REFERENCIA METODOLÓGICA PARA IMPLEMENTACIÓN DE SERVICIOS TELEMÁTICOS BASADOS EN IDENTIFICACIÓN DIGITAL

ANEXOS

JOSÉ JULIÁN REINA MATERÓN

DIEGO MAURICIO PAZ CARRILLO

UNIVERSIDAD DEL CAUCA

FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES

DEPARTAMENTO DE SISTEMAS

POPAYÁN - COLOMBIA

2006

REFERENCIA METODOLÓGICA PARA IMPLEMENTACIÓN DE SERVICIOS TELEMÁTICOS BASADOS EN IDENTIFICACIÓN DIGITAL

ANEXOS

JOSÉ JULIÁN REINA MATERÓN

DIEGO MAURICIO PAZ CARRILLO

Documento Final de Trabajo de Grado para optar al título de:

Ingeniero en Electrónica y Telecomunicaciones

Director:

SILER AMADOR DONADO

Ingeniero de Sistemas

UNIVERSIDAD DEL CAUCA

FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES

DEPARTAMENTO DE SISTEMAS

POPAYÁN - COLOMBIA

2006

CONTENIDO

ANEXO A.

PLAN DE DESARROLLO DEL PROYECTO

1. INTRODUCCIÓN 1

2. DEFINICIÓN DE LA IDEA DEL PROYECTO 1

3. OBJETIVOS 4

3.1. OBJETIVO GENERAL 4

3.2. OBJETIVOS ESPECIFICOS 4

4. CARACTERÍSTICA DEL SERVICIO DE IDENTIFICACIÓN DIGITAL 5

4.1. DESCRIPCIÓN DEL SERVICIO 5

4.2. LOS USUARIOS DEL SERVICIO DE IDENTIFICACIÓN DIGITAL 6

4.3. ANÁLISIS DOFA DEL SERVICIO DE IDENTIFICACIÓN DIGITAL 7

5. PLANEACIÓN DEL PROYECTO 8

6. CONCLUSIONES Y RECOMENDACIONES 8

ANEXO B.

PLAN DE DESARROLLO DEL SERVICIO DE IDENTIFICACIÓN DIGITAL

1. INTRODUCCIÓN 9

2. DEFINICIÓN DE LAS HISTORIAS 9

3. ESTIMACIÓN DE TIEMPO DE LAS HISTORIAS 10

4. PLAN DE ITERACIÓN 10

5. GRÁFICOS 14

6. CONCLUSIONES Y RECOMENDACIONES 15

ANEXO C.

ANÁLISIS DE RIESGOS DE LA ENTIDAD DE CERTIFICACIÓN DE LA UNIVERSIDAD DEL CAUCA 17

ANEXO D.

ESTUDIO DE INGENIERÍA DE LA ENTIDAD DE CERTIFICACIÓN DE LA UNIVERSIDAD DEL CAUCA

1. INTRODUCCIÓN 23

2.1. REQUERIMIENTOS GENERALES 23

2.2. REQUERIMIENTOS ADMINISTRATIVOS 24

2.3. REQUERIMIENTOS DE LAS APLICACIONES DE GESTIÓN 24

2.4. REQUERIMIENTOS DE LOS CERTIFICADOS PKI 25

2.5. REQUERIMIENTOS DE LAS LLAVES 25

2.6. REQUERIMIENTOS DEL DIRECTORIO 25

2.7. OTROS REQUERIMIENTOS 25

3. ARQUITECTURA DE LA ENTIDAD DE CERTIFICACIÓN 25

3.1. DESCRIPCIÓN DE LA ARQUITECTURA 25

3.2. DESCRIPCIÓN DEL PROCESO DE CERTIFICACIÓN 28

4. CONCLUSIONES Y RECOMENDACIONES 28

ANEXO E.

DECLARACIÓN DE PRACTICAS DE CERTIFICACIÓN 29

LISTA DE TABLAS

ANEXO B.

TABLA 1. ESTIMACIÓN DE TIEMPO DE LAS HISTORIAS 10

TABLA 2. TAREAS DE LA 1. SEMANA 11

TABLA 3. TAREAS DE LA 2. SEMANA 11

TABLA 4. TAREAS DE LA 3. SEMANA 11

TABLA 5. TAREAS DE LA 4. SEMANA 12

TABLA 6. TAREAS DE LA 5. SEMANA 12

TABLA 7. TAREAS DE LA 6. SEMANA 13

TABLA 8. TAREAS DE LA 7. SEMANA 13

TABLA 9. TRABAJO PENDIENTE DE LAS HISTORIAS AL FINAL DE LA CUARTA SEMANA 14

ANEXO C.

TABLA 1. MAL FUNCIONAMIENTO DE LA CA Y LA RA 18

TABLA 2. ACCESO INSEGURO A LAS BASES DE DATOS 18

TABLA 3. FALTA DE DOCUMENTACIÓN 18

TABLA 4. DESAPARICIÓN DE ADMINISTRADOR DE LA CA 19

TABLA 5. VULNERACION DE LA RA 19

TABLA 6. PERSONAL DESACTUALIZADO Y ADMINISTRACIÓN SIN EXPERIENCIA 19

TABLA 7. SISTEMAS OBSOLETOS 20

TABLA 8. REGISTRO DE USUARIOS DEFICIENTE 20

TABLA 9. SUPLANTACION DE NUEVOS USUARIOS 20

TABLA 10. ACCESO FÍSICO VIOLENTO A LA CA 21

TABLA 11. ACCESO NO AUTORIZADO AL SISTEMA (RA) 21

TABLA 12. FRAUDE DEL PERSONAL 21

TABLA 13. DESASTRES NATURALES 22

LISTA DE FIGURAS

ANEXO A.

FIGURA 1. ÁRBOL DE PROBLEMAS 2

FIGURA 2. ARQUITECTURA PKI 3

FIGURA 3. ARQUITECTURA DEL PROTOTIPO FINAL 5

FIGURA 4. PLANEACIÓN DEL PROYECTO 8

ANEXO B.

FIGURA 1. PORCENTAJE DE TRABAJO SEMANAL 14

FIGURA 2. MINUTOS DE DISCUSIÓN POST-ACTIVIDAD 15

ANEXO D.

FIGURA 1. ARQUITECTURA DE LA ENTIDAD DE CERTIFICACION DE LA UNIVERSIDAD DEL CAUCA 27

ANEXO A
PLAN DE DESARROLLO DEL PROYECTO

1. INTRODUCCIÓN

El presente documento busca ser el resumen del trabajo de exploración realizado durante los primeros días del proyecto de investigación. Los datos aquí contenidos reflejan los resultados de las distintas actividades donde se logró enfocar el horizonte del proyecto de implantación del servicio de correo electrónico certificado en la Universidad del Cauca.

2. DEFINICIÓN DE LA IDEA DEL PROYECTO

El presente proyecto de desarrollo, asume las siguientes premisas, de acuerdo a un estudio de necesidades realizado en la Universidad del Cauca:

- Se carece de un mecanismo para identificar usuarios de una manera eficiente y eficaz en la mensajería electrónica interna de la Universidad del Cauca
- Se carece de una infraestructura capaz de soportar procesos de negocio electrónicos dentro de la Universidad del Cauca
- No existe un mecanismo de generación, administración y revocación de certificados para los usuarios del servicio de hosting de la Universidad del Cauca

El análisis de las premisas anteriores dentro del contexto de la Universidad del Cauca, lleva al planteamiento de la siguiente pregunta:

- ¿Cómo implantar una infraestructura de seguridad que pueda garantizar la identidad, integridad, autenticación, autorización, aceptación y confidencialidad de la información en la red de datos, y que ofrezca servicios para llevar a cabo procesos de negocio académicos entre los usuarios de la Universidad del Cauca?

A raíz del interrogante anterior, se construye el siguiente árbol de problemas[1]:

1 Árbol de problemas es una estrategia utilizada para visualizar las relaciones de causa y efecto en la Metodología ZOPP (Ziel Orienterte Projekt Planung – Planeación de Proyectos orientada a objetivos).

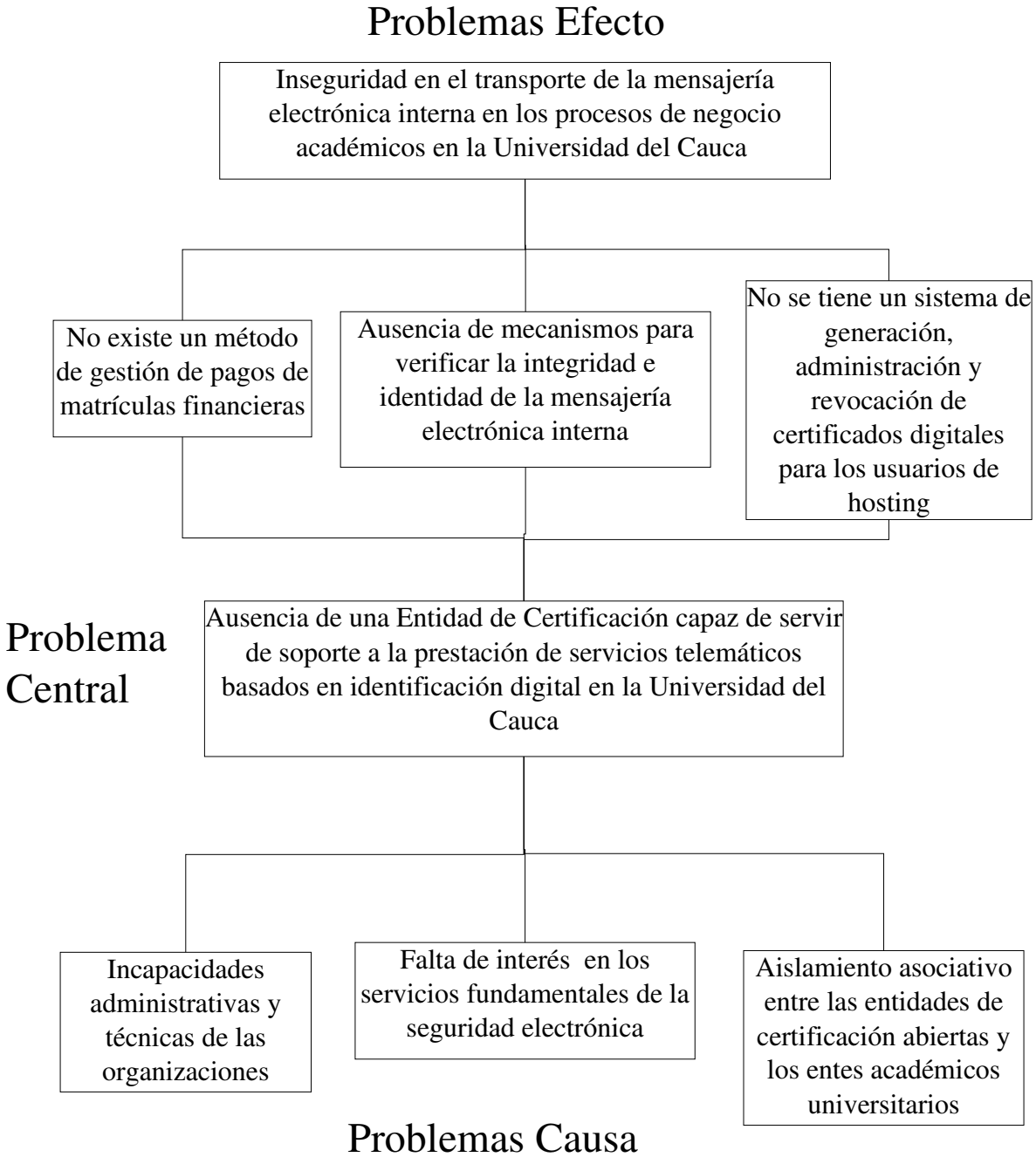


Figura 1. Árbol de Problemas

De este árbol, se deduce la siguiente pregunta central, que muestra la síntesis de las relaciones causa-efecto del contexto analizado: ¿Cómo construir una Entidad de Certificación capaz de prestar servicios telemáticos basados en identificación digital?

La hipótesis inicial del proyecto de desarrollo plantea la construcción de una Entidad de

Certificación Cerrada, que sirva de soporte a los problemas anteriormente planteados (Problemas Causa-Efecto) en el árbol de problemas.

Una aproximación de la solución a implantar, se puede resumir en la siguiente arquitectura:

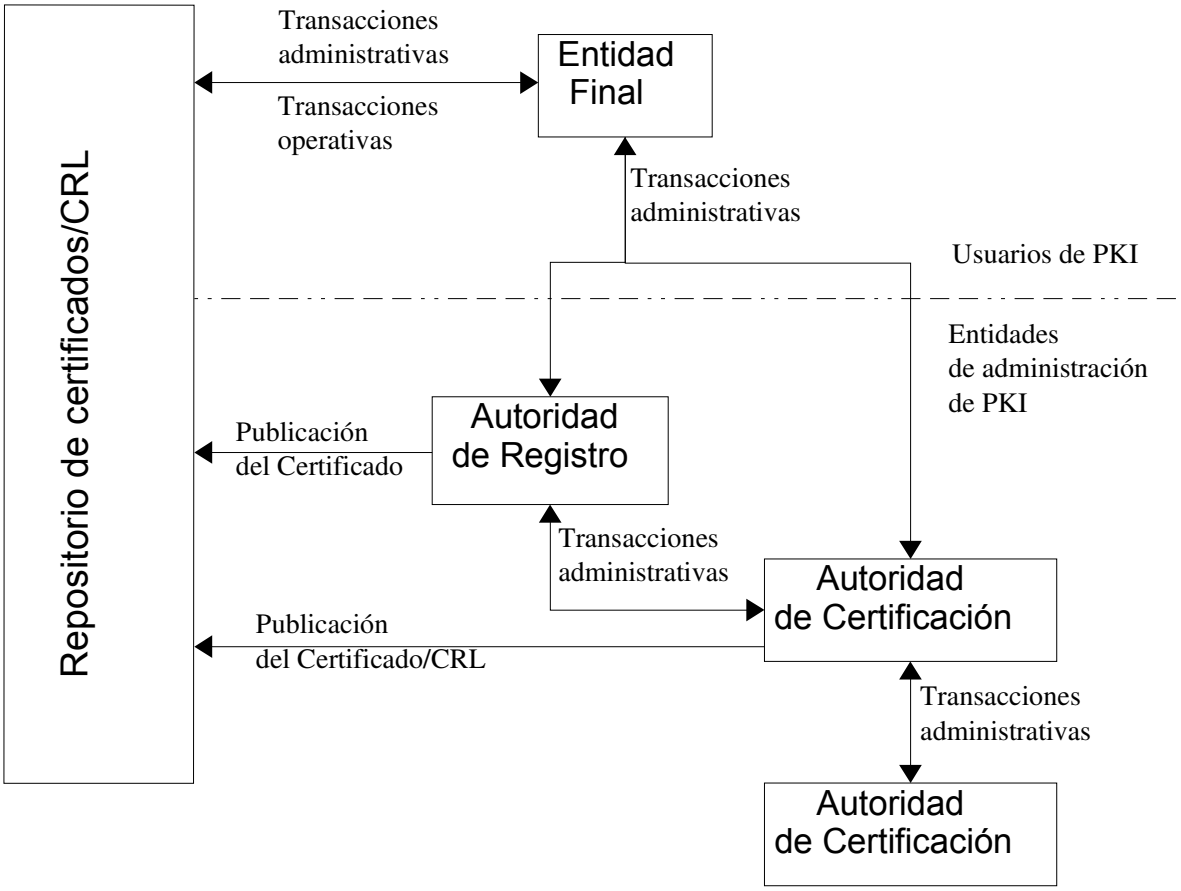


Figura 2. Arquitectura PKI

Entidad Final: Es el usuario de un certificado PKI. Es el cliente destino o el sistema que es el sujeto de un certificado PKI. Para nuestro proyecto, estos son los usuarios que hacen parte del directorio institucional de la Red de Datos de la Universidad del Cauca.

Autoridad de Registro: Es una entidad opcional dentro de la arquitectura PKIX responsable de las tareas administrativas asociadas con el registro de la entidad destino. Entre las funciones de una Autoridad de Registro se encuentran:

- Autenticación personal del sujeto que se registra para un certificado
- Verificación de la validez de la información suministrada por el sujeto

- Validar el derecho del sujeto a los atributos del certificado solicitado
- Verificar que el sujeto en realidad posee la llave privada que se va a registrar. Por lo general, ésto se conoce como POP (Prueba de posesión)
- Informar los casos de terminación o compromiso de llave donde se requiera renovación
- Asignación de nombres con propósitos de identificación
- Generación de la pareja llave privada/pública
- Almacenamiento de la llave privada
- Proceso de recuperación de llave

Autoridad de Certificación: Es la responsable de crear y expedir certificados de la entidad destino. Éstos asocian la identidad de le entidad destino del sujeto, por medio del nombre del sujeto que se registró con la llave pública correspondiente a la llave privada que poseía ese sujeto.

Repositorio: Se utiliza para el almacenamiento público de certificados y listas de revocación de certificados. Originalmente fue un directorio X.500. Para soporte de PKIX, el repositorio será un directorio LDAP (Lightweight Directory Access Protocol).

3. OBJETIVOS

3.1. OBJETIVO GENERAL

Implementar el servicio de correo electrónico certificado sobre una Entidad de Certificación cerrada para la comunidad académica de la Universidad del Cauca

3.2. OBJETIVOS ESPECÍFICOS

- Construir una Entidad de Certificación Cerrada que cumpla todos los requisitos legales nombrados en la Ley 527 de 1999, el Decreto 1747 de 2000 y que se encuentre avalada por la Superintendencia de Industria y Comercio (SIC)
- Construir una Entidad de Certificación Cerrada que cumpla los estándares PKIX, ISO 17799 e ISO 7816
- Desarrollar el servicio prototipo de certificación de mensajería electrónica interna en la red de datos de la Universidad del Cauca

4. CARACTERÍSTICA DEL SERVICIO DE IDENTIFICACIÓN DIGITAL

4.1. DESCRIPCIÓN DEL SERVICIO

El servicio a implantar va a ser el *servicio de correo electrónico certificado,* en el cual, todos los mensajes de datos a ser transportados puedan cifrarse y firmarse.

La arquitectura del prototipo final sería algo similar a la siguiente grafica:

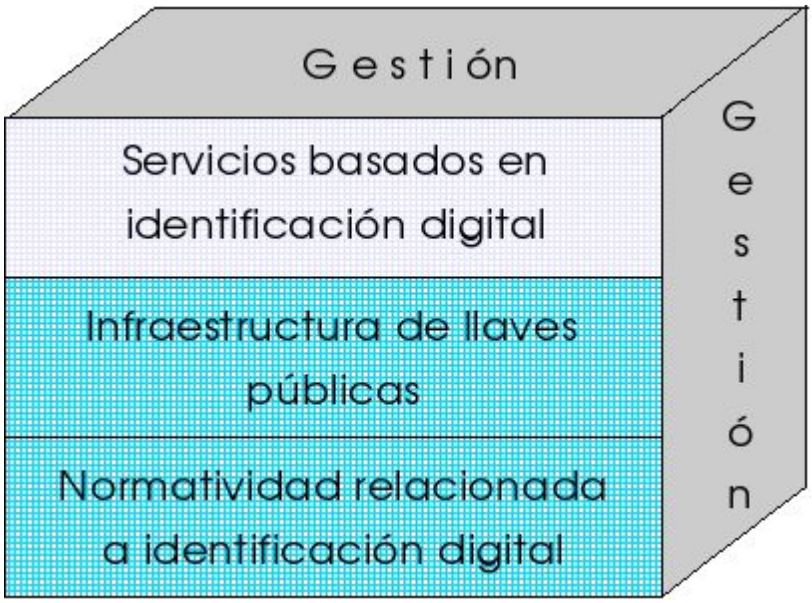


Figura 3. Arquitectura del Prototipo Final

Normatividad Relacionada a Identificación Digital: Es la base de la arquitectura, se constituye por todas las normas, y leyes que permiten la realización de firmas digitales, el uso de entidades de certificación, es decir toda actividad asociada a la certificación digital según su validez con la Ley, razón por la cual es de suma importancia al construir un sistema de Identificación Digital.

Infraestructura de Llaves Públicas: Corresponde a un sistema complejo necesario para la gestión de certificados digitales y aplicaciones de firma digital. Se basa en la criptografía, en sistemas sistematizados de registro, certificación y distribución de llaves.

Servicios Basados en Identificación Digital: Aquí es donde se va a ubicar el servicio de correo electrónico certificado y es "la punta del iceberg" de toda el sistema de seguridad.

Gestión: Constituye el control y administración de toda la arquitectura, vela por la aplicación adecuada de cada elemento en el sistema y su sostenimiento. Es de vital importancia en todas las etapas de desarrollo.

El sistema de seguridad a implementarse, debe cumplir con los estándares ISO 17799 para gestión de buenas prácticas, y las recomendaciones de gestión de riesgo emitidas por la NIST (National Institute of Standards and Technology).

La vida útil del servicio viene atada a la vida útil de la tecnología, no obstante, la implementación va a ser lo mas estándar posible, para así poder acomodarse mejor al cambio.

4.2. LOS USUARIOS DEL SERVICIO DE IDENTIFICACIÓN DIGITAL

Caracterización de los usuarios:

El mercado meta, al cual pretende llegar el siguiente proyecto se encuentra formado por las personas vinculadas a la Universidad del Cauca, ya sean Administrativos, Docentes, o Estudiantes. Desafortunadamente no todos el personal vinculado son usuarios de internet, por lo que se concluye que los usuarios del producto planteado son *los usuarios de internet vinculados a la Universidad del Cauca.*

Lo siguiente resume el mercado meta del Proyecto

Estudiantes	**10750**
Docentes	**960**
Administrativos	**500**
Usuarios de Directorio	**7000**

Por ser nuestro producto, un sistema cerrado, se puede deducir que no realiza ninguna interacción con usuarios externos, por lo que se debe concluir que no existe competencia externa, pensando en otras Entidades de Certificación.

4.3. ANÁLISIS DOFA DEL SERVICIO DE IDENTIFICACIÓN DIGITAL

DEBILIDADES

- Tiempo de realización de la solución
- Poco personal capacitado en el tema

OPORTUNIDADES

- Ser pioneros en la construcción de soluciones basadas en identificación digital
- Enorme interés por parte de los usuarios del servicio de directorio sobre la implantación de servicios de valor agregado por parte de la Universidad
- Ampliarse hacia el mercado de comercio electrónico

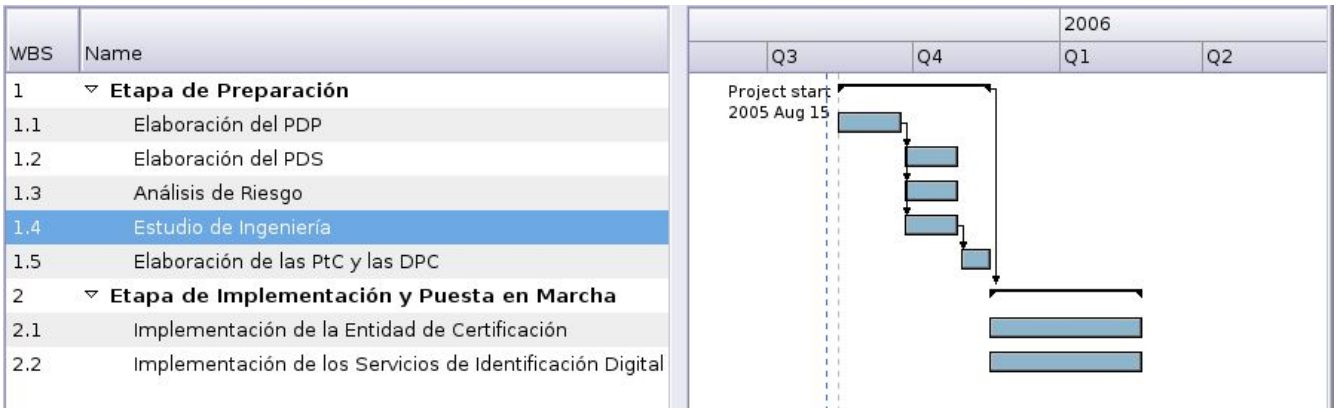
FORTALEZAS

- Manejo de la tecnología PKI
- Apoyo de la comunidad académica de la Universidad
- Experiencia en la administración de servidores y servicios de internet

AMENAZAS

- Desconocimiento por parte del público de los beneficios de la certificación digital
- Importación de la materia prima relacionada con la solución
- Dependencia de los cambios del proveedor

5. PLANEACIÓN DEL PROYECTO



PDP: Plan de Desarrollo del Proyecto

PDS: Plan de Desarrollo del Servicio

PTC: Políticas de Certificación

DPC: Declaración de Prácticas de Certificación

Figura 4. Planeación del Proyecto

6. CONCLUSIONES Y RECOMENDACIONES

Del anterior proyecto, se pueden realizar las siguientes recomendaciones y conclusiones:

- La implantación de servicios telemáticos basados en identificación digital se debe de realizar orientada por objetivos, donde cada objetivo (o servicio implementado) comprende un pequeño proyecto
- Es recomendable ofrecer la posibilidad de autenticación por medio de una tarjeta inteligente o de un token USB, pensando en la implementación de servicios posteriores, como el de pago de deudas financieras en línea
- Los antiguos problemas de suplantación de identidad y alteración de información en la mensajería electrónica interna de la Universidad del Cauca, serán solucionados gracias a la implementación del siguiente proyecto
- La certificación digital basada en dispositivos de autenticación abre una nueva tendencia en el mercado del comercio electrónico
- La Universidad del Cauca va a ser pionera en Colombia en el campo de acción de la creación de servicios basados en identificación digital

ANEXO B
PLAN DE DESARROLLO DEL SERVICIO DE IDENTIFICACIÓN DIGITAL

1. INTRODUCCIÓN

El presente documento es el encargado de mostrar el avance y las diferentes actividades que se realizaron en el Plan para desarrollar el servicio de correo electrónico certificado para la Universidad del Cauca.

El presente no es un documento de Análisis de Requerimientos de Software Orientado a Objetos (AOO)[2], ni tampoco pretende serlo. Es simplemente un plan para adaptar un software de cliente de correo libre a las necesidades del servicio, e implementarle la funcionalidad de correo certificado.

2. DEFINICIÓN DE LAS HISTORIAS

Hacer que los correos vayan firmados

Cuando un usuario se encuentre en la interfaz del cliente de correo web y desee enviar un correo electrónico, simplemente en el momento de redactarlo, debe señalar la opción de "Enviar Correo Firmado". (La interfaz debe solicitar una contraseña para firmar el correo).

Hacer que los correos sean verificados

En el momento que un usuario reciba un correo firmado, el cliente de correo debe mostrar un mensaje en el cual se verifique la autenticidad de la firma en el mensaje.

Hacer que los correos vayan cifrados

Cuando un usuario se encuentre en la interfaz del cliente de correo web y desee enviar un correo electrónico, simplemente en el momento de redactarlo, debe señalar la opción de "Enviar Correo Cifrado". (La interfaz debe solicitar una contraseña para cifrar el correo).

2 LARMAN, Craig. Applying UML and Patterns. An introduction to Object-Oriented Analysis and Design and the Unified Process. p 45.

Hacer que los correos sean descifrados

En el momento que un usuario reciba un correo cifrado, el cliente correo debe solicitar una contraseña para descifrarlo y posteriormente mostrarlo.

3. ESTIMACIÓN DE TIEMPO DE LAS HISTORIAS

Historia	***Tiempo Estimado (Semanas)***	***Asignada para la iteración***	***Asignado para la versión***
Hacer que los correos vayan firmados	3	1	Alfa
Hacer que los correos vayan cifrados	2	1	Alfa
Hacer que los correos sean verificados	1	1	Alfa
Hacer que los correos sean descifrados	1	1	Alfa

Tabla 1. Estimación de Tiempo de las Historias

4. PLAN DE ITERACIÓN

Hacer que los correos vayan firmados

- Acomodación de la Interfaz de Usuario ---- JR 1
- Creación de la librería de funciones SMIME para firmado y verificación de firmas ---- JR 1
- Integración entre la función de firmado y verificación de la librería y la interfaz de usuario ---- DP 1

Hacer que los correos vayan cifrados

- Acomodación de la Interfaz de Usuario ---- JR 1
- Creación de la librería de funciones SMIME para cifrado y descifrado ---- JR 1
- Integración entre la función de cifrado y descifrado de la librería y la interfaz de usuario ---- DP 1

* JR: José Julián Reina Materón
* DP: Diego Mauricio Paz Carrillo

SEGUIMIENTO DEL DESARROLLO SEMANA A SEMANA

Tareas de la 1. Semana

Tarea	***Persona a Cargo***	***Hecho (%)***	***Para hacer (%)***
Pruebas de bajo nivel con el motor criptográfico OpenSSL	DP	70	30
Prueba y configuración de diferentes clientes web libres	JR	85	15

Tabla 2. Tareas de la 1. Semana

Tareas de la 2. Semana

Tarea	***Persona a Cargo***	***Hecho (%)***	***Para hacer (%)***
Pruebas de bajo nivel con el motor criptográfico OpenSSL	DP	30	0
Prueba y configuración de diferentes clientes web libres	JR	15	0
Pruebas de integración de funciones entre PHP y OpenSSL	DP	45	55
Pruebas de usabilidad del cliente de correo web escogido	JR	80	20

Tabla 3. Tareas de la 2. Semana

Tareas de la 3. Semana

Tarea	***Persona a Cargo***	***Hecho (%)***	***Para hacer (%)***
Pruebas de integración de funciones entre PHP y OpenSSL	DP	20	35
Pruebas de usabilidad del cliente de correo web escogido	JR	20	0
Implementación de las funciones de cifrado y descifrado con las llaves emitidas por la entidad de certificación	JR	15	85

Tabla 4. Tareas de la 3. Semana

Tareas de la 4. Semana

Tarea	***Persona a Cargo***	***Hecho (%)***	***Para hacer (%)***
Pruebas de integración de funciones entre PHP y OpenSSL	DP	20	15
Implementación de las funciones de cifrado y descifrado con las llaves emitidas por la entidad de certificación	JR	50	35
Desarrollo de las librería PHP para cifrar, descifrar, firmar y verificar información, con base a las llaves provenientes de la entidad de certificación	DP	25	85
Adaptación de la interfaz del cliente web a las necesidades funcionales del software	JR	35	65

Tabla 5. Tareas de la 4. Semana

Tareas de la 5. Semana

Tarea	***Persona a Cargo***	***Hecho (%)***	***Para hacer (%)***
Pruebas de integración de funciones entre PHP y OpenSSL	DP	15	0
Implementación de las funciones de cifrado y descifrado con las llaves emitidas por la entidad de certificación	JR	35	0
Desarrollo de las librería PHP para cifrar, descifrar, firmar y verificar información, con base a las llaves provenientes de la entidad de certificación	DP	50	35
Adaptación de la interfaz del cliente web a las necesidades funcionales del software	JR	30	35
Integración entre la interfaz web y las funcionalidades de la librería PHP	JR,DP	50	50

Tabla 6. Tareas de la 5. Semana

Tareas de la 6. Semana

Tarea	***Persona a Cargo***	***Hecho (%)***	***Para hacer (%)***
Desarrollo de las librería PHP para cifrar, descifrar, firmar y verificar información, con base a las llaves provenientes de la entidad de certificación	DP	35	0
Adaptación de la interfaz del cliente web a las necesidades funcionales del software	JR	35	0
Integración entre la interfaz web y las funcionalidades de la librería PHP	JR,DP	25	25

Tabla 7. Tareas de la 6. Semana

Tareas de la 7. Semana

Tarea	***Persona a Cargo***	***Hecho (%)***	***Para hacer (%)***
Integración entre la interfaz web y las funcionalidades de la librería PHP	JR,DP	25	0

Tabla 8. Tareas de la 7. Semana

Trabajo pendiente de las historias al final de la cuarta semana

Historia	***Para Hacer***	***Comentarios***
Hacer que los correos vayan firmados	Hace falta terminar y probar la librería que se está construyendo para firmar los correos	Se deben hacer pruebas independientes para comprobar la funcionalidad de la firma de correos
Hacer que los correos sean verificados	Hace falta terminar y probar la librería que se está construyendo para verificar los correos	Se deben hacer pruebas independientes para comprobar la funcionalidad de la verificación de correos
Hacer que los correos vayan cifrados	Hace falta terminar y probar la librería que se está construyendo para cifrar los correos	Se deben hacer pruebas independientes para comprobar la funcionalidad del ciframiento de correos

Historia	***Para Hacer***	***Comentarios***
Hacer que los correos sean descifrados	Hace falta terminar y probar la librería que se está construyendo para descifrar los correos	Se deben hacer pruebas independientes para comprobar la funcionalidad del desciframiento de correos

Tabla 9. Trabajo pendiente de las historias al final de la cuarta semana

5. GRÁFICOS

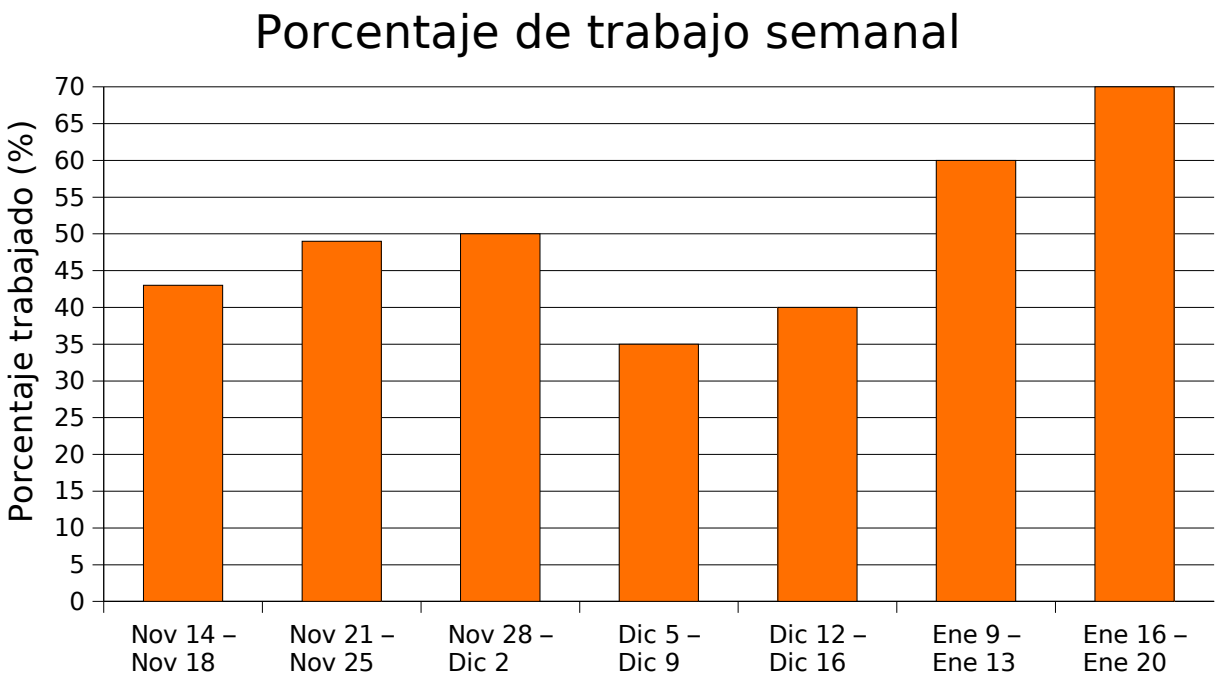


Figura 1. Porcentaje de Trabajo Semanal

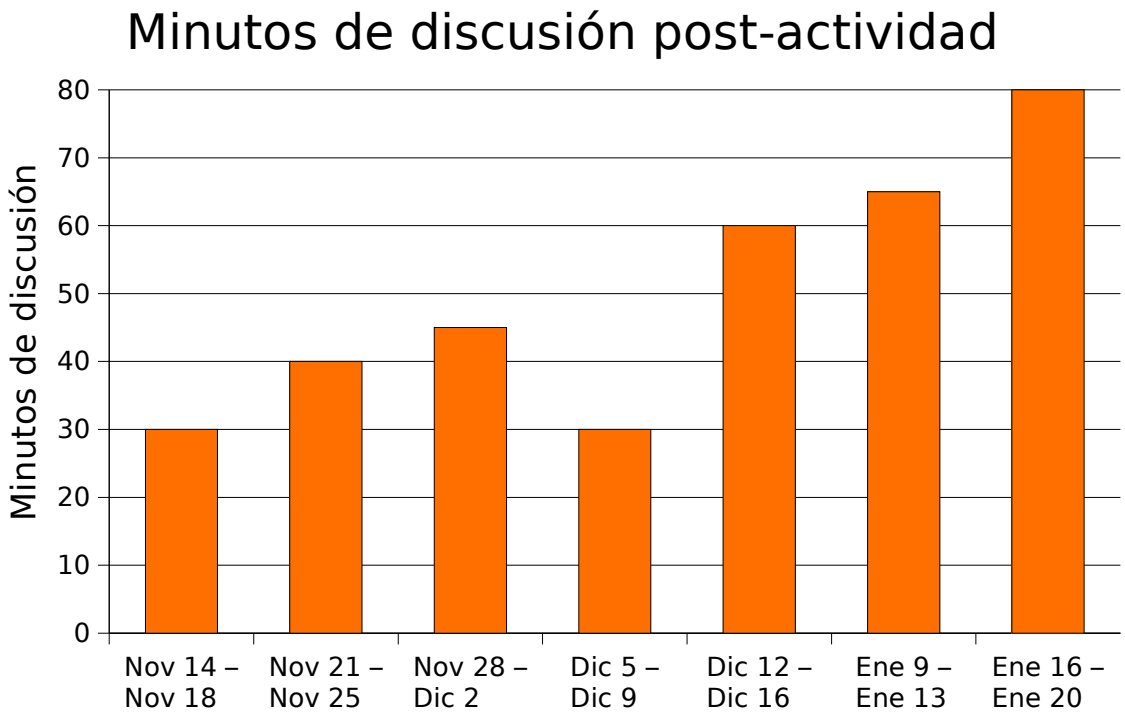


Figura 2. Minutos de Discusión Post-Actividad

6. CONCLUSIONES Y RECOMENDACIONES

- El uso de metodologías de desarrollo ágil fue un gran acierto al momento de realizar el trabajo de tomar software y mejorarlo

- Durante los periodos de tiempo que preceden las fiestas, los desarrolladores pueden sentirse agobiados por el trabajo y bajar su rendimiento laboral, por lo que en futuras iteraciones hay que buscar métodos de incentivación.

- La intensidad de trabajo se duplica y hasta triplica en los días anteriores a la entrega de la primera versión alfa.

- Los únicos elementos que garantiza el éxito de un proyecto de desarrollo de software es la actitud, la aptitud y el buen trabajo en equipo.

- El éxito de un buen proyecto de desarrollo de software que ha utilizado alguna metodología de desarrollo ágil es: "Libera rápido, libera frecuentemente" (Release early, release often)[3].

3 RAYMOND, Eric. La catedral y el bazar. <http://www.catb.org/~esr/writings/cathedral-bazaar/cathedral-

- Las historias son una forma eficiente para hacer entender al cliente el funcionamiento del software.

- Entre más se acerca el día de la entrega, se discuten más aspectos de la implementación de las historias.

bazaar/ar01s04.html>

ANEXO C

ANÁLISIS DE RIESGOS DE LA ENTIDAD DE CERTIFICACIÓN DE LA UNIVERSIDAD DEL CAUCA

El análisis de riesgos considera una evaluación a partir de la identificación de amenazas, vulnerabilidades, un análisis del impacto y una determinación del riesgo con medidas expresadas de forma cualitativa o cuantitativa.

Este documento está diseñado para capturar los riesgos potenciales en la implementación y funcionamiento de la Entidad de Certificación en la Universidad del Cauca.

Este identifica, en un orden de prioridad decreciente, los eventos que podrían llevar a un resultado negativo. A partir de una lista de riesgos que se puede mantener a través de todo el proyecto, se crea desde una fase temprana y se actualiza continuamente a medida que nuevos riesgos se descubran y a medida que los riesgos existentes sean mitigados.

Los riesgos se organizan en una tabla junto con su magnitud, descripción, impacto y estrategias de contingencia.

Las siguientes convenciones son necesarias:

Magnitud: Los riesgos están en un rango de 1 a 10, 1 es el riesgo más bajo y 10 el más alto. El rango se basa en qué tan crítico es el riesgo y su probabilidad de ocurrencia.

Descripción: Una descripción corta del riesgo identificado.

Impacto:

C - Crítico (Afecta absolutamente todas las funcionalidades)

A - Alto (Afecta la mayoría de las funcionalidades del producto)

M - Medio (Estos riesgos son sujetos a contingencias, pero la mayoría de las veces un plan se puede establecer para evitar el riesgo.

B - Bajo (Riesgos a los que un plan de contingencia rápido puede ser implementado. Usualmente se decide vivir con ese riesgo como una pequeña contingencia)

Mitigación/Contingencia: El plan para realizar, evitar o transferir los riesgos.

Riesgo: Mal Funcionamiento de la CA y la RA			
Magnitud	Descripción	Impacto	Estrategia de Mitigación
6	Problemas hardware y software por errores en instalaciones e implementaciones de la CA o de la RA	A	Implementar buenos analizadores de errores, de logs del sistema y constantemente revisar el funcionamiento de la CA o de la RA.

Tabla 1. Mal Funcionamiento de la CA y la RA

Riesgo: Acceso Inseguro a las Bases de Datos			
Magnitud	Descripción	Impacto	Estrategia de Mitigación
7	Los servicios que utilicen las bases de datos que intercambian información con la Autoridad de Certificación pueden permitir el acceso a información confidencial como las llaves privadas.	M	Se debe restringir el acceso a las bases de datos que interactúan con la Autoridad de Certificación.

Tabla 2. Acceso Inseguro a las Bases de Datos

Riesgo: Falta de Documentación			
Magnitud	Descripción	Impacto	Estrategia de Mitigación
7	La falta de documentación disponible relacionada con la Entidad de Certificación como instalación, configuración, formatos y estándares que implementa, etc.	A	Constantemente se debe actualizar la documentación disponible sobre como instalar, configurar y restaurar la Autoridad de Certificación.

Tabla 3. Falta de Documentación

Riesgo: Desaparición de Administrador de la CA			
Magnitud	Descripción	Impacto	Estrategia de Mitigación
2	-Fallecimiento, -enfermedad, -invalidez, -imposibilidad de cumplir con el trabajo por sanciones de la ley, -secuestro	A	Guardar la contraseña de Administrador en una caja de seguridad, cuya llave la guarde la empresa de seguridad contratada por la Universidad y solo puede ser solicitada por escrito por el representante legal de la Universidad (Rector)

Tabla 4. Desaparición de Administrador de la CA

Riesgo: Vulneración de la RA			
Magnitud	Descripción	Impacto	Estrategia de Mitigación
8	La RA puede ser vulnerada por medio de ataques informáticos por su contacto con la red de comunicaciones de la Universidad. Con la CA no ocurre ésto porque se encuentra separada físicamente.	A	Auditorías y actualizaciones de seguridad a las RA, uso de firewalls, VPNs y canales seguros de comunicación con las interfaces de administración.

Tabla 5. Vulneración de la RA

Riesgo: Personal Desactualizado y Administración sin Experiencia			
Magnitud	Descripción	Impacto	Estrategia de Mitigación
2	El rápido cambio tecnológico puede significar que la administración y el personal no comprendan completamente la naturaleza de la nueva tecnología o las actualizaciones que se realicen	B	Desarrollo del entrenamiento y capacitación como un proceso continuo. Desde la planeación se debe pensar en el entrenamiento.

Tabla 6. Personal Desactualizado y Administración sin Experiencia

Riesgo: Sistemas Obsoletos			
Magnitud	Descripción	Impacto	Estrategia de Mitigación
4	Retardos o interrupciones en la generación de los certificados, de las llaves públicas y privadas, y en la firma del certificado. Deficiencias en la integridad del sistema.	M	Revisiones regulares de las capacidades existentes en el hardware y software. Asignación de responsabilidades para actualizaciones a los sistemas y equipos.

Tabla 7. Sistemas Obsoletos

Riesgo: Registro de Usuarios Deficiente			
Magnitud	Descripción	Impacto	Estrategia de Mitigación
3	Empleados encargados de registrar a los usuarios en la RA pueden no entregar correctamente la petición de firmado para la Autoridad de Certificación o deficiencias en la forma de transporte de la petición.	B	Auditoría del desempeño de los empleados y de la forma como se transportan las peticiones hacia la Autoridad de Certificación

Tabla 8. Registro de Usuarios Deficiente

Riesgo: Suplantación de Nuevos Usuarios			
Magnitud	Descripción	Impacto	Estrategia de Mitigación
3	Los certificados se expiden a nombre de la Universidad y podrían darse a sus usuarios sin una identificación de identidad adecuada	M	Implementar medidas y controles de seguridad apropiados, realizar verificación de identidad de los usuarios de forma estricta.

Tabla 9. Suplantación de Nuevos Usuarios

Riesgo: Acceso Físico Violento a la CA			
Magnitud	Descripción	Impacto	Estrategia de Mitigación
5	Para robar las llave privadas o para vulnerar los equipos de la Universidad, o para robar equipos vitales para la Entidad de Certificación.	A	Aislar las instalaciones físicas de la RA y de la CA. Mejorar las restricciones de entrada a éstas instalaciones. Aumentar la vigilancia y seguridad de las instalaciones.

Tabla 10. Acceso Físico Violento a la CA

Riesgo: Acceso no Autorizado al Sistema (RA)			
Magnitud	Descripción	Impacto	Estrategia de Mitigación
8	-Acceso sin autorización a los sistemas internos -Información confidencial interceptada -Inyección de virus en el sistema(RA o CA) -Corrupción de datos y del sistema de forma deliberada.	A	Vigilancia y pruebas de penetración por vulnerabilidades, uso de firewalls, técnicas de ciframiento, autorización apropiada a los usuarios finales, y chequeo periódico de virus.

Tabla 11. Acceso no Autorizado al Sistema (RA)

Riesgo: Fraude del Personal			
Magnitud	Descripción	Impacto	Estrategia de Mitigación
5	Alteración de los datos por parte de empleados con acceso a la RA y a la CA, o robo de información específica como la llave privada.	M	Desarrollo de políticas para empleados nuevos. Controles internos institucionales, incluyendo segregación de tareas, auditoría del desempeño de los empleados

Tabla 12. Fraude del Personal

Riesgo: Desastres Naturales			
Magnitud	Descripción	Impacto	Estrategia de Mitigación
1	La ocurrencia de desastres naturales como terremotos, inundaciones, etc, sobre la Universidad del Cauca, donde se ubica la Entidad de Certificación	C	Backups (a la llave privada no se puede hacer backup por motivos legales) y otros servidores que puedan suplir la Entidad de Certificación y se ubiquen en otra instalación.

Tabla 13. Desastres Naturales

ANEXO D
ESTUDIO DE INGENIERÍA DE LA ENTIDAD DE CERTIFICACIÓN DE LA UNIVERSIDAD DEL CAUCA

1. INTRODUCCION

En el presente documento se pretende realizar el estudio técnico para la construcción de la Entidad de Certificación de la Universidad del Cauca y es el resultado del análisis del Plan de Proyecto y del Análisis de Riesgos.

La idea es construir una Entidad de Certificación que soporte inicialmente el servicio de correo electrónico certificado, y sea capaz de soportar a futuro, servicios de gestión de certificados de servidor web seguro y firma segura de documentos.

El presente documento está compuesto de dos grandes secciones. La primera llamada *Análisis de Requerimientos*, es donde se van a plantear los diferentes requerimientos técnicos, con los que debe cumplir la solución hardware/software de PKI.

En la segunda sección se realizará el diseño de la arquitectura PKI, así como una breve descripción del proceso de certificación en la Universidad del Cauca.

2. ANÁLISIS DE REQUERIMIENTOS

2.1. REQUERIMIENTOS GENERALES

- La Entidad de Certificación debe ser construida en un ambiente 24x7, donde los servicios se encuentran disponibles a todo momento.
- Todos los productos comprados y sus componentes (Hardware y Software) deben tener una garantía mínima de un año, después de la implementación.
- La solución propuesta debe incluir herramientas para integrarse con productos complementarios dentro de la PKI, según las necesidades del cliente.
- La solución propuesta debe permitir a la organización emitir y revocar llaves mapeadas en objetos X.500

- La capacidad de gestión de certificados debe mantener y distribuir certificados X.509 para asegurar las comunicaciones entre cualquier entidad que soporte la PKI.
- La solución propuesta debe asegurarse que las contraseñas no vayan a ser transmitidas en "texto plano" a través de la red o que vayan a ser almacenados sin ningún tipo de seguridad.
10. La arquitectura debe basarse en estándares y soportar al menos: X509v3, LDAP, PKCS #11 y S/MIME

2.2. REQUERIMIENTOS ADMINISTRATIVOS

- La solución PKI debe proveer la personalización de las funciones administrativas de la Entidad de Certificación.

- La solución debe incluir un plan de recuperación de llaves y que no comprometa la organización legalmente.

- La solución debe proveer mecanismos para la separación administrativa de funciones para garantizar la seguridad de los datos más importantes.

- La solución debe dar la posibilidad de ver el estado las transacciones por medio de herramientas de generación de reportes.

2.3. REQUERIMIENTOS DE LAS APLICACIONES DE GESTIÓN

- La solución debe dar la posibilidad de extender su dominio de confianza a través de otras autoridades de certificación de manera jerárquica o distribuida.

- La solución debe dar la posibilidad de instalar múltiples Autoridades de Registro para ejecutar funciones administrativas en la PKI.

- La solución debe tener mecanismos de generación de reportes para los usuarios finales y para los administradores.

- La solución debe dar la posibilidad de escoger entre varios tipos de certificados en la misma infraestructura y que puedan ser enviados a diferentes usuarios con diferentes perfiles.

- La solución debe estar provista de confidencialidad, integridad, aceptación, identificación, autenticación y autorización.

- La solución debe tener soporte para USB tokens, tarjetas inteligentes, dispositivos biométricos y

otros dispositivos de autenticación.

2.4. REQUERIMIENTOS DE LOS CERTIFICADOS PKI

- La solución debe brindar una interfaz de usuario amigable e intuitiva para gestionar los certificados digitales

- La solución debe tener la posibilidad de emitir certificados internamente, y externamente a otras entidades y clientes.

- La solución debe tener soporte para el uso de extensiones personalizadas y que puedan ser incluidas en los certificados emitidos por la Entidad de Certificación.

- La solución debe contar con la posibilidad de consulta de certificados digitales de los usuarios.

2.5. REQUERIMIENTOS DE LAS LLAVES

- La solución debe contar con la funcionalidad de recuperación de llaves, tanto a nivel de usuario como a nivel de administración.

- La solución debe almacenar con seguridad la llave privada de firmado de la Autoridad de Certificación raíz y sus subordinados.

2.6. REQUERIMIENTOS DEL DIRECTORIO

- La solución debe ser capaz de integrarse con otros directorios existentes y de otros fabricantes y poder compartir sus nombres y atributos.

2.7. OTROS REQUERIMIENTOS

- La solución debe estar basada en estándares abiertos.

- La solución debe brindar el código fuente.

3. ARQUITECTURA DE LA ENTIDAD DE CERTIFICACIÓN

3.1. DESCRIPCIÓN DE LA ARQUITECTURA

La arquitectura de la Entidad de Certificación de la Universidad del Cauca va a ser *jerárquica* y constará de una Autoridad de Certificación que no va a ser accedida por los clientes y que se encontrará totalmente aislada de la red de datos.

Inicialmente se contará con una única Autoridad de Registro, que va a ser la encargada de emitir, revocar y gestionar los certificados de los usuarios de cada una de las dependencias que solicite un certificado digital.

Se proyecta en un mediano plazo, descentralizar la administración de los certificados, y así poner catorce Autoridades de Registro a lo largo de la Universidad. Las catorce RAs previstas, corresponderían a las catorce Unidades Organizacionales (OU) del Servidor de Directorio.

La Entidad de Certificación contará con un Directorio Organizacional, basado en OpenLDAP, donde se almacenarán los datos de los certificados y además, con un motor de base que servirá de soporte para funciones intermedias y así no saturar el servidor de directorio. La base de datos escogida fue MySQL.

La Entidad de Certificación, se encontrará en una zona desmilitarizada (DMZ), aislada por un firewall externo. Además contará con un firewall personalizado en su configuración.

Una visión de la arquitectura de la Entidad de Certificación es la siguiente:

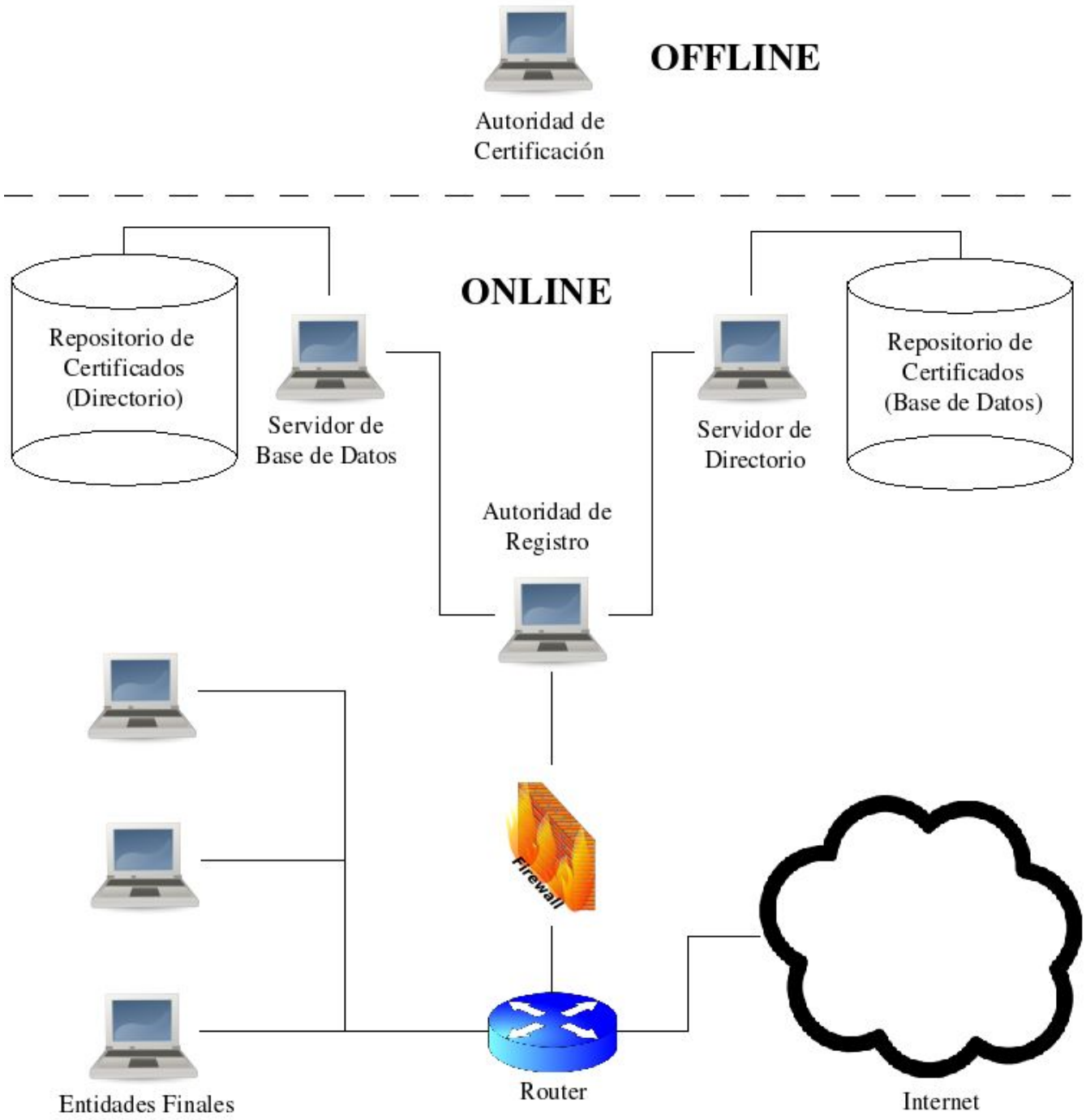


Figura 1. Arquitectura de la Entidad de Certificación de la Universidad del Cauca

3.2. DESCRIPCIÓN DEL PROCESO DE CERTIFICACIÓN

El proceso de certificación consistirá de los siguientes pasos:

1. El usuario solicitará el certificado digital, llenando el formulario de solicitud de prestación de servicios de identificación digital y presentando una copia del carné de vinculación a la Universidad y una copia de la cédula de ciudadanía.

2. El usuario recibirá la Declaración de Prácticas de Certificación y firmará un contrato de cumplimiento de las claúsulas descritas en éllas.

3. En un plazo de 5 días hábiles, se le será creado el perfil al usuario y se le serán asignados dos certificados digitales, acompañados por dos llaves privadas: una para la realización de procesos de firmado digital y la otra para fines de ciframiento de datos.

4. El usuario recibirá un correo con el manual de uso de su certificado digital y los diferentes servicios de identificación digital con los que cuenta.

NOTA: Dependiendo del tiempo de validez del certificado, éste tendrá que ser renovado cada cierto periodo.

4. CONCLUSIONES Y RECOMENDACIONES

1. Los requerimientos pueden ir cambiando, conforme va creciendo el proyecto. Parte de la planeación es saber prever estos requerimientos futuros.

2. La arquitectura planteada carece de un detector de intrusos (IDS). Se debe planear a futuro la incursión de éste.

3. Es realmente conveniente el uso de un espejo del repositorio de certificados digitales para uso de funcionalidades secundarias y para ser explotada por los servicios de identificación digital.

4. Se podría pensar en la refactorización de la aplicación software encargada de administrar la PKI. Sería interesante mejorar la interfaz de usuario, o agregarle nuevas funcionalidades.

ANEXO E
DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN

1. Introducción

1.1. ¿Qué es la Entidad de Certificación de la Universidad del Cauca?

La **Entidad de Certificación de la Universidad del Cauca**, es un ente de la Universidad del Cauca encargado de realizar la certificación de personas académicas, dentro de la institución, con el objetivo que éstas puedan realizar comunicaciones donde se garantice la integridad y la autenticidad.

1.2. ¿Qué certificados digitales expide la Entidad Certificación de la Universidad del Cauca?

La Entidad de Certificación de la Universidad del Cauca expide el siguiente certificado:

a) Certificado de correo electrónico certificado

Se expide a las personas académicas que deseen enviar correo certificado por la Entidad de Certificación con el fin de garantizar la identidad del emisor. También este servicio incluye la opción de ciframiento del correo electrónico.

1.3. Cuál es el tiempo de vigencia de un Certificado Digital?

El tiempo de vigencia de un certificado digital varía, dependiendo del usuario. De esta manera se han establecido los tiempos de vigencia así:

a) Certificados digitales para **Entidades Adscritas: 1 año.**
b) Certificados digitales para **Grupos de Investigación: 1 año.**
c) Certificados digitales para **Docentes Pensionados: 1 año.**
d) Certificados digitales para **Funcionarios Pensionados: 1 año.**
e) Certificados digitales para **Estudiantes de Pregrado: 6 meses.**
f) Certificados digitales para **Estudiantes de Posgrado: 1 año.**
g) Certificados digitales para **Contratistas: 6 meses.**
h) Certificados digitales para **Docentes Pensionados: 1 año.**

i) Certificados digitales para **Dependencias: 1 año.**
j) Certificados digitales para **Eventos: 6 meses.**
k) Certificados digitales para **Funcionarios: 1 año.**
l) Certificados digitales para **Egresados: 6 meses.**
m) Certificados digitales para **Grupos de Actividades: 6 meses.**

Al finalizar el periodo de vigencia del certificado, éste se podrá renovar. En caso que no sea renovado, éste será publicado en las listas de certificados revocados (CRL) de la entidad de certificación.

1.4. Qué se debe saber para usar un Certificado Digital?

Para usar un certificado, se debe saber:

a) La actividad de certificación digital es una actividad seria donde un tercero, conocido como **Entidad de Certificación** garantiza la identidad del emisor de un mensaje en una comunicación. Por ende, se debe ser cuidadoso con el manejo de contraseñas y las políticas de uso del certificado.

b) El documento donde se definen las políticas de uso del certificado se llama **Declaración de Prácticas de Certificación** y es obligación del usuario leer este documento antes de realizar la solicitud de cualquier servicio de identificación digital. El uso del certificado digital significa que el usuario acepta todas las claúsulas contenidas en la **Declaración de Prácticas de Certificación**.

1.5. Datos de la Entidad de Certificación

Nombre: Entidad de Certificación de la Universidad del Cauca
Tipo de Entidad de Certificación: Cerrada
Dirección: Calle 5 No. 4-70. Sede Tulcán.
Domicilio: Popayán - Cauca
Teléfonos: 8209800
Fax: 8209800
Dirección de correo electrónico: adminca@unicauca.edu.co
Sitio de Internet: http://www.unicauca.edu.co/ca

1.6. Peticiones, quejas y reclamos

Cualquier petición, queja o reclamo frente a cualquiera de los servicios o actividades de la **Entidad de Certificación de la Universidad del Cauca**, debe dirigirse al operador de registros y llenar la

solicitud de *Petición, Queja o Reclamo*.

1.7. Qué es la Declaración de Prácticas de Certificación?

Según el decreto 1747 de 2000, la **Declaración de Prácticas de Certificación** es la manifestación de la entidad de certificación sobre las políticas y procedimientos que aplica para la prestación de sus servicios.

1.8. Intervinientes y estructura de la Entidad de Certificación

Los siguientes son los bloques funcionales de la Entidad de Certificación de la Universidad del Cauca:

1.8.1. Autoridad de Certificación
Es el ente encargado de la realización de la firma de las peticiones de certificados. Es quien garantiza la identidad del dueño del certificado digital frente al servicio de identificación digital.

1.8.2. Autoridad de Registro
Es el ente encargado de registrar la petición del certificado, por parte del *solicitante*. También es función de la **Autoridad de Registro**, llevar manualmente las peticiones de los certificados a la autoridad de certificación, para que ésta los firme.

1.8.3. Operario de la Autoridad de Registro
Es el operario de la autoridad de registro encargado de explicarle al solicitante del certificado digital las responsabilidades que se tiene y las políticas del servicio. Es quien recibe los papeles y formularios y entrega una copia de la **Declaración de Prácticas de Certificación** al *solicitante.*

1.8.4. Solicitante
Es la persona académica que aún no posee el certificado digital, pero llena los requisitos para la solicitud de uno.

1.8.5. Usuario del Sistema
Es la persona académica que posee un certificado digital vigente y acepta las condiciones de uso de éste, al firmar el contrato de uso del certificado digital, donde se compromete a cumplir las políticas de manejo del certificado digital.

2. Generalidades

2.1. Clases de Certificados

La **Entidad de Certificación de la Universidad del Cauca**, expide el siguiente tipo de certificado digital:

a) Certificado digital para Correo Electrónico

El certificado digital se rige bajo las claúsulas de la **Declaración de Prácticas de Certificación.**

2.2. Obligaciones de los intervinientes

2.2.1. Obligaciones de la Entidad de Certificación de la Universidad del Cauca

La **Entidad de Certificación de la Universidad del Cauca** tiene las siguientes obligaciones en la prestación de sus servicios:

- Implementar y mantener los sistemas de seguridad que resulten razonables en función del servicio prestado y en general la infraestructura necesaria para la prestación de los servicios de identificación digital.

- Cumplir con la Declaración de Prácticas de Certificación (DPC) y con los acuerdos de responsabilidad, y las obligaciones que asume como interviniente en el proceso de identificación digital.

- Abstenerse de usar la llave privada del usuario.

- Permitir y facilitar la realización de las auditorías por parte de la Superintendencia de Industria y Comercio de Colombia.

- Actualizar la información que tiene registrada en la solicitud de autorización ante la Superintendencia de Industria y Comercio y toda aquella que esta entidad establezca.

- Informar a la Superintendencia de Industria y Comercio la ocurrencia de cualquier evento establecido en la Declaración de Prácticas de Certificación, que comprometa la prestación del servicio.

- Mantener el control y confidencialidad de la llave privada de los usuarios y establecer mecanismos

de seguridad para que ésta no sea vulnerada.

- Prestar permanentemente y de manera ininterrumpida los servicios de identificación digital.

- Informar al usuario dentro de los siguientes 3 días hábiles, la revocación de su certificado digital.

- Remover a los administradores o representantes que resulten incursos en las causales establecidas en el literal c del artículo 29 de la Ley 527 de 1999.

LA ENTIDAD DE CERTIFICACIÓN DE LA UNIVERSIDAD DEL CAUCA NO TIENE OBLIGACIONES ADICIONALES A LAS PREVIAMENTE NOMBRADAS, NI DEBE ENTENDERSE QUE EXISTEN OBLIGACIONES IMPLÍCITAS ADICIONALES A LAS EXPRESADAS EN ESTA DECLARACIÓN DE PRÁCTICAS DE CERTIFICACIÓN.

2.2.2. Obligaciones del Usuario del Sistema

- Solicitar la revocación del certificado digital que le ha sido entregado cuando se cumpla alguno de los supuestos previstos para la revocación de los certificados digitales.

- Asegurarse de que toda la información contenida en el certificado digital es cierta y notificar inmediatamente a la Entidad de Certificación de la Universidad del Cauca en caso de que se haya incluido cualquier información incorrecta o inexacta o en caso de que por alguna circunstancia posterior la información del certificado digital no corresponda con la realidad. Así mismo, se deberá comunicar de manera inmediata el cambio o variación que haya sufrido cualquiera de los datos que aportó para adquirir el certificado digital.

- Abstenerse de monitorear, alterar, realizar ingeniería inversa o interferir en cualquier otra forma la prestación del servicio de identificación digital.

3. Proceso de Solicitud de un certificado digital

3.1. Solicitud del certificado digital

El procedimiento de expedición de un certificado digital se inicia con la solicitud que hace cualquier persona académica vinculada a la Universidad del Cauca para que le sean prestado el servicio de identificación digital. Los trámites de solicitud del servicio será el siguiente:

a) El usuario solicitará el certificado digital, llenando el formulario de solicitud de prestación de servicios de identificación digital y presentando una copia del carné de vinculación a la Universidad

y una copia de la cédula de ciudadanía.

b) El usuario recibirá la Declaración de Prácticas de Certificación y firmará un contrato de cumplimiento de las claúsulas descritas en éllas.

c) En un plazo de 5 días hábiles, se le será creado el perfil al usuario y se le serán asignados dos certificados digitales, acompañados por dos llaves privadas: una para la realización de procesos de firmado digital y la otra para fines de cifrамiento de datos.

d) El usuario recibirá un correo con el manual de uso de su certificado digital y los diferentes servicios de identificación digital con los que cuenta.

NOTA: Dependiendo del tiempo de validez del certificado, éste tendrá que ser renovado cada cierto periodo.

3.2. Listas de certificados revocados (CRL)

El registro de los certificados digitales emitidos, se encontrarán disponibles al público para verificar la vigencia de un certificado digital.

La actualización de estas listas de certificados revocados será actualizada cada 24 horas y será accesible desde:

http://www.unicauca.edu.co/ca/ca.crl

4. Reglas de uso de los certificados digitales

4.1. Reglas generales

- El usuario sólo puede dar a los certificados digitales los usos que se especifican en esta Declaración de Prácticas de Certificación. Cualquier otro uso que se le dé se considerará una violación de ésta y constituirá una causal de revocación del certificado digital y de terminación del contrato con el suscriptor, sin perjuicio de las acciones penales o civiles a las que haya lugar.

- El usuario considera y acepta que los productos y servicios que se anuncian son tal y como se ofrecen individualmente, que no existe ningún tipo de información implícita que implique servicios o prestaciones adicionales a las expresadas y que la utilización de los mismos es de su exclusiva responsabilidad.

- Si durante el periodo de vigencia parte o toda la información contenida en el certificado digital pierde actualidad o validez, el usuario deberá iniciar el procedimiento de revocación del mismo de conformidad a lo establecido en la sección de Revocación de certificados digitales de esta Declaración de Prácticas de Certificación..

- Los certificados digitales deberán utilizarse tal y como son suministrados por la Entidad de Certificación de la Universidad del Cauca. Se encuentra terminantemente prohibido cualquier alteración de los mismos, sin excepción alguna.

4.2. Prohibiciones

- Los certificados digitales no podrán ser utilizados por ninguna persona y bajo ninguna circunstancia para fines u operaciones ilícitas.

- Se encuentra terminantemente prohibido cualquier uso de los certificados digitales que resulte contrario a la legislación colombiana, a las buenas costumbres, a las sanas prácticas comerciales y a todas las normas contenidas en esta Declaración de Prácticas de Certificación.

- Los certificados digitales no podrán utilizarse en ningún sistema cuyo fallo pueda ocasionar la muerte o lesión de personas y ocasionar un serio perjuicio al medio ambiente.

5. Revocación de los certificados digitales

La revocación de un certificado digital es el mecanismo por el que se dá por terminado el periodo de confiabilidad de éste.

5.1. Causales de revocación

5.1.1. Revocación voluntaria por parte de usuario

El usuario podrá voluntariamente solicitar a la Entidad de Certificación de la Universidad del Cauca la revocación del certificado digital emitido, en cuyo caso la Entidad de Certificación de la Universidad del Cauca iniciará el procedimiento de revocación del certificado digital.

5.1.2. Otros causales de revocación del certificado

La Entidad de Certificación de la Universidad del Cauca revocará el certificado digital respecto del

cual tenga conocimiento que se ha producido alguno de los siguientes hechos:

- Muerte o incapacidad del usuario.
- Por la confirmación de que alguna información o hecho contenido en el certificado digital es falso, así como la ocurrencia de hechos nuevos que provoquen que los datos originales no concuerden con la realidad.
- Por el cese de actividades de la Entidad de Certificación de la Universidad del Cauca, salvo que los certificados expedidos sean transferidos a otra Entidad de Certificación.
- Por orden judicial o de entidad administrativa competente.
- Por cualquier causa que induzca a creer el servicio de identificación digital haya sido comprometido hasta el punto que se ponga en duda la confiabilidad del certificado digital.
- El manejo indebido por parte del usuario del certificado digital.

5.2. Efectos de la revocación de un certificado

El efecto de la revocación del certificado digital es la pérdida de confiabilidad del mismo, originando el cese permanente de la operatividad de éste conforme a los usos que le son propios y, en consecuencia, de la prestación de los servicios de identificación digital.

Una vez cumplido el procedimiento de revocación, el certificado digital será publicado en la lista de certificados revocados (CRL), para notificar al público que dicho certificado ha sido revocado.

5.3. Procedimiento para la revocación

El usuario o cualquier tercero que tenga conocimiento de la existencia de las causales que dan lugar a la revocación de un certificado digital, podrá informar a la Autoridad de Registro para que la evalúe y proceda de conformidad con el procedimiento establecido.

El tercero que inicie un procedimiento de revocación de certificados digitales será el único responsable de los perjuicios que produzca dicha revocación al usuario y a terceros de buena fe.

Las autoridades judiciales o administrativas podrán, en aquellos casos contemplados en la ley, ordenar a la Entidad de Certificación de la Universidad del Cauca la revocación de cualquier certificado digital.

En caso que un usuario del servicio de identificación digital, desee la revocación de su certificado digital, deberá regirse bajo los siguientes parámetros:

- La solicitud de revocación de certificados digitales podrá hacerse telefónicamente llamando a

cualquier de los números que la Entidad de Certificación de la Universidad del Cauca ha destinado para el efecto.
- Si la persona que expone la revocación del certificado digital no es el usuario o en caso que éste no se identifique satisfactoriamente, deberá dirigirse personalmente a la Autoridad de Registro para la realización del trámite de revocación.

6. Terminación de la vigencia del certificado

- La vigencia de los certificados digitales terminará por el transcurso del periodo operacional del mismo, el cual se especifica en éste.
- La terminación de la vigencia del certificado digital producirá el cese permanente de su operatividad conforme a los usos que le son propios y, en consecuencia, de la prestación de los servicios de identificación digital.
- La terminación de la vigencia de un certificado digital impide el uso legítimo del mismo por parte del suscriptor, o de cualquier otra persona.

7. Renovación de los certificados digitales

- La Entidad de Certificación de la Universidad del Cauca notifica con al menos un (1) mes de anticipación a los usuarios la terminación de la vigencia del certificado digital. Esta notificación puede realizarse por correo electrónico o por cualquier otro medio de comunicación.

- Si el usuario desea renovar el certificado digital, debe diligenciar de nuevo el formulario de prestación del servicio de identificación digital. Este documento puede ser enviado de manera electrónica o de manera física.

- La Entidad de Certificación de la Universidad del Cauca verificará el formulario de prestación del servicio de identificación digital y de encontrarlo ajustado a sus políticas de certificación, realizará el procedimiento para la expedición de las llaves y los certificados, de acuerdo al numeral 3.1

- La Entidad de Certificación de la Universidad del Cauca se reserva el derecho de solicitar información o documentos adicionales para confirmar la identidad o cualquier otra información suministrada por el usuario de la renovación. Así mismo, se reserva el derecho de renovar nuevamente la totalidad de la información presentada.