcionaria de la DDTI en la UTN.

3.6.2. Instrumentos

Para la adquisición de datos experimentales y resultados de las entrevistas se utiliza como instrumentos: celular, correo electrónico, Base de Datos Oracle, IDE NetBeans, una herramienta de software libre para análisis correlacional.

Para las encuestas se utilizan fichas de encuesta.

3.7. Población

Actualmente, en el año 2018 la UTN cuenta con aproximadamente 8583 estudiantes según datos proporcionados por la DDTI-UTN. Por esta razón, se considera aplicar una muestra de 368 estudiantes para que una prueba comparativa tenga un nivel de confianza de 95%. Además se observa que durante el tiempo de esta investigación, el número de estudiantes aumenta a un ritmo promedio del 2,11% anual.

3.8. Fase 1: Determinar los requerimientos del Software para la gestión de servicios de mensajes de datos firmados en la UTN

Cumplir las siguientes etapas:

- Primera. Elicitación, documentación y validación de requisitos de calidad de software para gestión de trámites institucionales de la UTN adoptando parcialmente el Estándar ISO/IEC 29148.
- Segunda. Establecer un escenario de aplicación en el caso de uso que sirva de modelo para el uso en la gestión de trámites institucionales de forma general aplicable al caso de la UTN.
- Tercera. Determinar indicadores para valorar la usabilidad y seguridad de alternativas de software para la gestión de servicios de mensajes de datos firmados, entrevista

a: Ing. Juan Carlos García, Director DDTI UTN, Ab. Angélica Espinosa Trujillo,
Secretaria Abogada IP UTN.

3.9. Fase 2: Valorar usabilidad y seguridad de alternativas de software para la gestión de servicios de mensajes de datos firmados

Etapas:

- Primera. Determinar cuales alternativas son viables y especificar las características que cumplen o no según los indicadores de utilidad para la DDTI establecidos en la tercera etapa de cumplimiento del OE1.
- Segunda. Valorar las alternativas adoptando la ISO / IEC 9126-3 de acuerdo a los parámetros descritos en el documento de arquitectura de software del servicio de firmas digitales de la UTN.

3.9.1. Consideraciones de los estudiantes sobre la usabilidad

Ficha de Encuesta estudiantil

OBJETIVO

Determinar el grado de necesidad de software para gestión de trámites institucionales y establecer los parámetros de medida del impacto de su uso. Encuesta con nombres y apellidos del encuestado en los patios de la UTN.

ASPECTOS OPERATIVOS

1. Ha solicitado documentos firmados en alguna dependencia universitaria

2. Cuantos documentos estima Ud que ha solicitado durante su permanencia en la UTN
3. Tiene cuenta en QUIPUX
4. Tiene firma electrónica emitida por el registro civil
5. Cuantas veces la ha utilizado

ASPECTOS LEGALES

1. Cuales documentos fueron los principalmente requeridos para su matrícula

ASPECTOS DE USABILIDAD

1. Cual es su horario de entrada y salida
2. Tiene un reporte impreso de notas legalizado
3. Cual medio utiliza mas para gestionar su trámite WEB, IMPRESO, OTRO
4. Conoce la utilidad de la firma electrónica para la gestión del trámite institucional
5. Le gusta utilizar el servicio Web de gestion documental implementado
6. La gestión del trámite en su criterio dentro de la UTN es rápida o lenta

3.10. Fase 3: Diseñar la Arquitectura del Software para gestión de servicios de mensajes de datos firmados en las dependencias de la UTN considerando su factibilidad de implementación

3.10.1. Descripción del proceso de selección y adaptación de estilos arquitecturales aplicables

- Estilo arquitectural del SIIU en la UTN.
- Arquitectura para firmar y validar certificados XML con el estándar X.509 y firma electrónica emitida por el BCE.

3.10.2. DISEÑO MACRO

- Descripción del diseño que se incorpora al SIIU.
- Adaptacion a los drivers o interfaces que debe tener para acoplar el servicio de firma digital con el ERP de la UTN.

3.10.3. DISEÑO MICRO

Para cada bloque de la arquitectura se describe que hace, como se conecta y que atributos de calidad se cumplen. Se indica como medir esa calidad obtenida por cada atributo seleccionado.

3.10.4. EVALUACIÓN

Se determinan dos atributos de calidad para ser evaluados según la ISO / IEC 9126: Funcionalidad, usabilidad.

3.10.5. IMPLEMENTACIÓN

Para la implementación de la arquitectura se considera:

- Realizar la programación o adquisición de código existente basado en requerimientos establecidos
- Ajustar el diseño si se encuentra deficiencias
- Experimentar en ambiente controlado la implementación de los componentes
- Establecer una relación efectiva entre la nueva solución y el SIIU considerando estándares de comunicación.

Seleccionar uno de los siguientes procesos de gestión de trámites institucionales para verificar la factibilidad de implementación mediante el desarrollo de un conjunto de algoritmos de servicio de firmas digitales y relacionar este software con el ERP institucional:

- Procedimiento de trámites académicos
- Solicitud de matrícula
- Reingreso (cada facultad lo maneja diferente)
- Secretarios Jurídicos de las Facultades
- Secretarias de carrera
- Cambio de Horario (de estudiantes)
- Asentamiento de notas (por pedido de estudiante) (para casos en que no se asentó la nota)
- Practicas preprofesionales

- Proyectos de Investigación (doc tiempo completo)

3.11. Fase 4: Desarrollo del conjunto de algoritmos de servicio de firmas digitales dentro de los límites de la infraestructura física y lógica del SIIU (ERP de la UTN)

Para el desarrollo del conjunto de algoritmos de servicio de firmas digitales se sigue el siguiente proceso: Para cumplir con lo establecido en la arquitectura propuesta para incidir positivamente sobre los procesos de gestión de trámites basados en información obtenida del SIIU se desarrolla:

- Delimitación de los límites físicos y lógicos del ERP de la UTN
- Algoritmos para conectar a la base de datos del SIIU
- Algoritmos para firmar y validar documentos firmados digitalmente mediante SOAP en JAVA
- Algoritmos para generar documentos XML en PL/SQL

3.12. Fase 5: Relacionar el software de servicios del repositorio de firmas digitales con el ERP institucional integrando componentes más pertinentes según sea el caso

Para el cumplimiento de este objetivo se describe lo siguiente:

- Diseñar y valorar un prototipo de gestión documental GDTUTN, de propósito general basado en el SIIU considerando los criterios de ALMACENAMIENTO, NAVEGACIÓN y CONSULTA
- Obtener indicadores de uso basados en ALMACENAMIENTO, NAVEGACIÓN y CONSULTA experimentales que permitan tomar decisiones sobre el impacto del servicio de firma digital en la gestión de trámites institucionales basada en el SIIU de la UTN.

Capítulo 4

RESULTADOS Y DISCUSIÓN

4.1. RESULTADOS

A continuación se presenta los resultados y hallazgos obtenidos en cada fase por cada objetivo:

4.1.1. R1: Requerimientos del Software para la gestión de servicios de mensajes de datos firmados en la UTN

Funcionales

R1. El Sistema debe aceptar solicitudes de documentos firmados.

R2. El Sistema debe responder cada solicitud de forma AUTOMÁTICA o MANUAL.

R3. El Sistema debe emitir documentos firmados de forma AUTOMÁTICA en caso de ser pertinente.

No Funcionales

1. El formato de intercambio de los mensajes debe ser XML.

2. El protocolo de intercambio de mensajes de datos firmados debe ser SOAP.
3. Los documentos XML deben ser generados desde cualquier repositorio de firmas digitales de la UTN y almacenados en el cliente HTTP.
4. Los certificados XML firmados deben contener la firma electrónica en formato X.509 que es el estándar compatible con las entidades gubernamentales en el Ecuador al momento de la redactar este documento de informe.
5. Es obligatorio que los documentos XML contengan la línea de atributos: `<documento id=çcomprobante”versión=”1.0.0”>`
6. El servicio de firma debe almacenar la firma p12 en el repositorio de datos del SIIU
7. El cliente debe almacenar el documento XML a ser firmado en un repositorio HTTP que este soportado por un servidor web
8. El sistema de servicio de firma electrónica debe garantizar la protección de datos según el Habeas Data previsto en la constitución

Escenario de aplicación Caso de uso: CERTIFICADOS DE MATRÍCULA

Cualquier interesado puede solicitar la generación de un certificado matrícula. El sistema responde emitiendo el certificado o denegando la solicitud según la identidad del interesado y la existencia de su información en el SIIU.

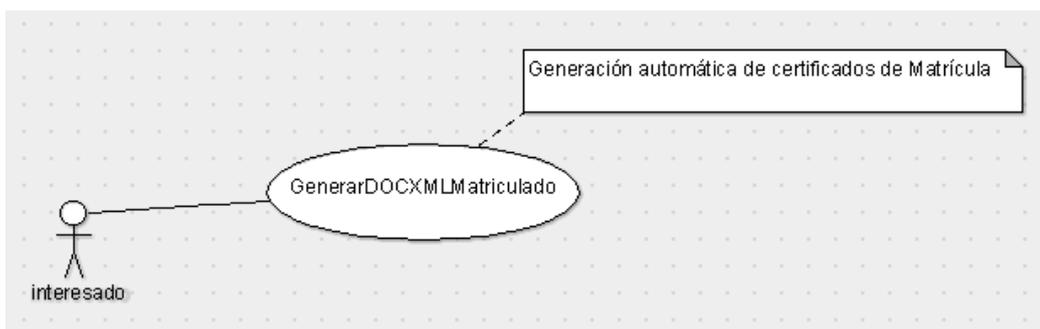


Figura 1: Caso de Uso: Emisión de certificados de Matrícula

ENTRADA	ES ESTUDIANTE	ESTA MATRICULADO	SALIDA
CEDULA, TRAMITE	V	V	AUTORIZADO
CEDULA,TRAMITE	V	F	SOLICITADO
CEDULA,TRAMITE	F	F	DENEGADO
CEDULA,TRAMITE	F	V	IMPOSIBLE

Indicadores de utilidad para el SIIU: Evaluación de requerimientos

Para obtener los indicadores de utilidad se describe el caso de uso en concordancia con lo requerido por la DDTI y se procede a verificar las tres reglas que debe cumplir el repositorio:

- I1. El Solicitante debe estar autenticado en el sistema y demostrar que no es un robot.
- I2. Las Solicitudes tienen un Tipo de Documento que indica el tipo de resolución que debe tomarse: Manual o Automática.
- I3. Se emiten certificados automáticos cuando el tipo de documento es Automático, la solicitud es VÁLIDA y el solicitante sea humano.

De acuerdo al caso de uso mostrado en la Figura 1 un posible suceso es:

1. Un interesado solicita un documento XML que indica si está matriculado mediante el

envío de un código puede ser su cédula; el interesado puede ser un usuario del SIIU externo (humano) u otro proceso automatizado un cliente de Aura Portal.

2. El proceso GenerarDOCXMLMatriculado revisa si el código (cédula) consta en la base de datos de matriculados
3. En caso de constar en la base de datos de matriculados genera el documento correspondiente y lo pone a disposición del interesado; la generación del documento implica: validar datos del interesado, firmar digitalmente y almacenar resultado obtenido
4. En caso de NO constar NO genera ningun documento

Intercambio de mensajería entre el interesado y el servicio usando SOAP

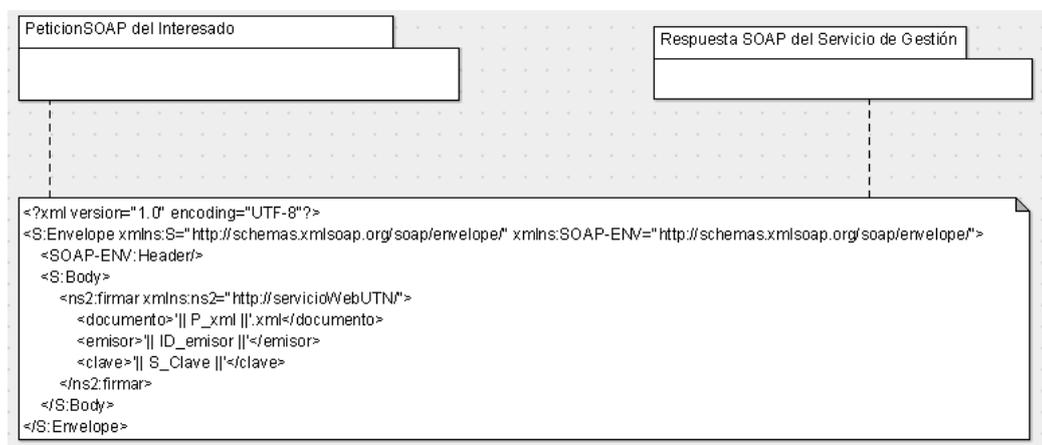


Figura 2: Intercambio de mensajes entre un interesado y el servicio de firma electrónica

Indicadores para valorar usabilidad y seguridad de alternativas de software para la gestión de mensajes de datos firmados

Los indicadores se listan en el capítulo 3.5 del documento de especificación de requerimientos.

Estos indicadores sirvieron a la DDTI para seleccionar un proveedor de software que los

cumpla.

En esta parte del proceso se resaltan solo los atributos compatibles con el estándar 9126: usabilidad, fiabilidad y portabilidad.

Para el cumplimiento de atributos de usabilidad: facilidad para solicitar un certificado, tiempo de respuesta aceptable, empatía con el software propuesto; para fiabilidad: cumplimiento del habeas data, tolerancia a fallos; y para portabilidad: adaptabilidad.

La matriz de evaluación de alternativas de software es la siguiente:

RQ.	INDICADOR	MEDIDA	FUENTE
facilidad uso	Opinión	SI/NO	ENTREVISTA
demoras	tiempo	minutos	SECRETARIA
empatía	Opinión	SI/NO	ENTREVISTA
cumplimiento LEY	Número	ACCESOS N/A	DDTI
tolerancia a fallos	Número	CAIDAS SERVICIO	DDTI
adaptabilidad	LÓGICO	SI/NO	SIIU

Estos criterios se recogen de las entrevistas en la DDTI y Secretaria Jurídica del Instituto de Posgrado de la UTN.

Los atributos de calidad se describen en el anexo sobre la Arquitectura del Software y están basados en la norma ISO / IEC 9126-3.

4.1.2. R2: Valoración de Usabilidad y seguridad del software para la gestión de servicios de mensajes de datos firmados. Atributos de calidad basados en el ISO 9126.

De acuerdo a la matriz de evaluación de alternativas, se procedió a seleccionar las alternativas viables para la gestión documental y la emisión de certificados firmados. En un focus group se escogió como alternativa para manejar el flujo de trabajo documental: AURA PORTAL, basados en la especificación de requerimientos entregados según consta en el anexo de este informe.

Las alternativas de software cuyos atributos de calidad se evaluaron por el AUTOR son: QUIPUX-UTN, GDTUTN(PROPUESTA DEL AUTOR) y BPM de Aura Portal que fue contratado por la DDTI mediante proceso de Compras Públicas y está en fase de desarrollo.

QUIPUX-UTN

Según información obtenida de EXINDA como consta en el anexo y se encontró lo siguiente:

RQ. FACILIDAD DE USO.

En aplicaciones de entrada (recepción de solicitudes de servicio), la gestión de procesos denominada Quipux-Utn consume un 5.92% de recursos mientras que en aplicaciones de salida (respuestas de solicitudes), la gestión de procesos apenas consume un 0.31%.

En la entrevista a dos funcionarias de la institución que emiten o reciben documentación mediante QUIPUX-UTN al preguntarles sobre la facilidad de uso del sistema de gestión documental QUIPUX, en su opinión dijeron que SI era fácil de usar. El resultado obtenido es 100% facil de usar consultado a 2 funcionarias.

RQ. DEMORAS

Basado en información proporcionada por la Secretaría de la DDTI se observa lo siguiente:

Las peticiones de servicio en total representan unos 1918.17MB mientras que los consumos o respuestas de servicio en total 5920.04MB; siempre es mayor la característica de descarga que la de carga en un servicio Web, por cuanto las peticiones suelen ser paquetes pequeños de datos con especificaciones de información requerida mucho mas extensa.

Al considerar que la mayoría de procesos de documentos que pueden certificarse automáticamente están almacenados en el Cloud-Utn, se considera que tanto los Procesos-Utn y la página Web-Utn cargarán datos firmados digitalmente con un incremento de carga que se descontará de la carga del Quipux-Utn hasta en un 6.00% que es el total de carga actual de consumo de servicio Quipux-Utn el cual paulatinamente dejara de atender solicitudes y se reemplaza por un subproceso de Cloud-Utn denominado GDTUTN para efectos de esta investigación.

Debido a la baja carga o volumen de certificados el QUIPUX-UTN no tiene retrasos significativos.

RQ. EMPATIA

De igual forma a las 3 secretarias les gusta usar QUIPUX-UTN para la gestión documental. Las tres personas respondieron SI. La valoración es de 100% de empatía con este

software denominado QUIPUX.

RQ. Cumplimiento de la Ley

La DDTI, informa que no habido incidentes ACCESOS NO AUTORIZADOS al QUIPUX-UTN en todos los departamentos de la UTN.

El número de accesos n/a es cero.

Los documentos manejados por QUIPUX-UTN, si son firmados con firmas electrónicas emitidas por el BCE tienen validez legal en Ecuador.

RQ. TOLERANCIA A FALLOS

La DDTI, informa que no se ha probado ni medido este indicador pues QUIPUX-UTN es un software obligatorio para la UTN la ser de gestion gubernamental.

Sin embargo para uso interno cualquier software que se implemente debe tener un mínimo aceptable de caidas del servicio.

RQ. ADAPTABILIDAD

Es extremadamente complejo adaptar el QUIPUX-UTN al SIIU en vista de ser un software de caja negra orientado a base de datos MYSQL lo cual resulta poco factible implementar cambios para adaptarlo a resolver los procesos de gestión documental institucional usando este software.

Tiene su propio mecanismo de almacenamiento y un propósito muy general que no permite obtener consultas estructuradas de la BASE DE DATOS para generar documentación en

forma automática, especialmente académica. Un proceso básico como es el de EMISIÓN DE CERTIFICADOS DE MATRÍCULA FIRMADOS DIGITALMENTE EN FORMATO XML DE ALGÚN ESTUDIANTE DE LA UTN es imposible de generar y obtener con QUIPUX-UTN.

GDTUTN. PROPUESTA DEL AUTOR

RQ. FACILIDAD DE USO.

La propuesta GDTUTN no contempla Uso humano directo sino que se enfoca atender necesidades del SIIU para ser aprovechado por otras aplicaciones de gestión documental.

Se propone un caso de uso de prueba: EMISIÓN DE CERTIFICADOS DE MATRÍCULA FIRMADOS DIGITALMENTE para valorar este requisito.

Se establece una muestra de 368 estudiantes para evaluar este software y se les pregunta SI/NO es facil de acceder 126 de 368 respondieron que SI.

RQ. DEMORAS

En la pregunta solo 3 de 368 dijeron que si habia reducción del tiempo de servicio

RQ. EMPATIA

Al preguntarles si se simplificaba los trámites, 363 de 368 dijeron que SI.

RQ. Cumplimiento de la Ley

Ha sido virtualmente imposible hasta el momento faltar el cumplimiento del Habeas Data usando el servicio de firma digital.

El reto siempre estará vigente hasta cuando haya alguien que pueda tener un ACCESO NO

AUTORIZADO al ServicioWebUTN del GDTUN.

RQ. TOLERANCIA A FALLOS

La infraestructura de firma digital siempre responde la petición con alguna respuesta. Esta infraestructura ha sido probada en ambientes previos. Durante las comunicaciones con el SIIU no habido incidentes de falla hasta el momento.

RQ. ADAPTABILIDAD

A diferencia de QUIPUX-UTN existe un proceso básico como es el de EMISIÓN DE CERTIFICADOS DE MATRÍCULA FIRMADOS DIGITALMENTE EN FORMATO XML DE ALGÚN ESTUDIANTE DE LA UTN y es posible de generar y obtener con SIIU debido a su orientación a SOA.

Reporte de valoración del servicio de gestión de trámites en la UTN

La columna uno representa el aspecto a evaluar, la columna dos indica el número de pregunta realizada de acuerdo a la ficha anterior, la columna 3 representa SI y la columna 4 representa NO.

Los resultados se obtuvieron al inicio de este trabajo de investigación con fecha 25 de junio de 2016, a una muestra de 368 estudiantes de la UTN de un total de 7993 estudiantes registrados como matriculados. Actualmente la población estudiantil es de 8583 estudiantes y representa un crecimiento del 6.34% respecto al año 2016.

Cuadro 1: Resultados encuesta estudiantil.Elaborado por: Autor

OPERATIVA	P1	126	
OPERATIVA	P2	363	
OPERATIVA	P3	3	
OPERATIVA	P4	35	333
OPERATIVA	P5	27	341
OPERATIVA	P6	MEDIA	1
LEGAL	P1	CEDULA, FOTO	TITULO BACHILLER
UTILIDAD	P1	ENTRA=7AM	SALE=7PM
UTILIDAD	P2	345	23
UTILIDAD	P3	IMPRESO	
UTILIDAD	P4	348	20
UTILIDAD	P5	368	0
UTILIDAD	P6	LENTA	

Resultados de las observaciones sobre los atributos de calidad basados en ISO / IEC 9126 del software de servicios del repositorio de firmas digitales GDTUTN

Cuadro 2: E6.1.2 Integridad, confidencialidad y no repudio SOAP

E6.1.2 Integridad, confidencialidad y no repudio SOAP			
AMENAZAS		ENCONTRADAS	PORCENTAJE
Suplantación de identidad		0	16.67
Modificación maliciosa datos		0	16.67
Carencia de rastreo de operaciones prohibidas		0	16.67
Divulgación de información		0	16.67
Denegación del Servicio		0	16.67
Elevación de privilegios		0	16.67
TOTAL		0	100.00

Fuente: DDTI

E6.4.1 cual es el tiempo de respuesta del servicio de firma digital y cual el de entrega

Cuadro 3: E6.1.3 ingresa XML y sale XML firmado con X.509

E6.1.3 ingresa XML y sale XML firmado con X.509		
Ambiente lógico	SIU	
IP del servicio de Base de datos	129.144.35.104	
Servicio	db11g.a429576.oraclecloud.internal	
Fecha hora de inicio de las pruebas automatizadas		30/04/2018 13:08
Fecha hora de finalización		30/04/2018 13:28
Número de solicitudes XML		158
Número de ingresos XML al servicio de firma digital		74
Número de documentos XML firmados a la salida		54
Tamaño en kilobytes de archivos ingresados		45,337
Tamaño en kilobytes de archivos firmados		249,720
Duración en segundos de la prueba		1109
Tiempo entre llegadas por archivo en segundos	15,63	
Tiempo de demora en el firmado en segundos	20,53	
CHARSET	AL32UTF8	
CPU	INTEL XEON E5-2683 V3@2.00GHz	
RAM UTILIZADA	690MB	

de certificados firmados se muestra en el cuadro anterior.

E6.4.2 cual es el consumo de recursos del servicio que tamaño en bytes consume el ancho de banda, la firma, la memoria de firmado, la base de datos los datos sobre el ancho de banda se observan en el el anexo EXINDA.

E6.4.3 los resultados obtenidos SI satisfacen las expectativas esperadas por la DDTI.

E6.6.3 Coexistencia con otras aplicaciones del SIIU pues se implementa como un nuevo servicio en el puerto 8181 y 8083 de www.utn.edu.ec y se aloja en un CLOUD diferente al de Base de Datos del SIIU.

4.1.3. R3: Arquitectura del Software de Gestión de Trámites institucionales de la UTN

Se diseña esta Arquitectura siguiendo las especificaciones de la ISO / IEC 29148 Anexo C.3 relacionado al cumplimiento del item 6.4.1.1 basado en la ISO / IEC 12207 item 6.4.3.3.1.1

DISEÑO MACRO

Según Humberto Cervantes (2016), existen al menos tres estilos arquitecturales:

ID	ESTILO	DESCRIPCIÓN
1	Capas	Aislamiento lógico.
2	N-tercios	distintos nodos físicos
3	Frameworks	Acoplarse a las capas.

Debido a la arquitectura física interna del SIIU UTN que mantiene su base de datos en CLOUD DE ORACLE y el SERVIDOR WEB en OTRO CLOUD DE ORACLE, se hace obligatorio la elección del estilo arquitectural Frameworks y adaptación del SIIU para

consumir servicios Web con SOAP sobre HTTP desde el servidor de firma electrónica implementado con Glassfish4 en ORACLE LINUX habilitando los puertos 8083 y 8080 para comunicación HTTP.

El proceso de diseño se describe así:

Requerimientos de la Arquitectura

La arquitectura que se propone se basa en los requerimientos del software de servicios de gestión de trámites institucionales basado en el cumplimiento del objetivo anterior.

Reglas de negocio de firma digital

- El formato del certificado digital es XML
- La infraestructura de certificados firmados digitalmente es X.509
- La firma digital es compatible con la emitida por el BCE
- La interface de comunicaciones es SOAP
- Los documentos XML se generan en el SIIU
- Los certificados electrónicos firmados se almacenan en el repositorio de firmas digitales de la UTN
- La validez de un certificado es nacional pudiendo generarse certificados válidos para uso interno de la UTN

Reglas de negocio de la gestión de trámites institucionales

- Responder las necesidades institucionales mediante flujos de trabajo especificados en BPM
- Generar documentación firmada electrónicamente mediante el repositorio de firmas digitales de la UTN
- Cumplir las reglas de negocio del repositorio de firmas digitales en estricto apego al Habeas Data

El diseño mostrado es una adaptación de las diferentes arquitecturas ya existentes y que son utilizadas para la implementación del SIIU en la UTN.

Se adopta SOA como Arquitectura para integración de software entre SIIU y el servicio de firma digital, basado en los requisitos establecidos por la DDTI-UTN.

Reglas de negocio para servicios de emisión de Certificados Electrónicos

- El Solicitante debe estar autenticado en el sistema y demostrar que no es un robot.
- El certificado emitido debe ser compatible con el estándar de infraestructura X.509 para usar firma electrónica emitida por el Banco Central del Ecuador.
- Opcionalmente debe adaptarse el reglamento interno para la gestión documental a fin de incorporar la nueva implementación del servicio gestión documental como válido legalmente al interior de la UTN.

De las diferentes arquitecturas de software existentes en el mercado, la DDTI-UTN escogió adaptar la arquitectura del SIIU con la arquitectura BPM de Aura Portal. Se tomó en cuenta

las recomendaciones del Autor sobre asuntos relacionados a la estructura de los mensajes XML y SOA para integración del software.

Se adaptó las Arquitectura BPM con SOA para integrar los procesos existentes en SIIU a los procesos que se gestionarán con BPM. Cabe indicar que el servicio de firma electrónica se estructuró orientado a SOA con la finalidad de adaptarlo al SIIU y al software de gestión de trámites institucionales implementado por la AuraPortal.

Los requisitos de habilidad deben satisfacerse, es decir debe existir información almacenada en el repositorio de base de datos Oracle integrado al SIIU.

Descripción de diseño que se incorpora al SIIU

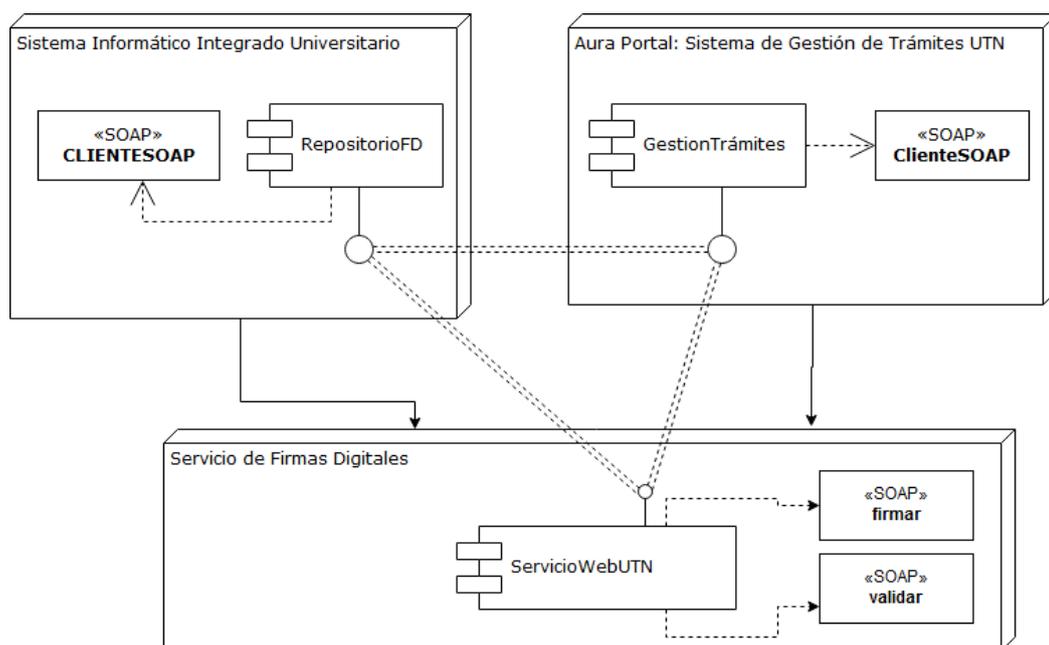


Figura 3: Diseño global integrador entre SIIU, AuraPortal, GDTUTN. Fuente: Autor

- RepositorioFD. Conjunto de tablas, procedimientos almacenados y funciones dentro del CloudUtn implementado en la base de datos Oracle sobre la que se almacena toda la información digital de la UTN.

- CLIENTES SOAP(SIIU). Procedimiento almacenado para solicitar al servicio de firmas digitales de la UTN dos cosas: firmar documentos XML o validar certificados XML firmados en formato X.509; utiliza el protocolo de intercambio de mensajes SOAP.
- GestionTrámites. Dentro de Aura Portal, se refiere al software BPM implementado por Aura Portal para la gestión de trámites de la UTN.
- ClienteSOAP(Aura Portal). Esta es una interface SOAP que debe implementarse en Aura Portal para conectar con el servicio de firmas digitales en caso de ser necesario. Por el momento esta interface no esta implementada debido a que es responsabilidad de Aura Portal hacerlo. El autor, entrego a la DDTI un documento especificando el formato de los mensajes que deben usarse y las características de seguridad sobre X.509 y PKCS#12 que deben adoptarse para su implementación.
- ServicioWebUTN. Conjunto de algoritmos implementados para firmar y validar certificados XML usando el estandar X.509 mediante infraestructura compatible con firma electrónica emitida por el Banco Central del Ecuador. Este servicio fue desarrollado por el Autor y entregado a la Dirección de Desarrollo Tecnológico e Informático de la UTN para su implementación.

Repositorio de Firmas Digitales

Es un modulo de la base de datos del SIIU que contiene contiene información sobre atributos de XML, certificados firmados digitalmente, documentos en formato XML extraidos de las consultas que generan información documental que para el caso de estudio contienen certificados de matrícula sin firmar aun, firmas digitales, parametros de configuración SOAP, solicitudes, tipos de documentos que son susceptibles de firmar o validar automáti-

camente por el ServicioWebUTN.

Interface para acoplar el servicio de firma digital. CLIENTESOAP

Es un procedimiento almacenado que gestiona la firma y validación de documentos en formato XML. Se comunica con el ServicioWebUTN mediante un mensaje SOAP. En este punto se aclara que el cliente SOAP de Aura Portal solo comparte el formato SOAP para poderse comunicar con el ServicioWebUTN o con el SIIU.

Interface externa para firmar y validar documentos enviados por CLIENTESOAP del SIIU. ServicioWebUTN

Mantiene activo dos funciones: firmar y validar. La función firmar tiene tres parámetros: P_xml de tipo String que extrae el código del documento del repositorio de firmas digitales para ser firmado, Id_emisor de tipo string es el número de llave del firmante (humano) al que representa el servicio automático de firma y S_Clave es la clave del firmante que para propósitos legales debe ser la otorgada a la persona por el Banco Central del Ecuador.

La función firmar localiza el URL especificado en los parámetros y el código de documento P_xml a ser firmado y devuelve un URL del documento firmado o DENEGADO en caso no haber fallado por alguna causa interna o externa.

Por razones de seguridad no avisa al cliente SOAP cual es la causa pero el servidor Web mantiene en la bitacora un registro de sucesos que pueden ser revisados para posterior seguimiento y auditoría.

El ServicioWebUTN se implementa con el siguiente descriptor URL= <https://www.utn.edu.ec:8181/firmarutn/ServicioWebUTN?wsdl> pudiendo ser cambiado a cualquier

otra IP pública y puerto, sin embargo para la validación el ServicioWebUTN esta conectado internamente al Cloud DE BASE DE DATOS de la UTN.

La función validar tiene los mismos parámetros que firmar, pero su resultado es ACEPTADO o DENEGADO.

Se acepta cuando el certificado enviado como parámetro se corresponde en código al certificado almacenado en el Repositorio de Firmas Digitales de la UTN.

Todas las funciones verifican la clave del emisor para devolver una respuesta.

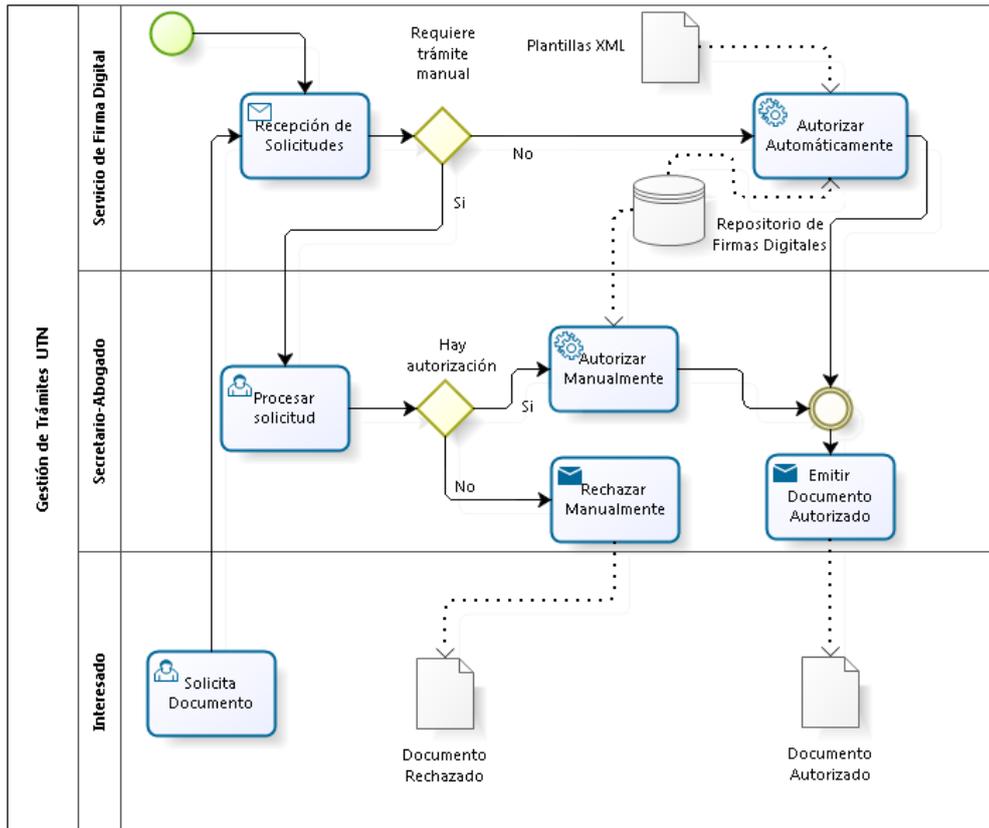
Al usar XML como formato de intercambio de mensajes, todos los mensajes que recibe y envía se pueden aprovechar de forma general para cualquier trámite institucional, en el presente trabajo de investigación se consideró solamente los Certificados de Matrícula firmados por el Servicio Web del Repositorio de firmas digitales de la UTN.

En forma general la automatización del proceso de gestión de trámites institucionales se esquematiza así:

Este esquema fue adoptado por la DDTI para desarrollar el software de gestión de trámites institucionales de la UTN, el mismo que por ser extremadamente complejo debido a la gran cantidad de procesos que deben implementarse aún se encuentra en desarrollo.

Sin embargo los procesos de firmado de documentos electrónicos y emisión de certificados digitales son parte integrada al SIIU.

Una página Web para recepción de solicitudes de diversos tipos, conforme a los especificados en el Cuadro 2.1, se muestran en la pantalla de recepción de solicitudes. Esta pantalla permanece disponible como servicio orientado a personas y tiene un esquema de decisión sobre el tipo de respuesta que debe darse a la solicitud. Para cada solicitud que se digita, esta deriva el requerimiento de trámite al proceso correspondiente. El SIIU pue-



Powered by
bizagi
 Modeler

Figura 4: Arquitectura del proceso de Gestión de Trámites de la UTN propuesto por el Autor

de responder con emisión de documentos autofirmados según lo especificado en el Cuadro 2.1; ciertos trámites requieren que la solicitud este firmada como se muestra en el campo FD REQ opción SI.

El proceso gestión de matrículas desencadena en la emisión del CERTIFICADO DE MATRÍCULA FIRMADO DIGITALMENTE, de acuerdo a la DDTI de la UTN es un proceso implementado en Aura Portal cuya arquitectura se muestra en el anexo correspondiente DOCUMENTO DE DISEÑO DE PROCESOS PARA IMPLEMENTACIÓN CON TECNOLOGÍA BPM

Adaptaciones a los drivers o interfaces que debe tener para acoplar la firma digital al ERP de la UTN

Para cada proceso de gestión documental debe generarse un repositorio de documentos XML que contiene la información legal que se requiera sea firmada en forma automática. Un ejemplo puede observarse en el anexo CREACIÓN DE CERTIFICADOS DE MATRÍCULA que sirve de modelo de proceso de emisión documental.

DISEÑO MICRO de la arquitectura de software para apoyar la gestión de servicios de mensajes de datos firmados

Se consideró la factibilidad de implementación de los servicios Web de firmar y validar certificados digitales sobre Glassfish4.1 en vez de WebLogic debido a su incompatibilidad con las librerías ECI-BCE(infraestructura X.509 implementada por el Banco Central del Ecuador para la emisión y validación de certificados firmados digitalmente con llaves de tipo PKCS#12).

Firma Digital

Es el repositorio de firmas digitales que se encuentra almacenado en la base de datos. Contiene todos los archivos de firmas digitales en formato PKCS#12.

Resolución firmada

Repositorio de documentos firmados digitalmente con el ServicioWebUTN o con cualquier otro software que facilite el proceso de firma digital; la DDTI-UTN puede usar indistintamente distintos tipos de servicios y se pueden almacenar resoluciones en formato XML en un campo de datos tipo BLOB. Existen dos estados de los documentos en el entorno de software propuesto, el uno es un documento XML sin firmar y el otro es un documento

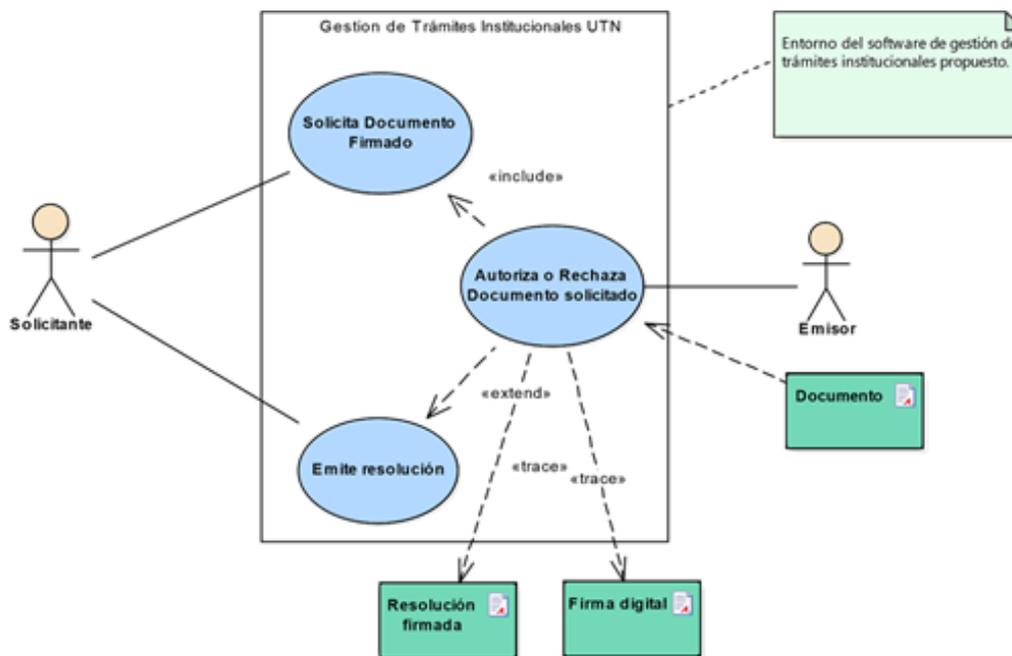


Figura 5: Servicio y uso del repositorio de firmas digitales

COLUMN_NAME	DATA_TYPE	NULLABLE	DATA_DEFAULT	COLUMN_ID	COMMENTS
1 NROFD	NUMBER	No	(null)	1	(null)
2 CONTENIDOFD	BLOB	Yes	(null)	2	(null)
3 CLAVE	VARCHAR2 (150 BYTE)	Yes	(null)	3	(null)
4 PROPIETARIO	VARCHAR2 (150 BYTE)	Yes	(null)	4	(null)
5 ACTUALIZADO	DATE	Yes	(null)	5	(null)

Figura 6: Firmas Digitales breve descripción de la Tabla en Oracle11g

COLUMN_NAME	DATA_TYPE	NULLABLE	DATA_DEFAULT	COLUMN_ID	COMMENTS
1 ID	NUMBER (6, 0)	No	(null)	1	(null)
2 DOCXML	CLOB	Yes	(null)	2	(null)

Figura 7: Documentos en formato XML breve descripción de la Tabla en Oracle11g

XML firmado. Esto da lugar a dos tablas de datos similares en estructura pero diferentes en contenido. Mientras en la una tabla solo se almacena el documento XML en la otra se

guarda el mismo documento firmado. De acuerdo a la norma ISO 9126 se consideran los siguientes atributos de calidad del software que deben cumplirse:

Atributos de calidad del Repositorio de firmas digitales

- Funcionalidad. Se consideran: seguridad de acceso y exactitud.
- Usabilidad. Se considera: capacidad para ser operado.

Atributos de calidad del servicio de firmas digitales

- Funcionalidad. Se consideran: seguridad de acceso y exactitud.
- Usabilidad. Se considera: capacidad para ser operado.

Indicadores de calidad considerados aceptables

En el presente trabajo se consideró:

ATRIBUTO	INDICADOR	MEDIDA	ACEPTABLE(%)
SEGURIDAD DE ACCESO	NÚMERO	ACCESOS N/A	0
	NÚMERO	PÉRDIDA CLAVES	1
	NÚMERO	ROBO IDENTIDAD	0
EXACTITUD	NÚMERO	XML DEFECTUOSOS	0
	NÚMERO	TIMEOUTS	1
OPERATIVIDAD	TIEMPO	LATENCIA	99.9 DIA
	TIEMPO	RESPUESTA	1 MINUTO
	TIEMPO	TRANSFERENCIA	1 MINUTO

Explicación: El sistema de firma digital impide accesos no autorizados mediante la implementación de funciones firmar y validar que piden el numero y clave de firma digital para habilitar el servicio. Además, el protocolo de intercambio de mensajes contempla ma-

nejo de https. En la UTN una falla de seguridad importante encontrada es el manejo de http que podría vulnerar la seguridad del servicio esta es una amenaza grave que podría afectar alcanzar 0 como el número de accesos no autorizados durante la vida útil del servicio.

La pérdida de claves es un factor humano inevitable, aunque se espera sea mínima, siempre existirá por lo que el servicio de firma digital no tiene manera de recuperar la clave, en su defecto se recomienda almacenar un nuevo certificado de firma digital con una clave conocida que no debería olvidarse. El ciclo de pérdida de clave y recuperación es manual. Aun se está lejos de alcanzar niveles de madurez con estándares internacionales como el ISO 27000 pero es un buen inicio.

Se espera que los procesos del SIIU generen peticiones válidas al servicio de firmas, esta seguridad solo puede garantizar la infraestructura lógica del ERP institucional. Hasta el momento no se ha detectado robo de identidad, es mejor prevenir.

Un documento XML defectuoso puede ser generado por la introducción de caracteres extraños en la estructura del documento XML. El servicio de firma retorna error cuando esto ocurre.

Timeouts, el tiempo de respuesta esperado es inferior a 1 minuto para peticiones de 32Kb. Es necesario configurar el tiempo de espera superior a 1 minuto para no tener este desagradable time out o si el paquete enviado es mayor es bueno probar cual es el settimeout de http que se adapta mejor a las necesidades.

Lo ideal es que el servidor nunca se caiga, pero por cualquier razon interna o externa el servicio puede fallar y toca volver a levantar el servidor especialmente Glassfish4.1; no se podido probar en WebLogic.

El tiempo de respuesta y de transferencia debe ser inferior a un minuto, aunque este último se debe a causas externas al servicio de gestión de mensajes de datos firmados.

IMPLEMENTACIÓN

Se realiza la programación del conjunto de algoritmos del repositorio de firmas digitales de la que se describe detalladamente en el siguiente subcapítulo y la DDTI adquiere un software para la gestión documental con Aura Portal.

No se encuentran hasta el momento deficiencias de diseño.

El proceso de desarrollo de software se lleva a efecto en el ambiente controlado del CLOUD DE TEISISTEMAS para lo cual se extrae una vista de 8583 estudiantes indicando código, facultad, especialidad, nivel con una vista de materias de un nivel de una facultad para desarrollar los algoritmos de servicio de firma digital.

SOLICITUD DE MATRÍCULA. SOLICITUD Y EMISIÓN DE CERTIFICADOS DE MATRÍCULA FIRMADOS DIGITALMENTE

De todos los procesos de gestión de trámites institucionales que se implementan en el ERP de la UTN, se escoge SOLICITUD Y EMISIÓN DE CERTIFICADOS DE MATRÍCULA FIRMADOS DIGITALMENTE para establecer un modelo de desarrollo de algoritmos integrados al SIIU para: (1) Solicitar el certificado de matrícula, (2) firmar automáticamente por el servicio de firma digital, (3) almacenar en el repositorio el certificado firmado.

El proceso detallado en AuraPortal de SOLICITUD DE MATRÍCULA, de ser correcto devuelve un documento de acreditación de la matrícula. Este documento debe ser firmado digitalmente por un emisor con firma electrónica obtenida del BCE para que tenga validez legal en Ecuador. Todos los procesos de petición, validación de datos y entrega de reportes se los efectúa en el SIIU; la responsabilidad de firmar el documento es del servicio de

firma digital mediante uso de firmas digitales almacenadas en el repositorio de la base de datos de la UTN. Para la experimentación se considera la implementación de un ambiente de pruebas controlado que emula las condiciones esenciales del ERP institucional de la UTN.

Establecer una relación efectiva entre GDTUTN y el SIIU mediante SOAP

El ServicioWebUTN es una implementación Java de dos Web services orientados a SOA: firmar y validar. Este servicio es externo al SIIU pero puede ser incorporado en el ERP institucional configurando un servidor Linux con Glassfish4.1 en el CLOUD de www.utn.edu.ec usando puertos distintos al 80 que es de http o al 443 que es de https. Se propone tentativamente usar los puertos 4848,8181 y 8080. La estructura general de los mensajes es:

ServicioWebUTN

Operations (2) Add Operation... Remove Operation

firmar

Parameters	Output	Faults	Description
Parameter Name			Parameter Type
documento			java.lang.String
emisor			java.lang.String
clave			java.lang.String

validar

Parameters	Output	Faults	Description
Parameter Name			Parameter Type
certificado			java.lang.String
clave			java.lang.String

Figura 8: Servicio de firma digital UTN

4.1.4. R4: Desarrollo del conjunto de algoritmos del repositorio de firmas digitales

Delimitación de la infraestructura física del ERP de la UTN

Ubicación

La UTN se encuentra, en la Avenida 17 de Julio, 5-21, y, Gral. José María Córdova. Código Postal 199. Ibarra-Ecuador. Según consta en la página Web institucional: <http://www.utn.edu.ec/wel>

El ERP de la UTN se encuentra implementado en la DDTI, físicamente accesible a servicios de plataforma en CLOUD de ORACLE.

Dependencias o Departamentos

- Dirección de Desarrollo de Tecnológico e Informática
- Secretario Abogado de cada Facultad e Instituto
- Asociaciones de Estudiantes, Docentes y Empleados

Delimitación lógica del ERP de la UTN

Actualmente, la base de datos ORACLE esta alojada en el CLOUD como se describe en la gráfica.

Algoritmos para conectar a la base de datos del SIIU

La base de datos del SIIU esta implementada en el CLOUD DE ORACLE 12c; el control de acceso permitido por el Director de DTI es necesario obtener como credenciales para poder acceder a los recursos de la base.

La parte más destacable es el constructor que requiere un parámetro para ubicar el host, el usuario y contraseña.

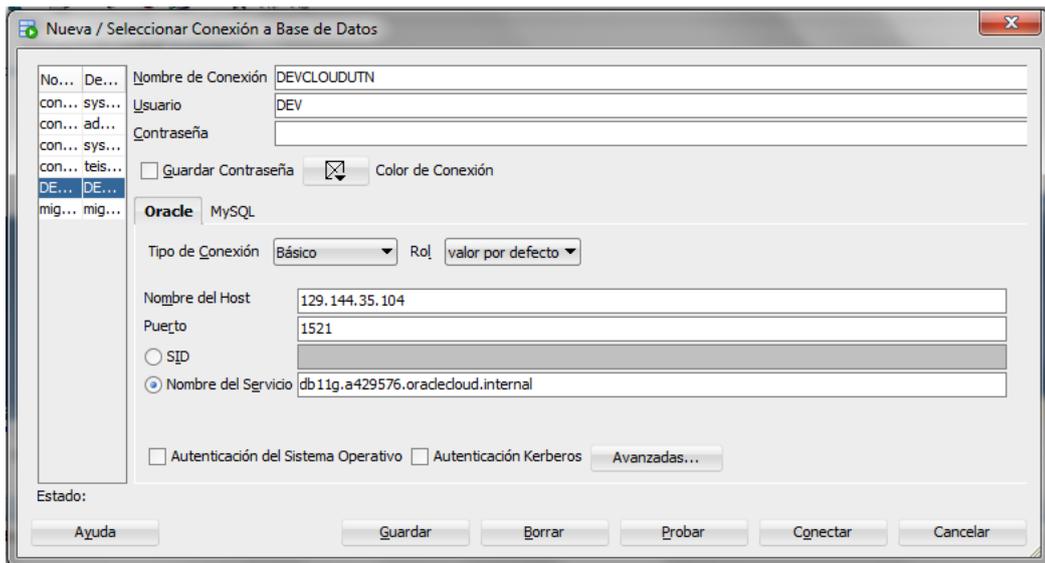


Figura 9: Acceso al SIIU en los límites de seguridad establecidos por ORACLE

El servicio de firma electrónica almacena y recupera las firmas digitales usando esta librería.

Cada función hace una sola tarea en particular indicada por su nombre descriptivo.

El algoritmo para usar esta librería de funciones en el proceso de firmado es:

- Inicializar la conexión a ORACLE (11g, 12c)
- Conseguir clave de firma digital por número de firma o por propietario
- descifrado de la clave de firma digital con clave x
- obtener llave del almacen de firmas digitales usando clave descifrada
- Aquí se puede usar esta llave para cualquier propósito, los algoritmos de firmar y validar lo usan para firmar documentos xml en este punto se podría usar para firmar documentos pdf pero esos algoritmos no están implementados (vease recomendaciones)
- Cifrado de clave x

Otros usos que se puede dar: validar documentos xml, cargar o guardar certificados de

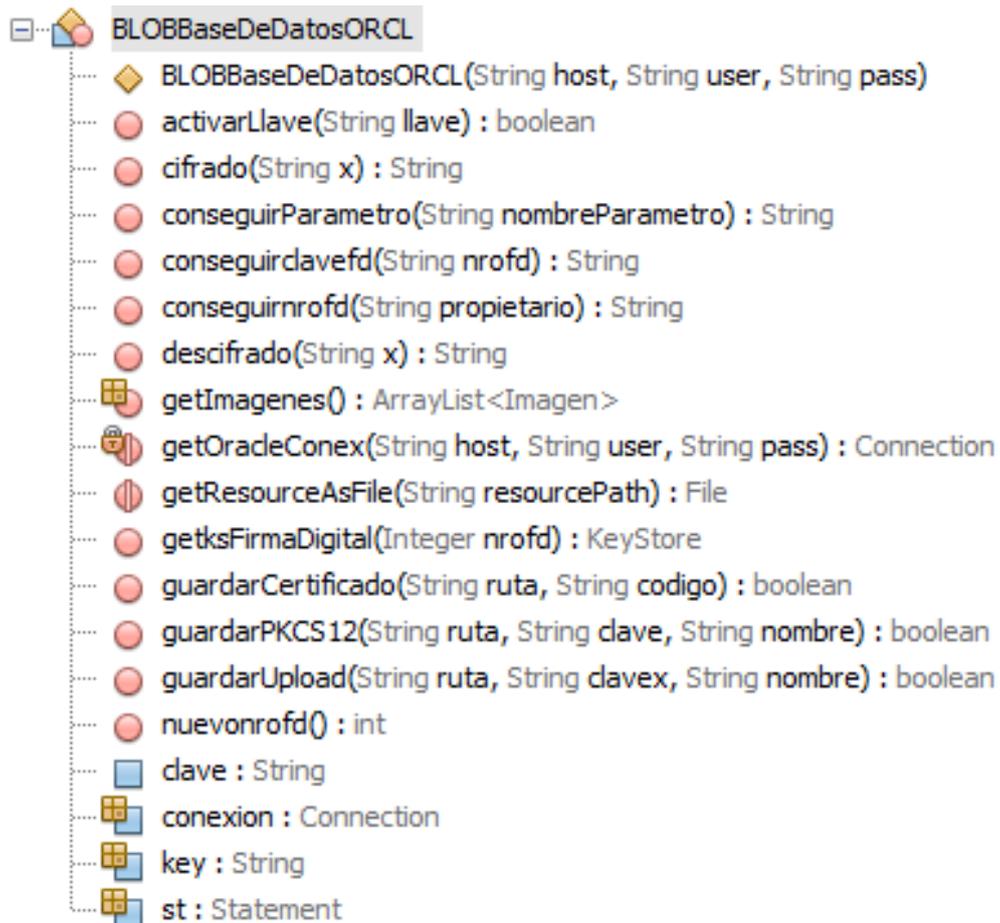


Figura 10: Algoritmos para conectar al repositorio de firmas digitales

firma digital subidos al host en la base de datos.

Este conjunto de funciones es de propósito general.

El autor las ha utilizado varios miles de veces para almacenar certificados de factura electrónica, desde el año 2014.

Puede decirse que la madurez de las funciones es de 4 años.

Más detalles se observa en anexos.

Algoritmos para firmar y validar documentos firmados digitalmente mediante SOAP en JAVA

Para firmar o validar un documento xml el ServicioWebUTN requiere lo siguiente:

- P_xml nombre del recurso xml que se firmará o validará; internamente se conoce la URL donde se encuentra el archivo físico mediante la funcion `getResourceAsFile(resourcePath)`;
- ID_emisor Numero de registro de firma digital almacenada en el repositorio;
- S_clave Contraseña del archivo.p12;

Los detalles de la implementación se encuentran en el anexo correspondiente.

Algoritmos para generar documentos XML en PL/SQL

La estructura general de un documento XML compatible con los comprobantes para comercio electrónico en el Ecuador debe contener la estructura mostrada en la figura:

```

create or replace procedure          crearDocXML(codigo in varchar2) is
begin
  insert into documentos values(sec_doc.nextval,(SELECT  concat('<?xml version="1.0" encoding="UTF-8"?>',XMLAGG (
    XMLELEMENT("documento",
      XMLATTRIBUTES(a.id AS "id",a.version as "version"),
      xmlelement("codigo",codigo),
      XMLFOREST((SELECT XMLAGG(XMLELEMENT("registro", XMLFOREST(c.id ,c.contenido ,c.fecha )))FROM  contenidos c) "lista_docs")
    )
  )AS "atributo" FROM  atributos a));
end crearDocXML;

```

Figura 11: Procedimiento general para crear documentos XML en PL/SQL compatibles con emisión de comprobantes de comercio electrónico ecuatorianos

4.1.5. R5: Relacionar el software de gestión basado en el ERP con la base de datos de la UTN

Flujo de trabajo para solicitudes de documentación legal en la UTN

Basado en el documento de Arquitectura del proceso de Gestión de Trámites de la UTN propuesto por el Autor y que fue recibido por la DDTI, se describen los componentes de este flujo de trabajo, que se muestra en la Figura 4, p.90; Existen tres instancias de la gestión de trámites UTN: Interesado, Secretario Jurídico y Servicio de Firma Digital.

Interesado

Accede al servicio de firma digital para solicitar algún documento y posteriormente recibe un documento Autorizado o Rechazado.

Servicio de Firma Digital

Es el primero en iniciar los procesos recibiendo solicitudes de documentos firmados. Según el documento solicitado por el interesado determina si requiere o no trámite manual. En caso de requerir trámite manual lo envía al Secretario Jurídico. En caso de NO requerir trámite manual lo autoriza automáticamente, generando un documento autorizado basado en la plantilla xml y la firma autorizada correspondiente para ese documento, envía una

copia al secretario jurídico y otra al interesado.

NO SE HA TENIDO HASTA EL MOMENTO ACCESOS N/A, este indicador hasta el momento de entrega sigue en 0 y es de esperarse que siga así debido a la fortaleza de la llave de cada firmante y otros factores de seguridad de acceso que afectan este indicador.

Secretario Jurídico

Recibe solicitudes de trámites que deben ser atendidos manualmente en su buzón y decide si hay autorización firma digitalmente el documento usando la firma correspondiente del repositorio de la UTN y lo envía al buzón del interesado. Caso contrario si NO hay autorización, envía una notificación de documento rechazado al buzón del interesado.

Este proceso es de propósito general y no puede ser implementado directamente pues cada tipo de documento solicitado por el interesado requiere un trámite específico para lo cual el proceso de recepción de solicitudes debe enviar el trámite al servicio correspondiente para completar el ciclo, este conjunto de servicios de gestión específicos lo implementa Aura Portal.

Mapa de ruta de CERTIFICADOS DE MATRÍCULA

El estado de emisión de un certificado de matrícula que nace del interesado y se entrega al mismo un documento de autorizado o rechazado tiene los siguientes estados:

1. SOLICITADO
2. RECIBIDO

3. ENVIADO A JURÍDICO
4. EN PROCESO DE FIRMA AUTOMÁTICA
5. EN PROCESO DE FIRMA MANUAL
6. AUTORIZADO
7. DENEGADO

En forma general este mapa de ruta permite conocer al interesado en que estado se encuentra su trámite requerido.

Generación de la documentación legal y documentos por estados de aceptación en las dependencias. Valoración del caso de uso: CERTIFICADOS DE MATRÍCULA

La documentación legal puede ser generada en forma automática o manual según el tipo de documento solicitado.

Esta especificación de atributo de calidad del documento es identificada por los funcionarios de la DDTI al momento de configurar los parámetros que pertenecen al XML del certificado a ser emitido.

Los estados de aceptación en dependencias son: AUTORIZADO, DENEGADO.

Como se puede contar los documentos en cada dependencia y por cada estado de aceptación esto genera información cuantificable.

Uso del repositorio de firmas digitales disponibles en la base de datos de la UTN

El uso del repositorio es de tipo general pues se limita a firmar documentos recibidos que cumplan solo tres parametros: documento xml, emisor de firma digital y clave.

Hola, bienvenid@ al sistema de gestión de trámites institucionales de la UTN

Ingrese su cédula:	●●●●●●●●
CICLO ACADEMICO:	ACTUAL ▾
DEPENDENCIA:	Maestría en Ingeniería de Software ▾
CAPTCHA:	Para prueba inhabilitado
Tipo de documento solicitado	CERTIFICADO DE MATRÍCULA ▾
<input type="button" value="SOLICITAR"/>	

Diseño: Tobías López (c) 2018

Figura 12: Formulario de Gestión de Trámites UTN

Cuadro 4: USO DEL REPOSITORIO DE FIRMAS DIGITALES EN LA UTN

MÉTRICA	INDICADOR	MEDIDA	ESPERADO	OBSERVADO
WS	Nro. certificados	XML	8583+	900+
TS	Nro. certificados/minuto	minutos	15XML/hora	3XML/minuto
Demora del WS	WS+TS	XML/minuto	18XML/minuto	5XML/minuto

Es por esta razón técnica que el repositorio puede usarse entre otras cosas para aplicaciones de gestión documental, facturación electrónica y otros servicios del SIIU o del flujo de trabajo que requiera aprovechar este repositorio.

Determinación de los indicadores de uso del repositorio de firmas digitales:

Estos resultados son obtenidos de las pruebas de integración entre el WebService y el SIIU, utilizando para ello un algoritmo de peticiones de firmado llamado firmarciclo activado en la Base de datos del SIIU para medir la carga del servicio.

La creación de firmas digitales y servicios del repositorio

La estructura PKCS#12 de la firma digital que se almacena permite que los servicios del repositorio sean sobre trámites internos o externo a la UTN.

Se entrega un anexo código fuente de la librería en formato HTML de dos formularios útiles para gestionar las firmas digitales en oracle y realizar solicitudes de CERTIFICADOS DE

MATRÍCULA.

Ingrese sus nombres y apellidos:

Ingrese su clave:

Cargue el archivo: No se ha seleccionado ningún archivo.

Figura 13: Formulario para subir la repositorio de firmas digitales de la UTN un archivo de firma electrónica en formato PKCS#12

El acceso a la base de datos de la UTN

Para que el repositorio pueda trabajar efectivamente en sus procesos se requiere procesos de configuración de la base de datos y la instalación de los archivos, tablas, procedimientos almacenados y funciones que se describen en este documento.

PRIVILEGIOS ORACLE	USUARIOS ADMINISTRADOR DEL PAQUETE
CONNECT	ADMINISTRADOR
RESOURCE	ADMINISTRADOR
SELECT	ADMINISTRADOR
INSERT	ADMINISTRADOR
UPDATE	ADMINISTRADOR
EXECUTE	ADMINISTRADOR
DELETE	ADMINISTRADOR

Las acciones legales documentadas de los funcionarios

Atender a todos los estudiantes a su cargo distribuidos por dependencias y facultades así:



Figura 14: Número de estudiantes de la UTN en el año 2018

Actividades legales documentadas del secretario jurídico

Son actividades dentro del flujo de trabajo: Procesar todas las solicitudes que llegan a su buzón de acuerdo al criterio profesional del secretario jurídico.

Número de firmas que se crean o modifican y operaciones de firmado que se realizan

Para almacenar las firmas estas se registran en una tabla de la cual se puede obtener estos indicadores aplicando una operación SQL para contar los registros almacenados.

Para obtener el indicador sobre el número de firmas digitales archivadas desde el SIIU se debe aplicar la siguiente consulta SQL:

```
SELECT COUNT NROFD FROM FIRMASDIGITALES;
```

Para obtener el indicador sobre el número de operaciones de firmado archivadas desde

el SIIU se debe aplicar la siguiente consulta SQL:

```
SELECT COUNT NROCERTIFICADO FROM CERTIFICADOS;
```

4.2. DISCUSIÓN

¿Cómo incide el repositorio de firmas digitales en la gestión de trámites institucionales de la UTN? Al comparar el servicio web de firma digital con el Quipux de la UTN, existen notables diferencias en cuanto a satisfacción de requerimientos de integración con el SIIU. Se comprueba experimentalmente que la integración con el BPM y SIIU esta sustentada en el Software subyacente SOA que trabaja en entornos Web sobre CLOUD privado o público.

La gestión de trámites a partir de la implementación del servicio Web mejora sustancialmente los procesos al dejarlo: Organizado, Auditable y Automático. Se obtienen verificadores de incidencia a partir de consultas SQL sobre instancias específicas en la base de datos del repositorio, lo que ha permitido la consecución de los objetivos del presente trabajo de desarrollo del Software.

4.2.1. Influencia tecnológica

El software de servicio de firma digital basado en repositorio de firmas, puede ser implementado en diferentes modelos de ejecución y arquitectura para satisfacer las demandas de flujo documental.

La implementación del servicio SOA incluye capacidad para almacenar en forma segura una cantidad creciente de firmas digitales, si se considera un estimado de 14KB por cada firma digital almacenada en formato PKCS12, el repositorio con clave primaria numérica

de 20 dígitos es capaz de almacenar todas las firmas digitales de la humanidad, en vista que somos 7.000.000.000 habitantes de la Tierra (un 7 con 9 ceros en total 10 dígitos, o sea 7 mil millones de habitantes), eso consume aproximadamente un total de 98.000.000.000.000 bytes (98 Tera bytes).

El tiempo que se demora en firmar un documento varía entre 1 a 60 segundos, en promedio unos 30,5 segundos por documento considerando un tamaño de certificado que va de 7KB hasta 30KB que fueron medidos con un incremento logarítmico del tiempo medido por servicio. Con esta información cada servicio Web para firma digital individual tiene capacidad de firmar en 24 horas laborables al día un total de 2880 documentos de tamaño promedio 30KB. En este punto es necesario aplicar la teoría de colas para decidir sobre la implementación de nuevos servicios SOA que operen en forma asíncrona concurrente para satisfacer la demanda de consumo del servicio Web.

Para satisfacer la demanda de documentos legales almacenados en el repositorio de archivos certificados, se considera una clave primaria numérica de 20 dígitos, al relacionar con el número de estudiantes de la UTN, unos 8000 que pudieran requerir hasta unos 14 tipos distintos de certificados digitales, se observa que la capacidad de almacenamiento mínimo necesario es de 3.360.000.000 (3.36 Giga bytes).

Para implementar adecuadamente el servicio es necesario asegurar la comunicación de datos mediante uso de https y algoritmos para cifrar y descifrar contraseñas en ambiente físico seguro, las consideraciones de seguridad física son un capítulo aparte que sale del alcance de esta investigación. Las recomendaciones de seguridad de ORACLE 12c y OPENSLL deben ser aplicadas para mantener estándares para comunicación de datos óptimos.

4.2.2. Influencia legal

Una característica útil del uso del repositorio de firmas digitales en la UTN es la capacidad de realizar auditoría de software en los procesos internos y externos mediante BPM, que facilita la localización del archivo certificado y responsabilidad del emisor y del solicitante sobre el contenido y la gestión documental realizada.

Por ejemplo, cuando un documento tiene cierta caducidad para ser transferido o comunicado, el BPM puede gestionar ese requisito sin embargo para certificar legalmente que el documento ha caducado es necesario la firma digital en el archivo XML o PDF y este debe estar almacenado en medio digital solo entonces tiene valor de verificador legal sobre un hecho o asunto.

Es necesario aplicar el reglamento de gestión documental interna y externa en la UTN para utilizar el servicio de firma digital y archivar en el repositorio los certificados generados en forma segura y útil para todos.

Capítulo 5

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

- La incidencia del uso del repositorio de firmas digitales en la gestión de trámites institucionales depende de un conjunto complejo de factores entre los que se encuentran: tecnológico, humano, económico. **El uso del repositorio de firmas digitales es fundamental para la gestión de trámites institucionales de la UTN porque permite obtener certificados electrónicos basados en reportes automáticos o manuales del SIIU con firma digital válida legalmente en Ecuador.**
- El uso del estándar X.509 en la generación de certificados electrónicos basados en el SIIU es el principal requerimiento de software para la implementación de servicios de gestión documental que faciliten la automatización de tareas administrativas y legales en la UTN, la adopción de mecanismos de seguridad a nivel de sesión, aplicación HTTPS, comunicaciones AES, base de datos DBCRYPT son algunas capas de seguridad mínimas para el cumplimiento del Habeas Data previsto en la Constitución y la Ley de Comercio electrónico.

- El servicio de firma digital está constituido por la base de datos de firmas digitales con su respectiva librería para manejo de BLOBs, el ServicioWebUTN?wsdl con su respectivo descriptor XSD, la firma digital creada con OpenSSL o adquirida al ECI-BCE a través del registro civil y se almacena en el repositorio de firmas digitales de la UTN conservando su integridad, confidencialidad y usabilidad por medio de SOAP o JDBC.
- La seguridad de la información almacenada tiene varias capas, la primera es el buen uso del CLOUD donde opera el SIIU, la segunda capa es la gestión de Base de Datos Oracle, la tercera es el protocolo de intercambio de información a través de HTTPS, la cuarta son las librerías y servicios implementados en Glassfish4.1 que pueden afectar el rendimiento si son configurados inadecuadamente y por último la arquitectura y algoritmos utilizados para manejo del repositorio de firmas digitales
- Por los resultados de la observación del uso del repositorio de firmas digitales en las Secretarías del IP y DDTI de la UTN, se concluye que la gestión de trámites requiere usar el repositorio de firmas digitales para emitir documentos firmados con validez legal en forma automatizada
- Se verificó que los tiempos de servicio y de espera se corresponden con un modelo típico de colas en las que comparativamente se obtienen mejores resultados esperando detrás de un servicio web que haciendo cola en la oficina del secretario abogado siempre que el certificado sea susceptible de ser emitido en forma automática como es el caso de los certificados de matrícula.
- El INEN propone la adopción de ISO/IEC 25010:2011, IDT como norma de calidad del Software. En el desarrollo del presente trabajo se establecieron criterios de

aceptación y métricas de calidad orientadas a Software de tipo SOA sobre protocolo X.509 que cumplen los criterios de la normativa NTE INEN ISO/IEC 25010:2011 y permiten medir la incidencia de uso del repositorio de firmas digitales en la gestión del trámite institucional utilizando el formato de mensajes XML y PDF según los criterios técnicos establecidos para automatizar la medida de calidad según la métrica correspondiente referente al Consumo de un Servicio Web.

- La aplicación de software entregada a la Dirección de DDTI-UTN como resultado de esta investigación, satisface las necesidades del DDTI-UTN, los requerimientos establecidos en el ERS-IEEE-29148 y ha sido recibida a entera satisfacción por el Director de Desarrollo Tecnológico e Informática de la UTN.
- La palabra interoperabilidad no está definida en el DLE, pese a que el IEEE sí le da un significado específico. Algunos términos técnicos se definen en la ingeniería de Software y son propios de ella pese a no tener equivalentes en la Lengua Española.
- Es de amplio uso el modelo de firma y validación XML denominado XADESBES cuyos objetos de clases para servicio desarrollados en Lenguaje JAVA han sido implementados y difundidos por el Ministerio de Industria, Energía y Turismo de España desde el año 2013. Estos formatos han sido adoptados para la operativización de la tecnología de Software subyacente a la aplicación de la Ley de Comercio Electrónico ecuatoriana, razón por la que este trabajo de investigación se lo hizo en torno de estos algoritmos con los que se desarrolló el servicio Web de firmado y validación de firmas digitales dentro de los documentos XML generados por el SIIU de la UTN. Un aspecto clave que genera discusión es la implementación embebida o no del archivo de firma dentro del código fuente del Webservice programado en JAVA, hasta el mo-

mento no se encuentra una diferencia significativa que implique debilidad de estos algoritmos adoptados y entregados.

- Es posible crear firmas digitales autografiadas sin necesidad de recurrir a entidades gubernamentales de orden jerárquico en el aspecto tecnológico, sin embargo en el aspecto legal su validez solo puede ser considerada al interior de la UTN luego de la modificación del marco legal para el uso del QUIPUX.
- Se puede modelar un servicio de firmas digitales mediante SOA considerando solo parte del estándar ISO / IEC 9126-3 de calidad interna y en contexto de uso del SOFTWARE. Los resultados obtenidos verifican la calidad del producto contra entrega e integración con el SIIU.
- Para usar el servicio de firmas digitales, en el SIIU se deben implementar generadores de documentos XML siguiendo el modelo de certificados de matrícula en que conste el contenido del comprobante de cualquier trámite en particular en que se pretenda dar uso al repositorio de firmas digitales.**El modelo de emisión de certificados de matrícula es una semilla para la generación de otros tipos de certificados basados en reportes del SIIU o en procesos BPM**

RECOMENDACIONES

- Adoptar el servicio de firma digital orientado a SOA en los diferentes procesos estructurados con BPMN en Aura Portal al interior de la UTN para gestionar los trámites internos y externos.
- Modificar el framework entregado al DDTI-UTN para darle la utilidad más adecuada

al momento de firmar documentos generados automáticamente por SIIU

- Implementar nuevos servicios de certificación y emisión de firmas digitales autografiadas con validez legal al interior de la UTN en formato de intercambio de certificados digitales X.509
- Socializar el uso del repositorio de firmas digitales GDTUTN, con todos los estudiantes cuando se hayan concluido los trabajos de integración del BPM de AuraPortal con el SIIU a fin de valorar su utilidad para reducir el consumo de papel y otros recursos naturales.
- Al no tener suficiente tiempo para medir la incidencia real del uso del software en la gestión de procesos documentales en la UTN, se recomienda un trabajo de investigación futuro encaminado a obtener esos resultados finales.
- Investigar la incidencia efectiva del uso de firmas digitales en la gestión de trámites institucionales y el grado en que se satisface a los usuarios sean estudiantes, docentes y ciudadanía en general.

Bibliografía

- Abad, Z. S. H., Noaen, M., y Ruhe, G. (2016, Sept). Requirements engineering visualization: A systematic literature review. En *2016 IEEE 24th International Requirements Engineering Conference (RE)* (p. 6-15). doi: 10.1109/RE.2016.61
- Alonso, J., Escalante, M., y Orue-Echevarria, L. (2016). Transformational cloud government (tcg): Transforming public administrations with a cloud of public services. *Procedia Computer Science*, 97, 43 - 52. Descargado de <http://www.sciencedirect.com/science/article/pii/S1877050916320956> doi: <http://dx.doi.org/10.1016/j.procs.2016.08.279>
- Amoroso, X. (2015). *Informe de labores enero-septiembre 2015* [Planificación Institucional].
- Andersen, I. (2015). They change it, they own it: Employee participation in change management. *Communication World*, 1. Descargado de <http://search.ebscohost.com/login.aspx?direct=true&db=bsx&AN=111072031&lang=es&site=eds-live>
- ANDES. (2015). *Agencia publica de noticias del Ecuador y Suramérica*. Descargado de <http://www.andes.info.ec/es/noticias/correos-ecuador-cumple-184-anos-vida-institucional.html>
- Antúnez Javier, P. M. (2013). *Aproximación para un método de elicitación y especificación de requerimientos de seguridad para el desarrollo de software*. Descargado de <http://sedici.unlp.edu.ar/bitstream/handle/10915/27186/Aproximaci%F3n+para+un+m%9todo+de+elicitaci%F3n.pdf;jsessionid=A6118FDCA6D96BE4A3BBBF03DC80E5F1?sequence=1>
- Ashibani, Y., y Mahmoud, Q. H. (2017). Cyber physical systems security: analysis, challenges and solutions. *Computers & Security*, -. Descargado de <http://www.sciencedirect.com/science/article/pii/S0167404817300809> doi: <http://doi.org/10.1016/j.cose.2017.04.005>

- Ayala, E. (2008). *Resumen de historia del ecuador*. Descargado de <http://repositorio.uasb.edu.ec/bitstream/10644/836/1/AYALAE-CON0001-RESUMEN.pdf>
- B.C.E. (2009). *Contrato de prestación de servicios entre la entidad de certificación y el usuario*. Descargado de [http://documentacion.asambleanacional.gov.ec/alfresco/d/d/workspace/SpacesStore/a72f6053-9641-447c-a4f8-e914c0bcc7b/CONTRATO%20CON%20EL%20BANCO%20CENTRAL%20DEL%20ECUADOR%20\(20-11-09\).pdf](http://documentacion.asambleanacional.gov.ec/alfresco/d/d/workspace/SpacesStore/a72f6053-9641-447c-a4f8-e914c0bcc7b/CONTRATO%20CON%20EL%20BANCO%20CENTRAL%20DEL%20ECUADOR%20(20-11-09).pdf)
- Casas-De-Barran, A., Griffin, A., Millar, L., y Roper, M. (2015). *Gestión de documentos del sector público desde una perspectiva archivística ii: organización y control de documentos administrativos*. Descargado de http://www.irmt.org/documents/educ_training/spanish/IRMT_Perspectiva_Archivistica_II.pdf
- Cavalieri, D. C., Bastos-Filho, T., Palazuelos-Cagigas, S., y Sarcinelli-Filho, M. (2015). On combining language models to improve a text-based human-machine interface. *International Journal of Advanced Robotic Systems*, 12. Descargado de <https://search.proquest.com/docview/1788910472?accountid=36862> (Copyright - Copyright InTech 2015; Última actualización - 2016-08-13)
- CEAACES. (2011). *Ley orgánica de educación superior*. Descargado de <http://www.ceaaces.gob.ec/sitio/wp-content/uploads/2013/10/rloes1.pdf>
- Chejerla, B. K., y Madria, S. K. (2017). Qos guaranteeing robust scheduling in attack resilient cloud integrated cyber physical system. *Future Generation Computer Systems*, -. Descargado de <http://www.sciencedirect.com/science/article/pii/S0167739X17302650> doi: <http://doi.org/10.1016/j.future.2017.02.034>
- CIESPAL. (1972). Chasqui primera Época 1. *Ciespal*. Descargado de <http://www.revistachasqui.org/index.php/chasqui/issue/view/01-1972>
- CIESPAL. (2016). Capitalismo cognitivo y comunicología. la subsunción del trabajo intelectual. *Chasqui*(133). Descargado de <http://www.revistachasqui.org/index.php/chasqui/issue/view/133-2016> doi: <http://dx.doi.org/10.16921/chasqui.v0i133>
- Constituyente, A. (2008). *Constitución de la república del ecuador*. Descargado de <http://www.pucesi.edu.ec/web/wp-content/uploads/2016/04/Constituci%C3%B3n-de-la-Republica-2008..pdf>
- C.O.R.D.I.S. (2016). *Advanced security service certificate for soa*. Descargado de <http://>

cordis.europa.eu/project/rcn/95250_es.html

- Costa, B., Pires, P. F., Delicato, F. C., y Merson, P. (2016). Evaluating {REST} architectures—approach, tooling and guidelines. *Journal of Systems and Software*, 112, 156 - 180. Descargado de <http://www.sciencedirect.com/science/article/pii/S0164121215002150> doi: <http://doi.org/10.1016/j.jss.2015.09.039>
- Cruz, Y. E., y Ramón López Paz, C. (2014). Procedimiento para desarrollar soluciones de gestión de procesos de negocio con tecnologías de oracle. *Ciencias de la Información*, 45(3), 45 - 54. Descargado de <http://search.ebscohost.com/login.aspx?direct=true&db=asx&AN=100306017&lang=es&site=eds-live>
- Cuenca, C. A., Gómez, J. G., y Scotti, S. (2012, May). Design an architecture that allows the interoperability between information systems, software or medical device adopting the standard hl7 v2.x. En *2012 ieee colombian communications conference (colcom)* (p. 1-7). doi: 10.1109/ColComCon.2012.6233647
- DRAE. (2017a). *Diccionario de la lengua española*. Descargado de <http://dle.rae.es/?id=VwxnN60>
- DRAE. (2017b). *Diccionario de la lengua española*. Descargado de <http://dle.rae.es/?id=DxeVsCQ>
- DRAE. (2017c). *Diccionario de la lengua española*. Descargado de <http://dle.rae.es/?id=0K2DI9N>
- DRAE. (2017d). *Diccionario de la lengua española*. Descargado de <http://dle.rae.es/?id=bCSFzKP|bCTJISY>
- DRAE. (2017e). *Diccionario de la lengua española*. Descargado de <http://dle.rae.es/?id=GikXRGw>
- DRAE. (2017f). *Diccionario de la lengua española*. Descargado de <http://dle.rae.es/?id=Tl21X5Z>
- DRAE. (2017g). *Diccionario de la lengua española*. Descargado de <http://dle.rae.es/?id=0hJNnuM>
- DRAE. (2017h). *Diccionario de la lengua española*. Descargado de <http://dle.rae.es/?id=AAkKXT5>
- DRAE. (2017i). *Diccionario de la lengua española*. Descargado de <http://dle.rae.es/?id=OH9tS8F>
- DRAE. (2017j). *Diccionario de la lengua española*. Descargado de <http://dle.rae.es/>

- ?id=LulHQaO
- DRAE. (2017k). *Diccionario de la lengua española*. Descargado de <http://dle.rae.es/?id=XTrgHXd>
- Ebert, C., y Duarte, C. H. C. (2016, Sept). Requirements engineering for the digital transformation: Industry panel. En *2016 IEEE 24th International Requirements Engineering Conference (RE)* (p. 4-5). doi: 10.1109/RE.2016.21
- Española, R. A. (2017). *Diccionario de la lengua española*. Descargado de <http://dle.rae.es/?id=Hyte6ty>
- Fraleay, J. B., y Cannady, J. (2016, Oct). Enhanced detection of advanced malicious software. En *2016 IEEE 7th Annual Ubiquitous Computing, Electronics Mobile Communication Conference (UEMCON)* (p. 1-6). doi: 10.1109/UEMCON.2016.7777866
- GETDSA. (2017). *¿qué debo valorar en un software de gestión documental?* Descargado de <http://www.gedsa.es/debo-valorar-software-gestion-documental-i/>
- Giuliani, F., Ottavi, M., Cardarilli, G. C., Re, M., Nunzio, L. D., Fazzolari, R., ... Zuliani, F. (2016, Sept). Design and characterization of a high-safety hardware/software module for the acquisition of eurobalise telegrams. En *2016 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT)* (p. 111-114). doi: 10.1109/DFT.2016.7684080
- Hernandez, J. L. (2016). Reflexiones desde un servicio de referencia: propuestas para mejorar la atención al ciudadano en los archivos. *Revista General de Información y Documentación*. doi: http://dx.doi.org/10.5209/rev_RGID.2016.v26.n1.53048
- Humberto Cervantes, L. C.-C., Perla Velasco-Elizondo. (2016). *Arquitectura del software. conceptos y ciclo de desarrollo*.
- INEN. (2014). *Nte inen - iso /iec 250 10 primera edición*. Descargado de http://www.normalizacion.gob.ec/wp-content/uploads/downloads/2014/02/nte_inen_iso_iec_25010.pdf
- ISO/IEC-JTC1-/SC-7/WG-6. (2002). *Iso/iec 9126-3: Software engineering – product quality – part 3: Internal metrics [Manual de software informático]*.
- ITIL. (2000). *Open guide*. Descargado de http://www.itlibrary.org/index.php?page=Incident_Management
- Jacobs, S. (2016). Authentication of subjects. En *Engineering information security: the application of systems engineering concepts to achieve information assurance*

- (p. 784-). Wiley-IEEE Press. Descargado de <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=7406340> doi: 10.1002/9781119104728.ch04
- Jafer, S., Liu, Q., y Wainer, G. (2013). Synchronization methods in parallel and distributed discrete-event simulation. *Simulation Modelling Practice and Theory*, 30, 54 - 73. Descargado de <http://www.sciencedirect.com/science/article/pii/S1569190X12001244> doi: <http://doi.org/10.1016/j.simpat.2012.08.003>
- Jendrock, E., Ball, J., Carson, D., Evans, I., Fordin, S., y Haase, K. (2017, febrero). *The java ee 5 tutorial for sun java system application server 9.1*. Descargado de <http://docs.oracle.com/javase/5/tutorial/doc/javaeetutorial5.pdf>
- Jimenez, A., Salamanca, P., y Garavito, L. (2007). Sistema de información orientado a procesos de negocio y flujos de trabajo en la universidad nacional de colombia. perspectivas y caso de estudio. *REVISTA INGENIERÍA E INVESTIGACIÓN*.
- Juristo, N., Moreno, A., y Sanchez-Segura, M. I. (2007, Nov). Guidelines for eliciting usability functionalities. *IEEE Transactions on Software Engineering*, 33(11), 744-758. doi: 10.1109/TSE.2007.70741
- León-Coca, J., Reina, D., Toral, S., Barrero, F., y Bessis, N. (2013). Authentication systems using id cards over nfc links: The spanish experience using dne. *Procedia Computer Science*, 21, 91 - 98. Descargado de <http://www.sciencedirect.com/science/article/pii/S1877050913008077> doi: <http://dx.doi.org/10.1016/j.procs.2013.09.014>
- Lillo, R. (2018). *Teoría de colas*. Descargado de http://www.est.uc3m.es/esp/nueva_docencia/comp_colleg/ing_info/io/doc_generica/archivos/tc.pdf
- López, T. (2016). *Especificación de requisitos para el desarrollo del software de gestión de trámites institucionales de la universidad técnica del norte según el estándar de ieee 830*. Descargado de <https://appsphp-teisistemas.rhcloud.com/tesisMSC/ieee830.pdf>
- López, T., y Rosero, I. (1999). *Modelo de comunicación entre dos sistemas operativos* (Tesis de grado para optar por el título de Ingeniero en Sistemas Computacionales). Ingeniería en Sistemas Computacionales - Universidad Técnica del Norte.
- Mara, R. (2006). *Procesos de software*. Descargado de <https://sg.com.mx/revista/1/procesos-software>
- Martinez, A., y Martinez, R. (2011, febrero). *Guía a rational unified process*. Des-

- cargado de <https://anaylenlopez.files.wordpress.com/2011/03/trabajo-guia20rup.pdf>
- Nacional, A. (2014). *Ley de comercio electrónico, firmas y mensajes de datos*. Descargado de <https://www.eci.bce.ec/documents/10180/1096676/LEY+DE+COMERCIO+ELECTRONICO%2C%20FIRMAS+Y+MENSAJES+DE+DATOS.pdf/b41d44af-0e84-4b30-9ff8-e257deb3f32e>
- Naranjo, M., y Chiliquinga, L. (2014). *Reglamento para el uso del sistema de gestión documental quipux en la universidad técnica del norte*. Descargado de www.utn.edu.ec
- Ocampo, J. A. (2015). Los retos del desarrollo latinoamericano a la luz de la historia/the challenges of latin american development in the light of history/les défis du développement latino-américain a la lumière de l'histoire/os desafios do desenvolvimento latino-americano sob a ótica da história. *Cuadernos de Economía*, 34(66), 479-506. Descargado de <https://search.proquest.com/docview/1694862116?accountid=36862> (Copyright - Copyright Universidad Nacional de Colombia 2015; Última actualización - 2015-10-23; SubjectsTermNotLitGenreText - Latin America)
- Paula-Izaurre, N.-A. (2018). *Trazabilidad ágil*. Descargado de <http://conaiisi.frc.utn.edu.ar/PDFsParaPublicar/1/schedConfs/7/113-528-1-DR.pdf>
- Reeve, A. (2013). Chapter 13 - core real-time data integration technologies. En A. Reeve (Ed.), *Managing data in motion* (p. 87 - 98). Boston: Morgan Kaufmann. Descargado de <http://www.sciencedirect.com/science/article/pii/B9780123971678000133> doi: <http://doi.org/10.1016/B978-0-12-397167-8.00013-3>
- Research on cloud resource optimization model based on users' satisfaction. (2016, Sept). En *2016 13th web information systems and applications conference (wisa)* (p. 99-102). doi: 10.1109/WISA.2016.28
- Runeson, P., y Höst, M. (2008). Guidelines for conducting and reporting case study research in software engineering. *Empirical Software Engineering*. doi: 10.1007/s10664-008-9102-8
- Sandoval, M. (2008). *La trazabilidad en el proceso de requerimientos de software*. Descargado de <http://www.iiis.org/cds2008/cd2008csc/cisci2008/>

- Sethi, P., y Sarangi, S. R. (2017). Internet of things: Architectures, protocols, and applications. *Journal of Electrical and Computer Engineering*. Descargado de <https://search.proquest.com/docview/1865278719?accountid=36862> (Copyright - Copyright © 2017 Pallavi Sethi and Smruti R. Sarangi. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited; Última actualización - 2017-02-06)
- Software and systems engineering software testing part 1:concepts and definitions. (2013, Sept). *ISO/IEC/IEEE 29119-1:2013(E)*, 1-64. doi: 10.1109/IEEESTD.2013.6588537
- Spinellis, D. (2017, Mar). The social responsibility of software development. *IEEE Software*, 34(2), 4-6. doi: 10.1109/MS.2017.48
- Suga, Y. (2014, Sept). Ssl/tls servers status survey about enabling forward secrecy. En *2014 17th international conference on network-based information systems* (p. 501-505). doi: 10.1109/NBiS.2014.101
- Takacs, B., Richter, G., Csizinszky, K., Mazzei, D., y Simon, L. (2015, Oct). Towards a unified control framework for humanoid robots and their virtual avatars in physical and virtual reality-based interactions. En *2015 15th international conference on control, automation and systems (iccas)* (p. 1905-1909). doi: 10.1109/ICCAS.2015.7364676
- Terán, E. (2016, Dec 21). *Una plataforma que agrupa a 50 mensajeros*. Descargado de <https://search.proquest.com/docview/1850745617?accountid=36862> (Copyright - Copyright (c) 2016 Lideres; Última actualización - 2016-12-21)
- TICAL. (2016). *Tical2017 abre llamado para presentar trabajos*. Descargado de <https://www.renata.edu.co/index.php/convocatorias/8949-tical2017-abre-llamado-para-presentar-trabajos>
- Tsamoura, E., Gounaris, A., y Manolopoulos, Y. (2011). Decentralized execution of linear workflows over web services. *Future Generation Computer Systems*, 27(3), 341 - 347. Descargado de <http://www.sciencedirect.com/science/article/pii/S0167739X10001433> doi: <http://dx.doi.org/10.1016/j.future.2010.07.009>
- Urton, G., y Brezine, C. (2009). *Khipu database project*. Descargado de <http://khipukamayuq.fas.harvard.edu/index.html>

- Usman, M., Britto, R., Börstler, J., y Mendes, E. (2017). Taxonomies in software engineering: A systematic mapping study and a revised taxonomy development method. *Information and Software Technology*, 85, 43 - 59. Descargado de <http://www.sciencedirect.com/science/article/pii/S0950584917300472> doi: <http://doi.org/10.1016/j.infsof.2017.01.006>
- UTN. (2014). *Maestría en ingeniería de software*. Descargado de http://www.utn.edu.ec/web/uniportal/?page_id=2886
- UTN. (2016). *Quipux*. Descargado de <http://quipux.utn.edu.ec/>
- Vilela, J., Castro, J., Martins, L. E. G., y Gorschek, T. (2017). Integration between requirements engineering and safety analysis: A systematic literature review. *Journal of Systems and Software*, 125, 68 - 92. Descargado de <http://www.sciencedirect.com/science/article/pii/S0164121216302333> doi: <http://doi.org/10.1016/j.jss.2016.11.031>
- W3C. (2007). *Soap*. Descargado de <https://www.w3.org/TR/2007/REC-soap12-part0-20070427/>
- Wilk, A. (2016, June). Cyber security education and law. En *2016 ieee international conference on software science, technology and engineering (swste)* (p. 94-103). doi: 10.1109/SWSTE.2016.21

Anexos

1 Especificación de Requisitos para el desarrollo del Software de gestión de trámites institucionales de la Universidad Técnica del Norte según el estándar de ISO/IEC 29148

ISO/IEC 29148

26 de Octubre de 2016

Resumen

En este documento se recopila y sintetiza los requisitos especificados por los USUARIOS PRINCIPALES del Software para la gestión de trámites institucionales de la Universidad Técnica del Norte en atención al pedido formulado por el Ing. Juan Carlos García, DIRECTOR DEL DEPARTAMENTO DE DESARROLLO TECNOLÓGICO E INFORMÁTICO DE LA UTN, la fecha en que arranca el proyecto de software es el 4 de julio de 2016.

Índice

1. Introducción	2
1.1. Propósito	2
1.2. Ambito del Sistema	2
1.3. Definiciones, Acrónimos y Abreviaturas	4
1.4. Referencias.....	6
1.5. Visión General del Documento	7
2. Descripción General.....	7
2.1. Perspectiva del Producto.....	8
2.2. Funciones del Producto.....	8
2.3. Características de los Usuarios.....	8

	2
2.4. Restricciones	9
2.5. Suposiciones y Dependencias	11
2.6. Requisitos Futuros	11
3. Requisitos Específicos	12
3.1. Interfaces Externas	19
3.2. Funciones.....	19
3.3. Requisitos de Rendimiento	20
3.4. Restricciones de Diseño	20
3.5. Atributos del Sistema	20
3.6. Otros Requisitos.....	22
4. Apéndices.....	22

1. Introducción

En esta sección se proporciona una introducción a todo el documento de Especificación de Requisitos Software (ERS). Consta de varias subsecciones: propósito, ámbito del sistema, definiciones, referencias y visión general del documento.

1.1. Propósito

Implementar un software de servicios de gestión de trámites institucionales firmados electrónicamente mediante el repositorio de firmas digitales de la Universidad Técnica del Norte, dirigido especialmente para la DIRECCION DE DESARROLLO TECNOLÓGICO E INFORMÁTICO de la U.T.N. y representado actualmente por el Ing. Juan Carlos García en calidad de Director del Departamento y CLIENTE principal del presente Proyecto.

1.2. Ámbito del Sistema

El nombre sugerido para el futuro sistema es GestionDeTramitesUTN en siglas (GDTUTN).

Básicamente lo que se trata de hacer es gestionar automáticamente los trámites institucionales que los estudiantes realizan en forma legal en la UTN mediante un software ubicuo (funcionando sobre Internet) que agilite el proceso de SOLICITUD, AUTORIZACIÓN, EMISIÓN y ARCHIVO de documentos firmados electrónicamente por funcionarios legalmente autorizados de la UTN y que son de utilidad para ESTUDIANTES, DOCENTES, EMPLEADOS y ADMINISTRATIVOS de la Institución; en amparo a: Ley de Comercio Electrónico, Firmas y Mensajes de Datos publicado en el Suplemento del Registro Oficial No. 557 de 17 de abril de 2002. Reglamento a la Ley de Comercio Electrónico, Firmas y Mensajes de Datos, publicado en el Registro Oficial No. 735 de 31 de diciembre de 2002. Decreto No. 181 publicado en el Registro Oficial No. 553 de 11 de octubre del 2011, en el cual norma la numeración de identificadores de campo y campos mínimos de los tipos de certificados.

No se sustituirá la obligación de que el Funcionario emita la Autorización de forma manual para los casos que requieran de análisis de la situación legal de la solicitud registrada. En forma general el sistema procura la seguridad del tratamiento de la información al nivel aceptable y en todo caso los errores serán considerados humanos y susceptibles de corrección sin que por ello se atribuya al software como causante de dificultades legales, contratiempos y procesos legales a favor o en contra de los beneficiarios que podrían derivarse del uso o mal uso, abuso, negligencia, malicia intencional o accidental, intrusión, inexperiencia, olvido u omisión de la ejecución del procedimiento seguro de operación, administración, instalación, cierre, respaldo o restauración de datos, fallas de energía eléctrica, incidentes esperados o inesperados, robo, hurto, y cualquier otra causa no especificada que no haya sido considerada y no será considerada parte de este documento y por lo tanto no se considerará un requisito que el sistema deba cumplir; lo cual exime y libera al desarrollador de la responsabilidad legal al momento de la firma del acta de entrega y recepción del software con la que el Ing. Tobías López, en calidad de desarrollador, se desvinculará legalmente de cualquier responsabilidad penal o civil que se derive de la Administración, Uso, Mantenimiento y Operación del Software de Gestión de Trámites Institucionales de la UTN desarrollado con finalidad investigativa y meramente experimental para la sustentación del Proyecto de Grado.

El principal beneficio esperado es la agilidad en la gestión de los diversos trámites institucionales que los Estudiantes, Docentes y Administrativos de la UTN realizan de forma regular. Los efectos colaterales esperados son: disminución del tiempo que se demora la gestión de un trámite de Solicitud, Autorización, Emisión y Archivo de un documento firmado por un funcionario responsable de la UTN; reducción del consumo de papel; optimización del proceso de comunicación legal interna entre las dependencias de la institución.

Las principales metas del proyecto son: (a) Influir positivamente sobre la gestión de trámites institucionales, (b) Aprovechar el repositorio de firmas digitales para emitir documentos legalmente válidos en forma automatizada, (c) Optimizar los procesos de Solicitud, Autorización, Emisión y Archivo de documentos con datos firmados digitalmente y almacenados en el repositorio documental de la Base de Datos de la UTN, (d) Crear una arquitectura de software que permita gestionar mensajes de datos firmados en la UTN usando estándares de intercambio de mensajes de datos especialmente XML.

1.3. Definiciones, Acrónimos y Abreviaturas

Definiciones:

Estudiante.- Cualquier persona matriculada en la Universidad Técnica del Norte.

Docente.- Cualquier persona acreditada como docente en la Universidad Técnica del Norte

Empleado.- Cualquier persona que trabaja o trabajó en la Universidad Técnica del Norte.

Secretario-Abogado.- Empleado de la Universidad Técnica del Norte que ejerce la función de Secretario y cuya profesión es Abogado de la institución.

Administrativo.- Empleado de la Universidad Técnica del Norte que ejerce funciones administrativas en cualquier dependencia institucional.

Términos:

GestionDeTramitesUTN.- Acrónimo para definir el software de gestión de trámites institucionales de la Universidad Técnica del Norte que se desarrolla en base a los requisitos especificados en este documento.

Oracle.- Líder de la industria de Sistemas de Gestión de Bases de Datos.

SGDBMS.- Sistema de gestión de la administración de bases de datos.

jQuery.- Es una biblioteca de JavaScript, creada inicialmente por John Resig, que permite simplificar la manera de interactuar con los documentos HTML.

CAPTCHA.- Prueba de Turing completamente automática y pública para diferenciar ordenadores de humanos.

Firma digital.- (Firma electrónica) La firma electrónica es un conjunto de datos electrónicos que acompañan o que están asociados a un documento electrónico y cuyas funciones básicas son: Identificar al firmante de manera inequívoca, Asegurar la integridad del documento firmado. Asegura que el documento firmado es exactamente el mismo que el original y que no ha sufrido alteración o manipulación, Asegurar la autenticidad del documento firmado. Los datos que utiliza el firmante para realizar la firma son únicos y exclusivos y, por tanto, posteriormente, no puede decir que no ha firmado el documento.

Bandeja.- Metáfora para representar el listado o catálogo de documentos entrantes o salientes en el repositorio asignado a un usuario.

Acrónimos:

GDTUTN.- Gestión de Trámites institucionales de la Universidad Técnica del Norte.

UTN.- Universidad Técnica del Norte.

ERP-UTN.- Sistema de gestión de recursos de la UTN.

PDF.- Es un formato de almacenamiento para documentos digitales independiente de plataformas de software o hardware. Este formato es de tipo compuesto (imagen vectorial, mapa de bits y texto).

XML.- Es una adaptación del SGML (Standard Generalized Markup Language), un lenguaje que permite la organización y el etiquetado de documentos. Esto quiere decir que el XML no es un lenguaje en sí mismo, sino un sistema que permite definir lenguajes de acuerdo a las necesidades.

HTML.- Es un lenguaje de programación que se utiliza para el desarrollo de páginas de Internet. Se trata de la sigla que corresponde a HyperText Markup Language, es decir, Lenguaje de Marcas de Hipertexto, que podría ser traducido como Lenguaje de Formato de Documentos para Hipertexto.

HTTPS.- Son las siglas en inglés de HiperText Transfer Protocol (en español, protocolo de transferencia de hipertexto). Es un protocolo de red (un protocolo se puede definir como un conjunto de reglas a seguir) que se utiliza para publicar páginas de web o HTML.

1.4. Referencias

Ley de Comercio Electrónico, Firmas y Mensajes de Datos publicado en el Suplemento del Registro Oficial No. 557 de 17 de abril de 2002.

Reglamento a la Ley de Comercio Electrónico, Firmas y Mensajes de Datos, publicado en el Registro Oficial No. 735 de 31 de diciembre de 2002.

Decreto No. 181 publicado en el Registro Oficial No. 553 de 11 de octubre del 2011, en el cual norma la numeración de identificadores de campo y campos mínimos de los tipos de certificados.

1.5. Visión General del Documento

Descripción de contenidos y organización del documento:

2. Descripción General

El entorno de la aplicación es el sistema integrado de la UTN sobre el cual operará el software GDTUTN, por lo cual existen aspectos de seguridad y usabilidad en que la fortaleza está limitada por las características inherentes al entorno del ERP-UTN.

Los usuarios se caracterizan por ser de dos tipos: SOLICITANTES y EMISORES. Los usuarios solicitantes se caracterizan por pedir un documento legalmente firmado a algún funcionario que lo autoriza o rechaza y emite la resolución. Los usuarios emisores se caracterizan por emitir o rechazar solicitudes de documentos firmados.

La principal restricción es que ningún documento solicitado puede ser emitido sin autorización del emisor. La segunda restricción es que para ser emisor se debe estar legalmente autorizado para el efecto y cumplir los requisitos estipulados en la Ley para emitir documentos firmados electrónicamente a nombre institucional.

Algunos usuarios emisores entregaran de buena fe, la custodia de su firma digital al Ing. Tobías López para usarla en ambiente de pruebas considerado seguro.

Se asume que el repositorio de firmas digitales esta resguardado y cuidado tanto física como lógicamente. La firma digital válida que se considera para este desarrollo es la que se encuentra en formato P12 y ha sido emitida por el Banco Central del Ecuador a fin de asegurar la identidad de una persona.

Los requisitos de compatibilidad de documentos y formatos pueden ser especificados para transferencia de mensajes de datos dentro y fuera de la institución siempre que se usen al menos uno de los formatos: PDF, XML.

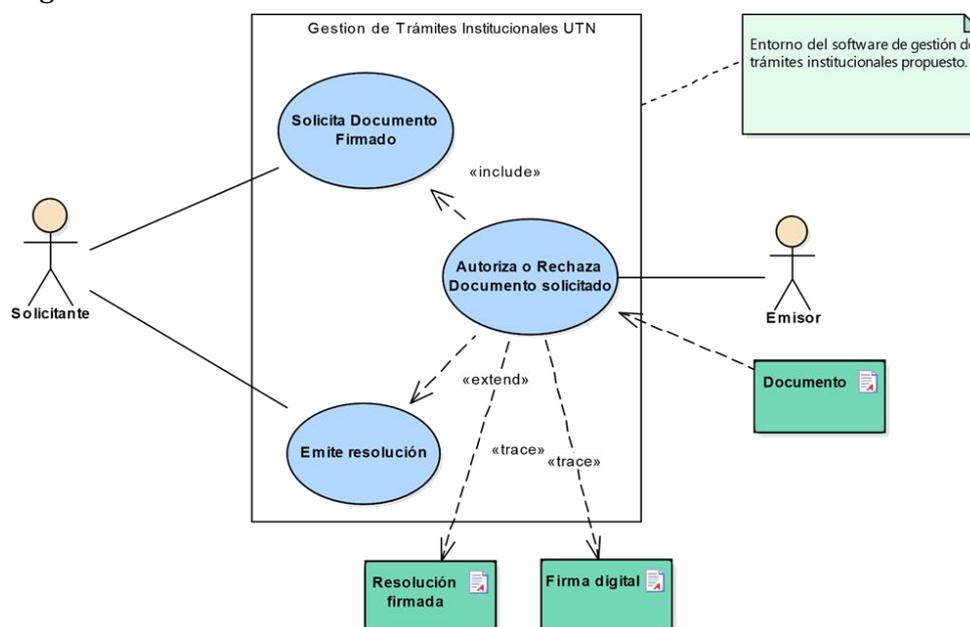
2.1. Perspectiva del Producto

El software GDTUTN a ser desarrollado es parte del ERP-UTN. Sin embargo podrá operar de manera independiente. Esto implica ambiente de pruebas libre e integrado y ambiente de operación libre e integrada.

2.2. Funciones del Producto

El solicitante solicita documento firmado mediante el GDTUTN a un emisor. El emisor autoriza o rechaza el documento solicitado y emite una resolución firmada sobre este hecho usando el repositorio de firmas digitales. Al final el solicitante recibe la resolución emitida sobre su documento solicitado mediante el GDTUTN.

El software GDTUTN gestionará lo siguiente: (a) Interacción con el solicitante para receptor solicitud de documento firmado, (b) Interacción con el emisor para autorizar o rechazar solicitudes, (c) Interacción con los repositorios de documentos, firmas digitales y resoluciones emitidas, (d) Entrega de resoluciones emitidas al solicitante.



2.3. Características de los Usuarios

Los usuarios definidos del software GDTUTN son: Estudiantes y Trabajadores de la UTN. Sin embargo los roles que se interpretan en el

entorno de software de gestión de trámites institucionales son dos: Solicitante y Emisor.

El Solicitante puede ser estudiante o trabajador de la UTN registrado en el sistema ERP-UTN. Debe saber al menos utilizar algún navegador de internet, conocer su ID y clave de acceso al GDTUTN, poseer un correo electrónico activo.

El Emisor puede y debe ser funcionario con nombramiento o contratado de la UTN, tener el rol de Docente, Empleado Administrativo o Secretario-Abogado. Debe saber al menos utilizar algún navegador de internet, conocer algún software de Ofimática que genere o emita documentos PDF o XML, disponer de firma digital vigente en formato P12 emitida por el Banco Central del Ecuador. Deberá entregar en el DTI-UTN una carta de entrega y el archivo digital en custodia de la firma electrónica para propósitos de gestión administrativa mediante el software GDTUTN.

2.4. Restricciones

Políticas de la UTN

Se adoptan las disposiciones referentes al manejo de QUIPUX-UTN con respecto al manejo de documentos internos y comunicaciones interinstitucionales.

Limitaciones del hardware

El sistema operará bajo las características físicas de la infraestructura existente que da soporte al ERP-UTN. Considerando que el espacio de almacenamiento adicional debe dejarse en la proporción que sea necesaria luego del cálculo del tamaño de los datos y su proyección de crecimiento correspondiente cuando se haya terminado el presente proyecto. La capacidad de procesamiento necesaria debe considerar la carga de solicitudes total en minutos críticos esperados según los resultados que se produzcan en la fase de pruebas de carga del software que se construye. De no asignarse los recursos correspondientes para operar el software construido, este reducirá su rendimiento en función de los recursos asignados incluso pudiéndose denegar el servicio por esta causa.

Interfaces con otras aplicaciones

La principal interface es la integración con el ERP-UTN siendo el software GDTUTN parte integrante fuertemente acoplada.

Operaciones paralelas

Las solicitudes de los solicitantes pueden requerirse en paralelo a otras solicitudes la limitante de paralelismo es la capacidad del hardware.

Las autorizaciones o rechazos de los emisores pueden ejecutarse en paralelo a otras autorizaciones o rechazos pudiéndose ejecutar estos procesos en distintos equipos interconectados con el software GDTUTN.

Funciones de auditoría

El software GDTUTN almacenará el historial de solicitudes en sus correspondientes estados: Iniciada, Entregada, Recibida, Autorizada o Rechazada, Entregada, Terminada.

El software GDTUTN almacenara el historial de autorizaciones o rechazos de los emisores con sus correspondientes estados: Abierta, Emitida, Autorizada, Negada, Entregada, Cerrada.

Se mantendrá un catálogo numerado de cada documento generado manual o automático por el software GDTUTN.

Funciones de control

Cada formulario de Entrada y Salida de datos mantiene relación con el usuario quien podra tener el control del seguimiento total de cada documento relacionado con su rol: Solicitante o Emisor.

Lenguaje(s) de programación

Por conveniencia del DTI-UTN el lenguaje de desarrollo puede ser Java, APEX, PL/SQL, CSS, JavaScript, HTML, XML, jQuery.

Protocolos de comunicación

Aceptado HTTPS sobre TCP/IP.

Requisitos de habilidad

Conocer Oracle DBMS, PL/SQL, Java.

Criticalidad de la aplicación

La aplicación es de nivel crítico por las exigencias de seguridad debido al tratamiento de información confidencial para sus usuarios.

Consideraciones acerca de la seguridad

La comunicación entre aplicaciones usara HTTPS para evitar que intrusos puedan leer o modificar la información sin autorización, los formularios de entrada y salida de información tendrán funciones de seguridad que garantizan la identidad de quien dice ser el emisor o receptor, se asegurara el perímetro de la información almacenada usando la potencia de seguridad de Oracle DBMS, los servicios a petición se abren, ejecutan y cierran tomando en cuenta el rol del usuario dentro del sistema.

Se tomarán de manera general y especifica todas las medidas que sean aplicables y que constituyen una práctica estándar de la industria para asegurar la información, los procesos y los recursos que se utilizan en el software GDTUTN.

2.5. Suposiciones y Dependencias

El sistema operara sobre una base de datos Oracle DBMS y las interfaces de usuario en alguno de los siguientes navegadores Web: Mozilla Firefox, Internet Explorer. La herramienta de desarrollo de interfaz de usuario será APEX.

Los principales elementos de diseño de interacción serán implementados en JavaScript, jQuery, CSS, HTML. Pudiéndose opcionalmente utilizar algún framework compatible con APEX.

El software GDTUTN funcionara en entornos Linux o Windows. No se prevé desarrollar interfaces a celular, pero se deja abierta la alternativa mediante la interface SOAP que puede ser accedida desde cualquier aplicativo en cualquier dispositivo.

2.6. Requisitos Futuros

A futuro un requisito que la interface de usuario sea implementada en dispositivos móviles.

3. Requisitos Específicos

RQ1: Solicitud de documento firmado

ACTORES	Solicitante
Pre-Condiciones	El Solicitante debe estar autenticado en el sistema y demostrar que no es un robot.
Acciones	<ol style="list-style-type: none"> 1. El sistema muestra al Solicitante el catálogo de tipos de documentos que puede solicitar. 2. El Solicitante indica el tipo de documento que requiere 3. El sistema muestra la plantilla del documento requerido para que el Solicitante llene los parámetros especificados en la plantilla. 4. El Solicitante llena todos los parámetros requeridos para completar la plantilla del documento solicitado y pulsa sobre el botón Enviar. 5. El sistema emite el mensaje indicando que el documento fue enviado para su correspondiente revisión por el Emisor del documento firmado, agradece al Solicitante y le invita a esperar en la bandeja de entrada la llegada de una respuesta a su solicitud. 6. El sistema muestra al Solicitante un cuadro de dialogo para seleccionar la siguiente acción

	<p>posible: (a) Realizar otra solicitud, (b) Recibir resolución en la bandeja de llegada de mensajes firmados, (c) Salir.</p> <p>7. El Solicitante decide que hacer y selecciona una de las tres opciones indicadas.</p>
Flujo alternativo 1	<p>ERROR AL LLENAR FORMULARIO</p> <p>1. El sistema muestra un mensaje amigable indicando que habido un error con la plantilla seleccionada e invita a elegir una de las siguientes acciones: (a) Realizar otra solicitud, (b) Recibir resolución en la bandeja de llegada de mensajes firmados, (c) Salir.</p> <p>2. El Solicitante decide que hacer y selecciona una de las tres opciones indicadas.</p>
Post-Condiciones	<p>El resultado esperado de este proceso es una Solicitud de Documento firmado enviado algún Emisor designado.</p>
Reglas de Negocio	<p>Los campos de plantilla mínima de solicitud contienen lo siguiente:</p> <p>ID Solicitante, Datos del Solicitante, ID Emisor, Rol del Emisor en la UTN {Docente, Administrador, Secretario-Abogado}, Tipo de Documento, Fecha y Hora de Solicitud, Tiempo máximo de espera de respuesta, Otros campos específicos según el tipo de plantilla de documento.</p>
Comentarios	<p>Ninguno</p>

--	--

RQ2: Respuesta a solicitud

ACTORES	Emisor
Pre-Condiciones	<p>El Emisor debe estar autenticado en el sistema, demostrar que no es un robot y tener registrada su firma electrónica válida legalmente.</p> <p>Las Solicitudes tienen un Tipo de Documento que indica el tipo de resolución que debe tomarse: Manual o Automática.</p>
Acciones	<p>1. El sistema muestra al Emisor el catálogo de solicitudes de tipo manual en su bandeja de entrada.</p> <p>2. Para cada Solicitud mostrada el Emisor puede elegir una de las siguientes acciones: Autorizar, Rechazar, Reenviar a otro destinatario {Emisor, Solicitante} y/o Comentar la acción a realizar, Agregar adjunto.</p> <p>INICIO DE CADA SOLICITUD:</p> <p>3. Según la acción especificada se realizará lo siguiente:</p> <ul style="list-style-type: none"> • Autorizar: Emite manual o automáticamente resolución de autorización y devuelve al solicitante.

	<ul style="list-style-type: none"> • Rechazar: Emite resolución de rechazo y devuelve al solicitante. • Reenviar a otro destinatario: Elige el destinatario y envía la solicitud sin cambios. <p>4. Opcionalmente el Emisor redacta comentarios y agrega archivos adjuntos.</p> <p>5. El Emisor pulsa sobre el botón Enviar.</p> <p>6. El sistema emite el mensaje indicando que el documento fue enviado.</p> <p>FIN DE CADA SOLICITUD.</p> <p>7. El sistema muestra al Emisor un cuadro de dialogo para seleccionar la siguiente acción posible: (a) Responder otra solicitud, (b) Emitir solicitud, (c) Salir.</p> <p>8. El Emisor decide que hacer y selecciona una de las tres opciones indicadas.</p>
Flujo alternativo 1	<p>ERROR AL RESPONDER SOLICITUD</p> <p>1. El sistema muestra un mensaje amigable indicando que habido un error con la plantilla seleccionada e invita a elegir una de las siguientes acciones: (a) Responder otra solicitud, (b) Emitir solicitud, (c) Salir.</p> <p>2. El Emisor decide que hacer y selecciona una de las tres opciones indicadas.</p>

Post-Condiciones	El resultado esperado de este proceso es la Resolución en respuesta a cada solicitud encontrada en la Bandeja de Entrada del Emisor.
Reglas de Negocio	<p>Los campos de plantilla mínima de resolución en respuesta a una solicitud contienen lo siguiente:</p> <p>ID Solicitante, Datos del Solicitante, ID Emisor, Rol del Emisor en la UTN {Docente, Administrador, Secretario-Abogado}, Tipo de Documento, Fecha y Hora de Solicitud, Tiempo máximo de espera de respuesta, Otros campos específicos según el tipo de plantilla de documento. Opcionalmente comentarios y Archivos adjuntos. Resolución. Firma Electrónica Autorizada.</p> <p>Solo documentos que requieren autorización manual son atendidos por el Emisor humano.</p>
Comentarios	Este proceso puede ser ejecutado automáticamente por el Sistema en respuesta algún Tipo de Documento sin requerir la intervención del Emisor humano.
Caso extendido	El sistema Emite resolución manual o automática según el tipo de documento del Solicitante.

RQ3: Emisión de resoluciones

ACTORES	Solicitante
Pre-Condiciones	El Solicitante debe estar autenticado en el sistema y demostrar que no es un robot.

	<p>Debe existir Solicitudes de documentos pendientes de ser atendidas y que son susceptibles de automatización.</p>
<p>Acciones</p>	<p>1. El sistema emite todas las resoluciones automáticas pendientes según las Solicitudes recibidas del Solicitante.</p> <p>2. El sistema forma el conjunto de resoluciones entregadas por el Emisor y las generadas automáticamente para depositarlas en la bandeja de llegada del Solicitante.</p> <p>3. Para cada resolución en la bandeja de llegada del solicitante, el Solicitante puede: Mirar, Imprimir, Descartar, Archivar, Responder.</p> <p>INICIO DE CADA RESOLUCIÓN:</p> <p>4. Según la acción que el solicitante escoja:</p> <ul style="list-style-type: none"> • Mirar: El sistema abre el documento con un visor PDF o XML • Imprimir: El sistema abre el documento con un visor PDF o XML y muestra la opción de Editar Impresión. • Descartar: El sistema oculta el documento del listado en la bandeja de llegada. • Archivar: El sistema muestra destinos donde enviar el documento posibles {Correo electrónico, Archivo, Exportar} • Responder: El sistema muestra un dialogo para escribir al Emisor el comentario sobre la notificación recibida. <p>FIN DE CADA RESOLUCION</p>

	<p>6. El sistema muestra al Solicitante un cuadro de dialogo para seleccionar la siguiente acción posible: (a) Realizar otra solicitud, (b) Recibir resolución en la bandeja de llegada de mensajes firmados, (c) Salir.</p> <p>7. El Solicitante decide que hacer y selecciona una de las tres opciones indicadas.</p>
Flujo alternativo 1	<p>ERROR AL REALIZAR UNA ACCIÓN</p> <p>1. El sistema muestra un mensaje amigable indicando que habido un error con la acción seleccionada e invita a elegir una de las siguientes acciones: (a) Realizar otra solicitud, (b) Recibir resolución en la bandeja de llegada de mensajes firmados, (c) Salir.</p> <p>2. El Solicitante decide que hacer y selecciona una de las tres opciones indicadas.</p>
Post-Condiciones	El resultado esperado de este proceso es una Acción sobre la Resolución recibida.
Reglas de Negocio	<p>Es necesario que existan Resoluciones en la bandeja de llegada.</p> <p>Cada Resolución guarda un historial de estados de acciones realizada</p>
Comentarios	Ninguno

3.1. Interfaces Externas

Navegadores Web: Internet Explorer, Mozilla Firefox.

Servicios del Repositorio de Firmas Digitales: SOA del ERP-UTN.

Protocolo de comunicación: HTTPS.

Red de Comunicaciones: Infraestructura de Internet de la UTN.

3.2. Funciones

El sistema deberá almacenar en forma segura las firmas digitales de los emisores en el repositorio de base de datos de la UTN, usando para el efecto el SGDBMS Oracle.

El sistema deberá incluir a todos los miembros de la comunidad universitaria entre los usuarios con rol de tipo Solicitante.

El sistema deberá incluir solo a los funcionarios autorizados por la UTN entre los usuarios con rol de tipo Emisor.

El tipo de Emisor deberá ser exclusivo sobre los privilegios de algún tipo de documento en particular.

El sistema podrá emitir automáticamente ciertos documentos auto-firmados que sean requeridos por el Solicitante, debiendo para el efecto conocerse que tipos de documentos mantienen esta condición, por ejemplo: Reportes de Calificaciones, Certificados de Matrícula y Asistencia.

El sistema deberá mantener interfaces de servicios de firma digital de documentos para ser utilizados por otras aplicaciones mediante SOA.

El sistema deberá tener una interfaz de recepción de Solicitudes de Usuarios Solicitantes a la cual se pueda ingresar desde los siguientes

navegadores Web: Internet Explorer y Mozilla Firefox. Opcionalmente deberá ser compatible con algún dispositivo móvil más comúnmente utilizado.

El sistema deberá tener una interfaz de administración de Solicitudes por parte del usuario Emisor de resoluciones.

La usabilidad del sistema deberá ser aceptable y realizar su proceso tomando en cuenta las características especiales de los diferentes tipos de usuarios.

La seguridad del sistema deberá mantener comunicación segura y garantizar la integridad, disponibilidad y confiabilidad de la información en un nivel aceptable.

3.3. Requisitos de Rendimiento

El sistema deberá atender en forma normal un promedio de 18 solicitudes por minuto como mínimo en hora y día pico.

El servicio manual deberá responder un promedio de 15 solicitudes por hora en cada Emisor como mínimo en hora y día pico.

El número mínimo de usuarios conectados en paralelo debe ser de 5.

No hay un requerimiento sobre el número de transacciones por segundo inicialmente, pues esto depende de los primeros resultados de la investigación sobre las pruebas reales de carga.

No hay un límite sobre el número de terminales conectadas pero cada interfaz Web de cualquier usuario se considera una terminal, se espera atender la demanda simultánea en día y hora pico desde 8500 usuarios solicitantes.

El número promedio esperado de solicitudes anuales atendidas es de 850000 es decir un promedio de 2 solicitudes por minuto continuamente.

3.4. Restricciones de Diseño

Limitado a lo que se pueda realizar con APEX.

3.5. Atributos del Sistema

Los atributos de calidad del sistema son los elementos que se pretende investigar exhaustivamente en la fase de pruebas, tomando en cuenta dos aspectos principales: Usabilidad y Seguridad.

El sistema deberá cumplir como mínimo los siguientes atributos de Usabilidad:

- Interfaz de usuario en español
- Ergonomía de usuario medible{número de clics por acción, número de opciones por formulario, número acciones automáticas, número de estados y mensajes}
- Mensajes de ayuda contextual automático
- Comportamiento uniforme predecible{mediante flujos de proceso de usuario}
- Método de navegación WYSIWYG {lo que ve es lo que obtiene}
- Número máximo de colores por página 5 incluido fondo y texto. Excepto en imágenes
- Minimización del número de Botones textuales e iconográficos
- Orden de lectura de izquierda a derecha y de arriba hacia abajo
- Ubicuidad de servicios
- Bandeja de entrada del Emisor para responder Solicitudes de documentos que deben ser firmados manualmente o con archivos adjuntos.
- Bandeja de salida del Emisor para mantener el Archivo de Resoluciones emitidas.
- Bandeja de entrada del Solicitante para revisar las Resoluciones recibidas del Emisor que atiende la solicitud correspondiente.
- Bandeja de salida del Solicitante para revisar las Solicitudes realizadas.

El sistema deberá cumplir los siguientes atributos de Seguridad:

- Manejar usuarios humanos autorizados autenticados mediante Identificador de usuario público, Clave privada, Preguntas de recuperación, CAPTCHA.
- Manejar comunicaciones de datos seguras mediante HTTPS.
- Aseguramiento de servidores Web mediante certificados de autenticidad firmados digitalmente en formato P12 emitidos por el Banco Central del Ecuador.

- Manejo de roles de usuarios humanos específicos para Solicitante, Emisor. Considerando que el Solicitante puede ser: Estudiante Matriculado, Aspirante a Estudiante, Ciudadano ecuatoriano o extranjero. Emisor puede ser: Autoridad, Empleado, Docente, Secretario-Abogado.
- Manejo de privilegios de usuarios según su rol y tipo de documento.
- Manejo de tipos de documentos manualmente firmados y automáticamente firmados.
- Control de secuencia de emisión de documentos para Solicitudes y Resoluciones.
- Almacenamiento encriptado.
- Privacidad de información del Solicitante.
- Privacidad de información del Emisor.
- Temporalidad de disponibilidad de formularios abiertos.

3.6. Otros Requisitos

Opcionalmente mejorar el cumplimiento de los atributos de usabilidad y seguridad de manera medible y demostrable. Plazo de entrega 6 meses.

4. Apéndices

La principal herramienta de desarrollo es APEX.

El costo del producto es de \$14 436,40 USD.

No se disponen formatos de pantalla pero se sugiere simplificar la interfaz comparada con QUIPUX-UTN.

Atentamente,

Ing. Juan Carlos García

DIRECTOR DTI-UTN

SOLICITO CONFORME

Ing. Tobías López

OFERENTE

ACEPTO CONFORME

DOCUMENTO DE ARQUITECTURA v.0.2:

Software para gestión de servicios de mensajes de datos firmados en las dependencias de la UTN considerando su factibilidad de implementación.

HISTORIAL DE CAMBIOS

1. 28/04/18 Primera versión basada en ISO / IEC 29148, estilo arquitectural SOA y UML-2.0.
2. Corrección de estilo en las vistas, validación contra requerimientos y especificaciones técnicas de IAAS. Se incorporan los Frameworks del servicio de firma digital a la vista lógica. Se describe el caso de uso primario.

Tabla de contenido

HISTORIAL DE CAMBIOS	1
ALCANCE	2
Referencias	2
ARQUITECTURA DEL SOFTWARE	3
OBJETIVOS DE LA ARQUITECTURA Y RESTRICCIONES	14
ARQUITECTURA LÓGICA.....	15
ARQUITECTURA DE PROCESOS	16
ARQUITECTURA DE DESARROLLO	17
ARQUITECTURA FÍSICA	17
ESCENARIOS	18

TAMAÑO Y DESEMPEÑO	20
Apéndices	20
A. Acrónimos y abreviaciones.....	20
B. Definiciones	21
C. Principios de diseño	21

No se encuentran elementos de tabla de ilustraciones.

ALCANCE

Propuesta de Arquitectura basada en: Especificación de Requisitos para el desarrollo del Software de gestión de trámites institucionales de la Universidad Técnica del Norte según el estándar de ISO/IEC 29148 (López Ruiz & García Pinchao, 2016)

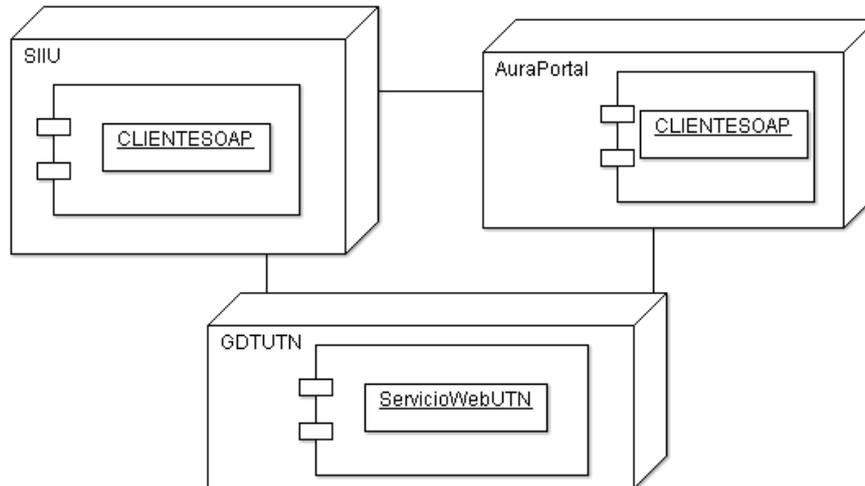
Referencias

López Ruiz, T. R., & García Pinchao, J. C. (26 de octubre de 2016). *TEISISTEMAS*.

Obtenido de TEISISTEMAS: <https://teisistemas.dyndns.org/tesismsc/ISO29148.pdf>

ARQUITECTURA DEL SOFTWARE

DIAGRAMA DE CONTEXTO



OBJETIVOS DEL NEGOCIO

ID	DESCRIPCIÓN DEL OBJETIVO DEL NEGOCIO
ON-1	Implementar en el ERP institucional los procesos de gestión de Trámites
ON-2	Desarrollar o adquirir una solución para Gestión de 11 procesos institucionales
ON-3	Automatizar la emisión de documentos firmados digitalmente con validez legal
ON-4	Implementar un repositorio de firmas digitales almacenadas en el SIIU de la UTN

ON-5	Recibir la solución de servicios de firma electrónica propuesta por el Maestrante
------	--

COMENTARIOS: CUMPLIR EL ON-2 ES RESPONSABILIDAD DE AURA PORTAL
NO DEL MAESTRANTE.

CARACTERÍSTICAS DEL SISTEMA

ID	DESCRIPCIÓN	PRIORIDAD	OBJETIVO DEL NEGOCIO ASOCIADO
C-1	El Solicitante debe estar autenticado en el sistema y demostrar que no es un robot.	ALTA	ON-3
C-2	El sistema debe mostrar al Solicitante el catálogo de tipos de documentos que puede solicitar.	ALTA	ON-3
C-3	El sistema debe emitir el mensaje indicando que el documento fue enviado para su correspondiente revisión por el Emisor del documento firmado, agradece al	MEDIA	ON-3

	Solicitante y le invita a esperar en la bandeja de entrada la llegada de una respuesta a su solicitud.		
C-4	El sistema debe mostrar al Solicitante un cuadro de dialogo para seleccionar la siguiente acción	BAJA	ON-3
C-5	El Emisor debe estar autenticado en el sistema y demostrar que no es un robot	ALTA	ON-3
C-6	El sistema debe mostrar al Emisor el catálogo de solicitudes de tipo manual en su bandeja de entrada.	ALTA	ON-3
C-7	El sistema debe procesar la decisión del Emisor: ACEPTAR, DENEGAR, COMENTAR y enviar al Solicitante el resultado.	ALTA	ON-3
C-8	El sistema debe firmar y emitir todas las resoluciones automáticas pendientes según las Solicitudes recibidas del Solicitante	ALTA	ON-3

C-9	Para cada resolución en la bandeja de llegada del solicitante, el sistema debe procesar: Mirar, Imprimir, Descartar, Archivar, Responder, Salir.	MEDIA	ON-3
C-10	El sistema debe cumplir la C-8 mediante el uso del repositorio de firmas digitales almacenadas en el SIIU de la UTN	ALTA	ON-4

ALCANCE

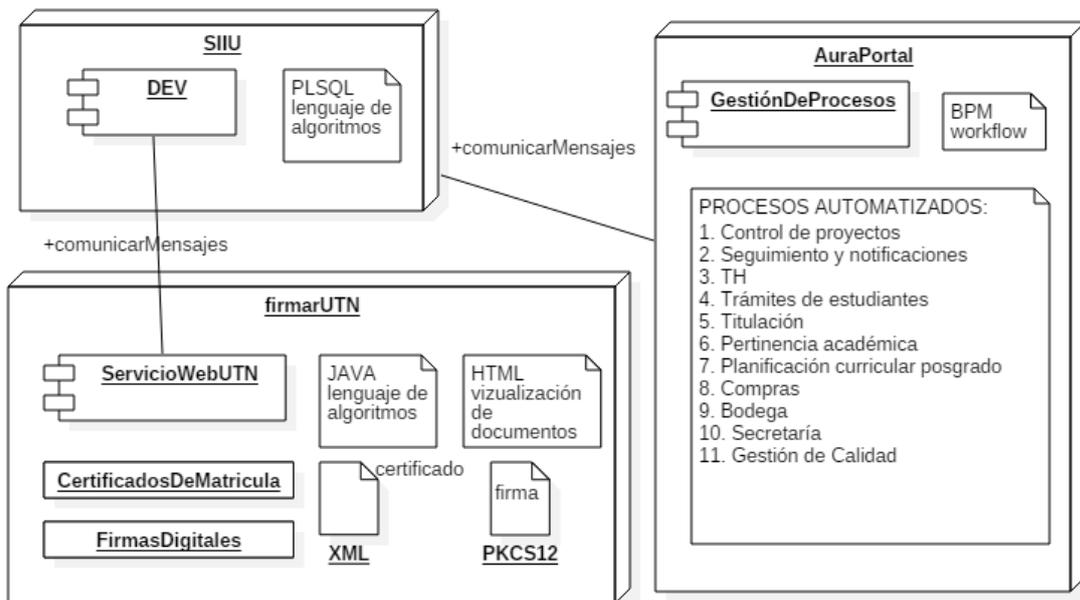
NÚMERO DE ENTREGA	TEMA PRINCIPAL	ID DE CARACTERÍSTICAS A INCLUIR
1.0	CRUD del repositorio de firmas digitales en el SIIU de la UTN	C-10
2.0	Formulario del Solicitante	C-1, C-2, C-3, C-4, C-8
3.0	Formulario del Emisor	C-5, C-6, C-7, C-9

INTERESADOS:

NOMBRE	DESCRIPCIÓN	RESPONSABILIDADES
JUAN CARLOS GARCÍA	DIRECTOR DDTI UTN	<p>Aprobar la visión y alcance del sistema</p> <p>Proporcionar acceso a la DDTI y servidores del SIIU</p> <p>Aprobar entrega del proyecto</p>
TOBIAS LÓPEZ	LÍDER DE PROYECTO	<p>Coordinar el proyecto y documentarlo con el equipo de desarrollo</p> <p>Entregar el proyecto al Director DDTI UTN</p> <p>Evaluar los resultados obtenidos</p>
DIEGO TREJO	ASESOR	<p>Asesorar la documentación del proyecto para cumplimiento de estándares de calidad de software</p>
EFRÉN LÓPEZ	PRUEBAS DE DESARROLLO	<p>Probar especificaciones de componentes</p> <p>Documentar el proceso de pruebas de software</p>

DAYANARA ROSERO	REDACCIÓN TÉCNICA	Corrección de la ortografía, sintaxis y semántica del Lenguaje utilizado
-----------------	-------------------	--

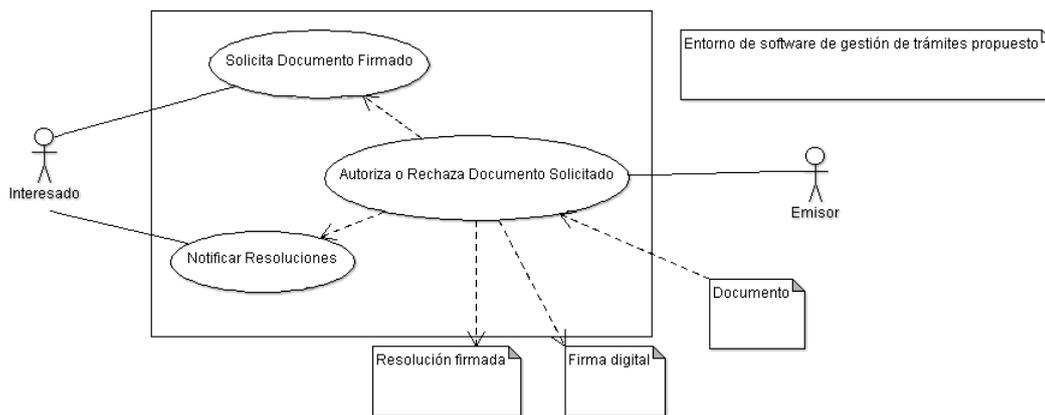
VISTA LÓGICA



- SIIU. Sistema de Información Integral Universitaria
- DEV. Conjunto de objetos de la base de datos Oracle (11g, XE, 12c). Contiene procedimientos almacenados para operaciones de CRUD sobre los datos almacenados (parámetros,certificados,documentos,firmasdigitales).
- PLSQL. Lenguaje de programación de Oracle.
- FirmarUTN Servicio web de firma electrónica y su validación
- ServicioWebUTN Servido web orientado a SOAP
- JAVA. Lenguaje de programación y desarrollo XML

- HTML Lenguaje de Hivervínculos para presentaciones Web
- XML Formato de intercambio de mensajes
- PKCS12 Formato de almacenamiento de firma digital
- AuraPortal Portal para gestión documental de todos los procesos de la UTN
- BPM Lenguaje de modelado orientado a procesos
- Gestión de Procesos Todos los Workflows o flujos de trabajo documental especificados en la lista de procesos automatizados.

CASOS DE USO



ID	DESCRIPCIÓN	CARACTERÍSTICA ASOCIADA
CU-01: solicita documento firmado	Permite solicitar al interesado un certificado del catálogo de documentos disponibles	C-1, C-2, C-3, C-4

CU-02: Autoriza o Rechaza documento solicitado	Permite firmar al emisor los documentos disponibles y emitir la resolución firmada para notificar al interesado	C-5, C-6, C-7, C-8, C-10
CU-03: Notificar resoluciones	Devuelve cualquier resolución tomada en forma manual o automática al interesado	C-9

ELECCIÓN DEL CASO DE USO PRIMARIO:

ID	CRITERIOS DE ELECCIÓN
CU-02	La firma digital de documentos es la razón primaria de ser de este sistema en el entorno de gestión de trámites institucionales de la UTN (ON-3, ON-4)

ATRIBUTOS DE CALIDAD:

Mapeo de Criterios de aplicación de los atributos indicados en la ISO / IEC 9126-3:

ID	9126	Atributos	Escenarios	Prioridad
EAC-1	6.1 Funcionalidad	1. Adecuación 2. Seguridad 3. Exactitud 4. Interoperabilidad	N/A E6.1.2 E6.1.3 E6.1.4	ALTA ALTA ALTA

		5. Conformidad	N/A	
EAC-2	6.2 Confiabilidad	1. Madurez 2. Tolerancia a errores 3. Recuperabilidad	N/A N/A N/A	
EAC-3	6.3 Usabilidad	1. Entendimiento 2. Aprendizaje 3. Operabilidad 4. Atracción 5. Conformidad	E6.3.1 E6.3.2 E6.3.3 E6.3.4 E6.3.5	ALTA ALTA ALTA ALTA ALTA
EAC-4	6.4 Eficiencia	1. Comportamiento de tiempos 2. Utilización de recursos 3. Conformidad	E6.4.1 E6.4.2 E6.4.3	BAJA BAJA MEDIA
EAC-5	6.5 Mantenibilidad	1. Capacidad de ser analizado 2. Cambialidad 3. Facilidad de prueba 4. Estabilidad 5. Conformidad	N/A N/A N/A N/A N/A	
EAC-6	6.6 Portabilidad	1. Adaptabilidad 2. Facilidad de instalación 3. Coexistencia 4. Remplazabilidad	N/A N/A E6.6.3 N/A	MEDIA ALTA

		5. Conformidad	E6.6.5	MEDIA
EAC-7	CALIDAD EN USO	1. ¿El software tiene niveles de Riesgo que causan daño al usuario final?	E7.1	ALTA

<p>N/A</p> <p>E6.1.2 Integridad, confidencialidad y no repudio SOAP</p> <p>E6.1.3 ingresa XML y sale XML firmado con X.509; se usa la firma electrónica autorizada BCE.</p> <p>E6.1.4 el servicio de firma implementado en Glassfish4 interactua con el SIIU en Oracle12c</p> <p>N/A</p>				
<p>N/A</p> <p>N/A</p> <p>N/A</p>				
<p>E6.3.1 es fácil de entender y reconocer la estructura y lógica de su aplicabilidad</p> <p>E6.3.2 es fácil de aprender a usar</p> <p>E6.3.3 es fácil de operar y controlar</p> <p>E6.3.4 es atractivo el diseño del software</p> <p>E6.3.5 esta el usuario conforme con el diseño y uso del producto</p>				
<p>E6.4.1 cual es el tiempo de respuesta del servicio de firma digital y cual el de entrega de certificados firmados</p>				

<p>E6.4.2 cual es el consumo de recursos del servicio que tamaño en bytes consume el ancho de banda, la firma, la memoria de firmado, la base de datos</p> <p>E6.4.3 los resultados obtenidos satisfacen las expectativas esperadas</p>
<p>N/A</p> <p>N/A</p> <p>N/A</p> <p>N/A</p> <p>N/A</p>
<p>N/A</p> <p>N/A</p> <p>E6.6.3 Coexistencia con otras aplicaciones del SIIU</p> <p>N/A</p> <p>E6.6.5 Esta conforme con la implementación en la DDTI</p>
<p>E7.1 Cumplimiento del Habeas Data: El repositorio de firmas digitales satisface las condiciones establecidas por la Constitución y las Leyes ecuatorianas.</p>

CRITERIOS RECOMENDADOS PARA EVALUAR LA CALIDAD:

TIPO DE SOFTWARE	CATEGORÍA	ORDEN DEL CRITERIO DE EVALUACIÓN	EVALUADORES

ADMINISTRATIVO	GESTIÓN DOCUMENTAL	<ol style="list-style-type: none"> 1. Tiempo de respuesta 2. Seguridad 3. Exactitud de la información 4. Recuperabilidad 	Personal de sistemas, administrativo, auxiliar, digitador
----------------	-----------------------	--	---

OBJETIVOS DE LA ARQUITECTURA Y RESTRICCIONES

OA1-OE1: Satisfacer los requerimientos de software para gestión de servicios de mensajes de datos firmados en la UTN

OA2-OE1: Proveer una función para firmar mensajes en formato XML y otra para dar validez como testigo de que un mensaje firmado consta en el repositorio de certificados digitales

OA3-OE2: No aplicable

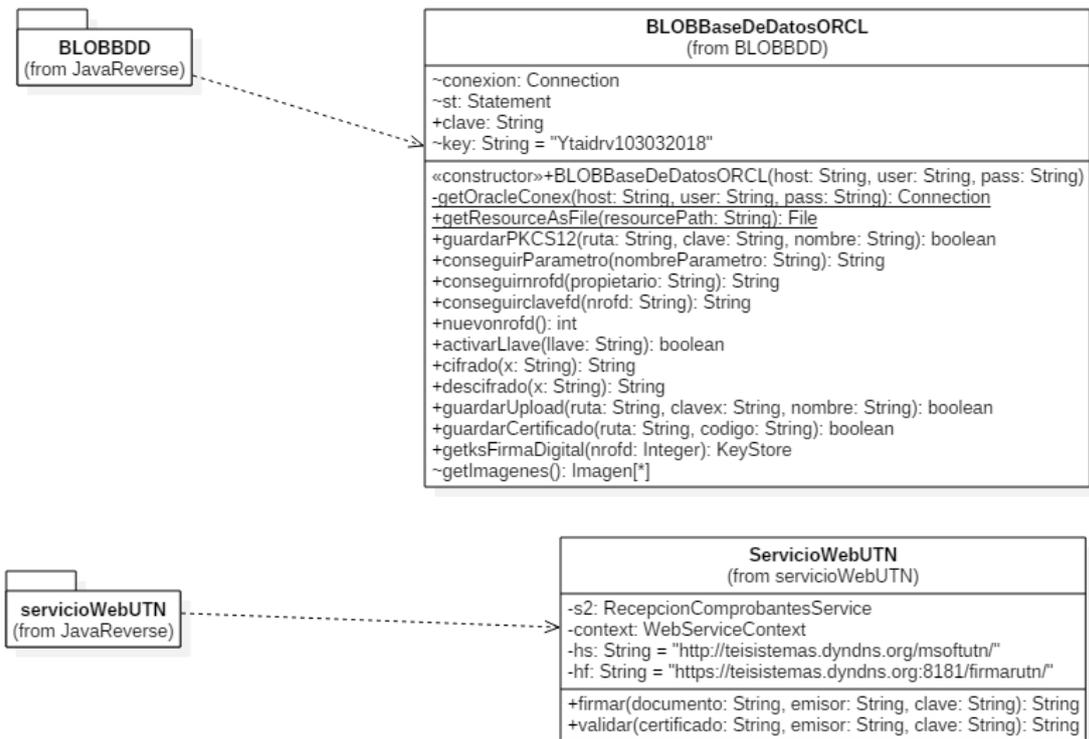
OA3-OE3: Apoyar la gestión de los certificados digitales firmados en las dependencias de la UTN

OA3-OE4: Considerar la factibilidad de implementación

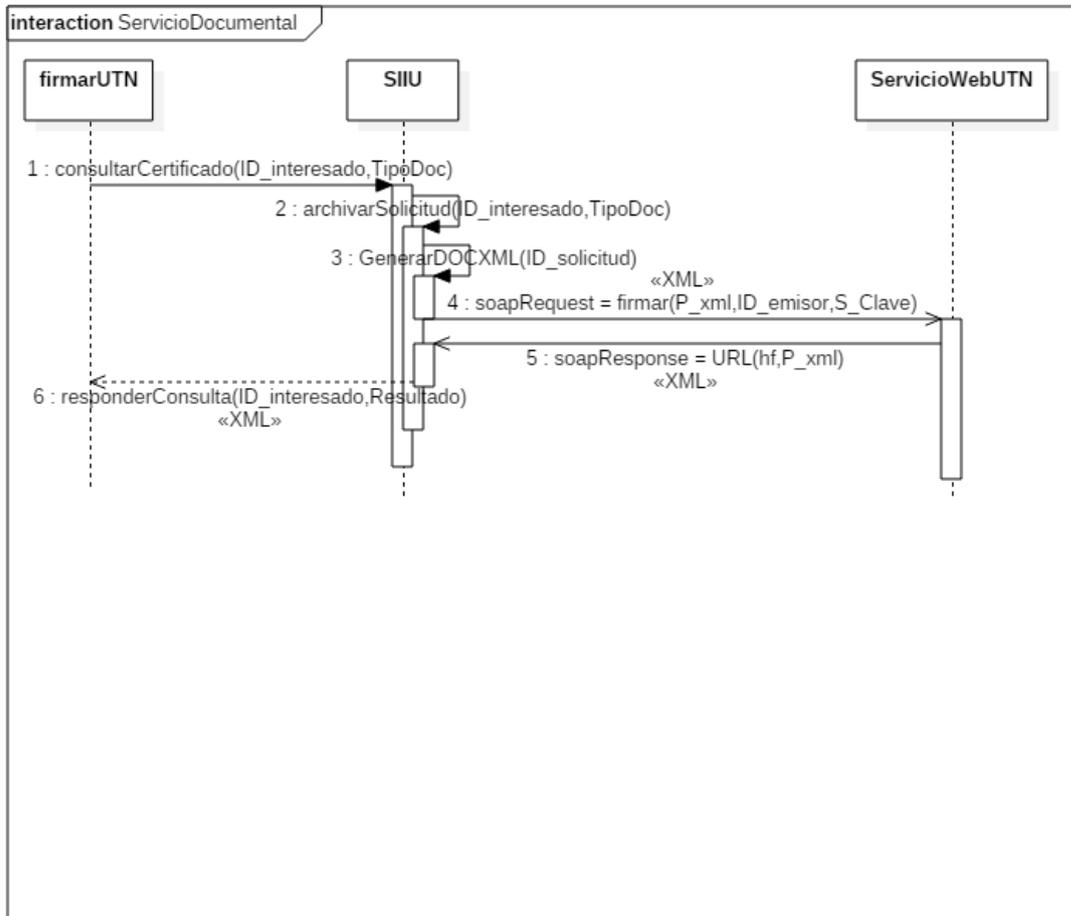
ALCANCE:

Proveer al SIIU de la UTN dos servicios básicos: firmar documentos XML y validar certificados XML almacenados en el repositorio del GDTUTN.

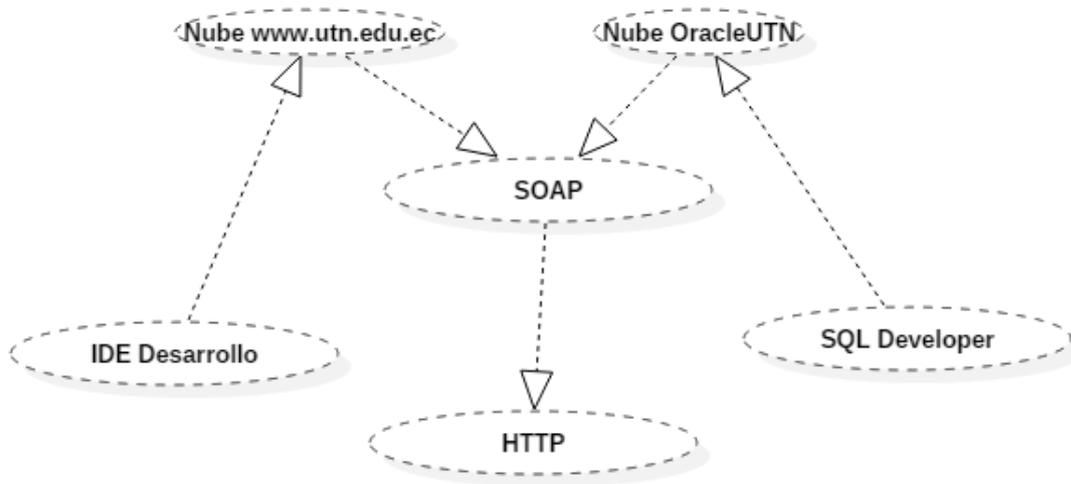
VISTA DE ARQUITECTURA LÓGICA



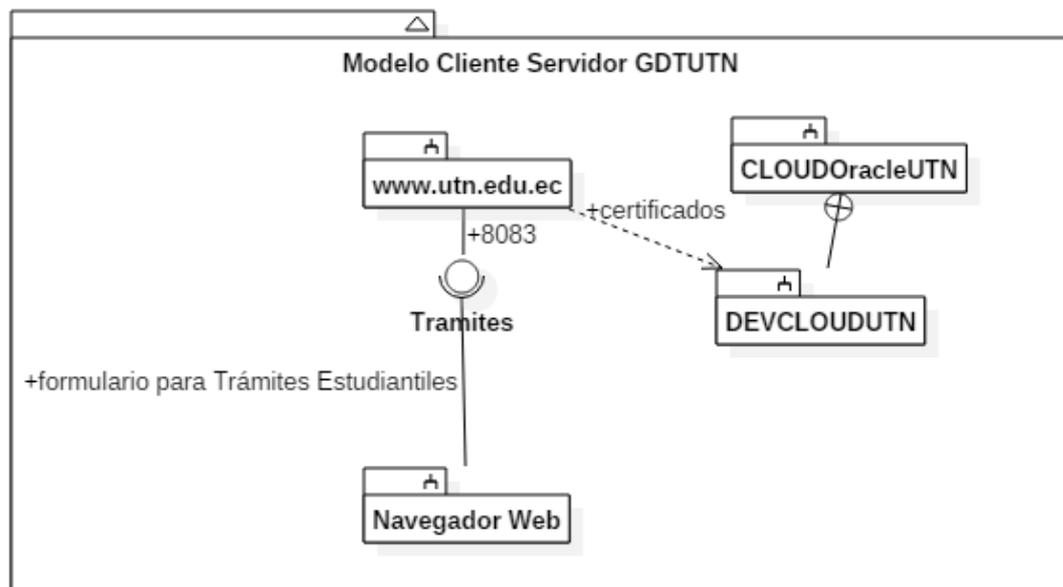
VISITA DE ARQUITECTURA DE PROCESOS



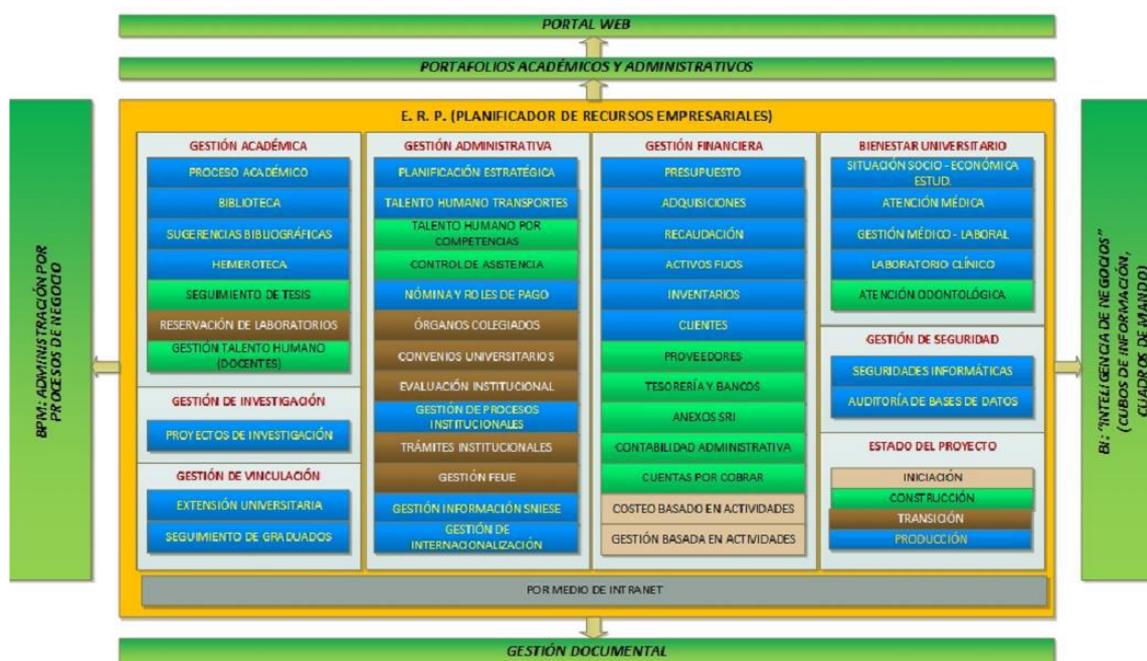
VISTA DE ARQUITECTURA DE DESARROLLO



VISTA DE ARQUITECTURA FÍSICA



ESCENARIOS:

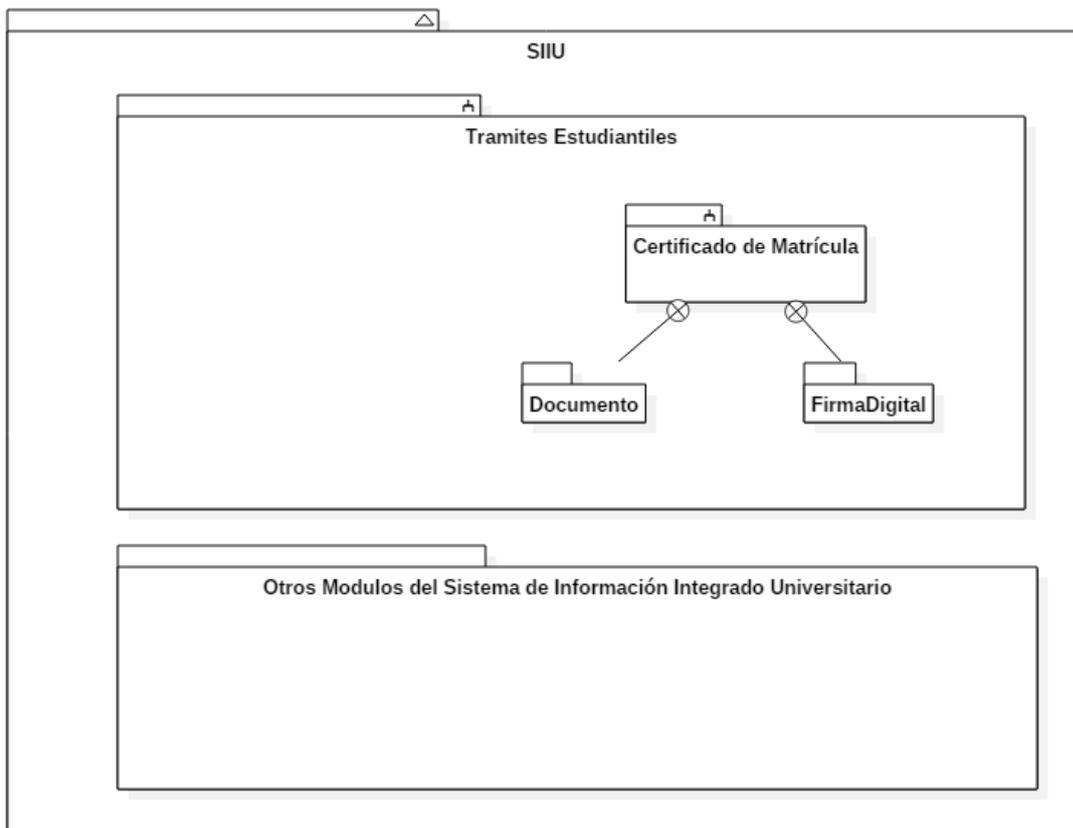


Sistema Integrado Universidad Técnica del Norte, Fuente: Dirección de Desarrollo Tecnológico de Informática.

Del proyecto de Trámites Institucionales, nacen dos proyectos: Software de Gestión de Procesos Institucionales que se implementa con Aura Portal (este capítulo sale de la responsabilidad del Autor); y, Servicios del repositorio de firmas digitales *ServicioWebUTN* aplicable para dar validez legal a la documentación generada por Terceros.

Entre los 11 procesos institucionales implementados en Aura Portal esta uno de Matriculación, al final de este proceso queda guardada la información de los estudiantes sobre su estado o situación legal como estudiante matriculado en la UTN.

Un caso específico de uso de esta Arquitectura aplicable es la EMISIÓN DE CERTIFICADOS DE MATRÍCULA AUTOMATIZADOS. Para este propósito, se adapta el sitio web de la UTN incorporando un servicio web soportado por Glassfish4 para implementar el sistema de *gestionDocumentalUTN* basado en la presente Arquitectura y que es de propósito demostrativo.



TAMAÑO Y DESEMPEÑO

El sistema deberá atender en forma normal un promedio de 18 solicitudes por minuto como mínimo en hora y día pico.

El servicio manual deberá responder un promedio de 15 solicitudes por hora en cada Emisor como mínimo en hora y día pico.

El número mínimo de usuarios conectados en paralelo debe ser de 5.

No hay un requerimiento sobre el número de transacciones por segundo inicialmente, pues esto depende de los primeros resultados de la investigación sobre las pruebas reales de carga.

No hay un límite sobre el número de terminales conectadas pero cada interfaz Web de cualquier usuario se considera una terminal, se espera atender la demanda simultánea en día y hora pico desde 8500 usuarios solicitantes.

El número promedio esperado de solicitudes anuales atendidas es de 850000 es decir un promedio de 2 solicitudes por minuto continuamente.

Apéndices

- A. Acrónimos y abreviaciones
- B. GDTUTN.- Gestión de Trámites institucionales de la Universidad Técnica del Norte.
- C. UTN.- Universidad Técnica del Norte.

- D. ERP-UTN.- Sistema de gestión de recursos de la UTN.
- E. PDF.- Es un formato de almacenamiento para documentos digitales independiente de plataformas de software o hardware. Este formato es de tipo compuesto (imagen vectorial, mapa de bits y texto).
- F. XML.- Es una adaptación del SGML (Standard Generalized Markup Language), un lenguaje que permite la organización y el etiquetado de documentos. Esto quiere decir que el XML no es un lenguaje en sí mismo, sino un sistema que permite definir lenguajes de acuerdo a las necesidades.
- G. HTML.- Es un lenguaje de programación que se utiliza para el desarrollo de páginas de Internet. Se trata de la sigla que corresponde a HyperText Markup Language, es decir, Lenguaje de Marcas de Hipertexto, que podría ser traducido como Lenguaje de Formato de Documentos para Hipertexto.
- H. HTTPS.- Son las siglas en inglés de HiperText Transfer Protocol (en español, protocolo de transferencia de hipertexto). Es un protocolo de red (un protocolo se puede definir como un conjunto de reglas a seguir) que se utiliza para publicar páginas de web o HTML.

I. Definiciones

SOA Arquitectura Orientada a Servicios (no es una tecnología en particular) pero se depende de varios protocolos para implementarla entre ellos HTTP, HTTPS, SOAP, JDBC y estructuras de intercambio de mensajes XML, X.509, HTML.

J. Principios de diseño

1. Para ser implementado en los servidores de la UTN
2. Compatible con el SIIU

3. Ergonomía de usuario
4. Seguridad de acceso al servicio.

Servicio Web

```
package servicioWeb;

import es.mityc.javasign.xades.examples.signformats.XAdESBESSignature;
import es.mityc.javasign.xades.examples.validations.CompleteValidation;
import java.io.File;
import java.io.IOException;
import java.io.InputStream;
import java.net.URL;
import javax.jws.WebService;
import javax.jws.WebMethod;
import javax.jws.WebParam;

import javax.annotation.Resource;
import javax.servlet.ServletContext;
import javax.xml.ws.WebServiceContext;
import javax.xml.ws.handler.MessageContext;
import javax.xml.ws.WebServiceRef;
import wcsriRC.RecepcionComprobantesService;

@WebService(serviceName = "ServicioWeb")
public class ServicioWeb {
    @WebServiceRef
    private RecepcionComprobantesService s2;

    @Resource
    private WebServiceContext context;

    private final String hs="http://localhost/msoftutn/";
    private final String hf="https://localhost:8181/";

    /**
     * Web service operation
     * @param documento
     * @return
     */
}
```

```

* @throws java.lang.InterruptedExcepcion
*/
@WebMethod(operationName = "firmar")

public String firmar(@WebParam(name = "documento") String documento)
    throws Exception {
//TODO write your implementation code here:
String xmlf;
byte [] xml;
String salida="SIN_RESPUESTA";
String numeroAutorizacion="";
final String TMP_DIR_PATH = "/carpetasUTN"; // esto forma parte de tu
    estructura de directorios del WAR
/* ServletContext context=null;
String realPath = context.getRealPath(TMP_DIR_PATH);*/
ServletContext servletContext =(ServletContext) context.
    getMessageContext().get(MessageContext.SERVLET_CONTEXT);
String realPath = servletContext.getRealPath(TMP_DIR_PATH);
XAdESBESSignature signature;
signature = new XAdESBESSignature();
//signature.saveDocumentToFile(documento, "/examples/documentoCli.xml");
signature.setSignatureFileName("f"+documento, hs+"carpetasUTN/PRUEBAS/
    documentos/"+documento);
int respuesta;
respuesta = signature.execute();
try{
XAdESBESSignature.copyFile_Java7(signature.miDir.getCanonicalPath()+File
    .separatorChar+"f"+documento, realPath+File.separatorChar+"f"+
    documento); // "C:/Users/MINEDUC/Documents/NetBeansProjects/wsSisfac/
    build/web/soapUTN/"+signature.ruta);
} catch (IOException e){
System.out.println(e.toString());
}
if(respuesta==0){
System.out.println("Recuperando_documento_firmado.." +realPath+File.
    separatorChar+"f"+documento);
salida=hf+"carpetasUTN/f"+documento;
if("RECIBIDA".equals(salida) || "DEVUELTA".equals(salida)){
return hf+"carpetasUTN/f"+documento;

```

```

}else{
return salida;
}
}
else{
return "RECHAZADO";
}
}

/**
 * Web service operation
 * * @param certificado
 * @return
 * @throws java.lang.InterruptedExpection
 */
@WebMethod(operationName = "validar")
public String validar(@WebParam(name = "certificado") String certificado
    ) throws Exception {
String xmlf;
byte [] xml;
String salida="SIN_RESPUESTA";
String numeroAutorizacion="";
final String TMP_DIR_PATH = "/carpetasUTN"; // esto forma parte de tu
    estructura de directorios del WAR
/* ServletContext context=null;
String realPath = context.getRealPath(TMP_DIR_PATH);*/
ServletContext servletContext =(ServletContext) context.
    getMessageContext().get(MessageContext.SERVLET_CONTEXT);
String realPath = servletContext.getRealPath(TMP_DIR_PATH);
CompleteValidation validador=new CompleteValidation();
//InputStream input = new URL(hf+"carpetasUTN/f"+certificado).openStream
    ();
XAdESBESSignature signature;
signature = new XAdESBESSignature();
Boolean resultado;
//resultado = signature.verificar(hs+"carpetasUTN/PRUEBAS/documentos/"+
    certificado);
resultado = signature.verificar(certificado);

```

```

//TODO write your implementation code here:
if(resultado)
return "ACEPTADO";
else
return "RECHAZADO";
}

}

```

UN MODELO DE DOCUMENTO XML EN FORMATO COMPATIBLE PARA X.509 GENERADO MEDIANTE STORE PROCEDURE EN PL/SQL DE ORACLE APPLICATION EXPRESS

```

create or replace procedure      p2 is
begin
insert into documentos values(sec_doc.nextval ,(SELECT  concat('<?xml_
      version="1.0" _encoding="UTF-8"?>' ,XMLAGG (
XMLELEMENT("documento",
XMLATTRIBUTES(a.id AS "id",a.version as "version"),
XMLFOREST((SELECT XMLAGG(XMLELEMENT("registro", XMLFOREST(c.id ,c.
      contenido ,c.fecha )))FROM  contenidos c) "lista_docs")
)
)
)AS "atributo" FROM  atributos a));

end p2;

```

UN MODELO PARA CONSUMIR EL SERVICIO WEB DE FIRMA ELECTRÓNICA USANDO PL/SQL ORACLE

```

create or replace procedure                               clienteSOAP(P_xml in
    varchar2) is

soap_request varchar2(30000);
soap_respond varchar2(30000);
http_req utl_http.req;
http_resp utl_http.resp;
resp XMLType;
i integer;

begin
soap_request:= '<?xml version="1.0" encoding="UTF-8"?><S:Envelope xmlns:
    S="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-ENV="http://
    schemas.xmlsoap.org/soap/envelope/">
<SOAP-ENV:Header/>
<S:Body>
<ns2:firmar xmlns:ns2="http://servicioWeb/">
<documento>' || P_xml || '.XML</documento>
</ns2:firmar>
</S:Body>
</S:Envelope>
';
http_req:= utl_http.begin_request
( 'http://localhost:8083/ServicioWeb'
, 'POST'
, 'HTTP/1.1'
);
utl_http.set_header(http_req, 'Content-Type', 'text/xml'); -- since we
    are dealing with plain text in XML documents
utl_http.set_header(http_req, 'Content-Length', length(soap_request));
utl_http.set_header(http_req, 'SOAPAction', ''); -- required to specify
    this is a SOAP communication
utl_http.write_text(http_req, soap_request);
http_resp:= utl_http.get_response(http_req);
utl_http.read_text(http_resp, soap_respond);
utl_http.end_response(http_resp);
resp:= XMLType.createXML(soap_respond);
resp:= resp.extract('/soap:Envelope/soap:Body/child::node()'
, 'xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"'

```

```

);
i:=0;
loop
dbms_output.put_line(substr(soap_respond,1+ i*255,250));
i:= i+1;
if i*250> length(soap_respond)
then
exit;
end if;
end loop;
end;

```

LIBRERIA ALGORITMOS PARA MANEJO DEL REPOSITORIO DE FIRMAS DIGITALES

```

/*
* LIBRERIA PARA EL MANEJO DEL REPOSITORIO DE FIRMAS DIGITALES
* AUTOR: ING. TOBIAS LOPEZ
* ENTREGADO A UNIVERSIDAD TECNICA DEL NORTE
* LICENCIA: LIBRE
*/
package BLOBBDD;

import BDDImagen.Imagen;
import es.mityc.javasign.issues.PassStoreKS;
import es.mityc.javasign.pkstore.keystore.KSStore;
import java.awt.image.BufferedImage;
import java.io.ByteArrayInputStream;
import java.io.File;
import java.io.FileInputStream;
import java.io.FileOutputStream;
import java.io.IOException;
import java.io.InputStream;
import static java.lang.Boolean.FALSE;
import static java.lang.Boolean.TRUE;
import java.nio.charset.StandardCharsets;
import java.security.InvalidKeyException;

```

```

import java . security . Key ;
import java . security . KeyStore ;
import java . security . KeyStoreException ;
import java . security . NoSuchAlgorithmException ;
import java . security . cert . CertificateException ;
import java . security . spec . InvalidKeySpecException ;
import java . security . spec . KeySpec ;
import java . sql . Blob ;
import java . sql . Clob ;
import java . sql . Connection ;
import java . sql . DriverManager ;
import java . sql . PreparedStatement ;
import java . sql . ResultSet ;
import java . sql . SQLException ;
import java . sql . Statement ;
import java . util . ArrayList ;
import java . util . Calendar ;
import java . util . logging . Level ;
import java . util . logging . Logger ;
import javax . crypto . BadPaddingException ;
import javax . crypto . Cipher ;
import javax . crypto . IllegalBlockSizeException ;
import javax . crypto . NoSuchPaddingException ;
import javax . crypto . SecretKey ;
import javax . crypto . SecretKeyFactory ;
import javax . crypto . spec . PBEKeySpec ;
import javax . crypto . spec . SecretKeySpec ;
import javax . imageio . ImageIO ;
import org . apache . commons . io . IOUtils ;

/**
 *
 * author TOBIAS LOPEZ
 */
public class BLOBBaseDeDatosORCL {
    Connection conexion ;
    Statement st ;
    public String clave ;
    String key="Ytaidrv103032018";

```

```

public BLOBBaseDeDatosORCL(String host, String user, String pass) throws
    SQLException{
try {
conexion = getOracleConex(host, user, pass);
st = conexion.createStatement();
} catch (SQLException ex) {
Logger.getLogger(BLOBBaseDeDatos.class.getName()).log(Level.SEVERE, null
    , ex);
}
}

private static Connection getOracleConex(String host, String user, String
    pass) throws SQLException{
//Registramos el driver odbc
DriverManager.registerDriver (new oracle.jdbc.driver.OracleDriver());
String rutaOracle=host;
//Creamos la conexion
Connection conn = DriverManager.getConnection(rutaOracle, user, pass);
//          driver          @machineName:port:SID, userid, password

//Devolvemos el statement sobre el que realizaremos consultas a la base
    de datos
return conn;
}

public static File getResourceAsFile(String resourcePath) {
try {
InputStream in = ClassLoader.getSystemClassLoader().getResourceAsStream(
    resourcePath);
if (in == null) {
return null;
}

File tempFile = File.createTempFile( String.valueOf(in.hashCode()), ".tmp
    ");
tempFile.deleteOnExit();
//System.out.println(tempFile.getCanonicalPath().toString());

try{
FileOutputStream out = new FileOutputStream(tempFile);

```

```

//copy stream
byte [] buffer = new byte [1024];
int bytesRead;
while ((bytesRead = in.read(buffer)) != -1) {
out.write(buffer , 0, bytesRead);
}
} catch (Exception ex) {
//ex.printStackTrace();
System.out.println(tempFile.getCanonicalPath().toString());
}
return tempFile;
} catch (IOException e) {
e.printStackTrace();
return null;
}
}

public boolean guardarPKCS12(String ruta ,String clave ,String nombre)
throws SQLException{
activarLlave(key);
String insert = "insert_into_dev.firmasdigitales_(nrofd ,contenidofd ,
clave , propietario , actualizado)_values (?, ?, ?, ?, ?)";
//FileInputStream fis = null;
PreparedStatement ps = null;
File file=null;
Calendar calendar = Calendar.getInstance();
java.sql.Date startDate = new java.sql.Date(calendar.getTime().getTime()
);

try {
conexion.setAutoCommit(false);
ps = conexion.prepareStatement(insert);
file=new File(this.getClass().getResource(ruta).getFile().toString());
ps.setInt(1, 0);
ps.setBinaryStream(2, this.getClass().getResourceAsStream(ruta) ,(int) file
.length());
clave=cifrado(clave);
ps.setString(3, clave);
ps.setString(4, this.getClass().getResource(ruta).getFile().toString());
ps.setDate(5, startDate);

```

```

ps.executeUpdate();
conexion.commit();
return true;
} catch (Exception ex) {
Logger.getLogger(BLOBBaseDeDatos.class.getName()).log(Level.SEVERE, null
, ex);
System.out.println(this.getClass().getResource(ruta));
System.out.println(this.getClass().getResource(ruta).getFile().toString
());
System.out.println(insert);
/*System.out.println(file.getAbsolutePath().toString());
System.out.println(file.getCanonicalPath().toString());*/

}finally{
try {
ps.close();
//fis.close();
} catch (Exception ex) {
Logger.getLogger(BLOBBaseDeDatos.class.getName()).log(Level.SEVERE, null
, ex);
}
}
return false;
}

public String conseguirParametro(String nombreParametro) throws
SQLException{
String resultado=null;
Statement s = conexion.createStatement();
ResultSet rs = s.executeQuery ("select _*_ from _dev.parametros _where _
nombreParametro='"+nombreParametro+"'");
while (rs.next())
{
System.out.println (rs.getInt (1) + " " + rs.getString (2)+ " " + rs.
getString(3));
resultado=rs.getString(3);
}
return resultado;
}

```

```

}
public String conseguirnrofd(String propietario) throws SQLException{
String resultado=null;
Statement s = conexion.createStatement();
ResultSet rs = s.executeQuery ("select nrofd from dev.firmasdigitales
where propietario='"+propietario+"'");
while (rs.next())
{
System.out.println (rs.getInt (1));
resultado=rs.getString(1);
}
return resultado;
}
public String conseguirclavefd(String nrofd) throws SQLException ,
IllegalBlockSizeException , BadPaddingException ,
NoSuchAlgorithmException , NoSuchPaddingException , InvalidKeyException
{
String resultado=null;
activarLlave(key);
Statement s = conexion.createStatement();
String sql="select clave from dev.firmasdigitales where nrofd="+nrofd;
//System.out.println (sql);
ResultSet rs = s.executeQuery (sql);
//String key = "Ytaidrv103032018"; // 128 bit key

// Create key and cipher
/*Key aesKey = new SecretKeySpec(key.getBytes(), "AES");
Cipher cipher = Cipher.getInstance("AES");

cipher.init(Cipher.DECRYPT_MODE, aesKey);*/
String decrypted;
while (rs.next())
{
System.out.println (rs.getString (1));
resultado=rs.getString(1);
/*decrypted = new String(cipher.doFinal(resultado.getBytes()));*/
decrypted=descifrado(resultado);
System.out.println("Decrypted:_" + decrypted);
resultado=decrypted;
}
}

```

```

//resultado=rs.getString(1);
}
//resultado=rs.getString(1);
return resultado;
}
public int nuevonrofd() throws SQLException{
int resultado=-1;
Statement s = conexion.createStatement();
ResultSet rs = s.executeQuery ("select dev.nrofd_seq.nextval as _
nuevonrofd_from_dual");
while (rs.next())
{
System.out.println (rs.getInt (1));
resultado=rs.getInt(1);
}
return resultado;
}
public boolean activarLlave(String llave) throws SQLException{
//int resultado=-1;
Statement s = conexion.createStatement();
try{
ResultSet rs = s.executeQuery ("execute sys.dbcrypt.setkey('+llave+');")
;
return TRUE;
} catch(SQLException e){
return FALSE;
}
}
public String cifrado(String x) throws SQLException{
String resultado="";
Statement s = conexion.createStatement();
activarLlave(key);
ResultSet rs = s.executeQuery ("select sys.dbcrypt.encrypt('" + x + "',
'+key+'') as _cifrado_from_dual");
while (rs.next())
{
System.out.println (rs.getString (1));
resultado=rs.getString(1);
}
}

```

```

return resultado;
}
public String descifrado(String x) throws SQLException{
String resultado="";
Statement s = conexion.createStatement();
activarLlave(key);
ResultSet rs = s.executeQuery ("select sys.dbcrypt.decrypt('"+ x + "', '
"+key+"') as descifrado from dual");
while (rs.next())
{
System.out.println (rs.getString (1));
resultado=rs.getString(1);
}
return resultado;
}
public boolean guardarUpload(String ruta ,String clavex ,String nombre)
throws NoSuchAlgorithmException , NoSuchPaddingException ,
InvalidKeyException , IllegalBlockSizeException , BadPaddingException ,
InvalidKeySpecException , SQLException{
activarLlave(key);
String insert = "insert into dev.firmasdigitales (nrofd ,contenidofd ,
clave ,propietario ,actualizado) values (?,?,?,?,?)";
FileInputStream fis = null;
PreparedStatement ps = null;
File file=null;
Calendar calendar = Calendar.getInstance();
java.sql.Date startDate = new java.sql.Date(calendar.getTime().getTime()
);

//ESTAS LINEAS NO SIRVEN EN CENTOS
/*Key aesKey = new SecretKeySpec(key.getBytes(), "AES");
Cipher cipher = Cipher.getInstance("AES");

// encrypt the text
cipher.init(Cipher.ENCRYPT_MODE, aesKey);
byte[] encrypted = cipher.doFinal(clavex.getBytes());
String clavexs;
clavexs = new String(encrypted);
System.out.println("Encrypted: " + new String(encrypted));*/

```

```

try {
conexion.setAutoCommit(false);
ps = conexion.prepareStatement(insert);
file=new File(ruta);
fis = new FileInputStream(file);
ps.setInt(1, nuevonrofd());
//String body = IOUtils.toString(fis, StandardCharsets.UTF_8.name());
Blob blob = conexion.createBlob();
byte[] datos = new byte[(int)file.length()];
int tf=fis.read(datos, 0, (int)file.length()-1);
//String texto=new String(datos);
blob.setBytes(1, datos);
ps.setBlob(2, blob);
//ps.setBinaryStream(2,fis,(int)file.length());
//ps.setClob(2,fis,(int)file.length());
String clavexs=cifrado(clavex);
//ps.setString(3, clavex);
ps.setString(3, clavexs);
ps.setString(4, nombre);
ps.setDate(5, startDate);

ps.executeUpdate();
conexion.commit();
return true;
} catch (Exception ex) {
Logger.getLogger(BLOBBaseDeDatos.class.getName()).log(Level.SEVERE, null
, ex);
System.out.println(this.getClass().getResource(ruta));
System.out.println(this.getClass().getResource(ruta).getFile().toString
());
System.out.println(insert);
/*System.out.println(file.getAbsolutePath().toString());
System.out.println(file.getCanonicalPath().toString());*/

} finally {
try {
ps.close();
//fis.close();
} catch (Exception ex) {

```

```

Logger.getLogger(BLOBBaseDeDatos.class.getName()).log(Level.SEVERE, null
    , ex);
}
}
return false;
}
public boolean guardarCertificado(String ruta,String codigo){
String insert = "insert_into_dev.certificados_(nrocertificado ,codigo ,
    certificado)_values(?,?,?)";
FileInputStream fis = null;
PreparedStatement ps = null;
File file=null;
//Calendar calendar = Calendar.getInstance();
//java.sql.Date startDate = new java.sql.Date(calendar.getTime().getTime
    ());
try {
conexion.setAutoCommit(false);
ps = conexion.prepareStatement(insert);
file=new File(ruta);
fis = new FileInputStream(file);
ps.setNull(1, java.sql.Types.INTEGER);
ps.setString(2, codigo);
ps.setBinaryStream(3, fis ,(int) file.length());
//ps.setString(4, nombre);
//ps.setDate(5, startDate);

ps.executeUpdate();
conexion.commit();
return true;
} catch (Exception ex) {
Logger.getLogger(BLOBBaseDeDatos.class.getName()).log(Level.SEVERE, null
    , ex);
System.out.println(this.getClass().getResource(ruta));
System.out.println(this.getClass().getResource(ruta).getFile().toString
    ());
System.out.println(insert);
/*System.out.println(file.getAbsolutePath().toString());
System.out.println(file.getCanonicalPath().toString());*/
}
}
}

```

```

}finally{
try {
ps.close();
//fis.close();
} catch (Exception ex) {
Logger.getLogger(BLOBBaseDeDatos.class.getName()).log(Level.SEVERE, null
, ex);
}
}
return false;
}
public KeyStore getksFirmaDigital(Integer nrofd) throws IOException,
SQLException, NoSuchAlgorithmException, CertificateException,
IllegalBlockSizeException, NoSuchPaddingException,
InvalidKeyException, BadPaddingException {
try {
KeyStore ks = KeyStore.getInstance("PKCS12");
activarLlave(key);
String cadSQL="SELECT _contenidofd ,clave ,propietario _FROM _dev .
firmasdigitales _WHERE _nrofd="+nrofd.toString();
ResultSet rs = st.executeQuery(cadSQL);

//String key = "Ytaidrv103032018"; // 128 bit key

// Create key and cipher
/* Key aesKey = new SecretKeySpec(key.getBytes(), "AES");
Cipher cipher = Cipher.getInstance("AES");

cipher.init(Cipher.DECRYPT_MODE, aesKey);
String decrypted;*/

//System.out.println(cadSQL);
while (rs.next())
{
//Blob blob = rs.getBlob("contenidofd");
Blob blob=rs.getBlob("contenidofd");
clave=rs.getString("clave");

```

```

/*          decrypted = new String(cipher.doFinal(clave.getBytes()
    ));*/
String decrypted = descifrado(clave);
System.out.println("Decrypted:_" + decrypted);
clave=decrypted;
String nombre = rs.getObject("propietario").toString();

byte[] data = blob.getBytes(1, (int)blob.length());
ks.load(new ByteArrayInputStream(data), clave.toCharArray());
return ks;
}
/*ks.load(this.getClass().getResourceAsStream(PKCS12_RESOURCE),
    PKCS12_PASSWORD.toCharArray());
storeManager = new KSSStore(ks, new PassStoreKS(PKCS12_PASSWORD));*/
} catch (KeyStoreException ex) {
System.err.println("No se puede generar KeyStore PKCS12");
ex.printStackTrace();
System.exit(-1);
} catch (NoSuchAlgorithmException ex) {
System.err.println("No se puede generar KeyStore PKCS12");
ex.printStackTrace();
System.exit(-1);
} catch (CertificateException ex) {
System.err.println("No se puede generar KeyStore PKCS12");
ex.printStackTrace();
System.exit(-1);
} catch (IOException ex) {
System.err.println("No se puede generar KeyStore PKCS12");
ex.printStackTrace();
System.exit(-1);
}
return null;
}
ArrayList< Imagen > getImagenes() throws IOException {
ArrayList< Imagen > lista = new ArrayList();
try {
activarLlave(key);
ResultSet rs = st.executeQuery("SELECT contenidofd , clave , propietario
FROM dev.firmasdigitales");

```

```

while (rs.next())
{
Imagen imagen=new Imagen();
Blob blob = rs.getBlob("contenidofd");
String nombre = rs.getObject("propietario").toString();
byte[] data = blob.getBytes(1, (int)blob.length());
BufferedImage img = null;
try {
img = ImageIO.read(new ByteArrayInputStream(data));
} catch (IOException ex) {
Logger.getLogger(BLOBBaseDeDatos.class.getName()).log(Level.SEVERE, null
, ex);
}

imagen.setImagen(img);
imagen.setNombre(nombre);
lista.add(imagen);
}
rs.close();
} catch (SQLException ex) {
Logger.getLogger(BLOBBaseDeDatos.class.getName()).log(Level.SEVERE, null
, ex);
}
return lista;
}
}

```



UNIVERSIDAD TÉCNICA DEL NORTE

Universidad Acreditada resolución 002-CONEA-2010-129-DC
Resolución No. 001-073-CEAACES-2013-13

DIRECCION DE DESARROLLO TECNOLÓGICO E INFORMÁTICO

CARTA DE ACEPTACION

DIRECCIÓN DE DESARROLLO TECNOLÓGICO E INFORMÁTICO

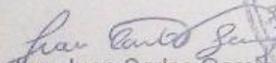
13 de octubre de 2017.

Magister
Jorge Caraguay Procel
DIRECTOR INSTITUTO DE POSGRADO UTN

De mi consideración:

Me permito informar a usted que el señor TOBIAS RAMIRO LÓPEZ RUIZ con número de cédula 1002176905, estudiante del Programa de Maestría en: Ingeniería de Software, han concluido de manera eficiente y satisfactoria el proyecto de investigación "INCIDENCIA DEL USO DEL REPOSITORIO DE FIRMAS DIGITALES EN LA GESTIÓN DE TRÁMITES INSTITUCIONALES DE LA UNIVERSIDAD TÉCNICA DEL NORTE" aplicado en la Dirección de Desarrollo Tecnológico e Informático de la UTN. Además debo informar que el sistema se encuentra implementado y funcionando correctamente.

Atentamente,


Ing. Juan Carlos García
DIRECTOR DDTI

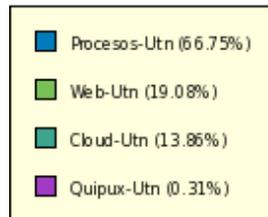
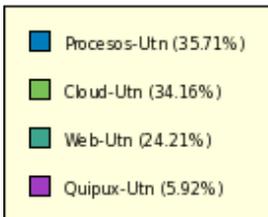
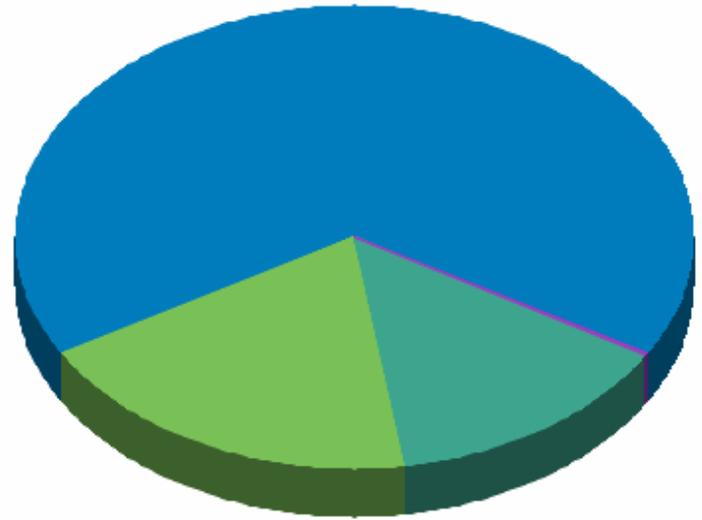
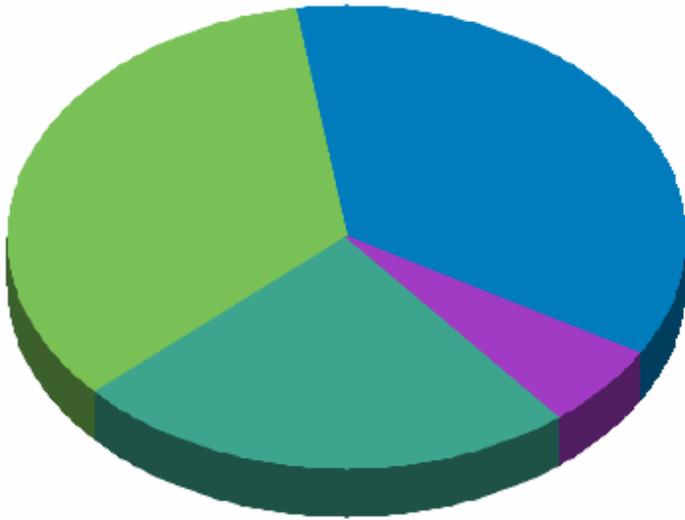


Visión Institucional

La Universidad Técnica del Norte en el año 2020, será un referente en ciencia, Tecnología e innovación en el país, con estándares de excelencia internacionales.

Top 8 Inbound Applications in Group UTN Services

Top 8 Outbound Applications in Group UTN Services



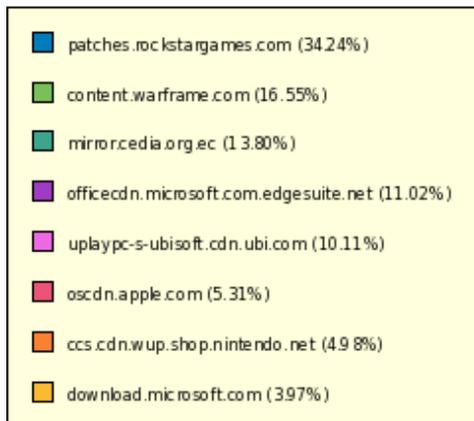
Top 8 Applications Represent 100.00% of 1918.71 MB

Top 8 Applications Represent 100.00% of 5920.04 MB

Top 45 Inbound Applications in Group UTN Services					
Name	Packets	Data (MB)	Throughput (kbps)		Flows
			Average	Max	
Procesos-Utn	2465113	685.244	43.47	308.28	1
Cloud-Utn	2586683	655.366	12.15	2365.71	57
Web-Utn	883800	464.546	43.23	2173.03	272
Quipux-Utn	114208	113.557	62.42	1552.76	44

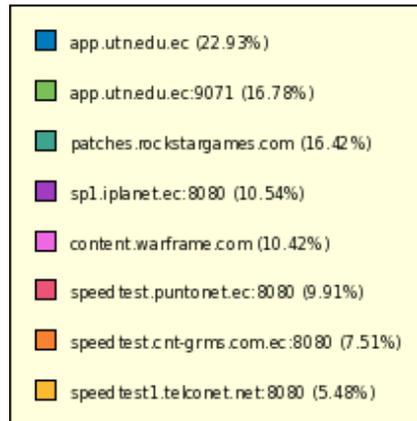
Top 45 Outbound Applications in Group UTN Services					
Name	Packets	Data (MB)	Throughput (kbps)		Flows
			Average	Max	
Procesos-Utn	3163859	3951.769	250.74	810.99	1
Web-Utn	1063467	1129.469	104.90	9594.59	272
Cloud-Utn	2839513	820.743	15.03	49.09	57
Quipux-Utn	67869	18.061	9.88	195.06	44

Top 8 Inbound URLs



Top 8 URLs Represent 39.86% of 595325.33 MB

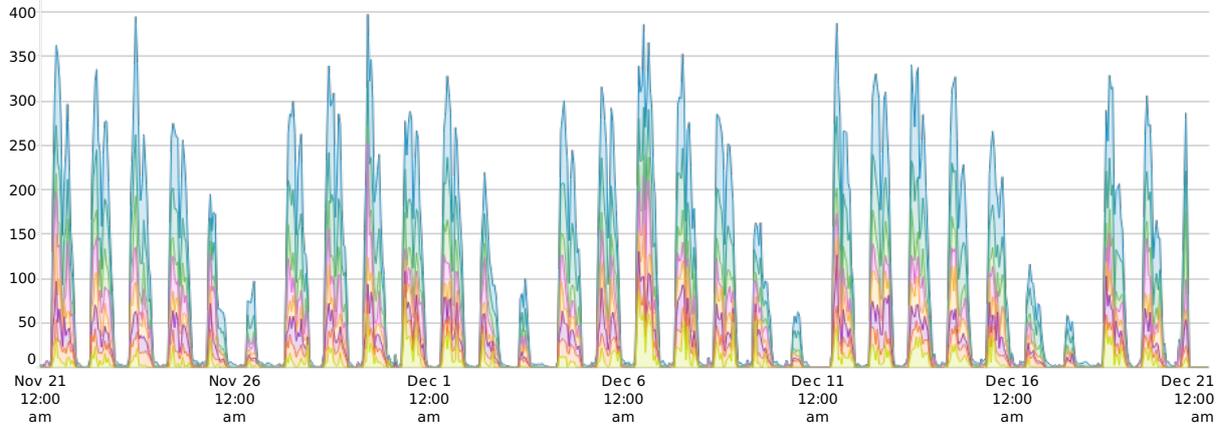
Top 8 Outbound URLs



Top 8 URLs Represent 58.12% of 25625.33 MB

Top 45 Inbound URLs					
Name	Packets	Data (MB)	Throughput (kbps)		Flows
			Average	Max	
patches.rockstargames.com	59490986	81252.124	29737.88	51403.39	1
content.warframe.com	31673115	39280.024	37787.24	66020.13	4
mirror.cedia.org.ec	23906023	32746.458	23478.39	42349.84	10
officecdn.microsoft.com.edgesuite.net	19109516	26156.893	4265.55	28248.05	195
uplaypc-s-ubisoft.cdn.ubi.com	17525466	23993.907	25413.57	48099.26	3
oscdn.apple.com	9206296	12595.670	11216.58	29390.42	3
ccs.cdn.wup.shop.nintendo.net	8632173	11825.335	38598.48	44847.56	2
download.microsoft.com	6890839	9431.391	13364.23	62496.76	4
droid11.gameloft.com	6786053	9302.500	12288.98	30652.58	4
download1271.mediafire.com	6661272	9133.493	11250.70	11547.07	1
mirror.epn.edu.ec	6592672	9038.408	13232.05	38201.64	4
osxapps.itunes.apple.com	6359887	8721.673	21455.34	16490.92	2
iosapps.itunes.apple.com	5947059	8150.479	9698.04	33943.96	20
app.utnedu.ec:9071	6828472	8085.319	559.38	9108.86	75
mirror.uta.edu.ec	4774544	6539.287	5179.94	8626.74	3
www58.uptobox.com	4553458	6244.519	10271.14	11858.21	1
download1495.mediafire.com	3710144	5086.456	4910.04	28636.80	2
download2128.mediafire.com	3693784	5064.913	8760.32	11308.65	3
download850.mediafire.com	3625965	4971.630	10073.68	12204.49	2
mirror.esepoch.edu.ec	3611252	4952.015	10570.10	8974.82	2
download782.mediafire.com	3476147	4766.705	8061.70	10830.26	1
mirror.nsc.liu.se	3321232	4554.610	12445.22	6341.08	1

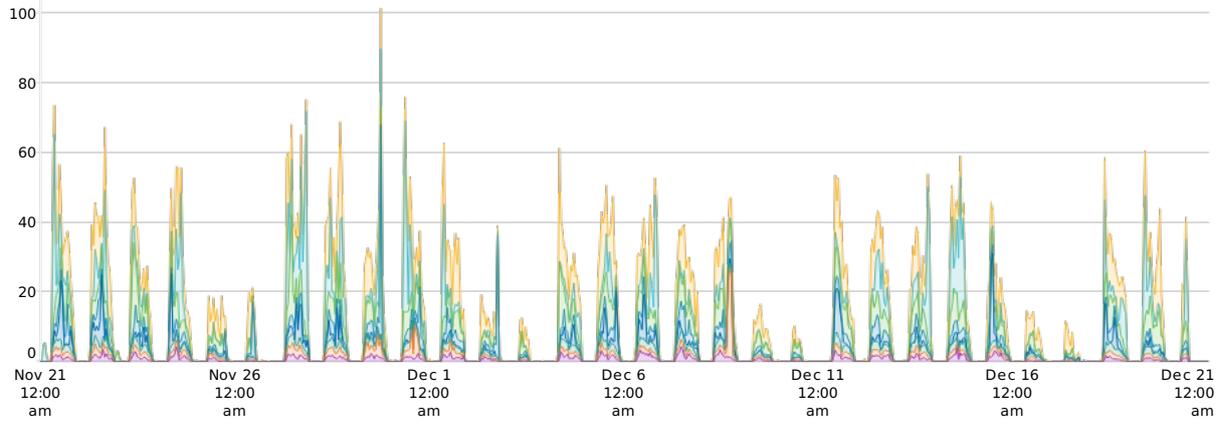
Throughput of Inbound Applications (Mbps)



Top Apps - Inbound (TB)

YouTube	8.906
Facebook File-transfer	6.347
HTTPS	2.934
Windows Updates	2.775
Google Shared Services	2.457
HTTP	2.393
Facebook Encrypted	1.937
Windows Store	1.838

Throughput of Outbound Applications (Mbps)



Top Apps - Outbound (GB)

Google Shared Services	1,385.691
Office365	858.386
HTTPS	783.789
YouTube	402.720
Skydrive	277.701
Facebook File-transfer	243.385
Facebook Encrypted	229.157
HTTP	184.059

Inbound Applications

Name	Total Volume	Avg Throughput
YouTube	8.906 TB	30.222 Mbps
Facebook File-transfer	6.347 TB	21.538 Mbps
HTTPS	2.934 TB	9.956 Mbps
Windows Updates	2.775 TB	9.417 Mbps
Google Shared Services	2.457 TB	8.338 Mbps
HTTP	2.393 TB	8.120 Mbps
Facebook Encrypted	1.937 TB	6.574 Mbps
Windows Store	1.838 TB	6.238 Mbps
WhatsApp	1.073 TB	3.642 Mbps
Office365	0.703 TB	2.385 Mbps
MEGA	0.615 TB	2.088 Mbps
Netflix	0.577 TB	1.959 Mbps
Amazon Cloud	0.235 TB	0.796 Mbps
MPEG	0.225 TB	0.765 Mbps
BitTorrent	0.215 TB	0.729 Mbps
Steam	0.181 TB	0.615 Mbps
Apple Updates	0.155 TB	0.527 Mbps
Unclassified	0.136 TB	0.460 Mbps
Adobe Updates	0.134 TB	0.455 Mbps
Twitter	0.131 TB	0.443 Mbps
Adobe Creative Cloud	0.119 TB	0.405 Mbps
Spotify	0.101 TB	0.343 Mbps
QUIC	0.092 TB	0.312 Mbps
DropBox	0.086 TB	0.293 Mbps
Web-Utn	0.069 TB	0.234 Mbps
RTSP	0.065 TB	0.221 Mbps
Live.com	0.061 TB	0.207 Mbps
CIFS	0.049 TB	0.166 Mbps

Inbound Applications

Name	Total Volume	Avg Throughput
GMail	0.047 TB	0.159 Mbps
Yahoo	0.043 TB	0.147 Mbps
Icecast	0.042 TB	0.144 Mbps
iOS App Store	0.042 TB	0.144 Mbps
Pinterest	0.038 TB	0.127 Mbps
Snapchat	0.036 TB	0.124 Mbps
Skype	0.036 TB	0.121 Mbps
Dailymotion	0.034 TB	0.114 Mbps
Google Docs	0.031 TB	0.106 Mbps
Android OS Update	0.030 TB	0.102 Mbps
IOS OS Update	0.029 TB	0.099 Mbps
Radius	0.028 TB	0.094 Mbps
iCloud	0.027 TB	0.090 Mbps
Skydrive	0.024 TB	0.082 Mbps
Wowza	0.024 TB	0.081 Mbps
League of Legends	0.024 TB	0.081 Mbps
Cloud-Utn	0.021 TB	0.072 Mbps

Outbound Applications

Name	Total Volume	Avg Throughput
Google Shared Services	1385.691 GB	4592.205 kbps
Office365	858.386 GB	2844.707 kbps
HTTPS	783.789 GB	2597.491 kbps
YouTube	402.720 GB	1334.621 kbps
Skydrive	277.701 GB	920.306 kbps
Facebook File-transfer	243.385 GB	806.582 kbps
Facebook Encrypted	229.157 GB	759.430 kbps
HTTP	184.059 GB	609.975 kbps
WhatsApp	128.757 GB	426.703 kbps
Unclassified	123.337 GB	408.741 kbps
BitTorrent	107.440 GB	356.058 kbps
iCloud	88.103 GB	291.975 kbps
Amazon Cloud	81.889 GB	271.382 kbps
MEGA	80.325 GB	266.198 kbps
Windows Updates	71.964 GB	238.490 kbps
Windows Store	51.228 GB	169.771 kbps
Google Drive	47.259 GB	156.617 kbps
Live.com	34.573 GB	114.576 kbps
DropBox	31.287 GB	103.686 kbps
QUIC	27.707 GB	91.821 kbps
Radius	22.096 GB	73.227 kbps
Google Docs	19.544 GB	64.769 kbps
RTP	16.029 GB	53.120 kbps
Netflix	14.417 GB	47.778 kbps
GMail	13.946 GB	46.217 kbps
Web-Utn	11.210 GB	37.150 kbps
Procesos-Utn	10.861 GB	35.994 kbps
Twitter	9.028 GB	29.919 kbps

Outbound Applications

Name	Total Volume	Avg Throughput
Facebook Chat	8.303 GB	27.516 kbps
Yahoo	8.108 GB	26.870 kbps
Snapchat	7.981 GB	26.449 kbps
Adobe Creative Cloud	7.405 GB	24.540 kbps
Skype	6.777 GB	22.459 kbps
Kaspersky	6.403 GB	21.220 kbps
Google Play	6.398 GB	21.203 kbps
MPEG	6.318 GB	20.938 kbps
Facebook Video	6.262 GB	20.752 kbps
Steam	5.393 GB	17.872 kbps
Spotify	4.646 GB	15.397 kbps
Cloud-Utn	4.537 GB	15.036 kbps
Skype for Business	3.938 GB	13.051 kbps
Apple Updates	3.565 GB	11.814 kbps
Pinterest	3.374 GB	11.181 kbps
Yahoo WebMail	3.312 GB	10.976 kbps
Adobe Updates	2.814 GB	9.326 kbps

INCIDENCIA DEL USO DEL REPOSITORIO DE FIRMAS DIGITALES EN LA
GESTIÓN DE TRÁMITES INSTITUCIONALES EN LA UTN

RÚBRICA DE ENCUESTA

DATOS PERSONALES

NOMBRES Y APELLIDOS:

FACULTAD: _____ ESPECIALIDAD: _____

FECHA: _____

ENCUESTADO POR: _____

INDICACIONES:

Marque con una X la respuesta que considere más aceptable respecto al tema.

SECCIÓN 1

Numeral 1.1 Califique el USO del repositorio de firmas digitales.

Elemento 1. El formulario de solicitud de trámites ONLINE es:

- a) Fácil de acceder SI() NO()
- b) Simplifica los trámites personales en la UTN SI() NO()
- c) El tiempo de servicio de un trámite es menor usándolo SI() NO()
- d) Es seguro y genera confianza SI() NO()

Elemento 2. Realizar trámites en línea en la UTN para recibir certificados es:

- a) Necesario SI() NO()
- b) Una oportunidad para ahorrar en transporte y otros gastos SI() NO()

c) Requiere de conocimientos de TIC SI() NO()

d) Requiere un cambio Legal Interno de la UTN SI() NO()

Elemento 3. Como estoy preparado para aprovechar el repositorio de firmas digitales en mi gestión documental.

a) Dispongo de una firma digital certificada por el gobierno SI() NO()

b) Utilizo mi firma digital si la tengo en algún trámite o negocio SI() NO()

c) Me gustaría disponer de una firma digital y usarla en la UTN SI() NO()

d) A menudo cuando realizo un trámite debo pagar el pasaje SI() NO()

Elemento 4. Influencia del repositorio en la gestión de trámites UTN.

a) El uso del repositorio incide positivamente SI() NO()

b) Se disminuye los costos para recibir certificados SI() NO()

c) Ahorra el consumo de papel para gestionar documentos SI() NO()

d) Tiene validez legal SI() NO()

Reflexión sobre la evaluación: En que otras aplicaciones debe usarse el repositorio de firmas digitales de la UTN según su criterio:

10 palabras máximo

Usted ha finalizado la valoración del uso del repositorio de firmas digitales en la gestión de trámites institucionales de la UTN.

Gracias por su valioso aporte.

UNIVERSIDAD TÉCNICA DEL NORTE

DOCUMENTO DE DISEÑO DE PROCESOS PARA IMPLEMENTACIÓN CON TECNOLOGÍA BPM

NOMBRE DEL PROCESO	Matriculación y Seguimiento de Documentos de Admisión
IDENTIFICACIÓN	MT-MATRICULACIÓN
DESCRIPCIÓN	El proceso de Seguimiento de Matriculación y Documentos de Admisión busca complementar el sistema SIIU de tal manera que se notifiquen los hitos más importantes del proceso y se genere un seguimiento que permita verificar el estado del trámite.
PROPÓSITO	Automatizar el proceso de Seguimiento de Matriculación y Documentos de Admisión, de modo que los estudiantes de la Universidad Técnica del Norte dispongan de las alertas y reportes necesarios para evidenciar el estado de su proceso de matriculación.
VERSIÓN	1.0

FIRMAS DE APROBACIÓN

Elaborado por	Revisado por	Aprobado por
Paulo Oñate LeadSolutions	Ing. Luis Aguilar Responsable del Proceso de Seguimiento Matrícula y Documentación	Econ. Jorge Proaño Administrador del Contrato

INDICE

1. OBJETIVO DEL DOCUMENTO	2
2. DEFINICIONES	2
3. OBJETIVO Y ALCANCE DEL PROCESO	2
4. ACTORES DEL PROCESO (ROLES)	2
5. DIAGRAMA BPM	4
6. REPORTES	10
7. DICCIONARIO DE TÉRMINOS	12

1. OBJETIVO DEL DOCUMENTO

Establecer una guía de referencia para la implementación del proceso de Seguimiento de Matriculación y Documentación, en el marco de la gestión por procesos, enfocada hacia su automatización mediante la plataforma AURAPORTAL BPMS.

2. DEFINICIONES

Coordinación de Carrera Es la instancia que se encarga de la articulación de los procesos académicos y administrativos de la carrera.

TP Tarea Personal, en el diagrama BPM corresponde a un formulario que se le asignará al buzón de tareas del responsable indicado para dicha tarea. Esta tarea debe ser ejecutada por una persona o grupo de personas según sea el caso.

TS Tarea de Sistema, tarea que se ejecuta de manera automática para cumplir fines de sistema como cálculos, notificaciones vía email o SMS, integración con otros sistemas, generación de documentos, etc.

Evento de Tiempo Objeto que se ejecuta automáticamente en una fecha y/y hora específica para dar inicio a un proceso.

UTN Universidad Técnica del Norte

SIU Sistema Integrado Universitario

3. OBJETIVO Y ALCANCE DEL PROCESO

El proceso de seguimiento de Matriculación y Documentación de admisión contempla los siguientes subprocesos

- Seguimiento Matriculación y Documentación
- Retiro de Materias
- Anulación de Matrículas
- Asignación Docente

4. ACTORES DEL PROCESO (ROLES)

ROL	DESCRIPCION
Coordinador de Carrera	Responsable de verificar la asignación de docentes en caso de ser necesario

Estudiante	Persona que inicia el proceso de matriculación y realiza el seguimiento del status del proceso.
Secretaría	Encargado de registrar desde el sistema los hitos que disparan los procesos para realizar notificaciones y alertas.

5. DIAGRAMA BPM

El siguiente diagrama esquematiza la secuencia de actividades que seguirá el proceso para notificar y generar el tracking del proceso de matriculación y seguimiento de documentos. También se dispone de 2 subprocesos adicionales correspondientes a Retirar Asignatura y Anular Matriculación.

El proceso de seguimiento a matrículas inicia cuando el estudiante realiza la auto matriculación o en su defecto cuando la secretaria ingresa una matrícula por el sistema SIIU, las cuales generan una de las alertas al estudiante indicándole que ya que se encuentra pre matriculado. De aquí en adelante el sistema esperará que se ejecuten los hitos de Cancelación del Pago y la legalización del acta para notificar que el proceso de matriculación.

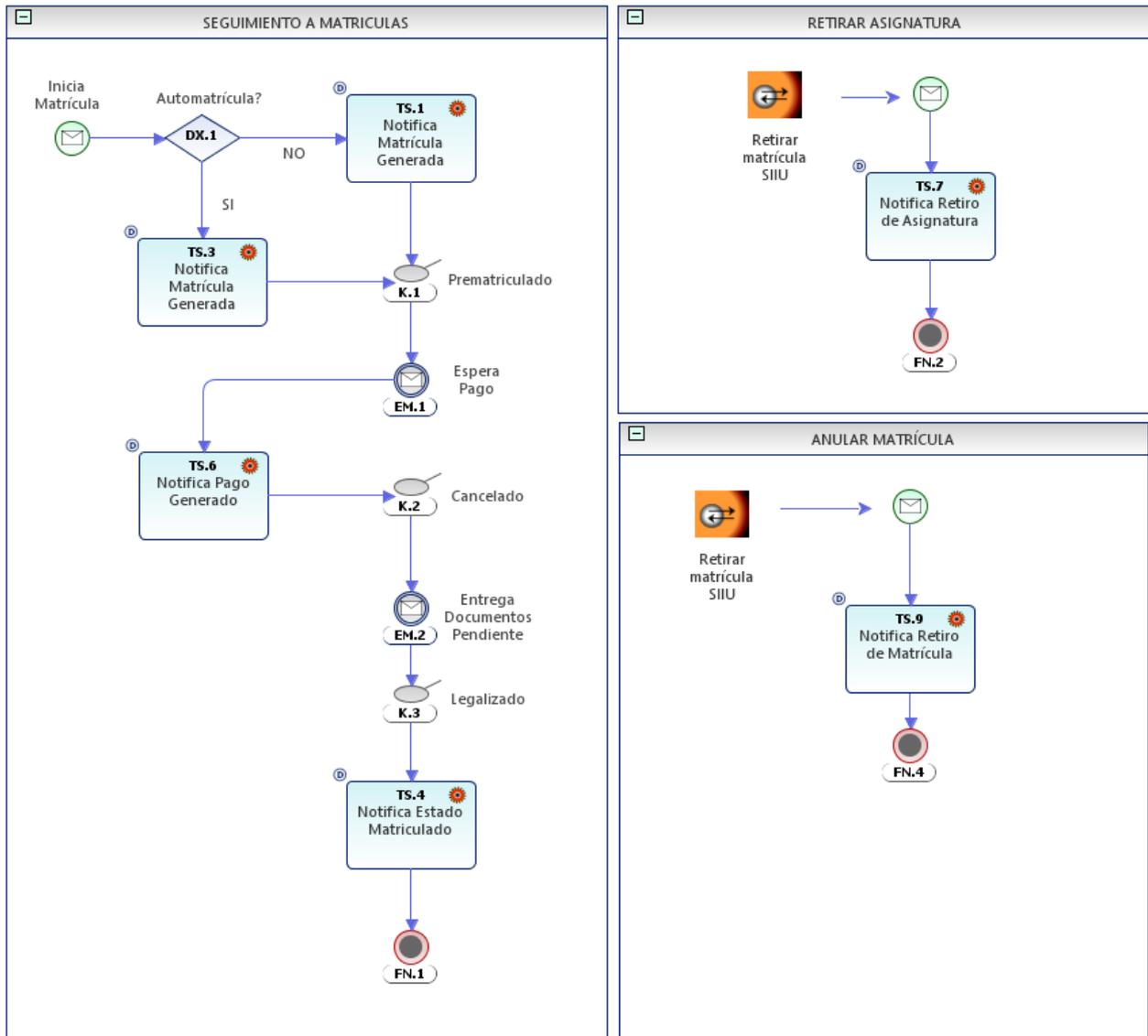


Ilustración 1 - Diagrama BPMN del Proceso de Seguimiento a Matrículas y Documentación

El siguiente subproceso se identifica con la necesidad de alertar a la secretaría de posibles estudiantes sin asignación de docentes al ser una acción manual en el sistema SIIU una vez que se registra la matriculación.

Este subproceso inicia con la fecha consultada del calendario académico en el cual inicia el período de matrículas en la UTN, en el cual consultará en el sistema SIIU aquellas materias que identifiquen estudiantes sin asignación de docentes y de cumplirse esto notificará cada 72 horas el listado correspondiente.

Una vez que finalice el período de matriculación se realizará una consulta adicional a las 2 semanas para verificar que no quede pendiente ningún estudiante, si existe algún caso se notificará a la secretaría y al Coordinador de Carrera para que realicen el seguimiento correspondiente.

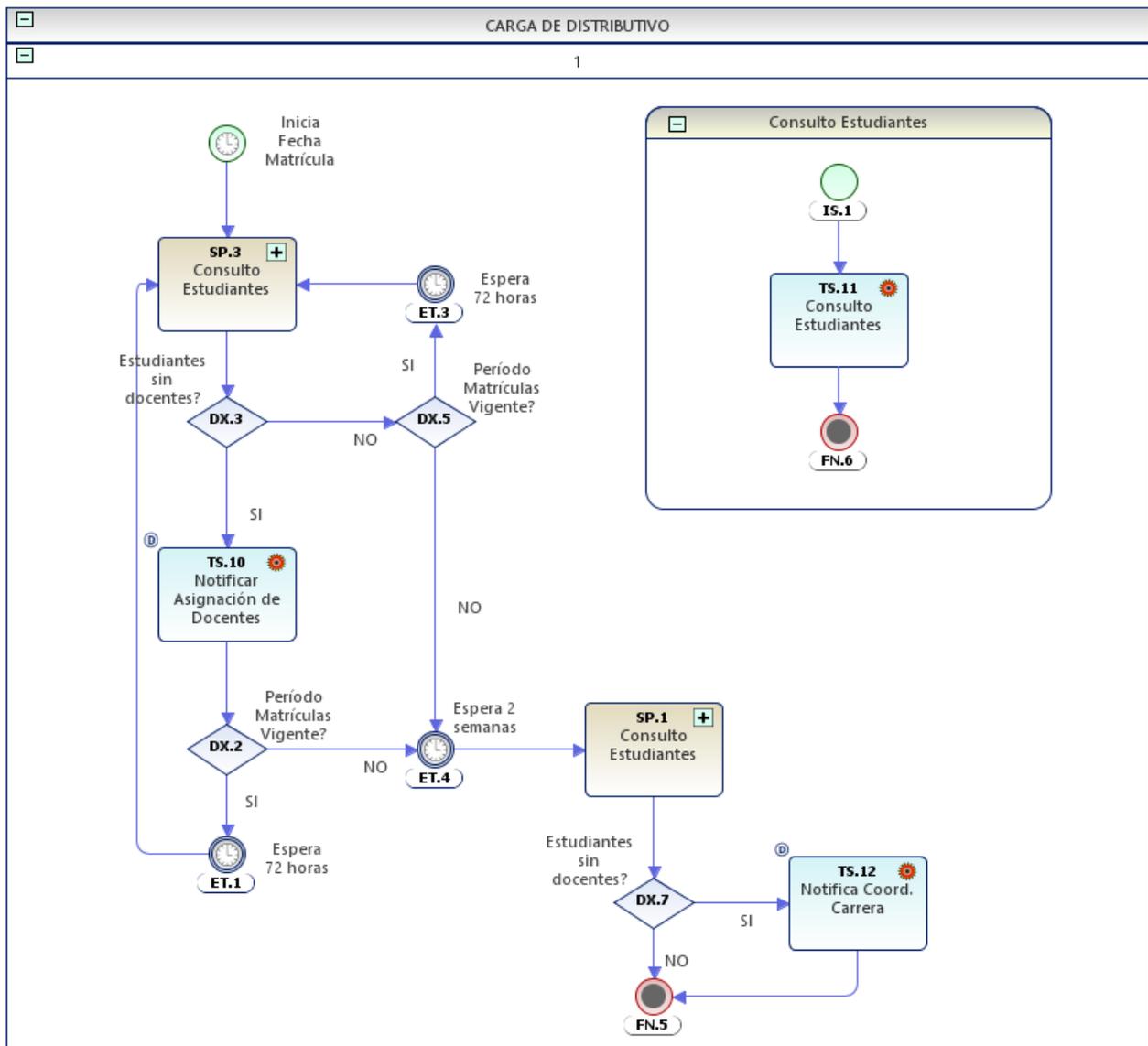


Ilustración 2 - Diagrama BPMN del Proceso de Seguimiento a Matrículas y Documentación

5.1 DESCRIPCION DETALLADA DEL PROCESO

En esta sección se describe en forma detallada los eventos, tareas y compuertas del proceso y su funcionamiento.

IDENTIFICACION	IM Inicia Matrícula
TIPO	Inicio de Mensaje
DESCRIPCION DE FUNCIONALIDAD	<ul style="list-style-type: none">• El proceso de seguimiento a matrículas iniciará el momento que se registre la matrícula por parte del estudiante en el SIIU o en su defecto realiza la secretaria directamente en el sistema.• Una vez creado el proceso e identificada la fuente de la matrícula se enviará la notificación vía correo electrónico según corresponda.
RESPONSABLE	Sistema
FORMULARIO	No aplica

IDENTIFICACION	TS.1, TS.3 Notifica Matrícula Generada
TIPO	Tarea de sistema
DESCRIPCION DE FUNCIONALIDAD	<ul style="list-style-type: none">• La tarea se ejecuta automáticamente enviando una notificación vía email al Estudiante indicándole que se ha iniciado un proceso de matrícula y los requisitos que se requieren para proceder con el requerimiento a matrículas.• La ejecución de cada tarea dependería de si el elemento procede desde la web (auto matrícula) o en otros casos directamente en el sistema SIIU.
RESPONSABLE	Sistema
FORMULARIO	Ilustración 2, Ilustración 3

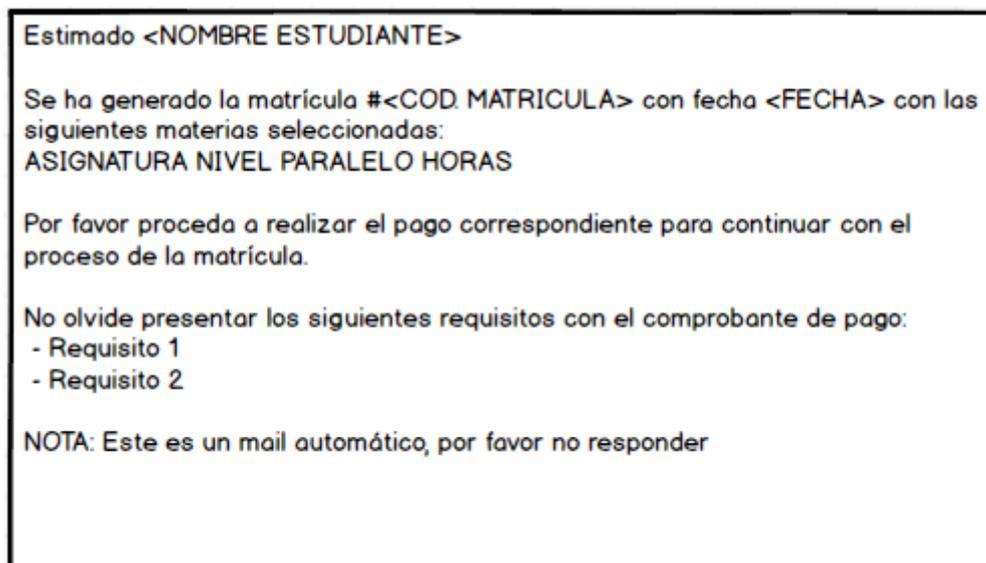


Ilustración 2 –Notificación Matrícula Generada desde Secretaría

Destinatario: Estudiante
 Asunto: Matrícula Generada

Estimado <NOMBRE ESTUDIANTE>

Se ha generado la matrícula #<COD. MATRICULA> con fecha <FECHA>

Por favor proceda a realizar el pago correspondiente para continuar con el proceso de la matrícula.

No olvide presentar los siguientes requisitos con el comprobante de pago:

- Requisito 1
- Requisito 2

NOTA: Este es un mail automático, por favor no responder

Ilustración 3 –Notificación Matrícula Generada desde Auto Matrícula

IDENTIFICACION	TS.6 Notifica Pago Generado
TIPO	Tarea de Sistema
DESCRIPCION DE FUNCIONALIDAD	<ul style="list-style-type: none"> • Esta notificación es disparada a través del objeto EM.1 Espera pago que será ejecutado desde el webservice de pagos que utiliza el banco el momento que registra una transacción de pago de matrícula para un estudiante
RESPONSABLE	Sistema
FORMULARIO	Ilustración 4

Destinatario: Estudiante
 Asunto: Pago Registrado

Estimado <NOMBRE ESTUDIANTE>

Se ha registrado existosamente el pago de la matrícula #<COD. MATRICULA> con fecha <FECHA>

No olvide presentar los siguientes requisitos con el comprobante de pago:

- Requisito 1
- Requisito 2

NOTA: Este es un mail automático, por favor no responder

Ilustración 3 – Notifica Pago Generado

IDENTIFICACION	TS.4 Notifica Estado Matriculado
TIPO	Tarea de Sistema
DESCRIPCION DE FUNCIONALIDAD	<ul style="list-style-type: none"> Este correo electrónico se dispara automáticamente a través del objeto EM.2 entrega de documentos pendiente, el cual se ejecuta el momento que la secretaria ha legalizado la matrícula y generado el acta correspondiente el sistema SIIU
RESPONSABLE	Sistema
FORMULARIO	Ilustración 5
PRECONDICIONES	Se deberá ajustar el sistema SIIU de tal manera que para presionar el botón Acta se haya chequeado la opción legalización, y una vez que se genera el acta bloquear la misma para que quede finalizado el trámite.

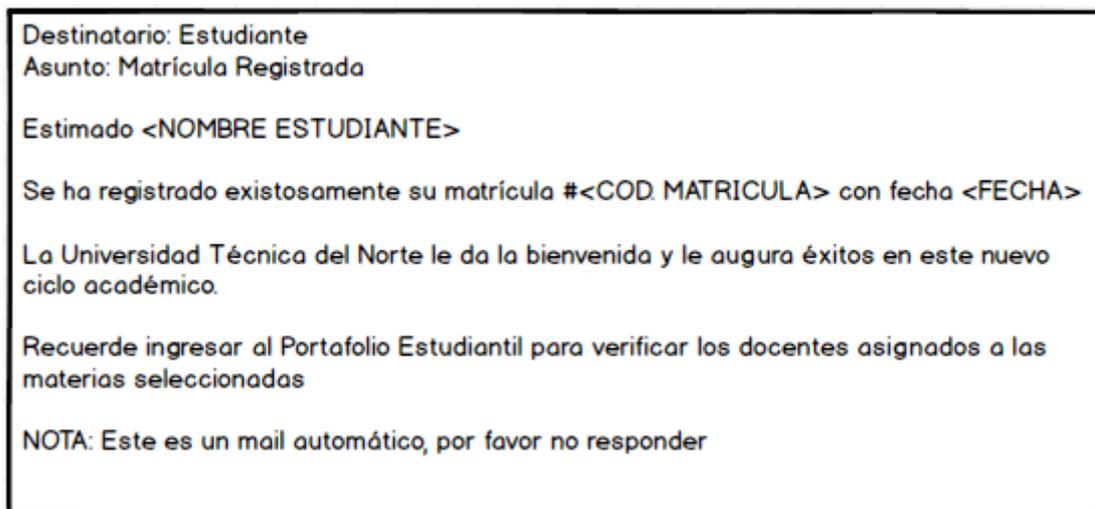


Ilustración 4 – Notifica Matriculación

IDENTIFICACION	TS.7 Notifica Retiro de Asignatura
TIPO	Tarea de Sistema
DESCRIPCION DE FUNCIONALIDAD	<ul style="list-style-type: none"> Esta notificación se ejecutará de manera independiente al seguimiento de la matrícula el momento que la secretaria registra en el sistema SIIU el retiro de la asignatura de un estudiante.
RESPONSABLE	Sistema
FORMULARIO	Ilustración 6

Destinatario: Estudiante
 Asunto: Retiro de Asignatura

Estimado <NOMBRE ESTUDIANTE>

Se ha registrado el retiro de la siguiente asignatura

Fecha: <FECHA RETIRO>
 Num Matrícula: <COD MATRICULA>
 Asignatura <ASIGNATURA>
 Nivel: <NIVEL>
 Paralelo: <PARALELO>
 Horas: <NUM HORAS>
 Resolución: <RESOLUCION>

A partir de este momento queda registrado el retiro de de dicha asignatura, cualquier novedad u observación acérquese a Secretaría.

NOTA: Este es un mail automático, por favor no responder

Ilustración 5 - Notifica Retiro de Asignatura

IDENTIFICACION	TS.9 Notifica Retiro de Matrícula
TIPO	Tarea de Sistema
DESCRIPCION DE FUNCIONALIDAD	<ul style="list-style-type: none"> Las tareas de sistema emitirán una alerta vía correo electrónico al ejecutor de la tarea que esté pendiente de completar, en el tiempo establecido dentro de cada tarea.
RESPONSABLE	Sistema
FORMULARIO	Ilustración 7

Destinatario: Estudiante
 Asunto: Anulación de Matrícula

Estimado <NOMBRE ESTUDIANTE>

Se ha registrado la anulación de su matrícula

Fecha: <FECHA RETIRO>
 Carrera: <CARRERA>
 Matrícula: <COD MATRICULA>
 Ciclo Académico: <CICLO ACADEMICO>
 Resolución: <RESOLUCION>

Cualquier novedad u observación acérquese a Secretaría.

NOTA: Este es un mail automático, por favor no responder

Ilustración 7 –Notifica Retiro de Matrícula

IDENTIFICACION	SP.3 Consulta Estudiantes
TIPO	Subproceso
DESCRIPCION DE FUNCIONALIDAD	<ul style="list-style-type: none"> Una vez que inicia el período de matrículas de acuerdo al calendario académico se ejecutará este subproceso que dispara la TS. 11 Consulta Estudiantes, la misma que ejecutará un script a la base de datos del sistema SIIU y generará la lista de estudiantes que no dispongan de un docente asignado.
RESPONSABLE	Sistema
FORMULARIO	No Aplica

IDENTIFICACION	TS.10 Notificar Asignación de Docentes
TIPO	Tarea de Sistema
DESCRIPCION DE FUNCIONALIDAD	<ul style="list-style-type: none"> Este mail se enviará automáticamente el momento que el sistema identifique estudiantes sin asignación de docente. El mismo contenido se enviará mediante la TS. 12 Notifica Coord. Carrera en el caso correspondiente
RESPONSABLE	Sistema
FORMULARIO	Ilustración 8

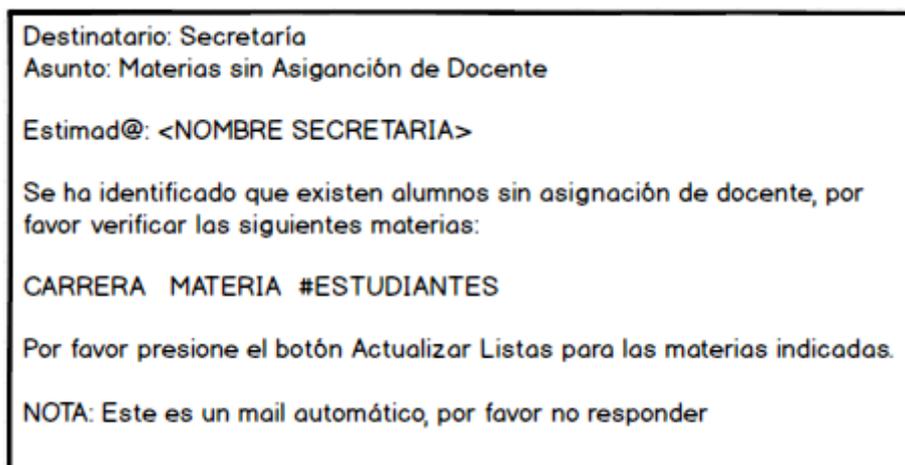


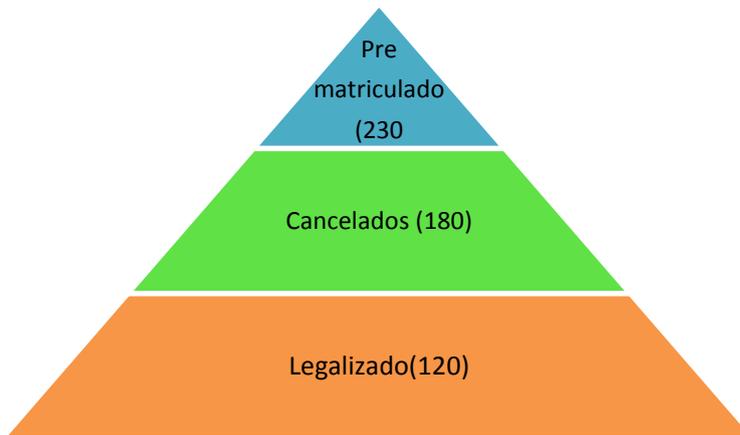
Ilustración 8 – Notificar Asignación de Docentes

6. REPORTES

6.1 PUNTOS DE CONTROL

Seguimiento de Puntos de Control – Seguimiento Matrícula

Generación de gráfica de seguimiento de Puntos de Control definidos en el proceso.



Se ha incluido los siguientes puntos de control que permitirán visualizar el estado de los hitos de seguimiento de matrícula de los estudiantes, en el cual se podrá observar el número de procesos que se encuentra en cada hito y al ingresar se podrá rastrear y visualizar más a detalle el proceso.

PRE MATRÍCULA: Procesos que se encuentran registrados mediante auto matrícula o secretaría pero tienen pendiente el pago.

CANCELADO: Procesos que se encuentran realizado el pago pero pendiente la entrega y legalización de documentos.

LEGALIZADO: Procesos que se encuentran generados el acta de legalización de matrícula y por ende oficialmente matriculados.

6.2 REPORTE

Se creará un reporte que le permita visualizar al estudiante el status de matriculación, el cual podrá contrastarlo con las notificaciones que se envía con el proceso de seguimiento en cada hito.



7. DICCIONARIO DE TÉRMINOS

TÉRMINO	TIPO DE DATO	OBSERVACIONES
codMatricula	Entero	Código o número de matrícula
Estudiante	Texto una línea	Nombre del Estudiante
codEstado	Entero	Código estado de matrícula
Materia	Texto una línea	
Ciclo	Texto una línea	
Fecha	Date	
Nivel	Texto una línea	
Paralelo	Texto una línea	
Horas	Entero	
resoluciónRetiro	Texto Multilínea	Observación de retiro de asignatura
resoluciónAnulación	Texto Multilínea	Observación de anulación de matrícula
cicloAcademico	Texto Multilínea	
Carrera	Texto Multilínea	
Facultad	Texto Multilínea	

CREACIÓN DE CERTIFICADOS DE MATRÍCULA DE LA UNIVERSIDAD TÉCNICA DEL NORTE PARA RELACIONAR EL SERVICIO DE FIRMAS DIGITALES CON LA EMISIÓN DE CERTIFICADOS DE MATRÍCULA

*/*FUNCION PARA VERIFICAR SI UN ESTUDIANTE ESTA MATRICULADO EN LA UTN */*

```
create or replace FUNCTION      MATRICULADO
(
  CEDULAX IN VARCHAR2,
  CICLO_ACADEMICO IN VARCHAR2,
  DEPENDENCIA IN VARCHAR2
) RETURN NUMBER AS

  NRO NUMBER(10);
BEGIN
  NRO:=-1;
  SELECT COUNT(E.ESTUDIANTE_CEDULA) INTO NRO FROM
UTNDB.ACA_TAB_MATRICULAS E WHERE
E.ESTUDIANTE_CEDULA=CEDULAX AND E.ESTADO NOT IN ('P','A')
AND E.DEPEN_CODIGO NOT IN ('00194','00238')
AND E.CICLO_ACAD_CODIGO=CICLO_ACADEMICO
AND E.DEPEN_CODIGO=DEPENDENCIA;
  RETURN NRO;
END MATRICULADO;
/*
eL estudiante solicita al coordinador
```

DATOS DEL ESTUDIANTE:

IDENTIFICACION, NOMBRES,

FACULTAD, CARRERA, MODALIDAD, CICLO_ACADEMICO,

(SI ES SECRETARIA GENERAL FIRMA EL SECRETARIO)

SINO EL SECRETARIO JURIDICO-

*/

-- Archivo creado - viernes-abril-20-2018

-- DDL for Procedure CREARDOCXMLMATRICULADO

set define off;

```
CREATE OR REPLACE EDITIONABLE PROCEDURE
"DEV"."CREARDOCXMLMATRICULADO" (PCODIGO in varchar2,
PCICLO_ACADEMICO in varchar2, PDEPENDENCIA in varchar2) is
  NRO number:= -1;
begin
SELECT DEV.MATRICULADO(PCODIGO, PCICLO_ACADEMICO,
PDEPENDENCIA) into NRO from dual;
IF(nro >0) then
  insert into documentos values(sec_doc.nextval,(SELECT concat('<?xml
version="1.0" encoding="UTF-8"?>',XMLAGG (
  XMLELEMENT("documento",
    XMLATTRIBUTES(a.id AS "id",a.version as "version"),
    xmlelement("codigo",concat('M',concat('2018',PCODIGO))),
    XMLFOREST((SELECT XMLAGG(XMLELEMENT("ESTUDIANTE",
XMLFOREST(MAT.ESTUDIANTE_CEDULA AS IDENTIFICACION,
INS_PCK_GENERAL.FUN_NOMBRES_PERSONA(MAT.ESTUDIANTE_CEDULA
AS NOMBRES,
'FACULTAD '||
SELECT FACULTAD
```

```

FROM REC_VIEW_DEPENDENCIAS
WHERE CODIGO_CA=PDEPENDENCIA
) AS FACULTAD,
(SELECT CARRERA
FROM REC_VIEW_DEPENDENCIAS
WHERE CODIGO_CA=PDEPENDENCIA)
AS CARRERA,
MO.DESCRIPCION AS MODALIDAD,
CA.CODIGO AS CICLO_ACAD_CODIGO,
CA.DESCRIPCION AS CICLO_ACADEMICO,
TO_DATE (SYSDATE, 'DD/MM/YYYY HH24:MI:SS') AS
FECHA_EMISION_CERTIFICADO)))FROM ACA_TAB_MATRICULAS MAT,
ACA_TAB_MODALIDADES_ESTUDIOS MO,
ACA_TAB_CICLOS_ACADEMICOS CA
WHERE MAT.ESTUDIANTE_CEDULA=PCODIGO
AND MAT.CICLO_ACAD_CODIGO=PCICLO_ACADEMICO
AND MAT.DEPEN_CODIGO=PDEPENDENCIA
AND MAT.MODA_ESTUD_CODIGO=MO.CODIGO
AND MAT.CICLO_ACAD_CODIGO=CA.CODIGO) "estudiante_matriculado"--,
-- XMLFOREST((SELECT XMLAGG(XMLELEMENT("MATERIAS",
XMLFOREST(M.ORD,CONCAT(CONCAT(M.APELLIDOS,' '),M.NOMBRES) AS
DOCENTE,M.MATERIA)))FROM DEV.MATERIAS M INNER JOIN
DEV.ESTUDIANTES E ON M.FACULTAD=E.FACULTAD AND
M.CARRERA=E.CARRERA AND M.NIVEL=E.NIVEL AND M.PARALELO='A'
WHERE E.CEDULA=codigo) "lista_materias")
)
).getclobval()
) AS "atributo" FROM dev.atributos a));
end if;
end crearDocXMLMatriculado;
/

```

--Requerimiento de firma digital mediante SOAP desde CLOUD-UTN

```
soap_request:= '<?xml version="1.0" encoding="UTF-8"?><S:Envelope  
xmlns:S="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-  
ENV="http://schemas.xmlsoap.org/soap/envelope/">
```

```
<SOAP-ENV:Header/>
```

```
<S:Body>
```

```
<ns2:firmar xmlns:ns2="http://servicioWebUTN/">
```

```
<documento>'|| P_xml ||'.xml</documento>
```

```
<emisor>'|| ID_emisor ||'</emisor>
```

```
<clave>'|| S_Clave ||'</clave>
```

```
</ns2:firmar>
```

```
</S:Body>
```

```
</S:Envelope>
```

```
;
```