ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

Maestría en Seguridad Informática Aplicada (MSIA)

"IMPLEMENTACIÓN DE CERTIFICADOS Y FIRMAS DIGITALES PARA SISTEMAS DE INFORMACIÓN TRANSACCIONALES EN UNA EMPRESA GUBERNAMENTAL."

TESIS DE GRADO

Previo a la obtención del título de:

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

JOHN GUILLERMO PALOMEQUE AVILA

GUAYAQUIL - ECUADOR

AÑO: 2015

AGRADECIMIENTO

El presente trabajo de tesis primeramente me gustaría agradecer a Dios por bendecirme, y ser mí guía diaria. A mi familia por brindarme el apoyo necesario, ser el pilar fundamental de mi carrera profesional, y ser mi motivo de lucha constante. A mi directora de tesis por permanecer siempre atenta a mis consultas, en fin a las personas que han estado siempre empujando y colaborando para seguir adelante buscando obtener mis metas planteadas.

DEDICATORIA

Dedico este proyecto de tesis a Dios y a mis padres. A Dios porque ha estado conmigo a cada paso que doy, cuidándome y dándome fortaleza para continuar, a mis padres, quienes a lo largo de mi vida han velado por mi bienestar y educación siendo mi apoyo en todo momento. Depositando su entera confianza en cada reto que se me presentaba sin dudar ni un solo momento en mi inteligencia y capacidad. Es por ello que soy lo que soy ahora. Los amo con mi vida

TRIBUNAL DE SUSTENTACIÓN

Ing. Lenin Freire Cobo

Coordinador MSIA

Presidente

Ing. Karina Astudillo

Director del Proyecto de Graduación

Ing. Robert Andrade

Miembro del Tribunal

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de esta Tesis de Grado, nos corresponde exclusivamente; y el patrimonio intelectual del mismo a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL".

Ing. John Palomeque Avila

RESUMEN

En el capítulo 1, se expone el ámbito teórico de la tesis, este contempla conceptos de organización, tipos de organizaciones y sus procesos; además presenta el significado de sistemas de información en los cuales se involucra la firma digital; permite conocer detalles de certificados digitales, firmas digitales, el uso, los organismos relacionados y leyes entre otros aspectos.

En el capítulo 2, presenta el análisis de procesos diseñados de una organización de gobierno para implementar el procedimiento de legalización de documentos mediante el uso de firma digital; expone propuesta de solución enfocándose en objetivos específicos para su implementación.

El capítulo 3, presenta la implementación de la solución expuesta en el capítulo anterior, permite conocer la infraestructura tecnológica de forma general, un esquema de seguridad generalmente utilizado en los sistemas de información basado en roles y permisos; el uso de los mecanismos de almacenamiento para la firma digital como es el token.

El capítulo 4, presenta el análisis de resultados, usando mecanismos de verificación y consulta en el sistema transaccional asociado al uso de la firma, indicadores de control, etc. permite conocer estadísticas de resultados. En este capítulo se exponen las observaciones realizadas en la

implementación de la solución, permite conocer los diferentes aspectos hallados, además de las mejoras que se requieren realizar. Este capítulo brinda el soporte necesario para determinar las conclusiones y recomendaciones del tema en estudio.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

ESP	ENTRUST SECURITY PROVIDER, Aplicativo para almacenamiento de certificados digitales para mecanismo ROAMING de la ECIBCE.
ECIBCE	Siglas de la Entidad de Certificación del Banco Central del Ecuador.
FRAMEWORK	Describe un ambiente de trabajo que conlleva estándar, políticas y lenguaje de programación entre otros, generalmente son herramientas versionadas.
HSM	Siglas de “HARDWARE SECURITY MODULE” (MODULO DE SEGURIDAD HARDWARE)
JAVA	Lenguaje de programación para aplicaciones empresariales, orientado a objetos
JBOSS/WILDFLY	Servidor de Aplicaciones Web.
PRIMEFACES	Herramientas de desarrollo para JAVA, incluye librerías de programación web.
USHAY	Termino en Idioma Quechua, Significa Facil.

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

Los sistemas transaccionales son herramientas de apoyo de uso cotidiano en el operar y gestionar de las organizaciones, colaborando en las labores funcionales de los empleados y mejorando su desempeño laboral. A través de la estructura organizacional se trasmite información por diversos medios de forma unidireccional o bidireccional, empleando jerarquías o lateralizando el entorno brindando control y seguimiento a la operatividad de los procedimientos y procesos; como consecuencia las organizaciones se han vuelto dependiente del manejo de herramientas que automaticen sus procesos, brindando agilidad y optimizando el uso de los recursos en la cadena logística, cadenas de distribución, control en la elaboración de servicios o bienes, agregando valor, por ende siendo fuentes de información para la toma de decisiones.

La significativa cantidad de información se extiende a un manejo burocrático desmesurado de documentos que existen en las operaciones u procesos con la finalidad de garantizar la calidad, la agregación de valor satisfactoria a un cliente o el simple hecho de controlar el camino correcto de un proceso o procedimiento; tal es el caso de los bancos con los procedimientos para la adjudicación de préstamos financieros a sus clientes, el registro de varios documentos con la legalización de los mismos, e inclusive en algunos casos notariados.

El tema aquí expuesto nos permite analizar esta situación, enfocándonos en un sistema transaccional que controla la adquisición de bienes y/o servicios en una

empresa pública y establecer una solución para la legalización de documentos, mediante la implantación de firma digital.

PROBLEMA

La Implantación de los diversos sistemas transaccionales, sistemas de tomas de decisión, sistemas de control, entre otros en el mercado, han generado beneficios para el desempeño de las labores cotidianas de las empresas, pero al mismo tiempo que se gana con la implementación de tales soluciones, las organizaciones se han visto envueltas en nuevos retos y nuevas mejoras por implementarse; las empresas están orientadas a buscar la calidad total en sus procesos y procedimientos con el fin de lograr mejores rendimientos en sus metas u objetivos.

Considerando para nuestro tema la organización pública que mantiene procesos y procedimientos inmersos en diversas situaciones, no solo conlleva la continua tarea de orientarse en la mejora de los mismos, sino además de ser lo más acertado posible en la decisión que se tome para las garantías que se requieren en tales procesos, considerándose las regulaciones, obligaciones, leyes, disposiciones, reglamentos internos que emiten cambios u modificaciones operacionales además la cultura del talento humano y el control de su desempeño.

Es continua la diversidad de documentos que se visualiza pasar de escritorio en escritorio en cada sitio de trabajo, por sencillo que parezca se mantiene el nivel y el control de legalización por órdenes y disposiciones externas a la organización, además del control interno, sin embargo en algunas situaciones entorpecen o retrasan los procesos, ante la avalancha de documentos que se genera; se

manifiesta la necesidad de formar parte de la tendencia “cero papeles”; abriendo el control virtual de documentación mediante “flujos de trabajo”, sin embargo existen brechas o campos de análisis por cruzar para cumplir este objetivo, entre ellos: legislación que la pueda soportar y conocimiento de sus directivos, además de la socialización entre sus usuarios.

Se considera para el análisis y evaluación a uno de los procesos de la cadena logística de la empresa gubernamental como es “La adquisición”. Se considera que la cadena logística inicia con la “necesidad” de un bien o servicio, la necesidad se puede convertir en la “adquisición” de NO encontrar lo requerido en las existencias del inventario, para finalizar en la “recepción” de lo necesitado; existen variantes en las organizaciones para la ejecución del proceso de adquisición, pero cabe mencionar que se rigen bajo las directrices que emite las normas de control interno de la CONTRALORÍA GENERAL DEL ESTADO.

Durante el ciclo logístico existen documentos y responsables según las normas de control interno para elaborar o definir la “necesidad”, de igual manera la “recepción”, “adquisición” y “distribución” en cada unidad de la organización. [1]

CAPÍTULO 1

SISTEMAS DE INFORMACIÓN TRANSACCIONAL, CERTIFICADOS, FIRMAS DIGITALES, LEGALIZACIÓN DE DOCUMENTOS Y PROCESOS.

1.1 CERTIFICADO DIGITAL Y FIRMA DIGITAL

El estudio de certificados y firmas digitales permite comprender la legalización de documentos y su veracidad, además de su vinculación con la información digital en el ámbito de seguridad, facilitando el no repudio.

Según la RAE [2] el término certificado indica: “Dicho de una carta o de un paquete: Que se certifica.”, y además el concepto de certificación menciona: “Documento en el cual asegura la verdad de un hecho”. Entonces es necesario que exista alguna

entidad u organismo que brinde la certificación para el reconocimiento de miembros de una organización, y es así como nacen las Autoridades de Certificación o CA.

Una CA o autoridad de certificación es un organismo que brinda el reconocimiento de dos o más entidades como legitimas.

1.1.1 QUÉ ES UN CERTIFICADO DIGITAL Y FIRMA DIGITAL

El certificado digital es un documento emitido por una entidad denominada autoridad de certificación, el documento o archivo digital describe la identidad de un usuario (datos personales), u organismo (datos de la organización), o servicio (datos del servicio), etc. El certificado digital puede ser emitido en varios formatos de archivo, la autoridad de certificación reconoce y avala los datos expuestos en el certificado digital, a través del mecanismo de criptografía de clave pública (de dos claves) o infraestructura de clave pública (***P****ublic* ***K****ey* ***I****nfrastructure*) brindando garantías para su uso.

La infraestructura de clave pública es un mecanismo que involucra hardware, software, políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptográficas como el cifrado, la firma digital o el no repudio de transacciones electrónicas.

La infraestructura de clave pública, permite que las entidades se autentiquen o se reconozcan con otras entidades a través de los certificados digitales o de identidad, además permite cifrar o descifrar mensajes, firmar digitalmente información, y garantiza el no repudio.

Los componentes más habituales de una infraestructura de clave pública son:

La autoridad de certificación (o, en inglés, CA, Certificate Authority): es la encargada de emitir y revocar certificados. Es la entidad de confianza que da legitimidad a la relación de una clave pública con la identidad de un usuario o servicio.

La autoridad de registro (o, en inglés, RA, Registration Authority): es la responsable de verificar el enlace entre los certificados (concretamente, entre la clave pública del certificado) y la identidad de sus titulares.

Los repositorios: son las estructuras encargadas de almacenar la información relativa a la PKI. Los dos repositorios más importantes son el repositorio de certificados y el repositorio de listas de revocación de certificados. En una lista de revocación de certificados (o, en inglés, CRL, Certificate Revocation List) se incluyen todos aquellos certificados que por algún motivo han dejado de ser válidos antes de la fecha establecida de uso dentro del mismo certificado.

La autoridad de validación (o, en inglés, VA, Validation Authority): es la encargada de comprobar la validez de los certificados digitales.

La autoridad de sellado de tiempo (o, en inglés, TSA, TimeStamp Authority): es la encargada de firmar documentos con la finalidad de probar que existían antes de un determinado instante de tiempo.

Los usuarios y entidades finales son aquellos que poseen un par de claves (pública y privada) y un certificado asociado a su clave pública. Utilizan un conjunto de

aplicaciones que hacen uso de la tecnología PKI (para validar firmas digitales, cifrar documentos para otros usuarios, etc.)

La firma digital es el mecanismo de criptografía de clave pública que permite brindar seguridad al receptor del documento firmado digitalmente; la firma digital emplea la clave privada del remitente para cifrar la información a enviar y el receptor emplea la clave pública del remitente para descifrarla, así se garantiza la autenticidad del origen de la información, y se verifica que ésta no ha sido modificada desde su creación.

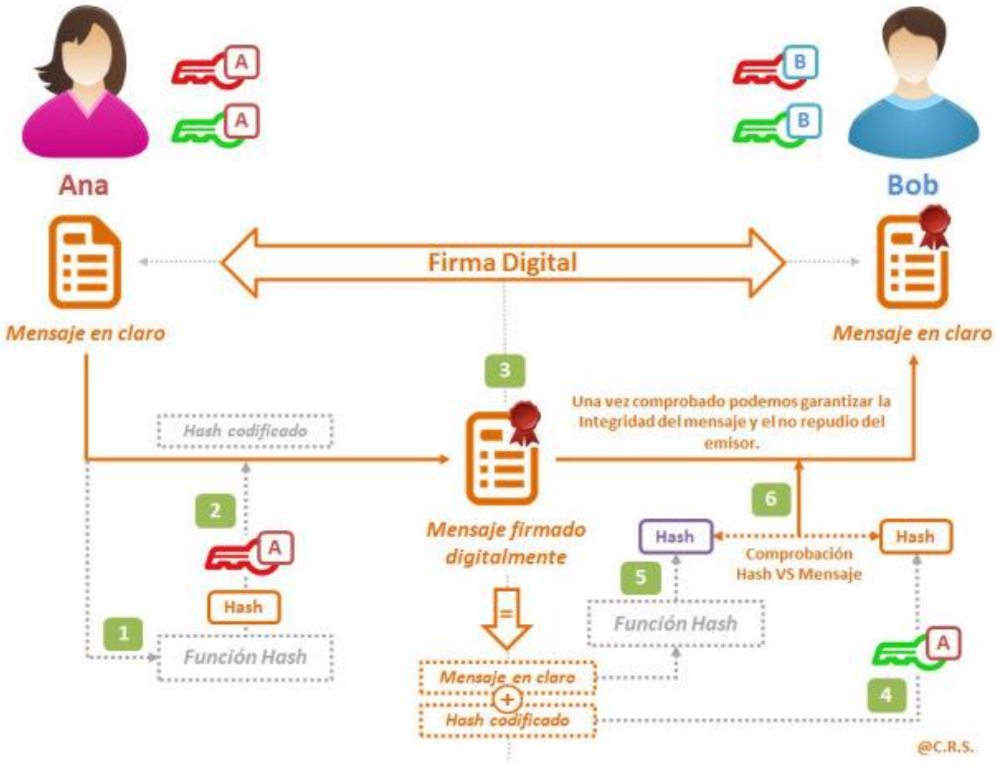

Figura 0.1 FIRMA DIGITAL (Secure-IT)

La imagen es tomada de https://securitcrs.wordpress.com/criptografia/criptografia-asimetrica-clave-privada-y-clave-publica/.

Según la SENATEL: “La firma electrónica no tiene relación alguna con el escaneo o digitalización de la firma autógrafa tradicional, sino que consiste en una combinación de algoritmos de encriptación que mediante el uso de una clave privada y una clave pública permiten cifrar y descifrar la información. Cada firma electrónica está vinculada a un certificado electrónico emitido por una Entidad de Certificación, el cual garantiza la identidad y autoría del firmante, tal como la cédula de identidad tradicional lo hace con nuestra firma autógrafa, con esto, el nivel de seguridad, confidencialidad, integridad, transparencia y no repudio en los procesos electrónicos, es mucho mayor que en los procesos físicos o manuales y el ahorro de tiempo y recursos genera beneficios tangibles a corto plazo.

A una firma electrónica, resulta una herramienta valiosa para el desarrollo social y económico tanto en el ámbito público como en el ámbito privado de nuestro país.” [3]

La firma digital y la firma manuscrita, tienen la misma validez legal y se encuentra amparada por la **Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos**. Desde el punto de vista técnico, la firma es un conjunto de datos digitales que se añaden a un archivo digital, los datos se obtienen del cifrado del archivo mediante programas computacionales. Los programas computacionales para cifrar emplean algoritmos o funciones de HASH, que permiten determinar un valor único empleando funciones matemáticas. El propósito de la función de HASH es tener un valor que referencie integridad del documento a enviar.

1.1.2 COMO FUNCIONA EL CERTIFICADO DIGITAL Y LA FIRMA DIGITAL

La imagen a continuación describe el proceso creando y verificando una firma digital.

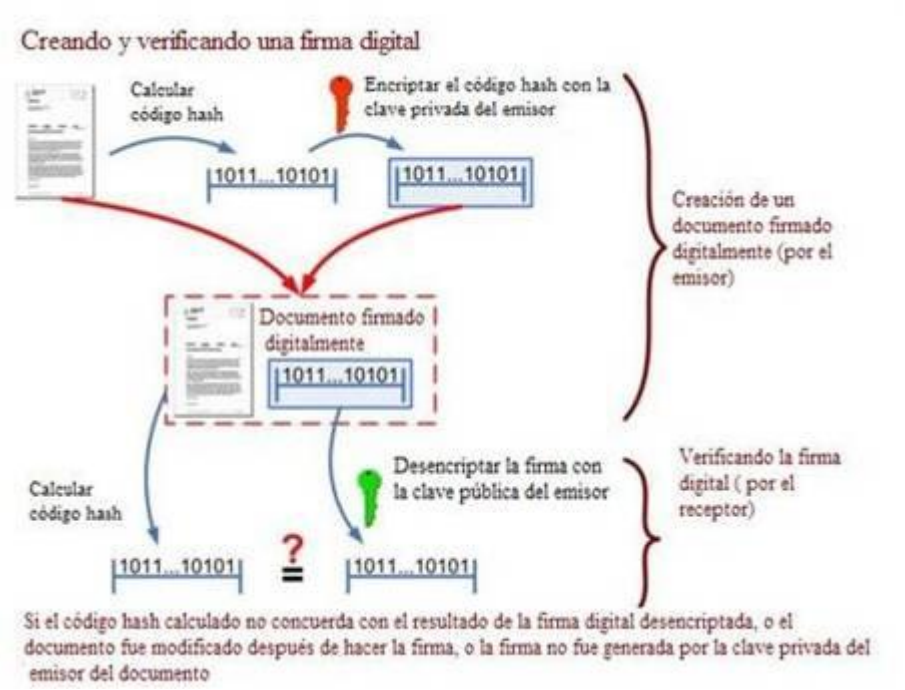

Figura 0.2 PROCEDIMIENTO PARA FIRMA DIGITAL

La imagen es tomada de http://roble.pntic.mec.es/jprp0006/tecnologia/4eso_informatica/tramites_online/firma_electronica.htm.

En la imagen se observa la obtención de HASH del documento a enviar; el valor de HASH se encripta o cifra empleando la clave privada del emisor, y se une al documento a enviar. Este procedimiento describe la firma digital del documento. En el receptor, al documento se le obtiene nuevamente el valor de HASH, con el fin de

comparar con el valor de HASH encriptado asociado al documento, si ambos valores son iguales el documento es integro. Para obtener el valor de HASH encriptado asociado al documento se debe emplear la clave pública del remitente, garantizando de esta manera la confidencialidad del envió.

La función del certificado digital inmerso en el documento enviado garantiza la identidad de la entidad emisora de la información (documentos, videos, pagina web), debido a que fue generado por la autoridad de certificación de la infraestructura de clave pública con sus lineamientos.

La función de la firma digital garantiza la integridad de los documentos, es decir verifica que el documento que se emite sea el mismo documento que se recibe, mediante algoritmos que permiten probar la autenticidad del documento.

La firma digital permite la transacción segura de documentos y operaciones en sistemas de información garantizando los siguientes aspectos:

- Identidad, reconoce unívocamente a un emisor como autor del mensaje.
- Integridad, el documento no puede ser alterado de forma alguna durante la transmisión.
- No repudio, el emisor no puede negar en ningún caso que un documento no fue firmado.
- Confidencialidad, solo las partes puedan leer el documento (si fuera el caso).

Algunos de los algoritmos de HASH para la integridad de datos son: derivados de HMAC (Hash-based message authentication code); HMAC-MD5, HMAC-SHA1,

HMAC-SHA256/384, y Authenticated Encryption (AE) or Authenticated Encryption with Associated Data (AEAD), entre otros.

1.1.3 COMO SE OBTIENE UN CERTIFICADO DIGITAL Y LA FIRMA DIGITAL

Para obtener un certificado digital, la persona o entidad que desea emplear certificados digitales debe cumplir procedimientos de la PKI de las diferentes entidades de certificación digital a nivel mundial o a nivel nacional, estas entidades son organizaciones denominadas “Autoridad de Certificación”.

Las Entidades de Certificación de Información y Servicios Relacionados, son las encargadas de la generación, gestión, administración, custodia y protección de las claves y los certificados de firma electrónica, así como de la validación de la identidad e información de los usuarios o solicitantes de firmas electrónicas, mediante el uso de la infraestructura pertinente y el recurso humano capacitado para operar dicha infraestructura con absoluta pericia y confidencialidad.

Según la SENATEL en el Ecuador existen las siguientes organizaciones reconocidas como Autoridad de Certificación:

Tabla 1 ENTIDADES DE CERTIFICACIÓN ACREDITADAS EN EL ECUADOR (BCE 2013)

	Resolución de Acreditación	Registro Público Nacional de Entidades de Certificación de Información y Servicios Relacionados Acreditadas y Terceros Vinculados
Banco Central del Ecuador **ENTIDAD DE CERTIFICACIÓN DE INFORMACIÓN Y SERVICIOS RELACIONADOS (ECIBCE)**	RES-481-20-CONATEL-2008 (08-10-2008)	SECCIÓN 1, TOMO 1 a FOJAS 1 OF-DGGST-2008-1006 (06-11-2008)
ANF Autoridad de Certificación	RES-639-21-CONATEL-2010 (22-10-2010)	SECCIÓN 1, TOMO 2 a FOJAS 1 OF-DGGST-2010-1794 (21-12-2010)
Security Data	RES-640-21-CONATEL-2010 (22-10-2010)	SECCIÓN 1, TOMO 3 a FOJAS 1 OF-DGGST-2010-1802 (23-12-2010)

Existen organizaciones o entidades relacionadas reconocidas por la SENATEL como TERCEROS VINCULADOS.

Tabla 2 TERCERO VINCULADO – SECURITY DATA (BCE 2013)

	Registro Público Nacional de Entidades de Certificación de Información y Servicios Relacionados Acreditadas y Terceros Vinculados

Cámara de Comercio de Guayaquil	SECCIÓN 2, TOMO 1 a FOJAS 1 OF-DGGST-2011-0799 (03-06-2011)
Kruger Corporation S.A.	SECCIÓN 2, TOMO 2 a FOJAS 1 OF-DGGST-2011-1169 (10-08-2011)
Telconet S.A.	SECCIÓN 2, TOMO 4 a FOJAS 1 OF-DGGST-2012-0329 (10-03-2012)
Optimsoft Software & Hardware CIA. LTDA.	SECCIÓN 2, TOMO 5 a FOJAS 1 OF-DGGST-2012-0373 (19-03-2012)
Federación Ecuatoriana De Exportadores FEDEXPOR	SECCIÓN 2, TOMO 6 a FOJAS 1 OF-DGGST-2012-0372 (19-03-2012)

Tabla 3 TERCERO VINCULADO - ANF Autoridad de Certificación (BCE 2013)

	Registro Público Nacional de Entidades de Certificación de Información y Servicios Relacionados Acreditadas y Terceros Vinculados
BANRED S.A.	SECCIÓN 2, TOMO 3 a FOJAS 1 OF-DGGST-2011-1569 (29-09-2011)

Para poder obtener el certificado digital, se debe realizar la solicitud de certificado a una de estas organizaciones en el mundo, la solicitud de certificado viaja con los datos que permitan conocer la entidad a ser certificada, por ejemplo en la web

existen servicios que son certificados para mantener la autenticidad del mismo a través de sus portales web o sistemas transaccionales, el certificado digital en este caso avala la autenticidad de este servicio en los diversos medios de publicación (navegadores o browsers).

En los navegadores básicamente la extensión del archivo del certificado se resume en:

Tabla 4 FORMATO DE CERTIFICADO DIGITAL PARA NAVEGADORES

.pfx:	✓	**Es la copia de seguridad con clave privada de un certificado (exportado desde Internet Explorer).**
.p12:	✓	Es la copia de seguridad con clave privada de un certificado.
.cer y .crt:	✓	Son formatos de exportación de clave pública de certificados.

Para obtener una firma digital, se genera mediante la clave privada del emisor de la información, siguiendo los pasos a continuación.

- Se debe seleccionar el documento a transferir.
- Sobre el documento seleccionado se aplica una función de hash.
- El resultado de la función de hash (huella digital) se encripta mediante la clave privada del emisor, recordando que la clave privada es el que emite una autoridad certificadora sobre la entidad que desee transferir información, garantizando así su autenticidad.
- Finalmente la firma digital es la huella digital encriptado del documento.
-

1.2 LEY DE COMERCIO ELECTRÓNICO

Los organismos de control encargados de la emisión de certificados y firmas digitales en el Ecuador son: La Secretaría Nacional de Telecomunicaciones –SENATEL- y el Consejo Nacional de Telecomunicaciones –CONATEL-

LA LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS **(Ley No. 2002-67**), establece:

Art. 1.- Objeto de la Ley.- Esta Ley regula los mensajes de datos, la firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas.

Art. 13.- Firma electrónica.- Son los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que puedan ser utilizados para identificar al titular de la firma en relación con el mensaje de datos, e indicar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos.

Art. 20.- Certificado de firma electrónica.- Es el mensaje de datos que certifica la vinculación de una firma electrónica con una persona determinada, a través de un proceso de comprobación que confirma su identidad.

Art. 30.- Obligaciones de las entidades de certificación de información acreditadas.- Son obligaciones de las entidades de certificación de información acreditadas:

a. Encontrarse legalmente constituidas, y estar registradas en el Consejo Nacional de Telecomunicaciones;
b. Demostrar solvencia técnica, logística y financiera para prestar servicios a sus usuarios;
c. Garantizar la prestación permanente, inmediata, confidencial, oportuna y segura del servicio de certificación de información.
d. Mantener sistemas de respaldo de la información relativa a los certificados;
e. Proceder de forma inmediata a la suspensión o revocatoria de certificados electrónicos previo mandato de la Superintendencia de Telecomunicaciones, en los casos que se especifiquen en esta ley;
f. Mantener una publicación del estado de los certificados electrónicos emitidos;
g. Proporcionar a los titulares de certificados de firmas electrónicas un medio efectivo y rápido para dar aviso que una firma electrónica tiene riesgo de uso indebido;
h. Contar con una garantía de responsabilidad para cubrir daños y prejuicios que se ocasionaren por el incumplimiento de las obligaciones previstas en la presente ley, y hasta por culpa leve en el desempeño de sus obligaciones. Cuando certifiquen límites sobre responsabilidades o valores económicos, esta garantía será al menos del 5% del monto total de las operaciones que garanticen sus certificados; e,
i. Las demás establecidas en esta ley y los reglamentos.

Las Leyes y reglamentos vigentes adicionales a la ley de comercio electrónica que regulan el correcto modelo operativo para la legalización y empleo de firma digital son las siguientes:

- Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.
- Reglamento a la Ley de Comercio Electrónico.
- Ley Orgánica de Defensa del Consumidor.
- Reglamento a la Ley Orgánica de Defensa del Consumidor.
- Ley Orgánica de Transparencia de la Información.
- Reglamento a la Ley Orgánica de Transparencia de la Información.
- Acreditación de CONATEL.
- Decreto No. 1356 del 29 de Septiembre del 2008.
- Norma de Control Interno (Contraloría General del Estado).

1.2.1 LEGALIZACIÓN DE DOCUMENTOS MEDIANTE FIRMA DIGITAL

La legalización de documentos consiste en emplear la firma digital mediante algún medio tecnológico, tales como el reconocimiento de patrón de huella digital como medio biométrico, o memorias de almacenamiento (USB) denominado en la actualidad como “token” (dispositivo USB que almacena la información digital de la

persona) se puede hacer similitud con un bolígrafo, y cumplir con las normas legales.

Art. 14.- Efectos de la firma electrónica.- La firma electrónica tendrá igual validez y se le reconocerán los mismos efectos jurídicos que a una firma manuscrita en relación con los datos consignados en documentos escritos, y será admitida como prueba en juicio.

Art. 15.- Requisitos de la firma electrónica.- Para su validez, la firma electrónica reunirá los siguientes requisitos, sin perjuicio de los que puedan establecerse por acuerdo entre las partes:

a. Ser individual y estar vinculada exclusivamente a su titular;
b. Que permita verificar inequívocamente la autoría e identidad del signatario, mediante dispositivos técnicos de comprobación establecidos por esta Ley y sus reglamentos;
c. Que su método de creación y verificación sea confiable, seguro e inalterable para el propósito para el cual el mensaje fue generado o comunicado.
d. Que al momento de creación de la firma electrónica, los datos con los que se creare se hallen bajo control exclusivo del signatario; y,
e. Que la firma sea controlada por la persona a quien pertenece.

Art. 16.- La firma electrónica en un mensaje de datos.- Cuando se fijare la firma electrónica en un mensaje de datos, aquélla deberá enviarse en un mismo acto como parte integrante del mensaje de datos o lógicamente asociada a éste. Se presumirá legalmente que el mensaje de datos firmado electrónicamente conlleva la

voluntad del emisor, quien se someterá al cumplimiento de las obligaciones contenidas en dicho mensaje de datos, de acuerdo a lo determinado en la Ley.

Art. 17.- Obligaciones del titular de la firma electrónica.- El titular de la firma electrónica deberá:

a. Cumplir con las obligaciones derivadas del uso de la firma electrónica;
b. Actuar con la debida diligencia y tomar las medidas de seguridad necesarias, para mantener la firma electrónica bajo su estricto control y evitar toda utilización no autorizada;
c. Notificar por cualquier medio a las personas vinculadas, cuando exista el riesgo de que su firma sea controlada por terceros no autorizados y utilizada indebidamente;
d. Verificar la exactitud de sus declaraciones;
e. Responder por las obligaciones derivadas del uso no autorizado de su firma, cuando no hubiere obrado con la debida diligencia para impedir su utilización, salvo que el destinatario conociere de la inseguridad de la firma electrónica o no hubiere actuado con la debida diligencia;
f. Notificar a la entidad de certificación de información los riesgos sobre su firma y solicitar oportunamente la cancelación de los certificados; y,
g. Las demás señaladas en la Ley y sus reglamentos.

1.2.2 DECRETO 867.

Cabe mencionar que con el DECRETO 867 del 1-SEP-2011, que aplica una Reformas al Reglamento de la empresa públicas indica: “Que es vital que todas las instituciones del Estado cuenten con certificados digitales de firma electrónica, considerando más existe normativa de control, como el Acuerdo 039 - Norma de Control Interno, emitido por la Contraloría General del Estado y publicado en el Registro Oficial N° 78 de diciembre 1 de 2009, que determina que las entidades del sector público deben aceptar y generar documentos electrónicos con firma electrónica; Que el uso de la firma digital o electrónica como herramienta informática tiende al incremento de la confianza de la ciudadanía en el uso de medios electrónicos y la transparencia en la información, lo cual debe ser una permanente contribución a la sociedad, tanto para el sector público como para el sector privado;”

Para dar cumplimiento a las obligaciones que dispone la ley y según el Acuerdo Ministerial 181 del Ministerio de Telecomunicaciones y de la Sociedad de la Información, se debe reconocer los tipos de certificados que pueden ser solicitados por las entidades públicas o servidores públicos, según su conceptualización descrita a continuación:

a) **Certificado de Persona Natural o Física:** Son certificados que identifican al suscriptor como una persona natural o física, y será responsable a título personal de todo lo que firme electrónicamente, dentro del ámbito de su actividad y límites de uso que correspondan.
b) **Certificado de Persona Jurídica, Representante legal o Miembro de Empresa:** Son certificados que identifican al suscriptor como una persona

jurídica de derecho público o privado a través de su representante legal o de las personas que actúen en su representación, quienes serán responsables en tal calidad de todo lo que firmen dentro del ámbito de su competencia y límites de uso que correspondan.

c) **Certificado Funcionario Público:** Son certificados que identifican al suscriptor como funcionario o servidor público, quien actuara a título de la Institución pública que representa y será responsable de todo lo que firme electrónicamente dentro del ámbito de su actividad y límites de uso que correspondan.

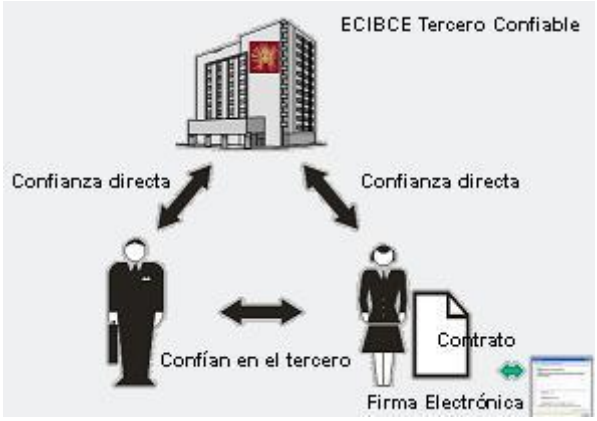

Figura 0.3 AUTORIDAD CERTIFICADORA CA

1.3 SISTEMAS DE INFORMACIÓN

Los conceptos de sistemas de información permiten conocer como pueden ser empleados estos medios o herramientas en la organización según su usabilidad o aplicabilidad, según el punto de vista empresarial, según su plataforma o arquitectura técnica, para nuestro estudio emplearemos su aplicabilidad.

Los sistemas de información buscan alcanzar tres objetivos básicos dentro de la organización.

1. Automatización de procesos operativos
2. Proporcionar información que sirva de apoyo al proceso de toma de decisiones
3. Lograr ventajas competitivas a través de su implantación y uso.

Un Sistema de Información es un conjunto de elementos que interactúan entre sí con el fin de apoyar las actividades de una empresa o negocio. En un sentido amplio, un sistema de información no necesariamente incluye equipo electrónico (hardware). Sin embargo en la práctica se utiliza como sinónimo de "sistema de información computarizado"

Los elementos que interactúan entre sí son: el equipo computacional, el recurso humano, los datos o información fuente, programas ejecutados por las computadoras, las telecomunicaciones y los procedimientos de políticas y reglas de operación.

Un Sistema de Información realiza cuatro actividades básicas:

- Entrada de información: proceso en el cual el sistema toma los datos que requiere para procesar la información, por medio de estaciones de trabajo, teclado, diskettes, cintas magnéticas, código de barras, etc.

- Almacenamiento de información: es una de las actividades más importantes que tiene una computadora, ya que a través de esta propiedad el sistema puede recordar la información guardada en la sesión o proceso anterior.

- Procesamiento de la información: esta característica de los sistemas permite la transformación de los datos fuente en información que puede ser utilizada para la toma de decisiones, lo que hace posible, entre otras cosas, que un tomador de decisiones genere una proyección financiera a partir de los datos que contiene un estado de resultados o un balance general en un año base.

- Salida de información: es la capacidad de un SI para sacar la información procesada o bien datos de entrada al exterior. Las unidades típicas de salida son las impresoras, maquinas generadora de gráficos, cintas magnéticas, diskettes, la voz, etc.

1.3.1 QUE ES UN SISTEMA DE INFORMACIÓN TRANSACCIONAL

Según su usabilidad los sistemas de información que automatizan procesos operativos, y de producción de una organización son llamados sistemas transaccionales, cuya función principal consiste en procesar transacciones tales como pagos, cobros, pólizas, planillas, entradas, salidas. Por otra parte, los sistemas de información que apoyan el proceso de toma de decisiones son los

sistemas de apoyo a la toma de decisiones (DSS, por sus siglas en inglés Decisión Supporting System). El tercer tipo de sistemas, de acuerdo con su uso u objetivos que cumplen, es de los Sistemas Estratégicos, los cuales se desarrollan en las organizaciones con el fin de lograr las ventajas competitivas, a través del uso de la Tecnología de Información (TI).

Los Sistemas de Información Transaccional o también conocido como sistema de procesamiento de datos, se denota con las siglas en ingles de TPS básicamente son manejadores de grandes volúmenes de datos, con actividades repetitivas desarrolladas por el nivel operativo de la organización, son sistemas de recolección continua de datos y se utilizan como base para los sistemas de toma de decisiones, sistemas ejecutivos y sistemas de administración gerencial.

Según el modelo organizacional de cadena de valor de Porter, se considera que los sistemas de información transaccionales son de apoyo para las actividades descritas en el modelo:

Figura 0.4 MODELO DE CADENA DE VALOR (PORTER)

Las principales actividades de los sistemas transaccionales se resumen así:

- A través de éstos suelen lograrse ahorros significativos de mano de obra, debido a que automatizan tareas operativas dela organización.
- Con frecuencia son el primer tipo de Sistemas de Información que se implanta en las organizaciones. Se empieza apoyando las tareas a nivel operativo dela organización.
- Son intensivos en entrada y salida de información; sus cálculos y procesos suelen ser simples y poco sofisticados.
- Tienen la propiedad de ser recolectores de información, es decir, a través de estos sistemas se cargan las grandes bases de información para su explotación posterior.
- Son fáciles de justificar ante la dirección general, ya que sus beneficios son visibles y palpables.

El Estado emplea los Sistemas de Información para mejorar la calidad en la administración gubernamental, mejorar la gestión en las diversas instituciones públicas y determinar los correctivos adecuados, a través de la SECRETARIA NACIONAL DE INFORMACIÓN. [4], los sistemas de información descritos en el portal de la SNI son:

Tabla 5 SISTEMAS DE INFORMACIÓN PARA LA ADMINISTRACIÓN PÚBLICA

ENLACE	SISTEMA DE INFORMACIÓN
	Ecuador en Cifras Información Estadística
	Banco Central del Ecuador
	Sistema Integrado de Indicadores Sociales del Ecuador
	Geo información 1:25000. Instituto Espacial Ecuatoriano
	Sistema de Información Nacional de Agricultura, Ganadería, Acuacultura y Pesca
	Sistema de Estadísticas Territoriales
	Registro Interconectado de Programas Sociales
	Sistema de Indicadores de Pasivos Ambientales y Sociales
	Sistema de Información para la Gestión del Patrimonio Cultural

En la tabla anterior se presentan algunos de los sistemas del Estado para la administración, sin embargo el gobierno presenta mecanismos de control adicionales inclusive para la administración de los bienes públicos, como son vehículos, fondos del Estado, además del desempeño del Talento Humano.

1.3.2 COMO SE CONSTITUYE UN SISTEMA DE INFORMACIÓN TRANSACCIONAL.

El Sistema de Información Transaccional se genera por la necesidad de automatizar un proceso o procedimiento en la organización, para automatizarlo se requiere tener los siguientes elementos:

Figura 0.5 COMPONENTES DEL SISTEMA DE INFORMACIÓN

Personas: son los usuarios operadores, analistas de sistemas y programadores, que tienen una preparación en el manejo de datos.

Software: Es un término amplio que se le da a las instrucciones que dirigen la operación del equipo y se puede clasificar en dos clases principales: software de sistemas y software aplicativos.

Hardware: Se refiere al sistema de computación físico y a los dispositivos asociados, los cual debe proveer las principales funciones: entrada o acceso, procesamiento, almacenamiento y salida.

Datos: Es un conjunto de información almacenada por registros que conforman un archivo. Los cuales pueden ser almacenados por medios físicos como CD'S, cintas magnéticas, disco duro, etc.

Procesos: Son las técnicas, medios, acciones que conllevan al funcionamiento del negocio.

1.4 PROCESOS Y ORGANIGRAMAS

Uno de los elementos para elaborar un sistema transaccional son los procesos; los mismos que determinan la estructura organizacional y funcional de una entidad pública o privada, a través de las actividades macro que desempeña una organización.

El organigrama generalmente define la organización vertical o jerárquica; mientras la organización que se lleva por procesos establece las entradas, salidas, resultados, etc. en función de brindar un servicio en equipo. Los diversos procesos inmersos en la organización requiere de una administración o control para el seguimiento de sus resultados, por tal motivo la gestión por procesos permite gestionarlos.

Los sistemas de gestión por procesos; normados por estándares de calidad ISO pretenden garantizar la atención a una necesidad estableciendo un resultado basado en la eficacia y eficiencia. Los procesos claves o principales de una

organización se describen en la cadena de valor de una organización. Las empresas gubernamentales forman parte del gasto público, dentro de sus procesos se encuentra la cadena de valor logística, que por lo general está ligada a proyectos de inversión a mediano o largo plazo.

La visión por procesos es un concepto para la operatividad de las organizaciones; las entidades gubernamentales no son la excepción. Para comenzar a diseñar la gestión por procesos se debe establecer un mapa de procesos.

Un proceso es una secuencia de actividades orientadas a generar valor sobre una ENTRADA para conseguir un resultado, y una SALIDA que a su vez satisfaga los requerimientos del Cliente/Usuario, las entidades de control gubernamentales buscan analizar a las organizaciones según su gestión por procesos.

La entidad Gubernamental encargada de regular, controlar, mejorar la calidad y establecer las directrices como lo indica su misión es la SECRETARIA NACIONAL DE ADMINISTRACIÓN PUBLICA, conformada por diversas subsecretarias orientadas a fines puntuales de la administración del Estado. [5]

1.4.1 QUE ES UN PROCESO ORGANIZACIONAL.

Un proceso organizacional es un conjunto de recursos y actividades interrelacionados que transforman elementos de entrada en elementos de salida. Los recursos pueden incluir personal, finanzas, instalaciones, equipos, técnicas y métodos.

Se habla de proceso si cumple con las siguientes características o condiciones.

- Se pueden describir las ENTRADAS y las SALIDAS.
- El proceso cruza uno o varios límites organizativos funcionales.
- Una de las características significativas de los procesos es que son capaces de cruzar verticalmente y horizontalmente la organización.
- Se requiere hablar de metas y fines en vez de acciones y medios. Un proceso responde a la pregunta "QUE", no al "COMO".
- El proceso tiene que ser fácilmente comprendido por cualquier persona de la organización.
- El nombre asignado a cada proceso debe ser sugerente de los conceptos y actividades incluidos en el mismo.

Todos los procesos tienen que tener un responsable designado que asegure su cumplimiento y eficacia.

Los procesos tienen herramientas de validación y valoración que permitan realizar un análisis mediante estadísticas, cuantificadores de desempeño e indicadores de gestión que permitan visualizar de forma gráfica la evolución de los mismos.

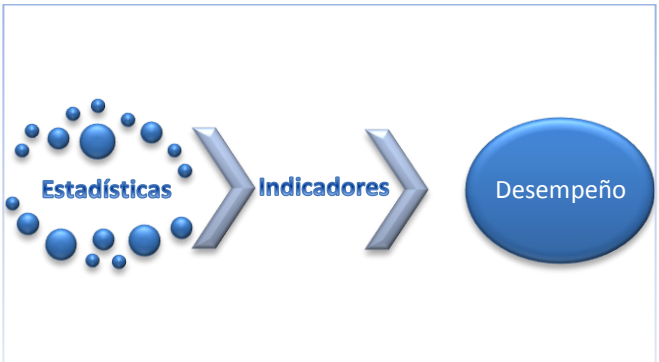

Figura 0.6 HERRAMIENTAS PARA MEDIR UN PROCESO

La arquitectura de un proceso estándar es el siguiente:

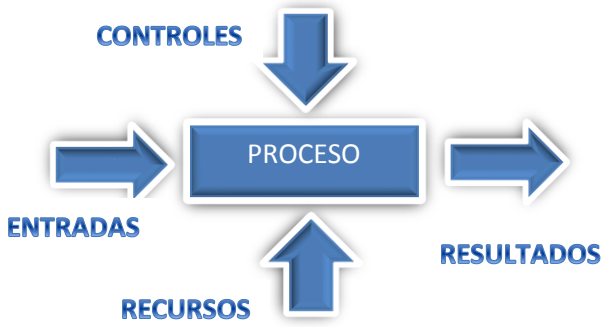

Figura 0.7 ARQUITECTURA DE UN PROCESO

1.4.2 QUE ES UN ORGANIGRAMA.

Un organigrama es la representación gráfica de la estructura de una empresa u organización. Representan las estructuras departamentales y, en algunos casos, las personas que las dirigen, hacen un esquema sobre las relaciones jerárquicas y competenciales de vigor en la organización.

El organigrama es un modelo abstracto y sistemático, que permite obtener una idea uniforme acerca de la estructura formal de una organización o empresa.

- Desempeña un papel informativo.
- Obtener todos los elementos de autoridad, los diferentes niveles de jerarquía, y la relación entre ellos.

En el organigrama no se tiene que encontrar toda la información, para conocer como es la estructura total de la empresa.

Todo organigrama tiene el compromiso de cumplir los siguientes requisitos:

- Tiene que ser fácil de entender y sencillo de utilizar.
- Debe contener únicamente los elementos indispensables.

Tipos de organigrama: Según su forma

1. Vertical: Muestra las jerarquías según una pirámide, de arriba a abajo.
2. Horizontal: Muestra las jerarquías de izquierda a derecha.
3. Mixto: Es una combinación entre el horizontal y el vertical.
4. Circular: La autoridad máxima está en el centro, alrededor de él se forman círculos concéntricos donde se nombran a los jefes inmediatos.
5. Escalar: Se usan sangrías para señalar la autoridad, cuanta mayor es la sangría, menor es la autoridad de ese cargo.
6. Tabular: Es prácticamente escalar, solo que mientras el escalar lleva líneas que unen los mandos de autoridad el tabular no.

Según sus funciones este criterio supone agrupar los trabajadores teniendo en cuenta sus tareas, este criterio hace que aparezcan los departamentos o áreas.

1.4.2.1 TIPOS DE ORGANIZACIÓN

Existen diversas formas de clasificar una organización, tales como:

Tabla 6 TIPOS DE ORGANIZACIÓN

Finalidad:	• Con fin de lucro (Empresas). • Sin fin de lucro (ONG).
Estructura:	• Formales. • Informales.
Tamaño:	• Grande. • Mediana. • Pequeña.
Localización:	• Multinacional – internacional. • Nacional. • Local o regional.
Producción:	• Bienes. • Servicios.
Propiedad:	• Pública. • Privada. • Mixta.
Grado de integración:	• Totalmente integrada. • Parcialmente integrada.
Actitud frente a los cambios:	• Rígido. • Flexible.
Toma de decisiones:	• Centralizada. • Descentralizada.
Jerarquía:	• Organización jerárquica • En red

1.4.2.2 ORGANIZACIÓN PLANA VS ORGANIZACIÓN JERÁRQUICA.

Una de las técnicas de clasificación que se emplea en las organizaciones durante las actividades o labores de trabajo en equipo que se realizan son:

Tabla 7 ORGANIZACIÓN PLANA VS JERÁRQUICA

Organización Plana u Horizontal.	Trabaja en función de metas grupales
Organización Jerárquica o Vertical.	Trabaja en función de cumplir metas expuestas del Director.

Las organizaciones gubernamentales buscan una organización mixta en función de procesos y estructura organizacional, se conceptualiza la idea de “Los procesos a través de la organización”

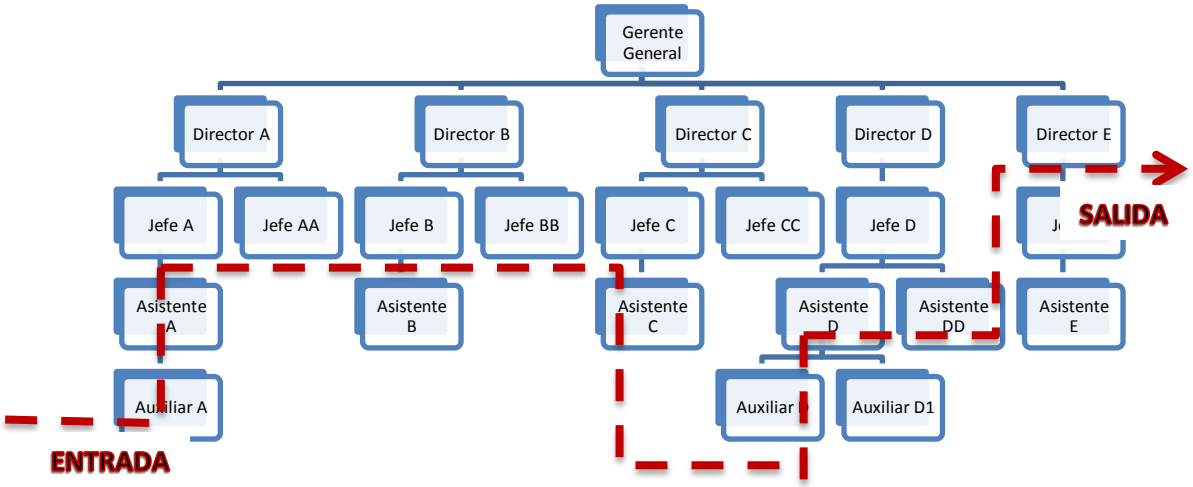

Figura 0.8 ORGANIZACIÓN MIXTA (PLANA Y JERÁRQUICA)

En un esquema organizacional por procesos se realizan las actividades en busca de objetivos; se realizan esfuerzos o trabajos organizados de forma consecutiva, fin culminar con la meta de los objetivos planteados. Los procesos en la organización

son de vital importancia porque permiten establecer las responsabilidades y límites de acción en la organización.

Es necesario mantener la comunicación como un medio o mecanismo de interconexión entre las partes relacionadas o recursos involucrados, la comunicación permite seguir el camino trazado para la elaboración y consecución de metas, el medio de comunicación generalmente empleado se rige bajo documentos de control, en los cuales se establecen disposiciones a ejecutar, responsabilidades delegados, o cuestiones de legalización.

El siguiente ejemplo cotidiano en una empresa manufacturera. Durante el proceso de producción; el proceso nace de la demanda de un producto por parte del cliente, si la demanda puede ser producida por la materia prima existente en las bodegas este se lo elabora, de no existir el material suficiente para la confección o elaboración de los productos, se debe adquirir a través de los proveedores calificados en la organización. La línea de producción finalmente entrega los productos al cliente para finalizar la cantidad requerida inicialmente por el cliente. En el flujo de trabajo de este proceso existen documentos de control legalizables que permiten la credibilidad y la ejecución de trabajo, cumpliendo y respetando las normas, reglamentos y políticas internas y externas de la organización. Los documentos se registran en sistemas transaccionales como parte del procedimiento y como salvaguarda para el manejo de información, un mecanismo de impresión repetitivo se observa necesario para la ejecución de tareas de legalizar funciones de trabajo.

Se relaciona la elaboración de procesos, el apoyo de sistemas transaccionales y el uso de documentos legalizables en el transcurso de la actividad de producción, se busca mejorar en lo posible la actividad de legalización de documentos empleando un mecanismo tecnológico que permita eliminar la fase de impresión, además del tiempo de la misma.

Figura 0.9 PROCESO DE PRODUCCIÓN (COMUNICACIÓN)

1.4.3 GESTIÓN POR PROCESOS.

Es una forma de organización diferente de la clásica organización funcional, en el que prima la visión del cliente sobre las actividades de la organización. Los procesos definidos son gestionados de modo estructurado y su mejora se basa la de la propia organización a través de la eficiencia y eficacia.

La gestión por procesos aporta una visión y unas herramientas con las que se puede mejorar y rediseñar el flujo de trabajo para hacerlo más eficiente y adaptado a las necesidades de los clientes. No hay que olvidar que los procesos lo realizan personas y los productos los reciben personas, y por tanto, hay que tener en cuenta en todo momento las relaciones entre proveedores y clientes.

La gestión por procesos permite mejorar a través de sus indicadores la elaboración de las actividades; buscando la reducción de tiempo y recursos.

CAPÍTULO 2

ANÁLISIS, DISEÑO DE PROCESOS EN UNA ORGANIZACIÓN GUBERNAMENTAL PARA LA IMPLEMENTACIÓN DE FIRMA DIGITAL EN SISTEMAS DE INFORMACIÓN TRANSACCIONALES.

Se ha descrito los diversos tipos de organizaciones, la relación de los sistemas de información con procesos, la legalización de documentos inmersos en los procesos para relacionarlos con los sistemas de información; se necesita analizar los procesos que requieren se implemente un mecanismo que agilite el trámite burocrático de firma.

Existen roles en cada sistema transaccional que describe el nivel de acceso para que cada usuario opere desempeñando la actividad delegada para la ejecución de un proceso, una de estas actividades puede ser la elaboración de una orden de compra, en la cual se describen los bienes a ser adquiridos por la organización; la orden de compra debe ser legalizada, el usuario elaborador de la orden debe transmitir el documento y esperar la firma de su autoridad inmediata para proceder con el trámite, el tiempo en espera para su legalización puede variar y de ser una necesidad urgente se debe atender de forma inmediata.

Se desea realizar la legalización de documentos en los procesos organizacionales empleando el sistema transaccional a través del mecanismo de firma electrónica. Con la firma electrónica se realizan diferentes tipos de transacciones a través de la Internet e Intranet sin tener la necesidad que el personal se movilice o desplace de un lugar a otro; los trámites públicos se agilitan aumentando la transparencia, lo que se traduce en ahorros significativos de tiempo y dinero. En los sistemas transacciones las aplicaciones de la firma digital son diversas. Se cita algunas de ejemplo a continuación:

- Compras públicas
- Trámites ciudadanos (Gobierno electrónico)
- Gestión documental
- Operaciones bancarias
- Dinero (pago) electrónico
- Balances electrónicos
- Trámites judiciales y notariales

- Comercio electrónico
- Facturación electrónica

En este capítulo se analiza una de las fases del ciclo logístico como lo es la adquisición de bienes y servicios o denominado compras. Este proceso abastece a los diferentes departamentos funcionales/operativos de la organización.

En el análisis se ponen a consideración los elementos, documentos, que se emplean para cumplir con el resultado del proceso, su legalización física y por ende la factibilidad de una legalización digital.

2.1 SITUACIÓN ACTUAL EN LA LEGALIZACIÓN DE DOCUMENTOS TRANSACCIONALES ELABORADOS EN EL SISTEMA LOGÍSTICO DE UNA ORGANIZACIÓN GUBERNAMENTAL.

Las tareas o actividades del «ciclo logístico» son acciones encaminadas a la ejecución de las funciones de abastecimiento de bienes necesarios de una organización. Este proceso debe producirse en forma ordenada, ya que a través de él se logra una acertada administración de los recursos.

Las actividades del sistema logístico se describen como: La determinación de las necesidades, la obtención y la distribución; Uno de los aspectos inherentes a la organización gubernamental está tipificado en la ley mediante el cumplimiento de las normas de control interno de acuerdo al código 406 “Administración Financiera: Administración de Bienes”, en la que describe aspectos relacionados a la planificación, contratación, almacenamiento y su distribución. [6]

La determinación de las necesidades se basa en la planificación de los recursos necesarios que satisfagan la demanda de la organización, se conoce que una organización gubernamental además de abastecerse de recursos para su funcionamiento debe precautelar los fondos del gasto público.

La etapa de obtención es una medida que permite establecer lo requerido contra lo necesario, las organizaciones de gobierno planifican las necesidades y se establecen prioridades para el cumplimiento de sus actividades; para obtener los bienes planificados se mantiene el criterio de prioridad además de brindar lo que puede cumplirse.

La distribución del bien cumple las especificaciones brindadas en la etapa de obtención, es decir lo que se estableció obtener se debe entregar.

Figura 0.1 CICLO LOGÍSTICO

Planificación: Determinación de las Necesidades

Adquisición: Obtención

Ingreso y Despacho: Distribución

A las organizaciones gubernamentales se les dispone el uso de compras públicas [7] que relaciona al ciclo logístico en la fase o etapa de obtención de las necesidades mediante mecanismos técnicos para adquirir los bienes y servicios de forma transparente, es decir la fase o etapa de adquisiciones se integra a un proceso elaborado por el Estado para la ejecución de compras; La organización pública encargada de monitorear, controlar los procesos de las adquisiciones es SERCOP (Servicio Nacional de Contratación Pública), las organizaciones públicas constan de unidades de compras encargadas de realizar la ejecución de las mismas a los departamentos solicitantes, delegaciones u otras entidades que emitan las necesidades o requerimientos.

Los sistemas de apoyo logísticos o sistemas de información transaccionales empleados para la realización del trámite de compras son repositorio de datos de las transacciones relacionadas, sin embargo para la legalización de las transacciones se considera la impresión de documentos como un formalismo para garantizar el correcto intercambio de aceptación entre el beneficiario y proveedor del bien o servicio.

¿Qué es Compras Públicas?

La compra pública es un mecanismo gubernamental que busca garantizar la transparencia para la obtención de bienes y servicios de las organizaciones gubernamentales, brindando igualdad de opciones para todos en el mercado, permitiendo así la legitimidad en el proceso de selección de proveedores por menor costo, calidad y distribuyendo las oportunidades tanto a ofertantes como demandantes en un proceso de compra.

Toda compra pública se realiza a través de herramientas tecnológicas de control de gobierno, la herramienta empleada para la organización es el portal de comprar públicas https://www.compraspublicas.gob.ec, actualmente el portal permite el ingreso de necesidades, validación de ofertas, y en algunos casos la selección de bienes a ser adquiridos mediante un catálogo electrónico.

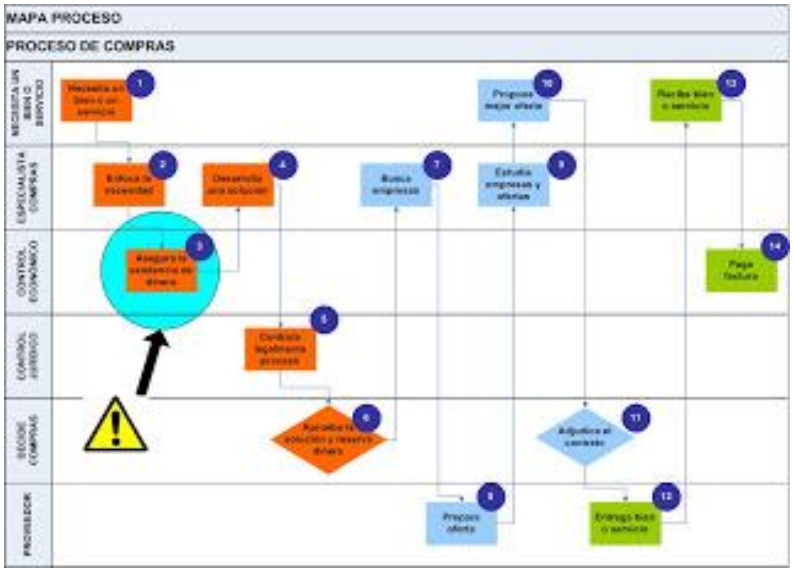

Figura 0.2 MACRO PROCESO DE COMPRAS [7]

2.2 LEVANTAMIENTO DE REQUERIMIENTO PARA LA IMPLEMENTACIÓN DE FIRMA DIGITAL EN DOCUMENTACIÓN DEL SISTEMA TRANSACCIONAL.

Para la implementación de la firma digital se realiza el levantamiento de requerimiento, el cual es un procedimiento establecido para la ejecución y cumplimiento de tareas de desarrollo y de proyectos previo a la etapa de análisis.

Se dispone a través de la norma de control interno que toda organización gubernamental debe implementar el uso de firma digital para la legalización de documentos. [6]

En la actualidad el Estado a través de varias instituciones públicas ha dispuesto implementar el uso de la firma digital; Por ello el requerimiento de implementar es una necesidad que se ve inmersa en cada institución del Estado que lo debe socializar con el fin de acrecentar esta cultura; El procedimiento para realizar la implementación consiste en la revisión de procesos que relacionen documentos transaccionales públicos, o de control interno requeridos por la Contraloría General del Estado según su Norma de Control Interno.

Se puede extender el listado de procesos seleccionando aquellos en los que se relacionen documentos legalizables, pero para el propósito de implementación de estudio se limita el análisis de documentos al proceso de adquisición de bienes.

La entidad responsable de realizar las compras es la encargada de gestionar el requerimiento para su análisis, las normas de control interno establecen los documentos legalizables auditables, sin embargo el listado de documentos indicados en las normas debe discriminarse para su uso según la organización:

Las normas de control interno manifiesta en su código 406:

406 Administración financiera - ADMINISTRACIÓN DE BIENES

406-01 Unidad de Administración de bienes Toda entidad u organismo del sector público, cuando el caso lo amerite, estructurará una unidad encargada de la administración de bienes.

La máxima autoridad a través de la unidad de administración de bienes,

instrumentará los procesos a seguir en la planificación, provisión, custodia, utilización, traspaso, préstamo, enajenación, baja, conservación y mantenimiento, medidas de protección y seguridad, así como el control de los diferentes bienes, muebles e inmuebles, propiedad de cada entidad u organismo del sector público y de implantar un adecuado sistema de control interno para su correcta administración.

Tabla 8 DOCUMENTOS HABILITANTES SEGÚN CGE

En el enunciado del código establece que se debe registrar desde la planificación, custodia, utilización, traspaso, préstamo, entre otros; así como el control de bienes, muebles e inmuebles, propiedad de cada entidad, por ende su correcta legalización.

2.3 ANÁLISIS DE PROCESOS TRANSACCIONALES EN LOS CUALES SE INVOLUCRA DOCUMENTACIÓN LEGALIZABLE.

Las etapas o fases a analizar para determinar la factibilidad de la implementación de firma son los siguientes en el ciclo logístico:

Tabla 9 PROCESO LOGÍSTICO

CICLO LOGÍSTICO
Planificación: Determinar las Necesidades
Adquisición: Obtención
Ingreso y Despacho: Distribución

En las etapas del macro proceso existen actividades o sub procesos en los cuales se desarrollan documentos en función del control interno, y entre ellos se encuentran documentos establecidos por la ley de compras y contraloría.

Tabla 10 PROCESOS Y DOCUMENTOS DEL CICLO LOGÍSTICO

Proceso	Documento	Firmante
Planificación de Compra	-	-
Adquisición	Solicitud de Compra	Jefe del Dpto. Solicitante
		Emisor de Solicitud
	Cotización	Jefe del Dpto. de Adquisiciones
		Asistente del Dpto. de Adquisiciones
	Orden de Compra	Jefe del Dpto. de Adquisiciones
		Asistente del Dpto. de Adquisiciones.
	Informe de Necesidad	Emisor de Solicitud
	Certificación Presupuestaria	Jefe Dpto. Financiero.
		Asistente Financiero
Recepción de Bienes	Factura o Guía de Remisión, Orden de Compra	Jefe de Bodega
		Bodeguero
	Acta de Inspección del Bien, Traspaso de Material	Jefe de Bodega
		Bodeguero
	Lista de chequeo de calidad	Jefe de Bodega
		Responsable Técnico

Despacho de Bienes	Entrega Directa	
	Nota de Pedido y Despacho	

Para el propósito de desarrollo e implementación se considera el proceso de adquisiciones del ciclo logístico o contratación según CGE. En el inventario de documentos podemos considerar según el proceso expuesto que existen 2 documentos básicos y esenciales para la adquisición además de la planificación como son:

- ✓ Solicitud de Compra
- ✓ Orden de Compra

La solicitud de compra es el documento habilitante que indica los bienes a ser adquiridos por la entidad, junto a un informe de necesidad, un documento de certificación presupuestaria para el gasto, además de algunas aprobaciones y legalizaciones internas dan lugar al documento de orden de compra, que finalmente será el documento que el proveedor reciba para la ejecución de la compra, este documento debe ser legalizado por la máxima autoridad competente de la organización.

2.4 SELECCIÓN DE PROCESOS QUE INVOLUCRAN DOCUMENTOS LEGALIZABLES EN EL SISTEMA TRANSACCIONAL.

Los procesos que involucran documentos legalizables son:

Tabla 11 DOCUMENTOS LEGALIZABLES

Proceso	Documento	Firmante	Legalizable
Adquisición	Solicitud de Compra	Jefe del Dpto. Solicitante	X
	Orden de Compra	Jefe del Dpto. de Adquisiciones	X
	Certificación Presupuestaria	Jefe Dpto. Financiero.	X
	Acta de Inspección del Bien, Traspaso de Material	Jefe de Bodega	X

Se realiza la selección de uno de ellos para el proceso de implementación de la firma por la importancia que tiene en el proceso logístico, reducir tiempos en el proceso de adquisiciones, reducción en el consumo de suministros como papel, tinta, etc., mantener la Integridad, Confidencialidad y Disponibilidad del documento firmado.

2.5 PROPUESTA DE SOLUCIÓN.

La solución a implementar permite firmar documentos transaccionales empleando un dispositivo que garantiza la seguridad de la operación en un sistema de información transaccional mediante certificado emitido por una CA[1], generando de esta manera agilidad en el tiempo de espera de legalización de documentos, disminución de gastos de suministros de papelería, además de la confiabilidad en la seguridad de los sistemas informáticos transaccionales que emplee una organización.

[1] Certificate Authority

La solución se desarrolla en ambiente web a través de un canal seguro TLS (Transport Layer Security), empleando tecnología Java; conexión a base de datos mediante controladores JDBC; base de datos transaccionales con soporte a documentos cifrados para el manejo de firmas digitales. La solución además permite la elaboración del proceso de legalización sin almacenar en el terminal o computador de acceso ningún rastro de documento alguno.

El acceso al sistema web se realiza por medio de credenciales de usuario y clave. El proceso técnico consiste en recuperar el certificado digital almacenado en el dispositivo transportador que al momento de conectar el computador solicita una clave de acceso al dispositivo; mediante el uso del certificado el usuario podrá firmar de manera digital el documento digital.

La solución permite elaborar la consulta de documentos en proceso de adquisición de una organización, los documentos están a la espera de ser firmados digitalmente para proceder a realizar la compra, el pago o el ingreso del material a las bodegas de la institución para proceder luego a realizar el despacho.

2.6 OBJETIVO GENERAL DE LA PROPUESTA

Aplicar tecnología de innovación de seguridad al procedimiento de legalización de documentos en el proceso de adquisición de la organización a través del sistema transaccional, manteniendo la confidencialidad e integridad del documento, optimizando tiempos de respuestas en los procesos, reduciendo consumo de papelería, y mejorar la satisfacción de los usuarios en la recepción de los productos o bienes solicitados a través de un sistema transaccional de gestión.

2.7 OBJETIVOS ESPECÍFICOS

- ✓ Garantizar y mantener la confidencialidad e integridad de documentos transaccionales.
- ✓ Reducir tiempos en procesos operativos, administrativos con la incorporación de la seguridad en los mismos.
- ✓ Agilitar trámites administrativos para el pago de proveedores, mediante la aprobación de documentos.
- ✓ Legalizar documentos transaccionales mediante el registro de firmas digitales.
- ✓ Reducir insumos de papelería, previniendo la contaminación y beneficiando al cuidado del medio ambiente, garantizado mediante tecnología segura.
- ✓ Beneficiar al usuario final mejorando su desempeño.

2.8 DISEÑO DE LA IMPLEMENTACIÓN EN LA LEGALIZACIÓN DE DOCUMENTOS TRANSACCIONALES EN EL SISTEMA LOGÍSTICO.

La implementación dentro del sistema logístico en el proceso de adquisición consiste en realizar el siguiente procedimiento:

Para FIRMAR:

1. El usuario ingresa al sistema mediante el uso de credenciales de acceso.

2. El usuario cuenta con el perfil necesario para poder realizar la consulta de documentos para iniciar un proceso de adquisiciones, o para elaborar documentos nuevos, tales como: AUTORIDAD u OPERADOR.

- ✓ Si el perfil es de tipo autoridad o directivo tendrá la facultad de firmar los documentos que tenga asignados mediante un certificado digital o archivo certificado, el cual obtendrá de un dispositivo “token” mediante una clave.

- ✓ Si el perfil es de tipo operador o asistente tendrá la facultad de realizar documentos y establecer sus firmantes, este perfil asigna al directivo que deba firmar el documento.

3. Si el documento del proceso es nuevo el usuario deberá establecer quien debe firmarlo; en el sistema existe personal para la firma de documentos según el área que este se encuentre, en algunos casos pueden existir 3 personas que puedan autorizar la adquisición, pero para iniciar el proceso se requiere la firma de uno.

4. Si el documento del proceso es para continuar el proceso, el usuario deberá elegirlo para establecer quien debe firmarlo para su continuidad.

5. El documento aprobado para la compra es precedente para la realización del pago de la misma.

6. El documento pagado es precedente para la realización del ingreso del material a las bodegas de la organización o en su defecto a su localidad destino.

Para OBTENER el CERTIFICADO DIGITAL:

1. La autoridad o directivo debe contar con un dispositivo electrónico en el cual se almacena el certificado digital, el dispositivo puede obtenerse al momento de solicitarlo al personal te Talento Humano, encargado de designarlo en rol de AUTORIDAD en el sistema transaccional.

2. El operador del sistema transaccional, en la sección de recursos humanos, registra a la autoridad con el rol de AUTORIDAD, además genera el certificado digital a través del sistema de la autoridad certificadora empleando los datos de la AUTORIDAD propietaria del certificado.

3. El certificado digital es generado en el sistema de la autoridad certificadora con un mecanismo de seguridad propio de la CA[2], es decir empleando un algoritmo de cifrado, y empleando claves pública y privada.

4. El certificado es copiado a través de la CA al dispositivo de almacenamiento (token).

5. El dispositivo es entregado a la AUTORIDAD, con la respectiva indicación de uso.

Para REVOCAR el CERTIFICADO DIGITAL.

1. El certificado digital se revoca a través del sistema de la autoridad certificadora, por motivos como: fecha de vencimiento del certificado, pedido de la AUTORIDAD, cese de funciones de la AUTORIDAD, pérdida del dispositivo.

2. El procedimiento de revocación debe ser formalizado y enviado al departamento de TALENTO HUMANO.

[2] Certicate Authority

CAPÍTULO 3

IMPLEMENTACIÓN DE FIRMA DIGITAL EN EL SISTEMA TRANSACCIONAL EN PROCESOS DE UNA ORGANIZACIÓN GUBERNAMENTAL, INNOVACIÓN TECNOLÓGICA SEGURA EN LA CADENA LOGÍSTICA.

La implementación de firma digital en una organización que gestiona procesos empleando documentos de un sistema transaccional, debe establecer pasos que permitan desarrollar un correcto funcionamiento en el uso de la firma digital.

La organización determina el alcance de legalización de documentos para implementar el uso de la firma; se realiza la elección de una CA[3] acorde a las necesidades y como un componente fundamental de una Infraestructura de Clave Pública (PKI).

1ero. Instalar y Configurar una CA en el caso de ser interna, de ser externa se debe cumplir procedimientos establecidos por la CA seleccionada:

- ✓ Interno: interna a la organización.
- ✓ Externo: externa a la organización y con reconocimiento internacional.

La elección del alcance de la CA depende de la organización; la organización determina si el reconocimiento de las firmas tendrá un ámbito interno o externo, de esta manera permite establecer procedimientos para su obtención; indica el cumplimiento de reglamentos, la ley vigente de comercio electrónico, y fundamentalmente la documentación interna o externa que se legalice para su reconocimiento. De ser interna la CA garantiza la revocación y validez de cada certificado cumpliendo principios de una PKI y de una CA externa.

El propósito de la CA interna es medir, analizar y evaluar la capacidad de gestión de una organización en sus procesos mediante la implementación. Una vez alcanzado un grado de madurez adecuado con una CA interna se sugiere emplear la CA externa.

[3] CA Certificate Authority

2do. Instalar y Configurar una RA (Autoridad de Registro), la RA permite obtener los datos a través de formularios que permiten la generación de la información que se registra en los certificados digitales, para el estudio se trata de personas de la organización, sin embargo el ámbito de extensión de certificados pueden ser inclusive para servicios de la misma organización, entre otros.

3ero. Elegir el o los mecanismos de almacenamiento de los certificados para su uso; En el mercado actualmente se emplean diversos mecanismos de almacenamiento de certificado, autenticación y firma digital asociados a los formatos o principios criptográficos de una PKI. El mecanismo a emplearse en el contexto del desarrollo de este tema es el eToken, mecanismo empleando en la PKI.

4to. El mecanismo determina la factibilidad de uso, procedimientos, almacenamiento del certificado digital, además de los algoritmos de integridad de datos que se usan.

Por lo tanto todo proceso que involucre firma digital requiere de una autoridad de certificación; la autoridad es el ente notarial para el reconocimiento de firmas a través de sus certificados digitales. La CA[4] establece su legitimidad y su uso público, además los algoritmos de cifrado o criptografía que se emplean.

La RA [5] junto con la CA determinan el reconocimiento institucional o nivel internacional de la firma; si la implementación se la realiza mediante la autoridad de registro (RA) del Banco Central del Ecuador, su reconocimiento será de ámbito nacional; si requiere el reconocimiento institucional únicamente, se puede emplear

[4] Certificate Authority
[5] Register Authority

una RA inmersa en el EJBCA[6], y designar al departamento de Talento Humano que cumpla la función de emisor de certificado digital.

Durante el estudio en cuestión se emplea EJBCA, un aplicativo de uso libre en su versión no comercial que brinda las bondades de una CA.

EJBCA es un software de Autoridad Certificadora PKI, desarrollada en tecnología Java (JEE) con versiones comercial (Enterprise) y no comercial (Community), es una plataforma independiente, robusta, flexible, de alto performance, escalable, y componentes basados en una CA para ser usado como stand-alone o integrarse con otras aplicaciones. [8]; EJBCA soporta algoritmos para cifrado como son: RSA hasta 8192 bits, DSA[7] con 1024 bits, ECDSA[8]; múltiples algoritmos de hash para firmas basados en SHA-1, SHA-2.

Si el alcance de la CA es externo esta a su vez debe emplear una RA externa; La Subsecretaría de Gobierno Electrónico y SENATEL reconocen al Banco Central del Ecuador como el ente gobernante, autorizador de certificados y firmas digitales en el País, el BCE establece los procedimientos para la obtención de la firma digital acorde estándares de criptografía tales como: PKCS (Public-Key Cryptography Standards) y CMS (Cryptographic Message Syntax), estos procedimientos son similares a los empleados en el EJBCA no comercial, con la diferencia que para la implementación los certificados serán reconocidos en el medio interno que se lo realice.

[6] Enterprise Java Bean Certificate Authority
[7] Digital Signature Algorithm
[8] Elliptic Curve Digital Signature Algorithm

Para el reconocimiento a nivel nacional o para emplear el uso de una CA externa, uno de los principales procedimientos es la obtención de firma digital de la CA Banco Central del Ecuador, el solicitante puede generar una solicitud de certificado a través de la dirección web del Banco Central del Ecuador:

“http://www.eci.bce.ec/web/guest/solicitud-de-certificado”. En la opción Certificacion Electronica.

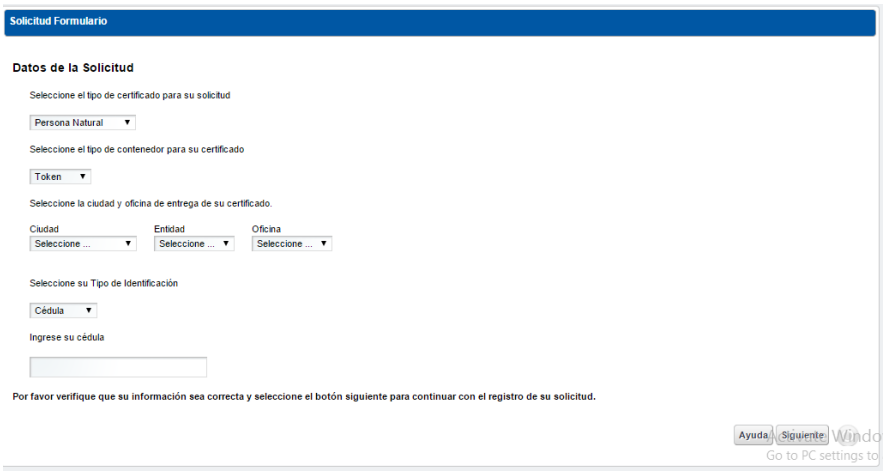

Figura 0.1 SOLICITUD FORMULARIO DE FIRMA

En la solicitud se detalla los parámetros necesarios para obtener la firma como son:

- El Tipo de certificado: Funcionario Público, Persona Natural, Persona Jurídica.
- El tipo de contenedor para el certificado: Token, Archivo, HSM y Roaming.
- Lugar de entrega del certificado: Quito, Guayaquil o Cuenca.
- Tipo de identificación: Cedula o pasaporte.

La CA[9] remitirá la firma luego que la organización o ente solicitante envié la documentación necesaria para obtener la misma, cabe mencionar que una persona podrá disponer de más de un certificado dentro de los niveles de firma que existen para el efecto: persona natural, persona jurídica (representante legal y/o perteneciente a empresa), funcionario o servidor público.

La organización o entidad solicitante será la encargada de recopilar la información sujeta a los formatos establecidos por la CA, para la generación de firmas a través de: tokens, archivos u otro medio.

El certificado almacenado contendrá la información:

a. Identificación de la Entidad de Certificación de Información.
b. Los datos del titular del certificado que permitan su ubicación e identificación.
c. Las fechas de emisión y expiración del certificado.
d. El número único de serie que identifica el certificado.
e. Clave pública del titular del certificado.
f. Puntos de distribución (URL) para verificación de la CRL.

Los certificados digitales pueden ser almacenados en cuatro tipos de contenedores:

- Token (Dispositivo seguro USB), ideal para transacciones en donde el usuario a través de una clave de mínimo 8 dígitos (PIN Token), posee físicamente dicho dispositivo al momento de hacer cada transacción, funciona en ambiente Windows preferentemente, en otros plataformas es

[9] Certificate Authority

necesario conocer su compatibilidad de acuerdo al modelo y versión de sistema operativo.

- Archivo, ideal para realizar transacciones de forma masiva, se lo puede colocar en un servidor o en computador. El usuario debe proteger en todo momento dicho archivo y las copias que realice del mismo, el certificado posee una clave acceso. Sirve en cualquier sistema operativo es un certificado estándar x.509 en formato p12 o PFX

- HSM [10] , dispositivo de alta seguridad que permite realizar varias transacciones por segundo (transacciones de forma masiva), cumple con altos estándares de seguridad.

- ROAMING, le permite realizar operaciones mediante el uso del applet publicado por la ECIBCE o un aplicativo opcional llamado ESP[11].

Una vez que la CA[12] genero el certificado, el usuario propietario del certificado lo almacena en un mecanismo propicio para su uso tal como se describe anteriormente, el procedimiento se lo realiza solo la primera vez estableciendo un nexo entre el certificado y el mecanismo de almacenamiento, garantizando confidencialidad en la recepción del certificado.

Habiéndose relacionado los datos del firmante con el certificado almacenado en el dispositivo, se podrá firmar digitalmente los documentos mediante el mecanismo de almacenamiento; si el sistema transaccional permite la lectura del certificado digital

[10] HSM (Hardware Security Module)
[11] ESP (Entrust Security Provider). Proveedor de Seguridad Confiable.
[12] CA Certificate Authority

almacenado. Existen librerías desarrolladas en Java como son: ItextPdf[13] y Bouncy Castle[14], que permiten esta funcionalidad.

ItextPdf es una librería que permite la elaboración de documentos digitales en diversos formatos, el empleado para el estudio es PDF, permite firmar el documento manteniendo su creación y lectura en memoria.

Bouncy Castle es una librería que aplica criptografía en el desarrollo de la firma, y que se relaciona con ItextPdf. Con el mecanismo de firma, los dispositivos pueden ser leídos por la API o librerías de acceso, para lo cual el desarrollador de la aplicación deberá emplear su destreza para elaborar la lectura del certificado y plasmar la firma en el documento.

3.1 INFRAESTRUCTURA TECNOLÓGICA DE LA FIRMA DIGITAL.

La infraestructura tecnológica se divide en dos aspectos: Software y Hardware.

Tabla 12 SOFTWARE DE IMPLEMENTACIÓN y PROTOCOLOS

SOFTWARE	
Servicios EJBCA	**EJBCA / RA.** El RA es una aplicación web que permite el registro de las entidades que requieren de certificados válidos para firmar, su implementación está basada en Jboss 8 (Wildfly 8.1). Como instalar y configurar EJBCA (Ver Anexo 5)
	EJBCA / CA El CA es una aplicación web que permite la emisión y revocación de certificados digitales, su implementación está basada en

[13] Librería o API de Java
[14] Comunidad Open Source Criptográfico.

	Jboss 8 (Wildfly 8.1). Como instalar y configurar EJBCA (Ver Anexo 5)
Sistema Transaccional	El sistema transaccional permite elaborar documentos transaccionales como ordenes, actas de recepción, entre otros, desarrollados usando las librerías ITextPDF y Bouncy Castle, un framework para la capa Web denominado Primefaces 5, que permite visualizar los documentos elaborados y a su vez firmarlos empleando ITextPDF. El sistema de información transaccional emite documentos dispuestos para la firma, este servicio permite la interoperabilidad del dispositivo de almacenamiento y el documento a legalizar.
	Con el propósito de mitigar las vulnerabilidades presentadas en SSLv3 a través de POODLE (Padding Oracle On Downgraded Legacy Encryption, o en su traducción, "Oráculo del relleno para cifrado antiguo y degradado"), los servicios o servidores de aplicación únicamente permiten el uso de TLS en las versiones 1.0, 1.1, y 1.2.

El sistema transaccional se desarrolla con un framework[15] que permite trabajar con componentes que soportan HTML5, esta versión de HTML en la actualidad se soportan únicamente por Firefox, Google Chrome pero no Internet Explorer, por lo cual una de las limitantes para el uso de la solución son los navegadores.

La implementación de TLS en Jboss 8 se la realiza a través de la siguiente configuración:

Tabla 13 LÍNEA DE CONFIGURACIÓN TLS PARA JBOSS 8

Línea de Configuración para Soportar TLS en Jboss 8
<https-listener name="httpspriv" socket-binding="httpspriv" security-realm="SSLRealm" verify-client="REQUIRED" enabled-protocols="TLSv1,TLSv1.1,TLSv1.2" />

[15] Herramienta para desarrollo de programación.

Los elementos de software se asocian a los elementos de hardware siguientes:

Tabla 14 HARDWARE DE IMPLEMENTACIÓN

HARDWARE	
Dispositivo de Almacenamiento	

Figura 0.2 eToken Pro 72K (Java)

Los elementos de software y hardware se relacionan de la siguiente manera, permitiendo el funcionamiento para la elaboración de la firma en el documento.

El fragmento de código Java empleado para implementar la firma digital a través de las librerías ITextPdf en el documento es:

Tabla 15 FRAGMENTO DE CÓDIGO JAVA PARA FIRMAR DOCUMENTO

Fragmento de Código Java para Firmar.

```
public ByteArrayOutputStream signPdf(Documento documento, PrivateKey pk,
Certificate[] chain, String providerBC) throws IOException,
DocumentException, GeneralSecurityException {

    // reader and stamper

    PdfReader reader;

    reader = new PdfReader(documento.getDocumentoFile());
```

```
        ByteArrayOutputStream output = new ByteArrayOutputStream();

        PdfStamper stamper = PdfStamper.createSignature(reader, output, '\0', null, true);

        // appearance

        PdfSignatureAppearance appearance = stamper.getSignatureAppearance();

        appearance.setReason("I've written this.");

        appearance.setLocation("Foobar");

        appearance.setVisibleSignature(new Rectangle(72, 732, 144, 780), 1, "first");

        // digital signature

        ExternalSignature es = new PrivateKeySignature(pk, DigestAlgorithms.SHA256, providerBC);

        ExternalDigest digest = new BouncyCastleDigest();

        //añadiendo un CRL list al PDF

        List<CrlClient> crlList = new ArrayList<CrlClient>();

        crlList.add(new CrlClientOnline(chain));

        MakeSignature.signDetached(appearance, digest, es, chain, crlList, null, null, 0, CryptoStandard.CMS);

        return output;

    }
```

La función signPdf empleada requiere los parámetros como:

Tabla 16 PARÁMETROS PARA FUNCIÓN DE FIRMA DIGITAL

Parámetro	Definición
Documento documento	Es el documento que se procede a firmar, Documento es la entidad mapeada de la base de datos, la misma que cuenta con los datos de cabecera y detalle del documento, como el listado de bienes.
PrivateKey pk	Es la clave privada almacenada en el dispositivo que se emplea para cifrar el documento.
Certificate[] chain	Es el certificado digital para establecer quien firma el documento.
String providerBC	El nombre del dispositivo de almacenamiento.

La función retorna un objeto ByteArrayOutputStream, que es el objeto de Java que permite manipular la memoria RAM, tipo buffer. En el Objeto ByteArrayOutputStream se almacena temporalmente el documento firmado que luego se procede a ser registro en la base de datos transaccional.

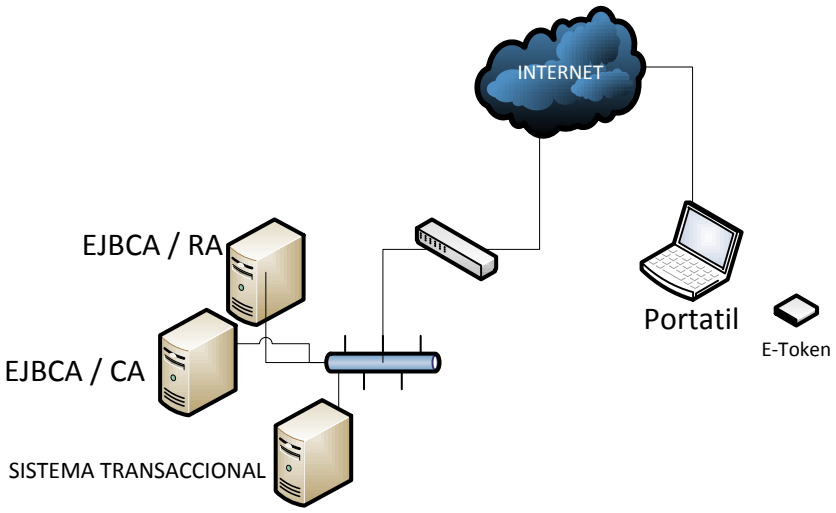

Figura 0.3 ESQUEMA DE LA IMPLEMENTACIÓN DE CA

El gráfico presenta el esquema de implementación de una CA interna, los servicios a emplearse para el propósito de implementación; Con este modelo el usuario debe ingresar el etoken al computador para elaborar la firma en un documento transaccional.

En el uso de la infraestructura tecnológica del Banco Central del Ecuador la firma digital o el diseño de la firma emplea formatos establecidos por la ietf.org (The Internet Engineering Task Force), referenciados en su RFC (Request for Comments), algunos formatos o estándares autorizados por el Banco Central del Ecuador para firma electrónica son los siguientes:

1. PKCS#7 / CMS.
2. Firma XML
3. PDF (PKCS#7)

Existen técnicas o infraestructuras para la elaboración del firmado de documentos:

1. Aplicación completamente cliente.
2. Aplicación completamente servidor.
3. Aplicación cliente/servidor.

3.2 ESQUEMA DE SEGURIDAD, NIVELES, ROLES, OBTENCIÓN DE "TOKENS" DE FIRMAS.

Para la obtención de tokens se mantiene el nivel de privacidad realizado por el Banco Central del Ecuador, el cual describe que para su obtención debe el solicitante acercarse con documentos de identificación para su elaboración y retiro, se sociabiliza el registro y uso de token al usuario.

Durante la entrega del certificado se relaciona el rol de autoridad en el sistema transaccional al usuario solicitante autorizado, así se reconoce a la autoridad y al operador.

En el esquema de seguridad; El sistema transaccional genera los respectivos controles de accesos por usuario y clave, brinda los permisos a las opciones para firmar documentos mediante la creación de roles, en este caso el rol de directivo o en su defecto autoridad se encarga de legalizar documentos, y el rol de operador es el encargado de elaborar la documentación a firmar o legalizar.

Tabla 17 ROLES Y PERMISOS

ROLES Y PERMISOS	
DIRECTIVO O AUTORIDAD	Encargado de legalizar la documentación necesaria para iniciar o dar continuidad a un proceso de la organización.
OPERADOR	Encargado de elaborar la documentación requerida para el inicio o continuidad de un proceso.

El nivel de acceso del sistema transaccional básicamente se debe a las credenciales (usuario y clave) facilitadas por el personal de administración del sistema, estas credenciales pueden identificar si la persona autenticada es o no un directivo autorizado para firmar documentos.

Ejemplo: Luis Peña Herrera registra en el sistema transaccional ser un usuario con el rol de autoridad, pero no cuenta con el certificado emitido por el sistema EJBCA; Luis no se encuentra autorizado a firmar documentos, mientras que Ana Gabriel Gerente del área de TI cuenta con el rol de autoridad y con el certificado emitido por el EJBCA, por lo tanto puede con un etoken firmar documentos, pero el sistema permite firmar únicamente los documentos que deba realizarlo, es decir, la autoridad de TI no controla bodegas por lo tanto no debe firmar tales documentos, sin embargo puede firmar el documento de solicitud de compra para iniciar un proceso como necesidad.

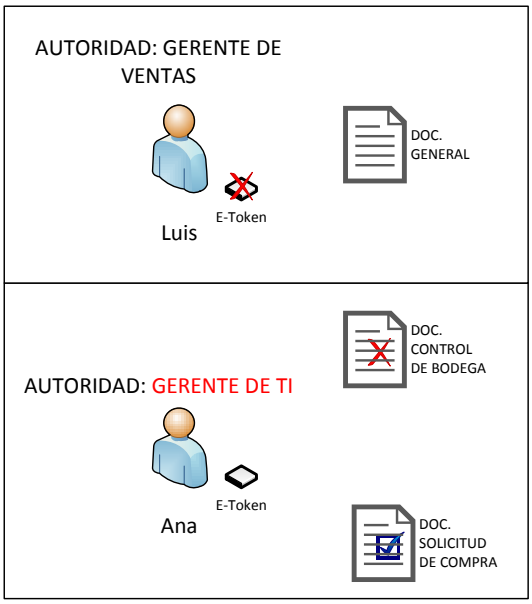

Figura 0.4 ROL DE AUTORIDAD

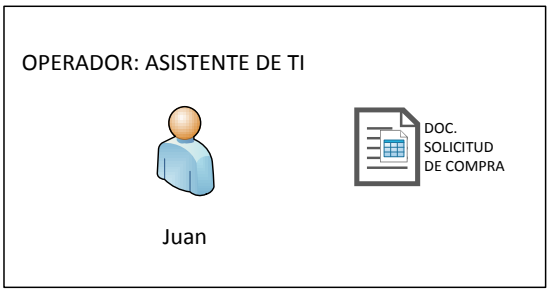

Figura 0.5 ROL DE OPERADOR

Juan, Asistente de TI elabora con el rol de operador asignado el documento de solicitud de compra de TI, uno de los documentos habilitantes para iniciar un proceso de adquisiciones; Juan registra el documento, el mismo que se transfiere al guardarlo a Ana para revisarlo y firmarlo; Ana autoridad del departamento TI legaliza el documento empleando el certificado del e-token.

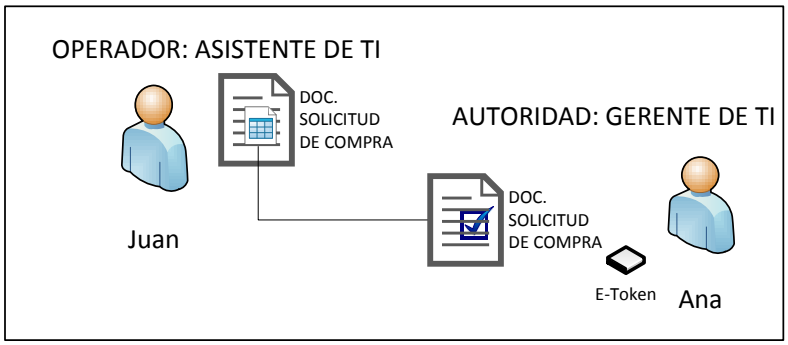

Figura 0.6 PROCESO DE OPERADOR

El mecanismo para asignar roles, está sujeto a la responsabilidad delegada que tiene cada directivo de la organización, el mismo que debe ser controlado por el personal de Talento Humano de la organización.

3.3 VERIFICACIÓN DE FIRMAS EN LA LEGALIZACIÓN DE DOCUMENTOS DURANTE LA ELABORACIÓN DE PROCESOS TRANSACCIONALES.

Existen situaciones en las cuales personal de la organización se retira entregando el cargo definitivo, por cualquier motivo; En estos casos se debe aplicar el procedimiento de revocación de certificado. Si el personal que deja funciones tiene el rol autoridad en la organización, el Departamento de Talento Humano debe retirarle permisos, roles, liberar el token mediante la eliminación del certificado, y finalmente revocar el certificado emitido en el EJBCA inmediatamente se desligue de sus funciones. El Departamento de Talento Humano debe asignar la responsabilidad al nuevo personal siguiendo el procedimiento de asignación de rol y certificado al cargo de la autoridad saliente con un nuevo certificado correspondiente emitido y almacenarlo en el etoken liberado.

Si el personal se retira temporalmente, en el sistema se puede generar delegaciones estableciéndose cargos temporales para firmar documentos en sustitución del personal saliente.

Si un certificado se revoca este no podrá ser usado para firmar digitalmente ningún documento de la organización como política de seguridad. Si la persona logoneada al sistema, quiere usar el certificado revocado el sistema evaluara la CRL (Lista de Certificados Revocados) en la cual consta que no cuenta con la validez necesaria para firmarlo.

Previa la firma de un documento, se verifica la validez del certificado contra la CA, a través de las CRL (Listas de revocación), este procedimiento es dependiente de las condiciones que se establezcan por el personal de Talento Humano, es decir si no se revoca el certificado este mantendrá su validez durante el tiempo que se haya designado.

Figura 0.7 VERIFICACIÓN DE FIRMA

Si un documento se elimina, el documento queda inactivo sin embargo el firmante permanecerá asociado como histórico; si al usuario se le retira el rol de autoridad, el sistema mantiene la constancia de la gestión realizada como firmante autorizado durante el periodo laboral.

3.4 PROCESOS DE LA CADENA LOGÍSTICA IMPLEMENTANDO FIRMA DIGITAL.

Se realiza el procedimiento de firma en los diversos procesos y niveles de la cadena logística, se conserva el grado de responsabilidad que conlleva tener el rol de autoridad para firmar un documento digitalmente, es similar al de la firma manual; se distingue entre documentos oficiales como: memo, oficio y documentos transaccionales como: solicitud de compra, acta de inspección en la que se involucra básicamente los bienes o servicios a recibir descritos en detalle.

En capítulos anteriores se menciona el ciclo logístico y sus fases; En este trata las fases del ciclo en detalle para conocer la relación con la firma digital.

Previo el inicio del desglose de las fases, cabe mencionar que durante las etapas o fases del ciclo logísticos se denotan dos tiempos: tiempo B o año actual y tiempo B+1 o año siguiente. En el año actual se debe elaborar la ejecución del gasto público de lo planificado el año anterior, y además se debe elaborar la planificación de la necesidad del siguiente año o B+1.

En el proceso de planificación, el documento habilitante en las organizaciones gubernamentales se denomina PAC[16], el PAC o Plan Anual de Contrataciones es el documento que permite realizar una planificación general para la organización. El plan anual contempla la planificación a nivel de departamentos, partidas y sus respectivas estructuras financieras.

Planificación.-

La planificación se elabora por cada departamento y se revisa por la autoridad departamental pertinente para su aprobación, la planificación revisada y aprobada se envía al Director de Planificación de la organización; El director verifica, consolida de ser necesario la planificación, legaliza y entrega al SERCOP [7] a través del SOCE (SISTEMA OFICIAL DE CONTRATACIÓN), el PAC es el documento de planificación anual, que se utiliza en ejecución el año siguiente o también denominado financieramente B+1.

El bien o servicio que no conste en el PAC durante el año de ejecución no puede ser adquirido, para adquirirse debe agregarse al PAC con previa autorización, además se debe elaborar las reformas presupuestarias necesarias para adquirirlo.

[16] Plan Anual de Contratación

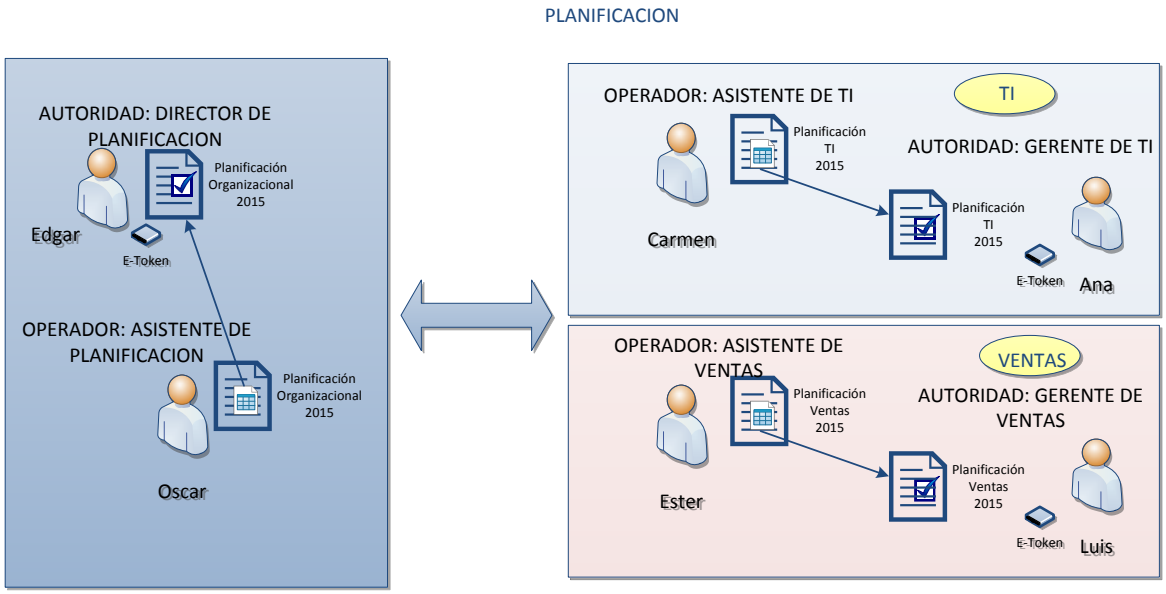

Figura 0.8 PROCESO DE PLANIFICACIÓN

Como se muestra en la gráfica; Durante el proceso de planificación se elabora el documento transaccional de planificación el mismo que se legaliza y revisa por la autoridad departamental, la planificación elaborada entre operador y autoridad de cada departamento se registra en el sistema transaccional cuantificando las revisiones pertinentes previo envió al Director de planificación.

El Director de planificación recibe la planificación por unidad organizacional, consolida, revisa, legaliza y presenta observaciones de ser necesario a los respectivos departamentos involucrados, establece las cantidades consolidadas.

El Director de Planificación revisa, y establece los montos requeridos para el gasto público del siguiente año, se envía el PAC al SERCOP en espera de su revisión por el Ministerio de Finanzas, el PAC de la organización se analiza en conjunto a los

demás PACS de las otras entidades gubernamentales, fin establecer acuerdos de fondos públicos para la ejecución el siguiente año, acorde a las prioridades del Gobierno. Entre los acuerdos adquiridos se suscitan cortes presupuestarios, modificaciones, etc.

Con las modificaciones acordadas se ajusta la planificación inicial a los montos definidos por el ministerio para iniciar la etapa del ciclo logístico denominada adquisición durante los primeros meses del año siguiente; en esta etapa el PAC es el documento referente para elaborar las contrataciones, además las respectivas modificaciones de existir bienes o servicios no contemplados en la planificación.

Adquisición.-

El SERCOP brinda un servicio o aplicativo configurable denominado USHAY[17], el aplicativo permite la elaboración de pliegos contractuales; en los pliegos se describe las consideraciones de contratación, los montos, las partidas presupuestarias, garantías técnicas, personal que se requiere con el aval técnico requerido, entre otros aspectos destinados para gestionar el contrato.

El pliego elaborado se legaliza como documento habilitante para la compra, sin embargo existen documentos adicionales como son: Informe de Necesidad, Orden de Compra, Certificación Presupuestaria, que requieren ser gestionados, para emitir la documentación requerida por la Unidad de Compras y gestione la adquisición de lo requerido.

[17] Termino en Idioma Quichua.

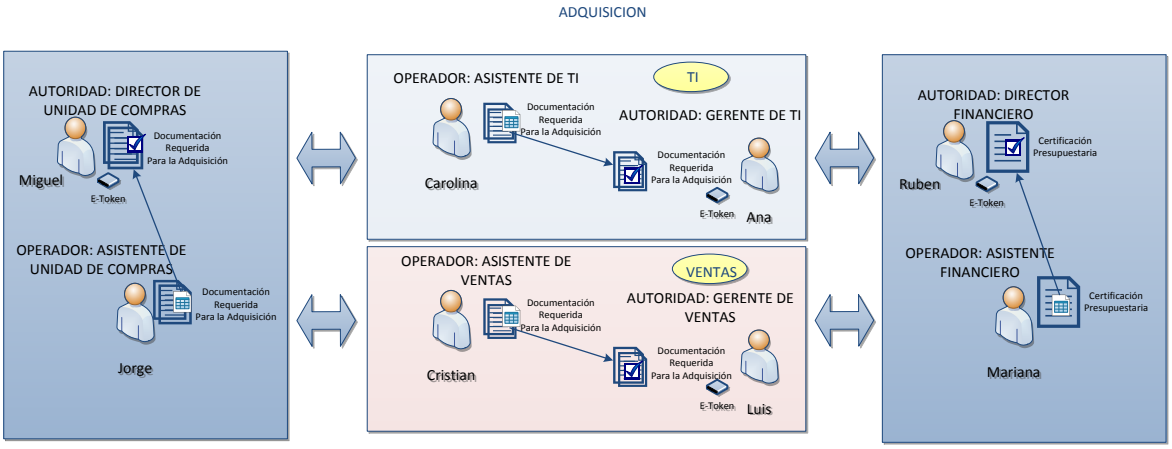

Figura 0.9 PROCESO DE ADQUISICIÓN

Las unidades o departamentos de cada entidad pública cuentan con un administrador financiero o director financiero, esta entidad controla la entrega de fondos durante la etapa de ejecución; el documento que certifica los fondos necesarios para la adquisición es la certificación presupuestaria; la certificación la emite el departamento financiero y en el se indica la estructura financiera a ser empleada en el proceso de adquisición, además de confirmar la existencia de fondos necesarios y suficientes para la compra.

El Informe de necesidad permite detallar el porqué de la adquisición o contratación, indica la problemática hallada y los beneficios al adquirirse lo expuesto en él documento, el informe detalla en forma general lo que está por adquirirse, además de remitirlo a la unidad de compras como documento habilitante para la adquisición, se debe remitir a la unidad financiera para el trámite o gestión de la certificación presupuestaria.

Se elabora un documento adicional que se denomina solicitud de compra, este documento describe los bienes a ser adquiridos, detallando las características específicas como son: modelo, serie, cantidad, precio, y monto total estimado de compra, es similar a la cotización o proforma emitida por un proveedor; la solicitud de compra se elabora por el departamento que emite el informe de necesidad. El documento de solicitud se transmite a la unidad de compra legalizada por la autoridad departamental pertinente.

Finalmente elaborados: informe de necesidad, solicitud de compra, gestionada la certificación presupuestaria o financiera, elaborado pliego en USHAY, la unidad de compras recibe la documentación para revisión, análisis, e iniciar el proceso de contratación empleando el mecanismo del portal de compras públicas.

El proceso de adquisición a través del portal tendrá el tiempo necesario para llegar a un acuerdo expuesto tanto por la parte contratante como la oferente. Una vez llegado a un mutuo acuerdo la unidad de compras elabora la orden de compra o servicio, que describe los bienes que se adquieren, el precio real de adquisición, montos acordados de pagos, tiempo de entrega, lugar de entrega, etc.

El documento de orden de compra se legaliza por la unidad de compra, y se remite al departamento de contabilidad para tramitar los pagos respectivos en los tiempos y plazos acordados; luego que se realiza el pago parcial o pago total de la orden de compra, se puede realizar el ingreso del material o bienes a bodega para su correspondiente distribución.

Distribución.-

Para el registro de materiales en bodega y su distribución se necesita: la orden de compra legalizada por la unidad de compras, y la unidad de contabilidad del departamento financiero, dando garantías de los pagos acordados; el director de bodegas adicional se le suma el proceso generado en el portal de compras públicas, que brinda la constancia de la adquisición.

DISTRIBUCION

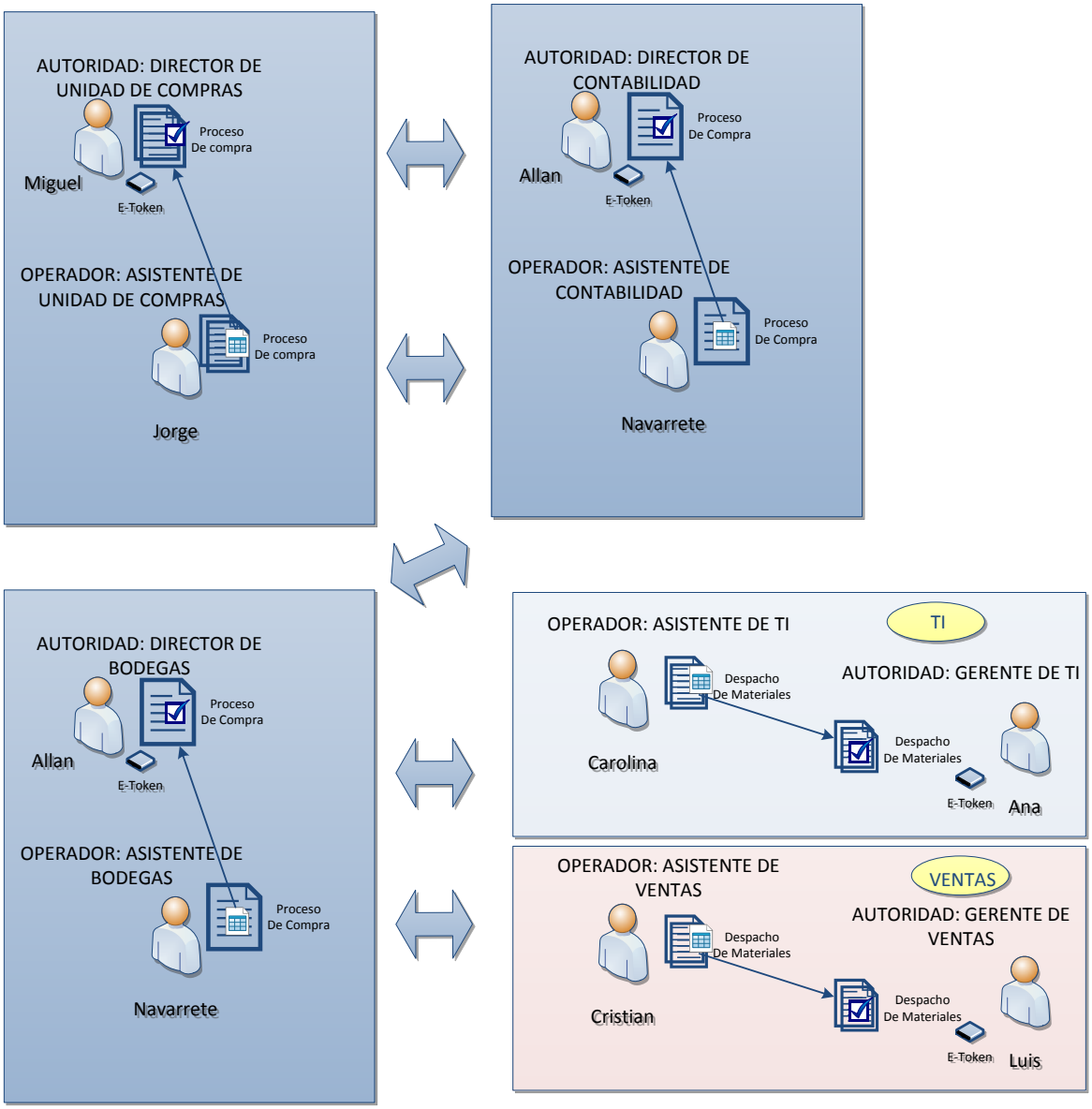

Figura 0.10 PROCESO DE DISTRIBUCIÓN

El registro de materiales en la bodega se inicia con la recepción de la orden de compra legalizada, mediante su revisión y aprobación se procede a realizar el registro del material mediante el acta de inspección o comprobante de ingreso del

material, se verifica que el material sea nuevo, buen estado, con las especificaciones y garantías técnicas descritas en el pliego, se recibe el bien junto al personal técnico correspondiente que audite la entrega.

Realizada la inspección técnica y luego de haber elaborado el acta de inspección o comprobante de ingreso en la bodega de tránsito, se legaliza el acta o comprobante de la recepción para elaborar el traspaso a la bodega final o definitiva del material revisado; se incrementa existencias o nuevos registros del material a la bodega mediante el documento de traspaso, se verifica los movimientos de los bienes ingresados a través de las existencias y se procede a legalizar el traspaso; el traspaso realizado habilita la realización del despacho del material de la bodega a su destino final.

Con los valores de las cantidades registradas en las existencias, y el documento de traspaso legalizado; se elabora el documento de despacho del material para la entrega a su destino final. De esta forma de presenta la implementación en el ciclo logístico de la firma digital, se da a conocer los pasos que se elaboran desde la adquisición hasta la recepción del material necesario en una organización pública.

CAPÍTULO 4

ANÁLISIS DE RESULTADOS.

4.1 VERIFICACIÓN DE LOS DOCUMENTOS QUE SE HAN LEGALIZADO MEDIANTE LA IMPLEMENTACIÓN DE FIRMA DIGITAL.

La verificación de documentos permite consultar los documentos firmados digitalmente en el sistema transaccional; brinda continuidad a los respectivos procesos internos de la organización, facilita la verificación mediante la respectiva numeración y código del documento; entre las opciones de consulta se puede realizar mediante el parámetro del tipo de transacción o documento de manera general.

La verificación permite visualizar la trazabilidad del documento firmado, es decir quien lo elaboro, quien lo firmo, quien lo recibe, etc. Facilita el seguimiento y control de los documentos en un proceso.

Figura 0.1 PANTALLA DEL RECORRIDO DEL DOCUMENTO

Uno de los mecanismos de verificación de firma digital empleado por la PKI es la CRL[18] (Lista de Certificados Revocados), La CRL indica si el certificado se ha revocado, el certificado puede ser utilizado sin embargo la firma no es válida.

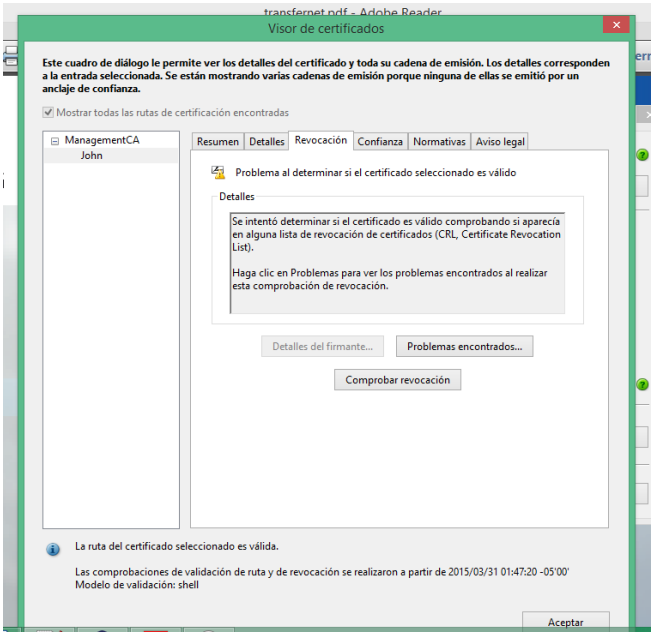

Figura 0.2 VISOR DE CERTIFICADO CRL LIST

[18] Certificate Revocation List

La CRL es un mecanismo de control propio de la CA[19], la programación realizada en Java permite obtener la lista y determinar la validez del certificado.

4.2 INDICADORES DE CONTROL DEL SISTEMA TRANSACCIONAL EN LA LEGALIZACIÓN DE DOCUMENTOS MEDIANTE FIRMA DIGITAL.

Los indicadores de control del sistema transaccional, permite conocer si existen documentos que se han quedado sin tramitar, se realizan observaciones para realizar correcciones y mejoras en procesos similares y futuros.

El indicador de control que permite analizar la relación de documentos firmados contra documentos elaborados de procesos registrados en el sistema transaccional pertenecientes a un departamento organizacional es:

Tabla 18 INDICADOR DE CONTROL DE DOCUMENTOS

CONTROL DE DOCUMENTOS DE SOLICITUD DE COMPRA X LEGALIZAR
Solicitudes Firmadas / Solicitudes Elaborados.

El indicador de control manifiesta la gestión de documentos de procesos que un departamento realiza entre la autoridad y operador; se compara la actividad de un departamento contra otro que desempeña similar gestión, y se obtienen mejoras en el caso que las relaciones demuestren resultados positivos con el departamento comparado; finalmente si el indicador es cercano a uno se observa que la actividad realizada entre autoridad y operador es casi simultaneo por ende los procesos no son dejados en tiempos muertos ni en cola; Si el indicador de control es menor a 0.5

[19] Certificate Authority

se deben tomar precauciones y realizar correctivos porque se puede tender a pérdida de tiempo en procesos innecesarios, vista los documentos se tramitan muy lento. El indicador se extiende en su uso a la orden de compra y al acta de ingreso a bodega para la emisión de pagos.

Durante la fase de inducción del mecanismo de firma digital en la organización se tuvo el indicador para medir la aceptabilidad del cambio, el mismo que determino la reacción negativa del personal.

El indicador de control para determinar la relación de procesos culminados con éxito mediante firma digital contra procesos culminados con éxito mediante firma manuscrita.

Tabla 19 PROCESOS EXITOSOS CON FIRMA DIGITAL VS MANUSCRITA

PROCESOS EXITOSOS CON FIRMA DIGITAL VS MANUSCRITA
Procesos Con Firma Digital / # Procesos Con Firma Manuscrita.

El indicador al inicio de la implementación era desalentador, debido a la reacción negativa al cambio, después de un tiempo y durante una ardua socialización de la solución se pudo lograr un incremento a tal punto que la relación fue equitativa, es decir una relación 1:1, sin embargo mediante las mejoras adecuadas en el proceso y procedimiento, el indicador demuestra la aceptación.

El indicador destinado a medir el tiempo de firmar digitalmente un documento contra el firmado manuscrito se considera equitativo, es decir se considera el mismo tiempo de uso; se considera el manejo de otros recursos como son: suministros de oficina y el talento humano; firmar el documento manuscrito conlleva el uso de un

bolígrafo, firmar un documento digital emplea el mecanismo de almacenamiento token; el tiempo en ejecutar la acción sería similar, pudiendo variar si se toma a consideración que el bolígrafo tenga o no tinta para la manuscrita, o si el computador se inhibe o no para la digital.

El indicador de control de tiempo en la gestión por procesos es:

Tabla 20 TIEMPO CON FIRMA DIGITAL VS MANUSCRITA

TIEMPO CON FIRMA DIGITAL VS MANUSCRITA
Tiempo de gestión x Proceso con FD / Tiempo de gestión x Proceso con FM

De forma similar como el indicador de aceptabilidad al cambio, el indicador de tiempo de gestión por procesos durante la etapa de inducción e implantación del servicio, presenta relaciones de tiempos elevados, en algunos casos tiempos de perdida hasta en meses con procesos no finalizados; Los tiempos se miden desde el inicio de proceso hasta su culminación, es decir, hasta la recepción del material por departamento organizacional; el indicador es medible en días, se aplica socialización del proceso para firmar, se impulsa el uso mediante la reducción de documentos físicos. Se logra estimar una relación aceptable, y se encuentra que los tiempos de gestión por procesos comparados contra los elaborados con firma manuscrita se mantienen similares. El motivo se aclara por: El proceso gestionado de adquisición depende de mecanismos externos al de legalización de documentos que considera tiempos establecidos ajenos al procedimiento de legalización de documentación; sin embargo si se asocia al indicador de control de documentos firmado contra documento elaborado se podrá notar reducción de tiempo en esta etapa del proceso.

El mecanismo de control para verificar el número de certificados revocados, permite obtener información de los diversos motivos por los que el certificado generalmente se revoca. Uno de los inconvenientes presentes en las observaciones, es el daño del dispositivo o pérdida por parte de los usuarios.

Tabla 21 CERTIFICADOS REVOCADOS VS EMITIDOS

CONTROL DE CERTIFICADO REVOCADO CONTRA EMITIDO
Certificado Revocado / Certificado Emitido.

Con el indicador se puede determinar que existe un desinterés por parte del personal al momento de manejar el dispositivo, por lo que se presentan los acuerdos con el usuario para su uso, uno de ellos es la adquisición personal del dispositivo luego de la pérdida o daño, reduciendo de esta manera la revocatoria de certificado por pérdida o avería, manteniendo un indicador bajo.

4.3 INDICADORES DE RESULTADOS ACERCA DE LA OPTIMIZACIÓN DEL TIEMPO Y OTROS RECURSOS EN LOS PROCESOS DE ADQUISICIONES Y PAGOS.

Los indicadores de resultado, totalizan los documentos tramitados con la firma digital o firma manuscrita, indica el desempeño mediante la reducción de tiempo adquirido en los procesos, además nos permite conocer resultados históricos.

Durante los años 2008, 2009, 2010 se registraron disposiciones gubernamentales que establecieron cambios que afectaron el funcionamiento operativo de las organizaciones de gobierno, tal es el caso de la creación del sistema financiero ESIGEF; la innovación e implementación del sistema impacta en el control presupuestario/financiero, manifestándose en la reducción de las compras excesivas y sin mesurar de años anteriores por las organizaciones gubernamentales, reduciendo las deudas transferidas y acumuladas año a año.

Durante los años 2011, 2012 se incorporan organismos de control como lo es el PORTAL DE COMPRAS PUBLICAS, y sus diversas innovaciones con el fin de transparentar los procesos de adquisiciones en las organizaciones gubernamentales, el índice de compras se redujo nuevamente, eliminando las adquisiciones a proveedores fijos.

Para fines del 2012 e inicios del 2013, los tiempos de procesos en la cadena logística se vuelven cuestionables; existían consideraciones relevantes más allá del tema de legalización, y de la incorporación de los diversos mecanismos

implementados por el Gobierno, se presentaban situaciones de perdida de documentación legalizada, modificaciones no registrados en los sistemas transaccionales, además de la dependencia del personal para ejecutar la acción laboral, el desconocimiento de nuevos procedimientos, la realidad requería una solución al problema mencionado.

En el año 2012, se implementa la firma digital en los procesos y procedimientos de la cadena logística; A través de diversos indicadores de control y socialización del proceso presenta una mejora sustancial en la reducción de perdida de documentación legalizada, dependencia del personal, reducción del material empleado, esto no soluciona en totalidad el problema debido a que existen diversos controles que se destinan al laborar en múltiples actividades al personal. En algunas ocasiones se llega a elaborar la tarea dos y tres veces, por el registro de información en varios sistemas de información. Así se decide integrar los sistemas quedando pendiente el estudio y el análisis de esta mejora para próximos años.

La siguiente imagen presenta la relación de líneas de tendencia por año de compras realizadas, y el tiempo promedio en días para elaborar cada una.

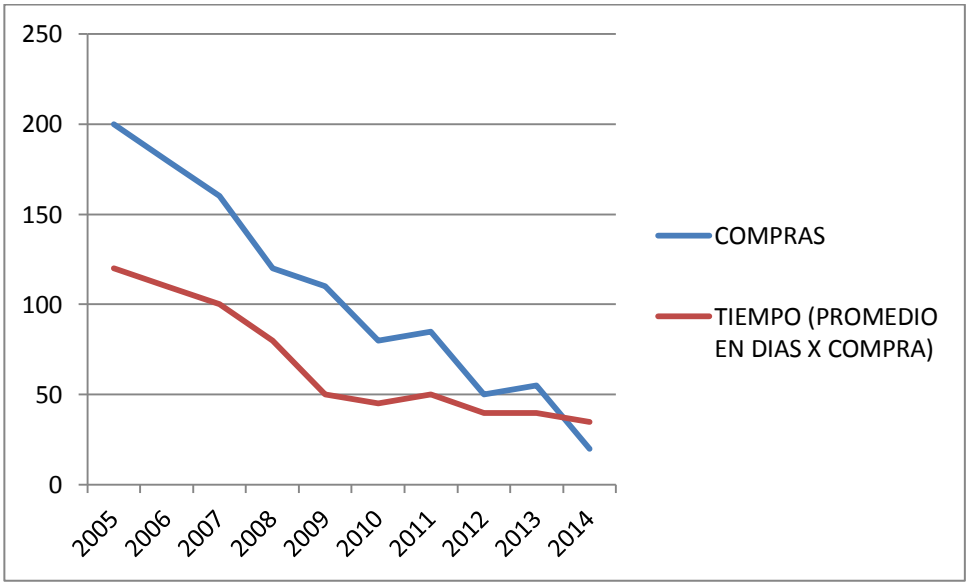

Figura 0.3 RESULTADOS DE COMPRAS ANUALES

Los datos fueron obtenidos del departamento financiero, el cual maneja el registro histórico de pagos, y procesos cancelados por año en físico.

Tabla 22 DATOS DE COMPRAS ANUALES Y TIEMPOS PROMEDIOS EN REALIZARLAS

AÑO	COMPRAS	TIEMPO (PROMEDIO EN DÍAS X COMPRA)	MECANISMO
2005	200	120	
2006	180	110	
2007	160	100	
2008	120	80	
2009	110	50	ESIGEF
2010	80	45	ESIGEF
2011	85	50	ESIGEF
2012	50	40	SERCOP
2013	55	40	SERCOP
2014	20	35	SERCOP

Se observa una tendencia en la reducción de compras, debido a los mecanismos de control de Gobierno; se realizan mejoras para planificar y adquirir por volumen (reduciendo gasto público), destinando que la compre la realice un único

departamento responsable. Por otro lado los tiempos promedios para la adquisición se mantienen constantes desde 2012 con poca variabilidad en el 2014, esto se debe a la elaboración de pliegos contractuales; documentos requeridos por el PORTAL DE COMPRAS PUBLICAS, que mantiene tiempos fijos en la ejecución de la adquisición, sin embargo los indicadores de control presentan una mejoría en los procesos internos; los indicadores de resultados por ser generales mantienen la tendencia de tiempo promedio, sin embargo no puntualizan las mejoras visibles de los indicadores de control.

4.4 CUADRO COMPARATIVO DE LAS VENTAJAS Y DESVENTAJAS QUE SE PRODUCEN AL IMPLEMENTAR FIRMA DIGITAL EN LOS PROCESOS DE ADQUISICIÓN Y PAGOS EN UNA ORGANIZACIÓN GUBERNAMENTAL.

Como se observa en los indicadores de resultados en la optimización de tiempos, la tendencia no presenta mejoría, sin embargo las observaciones halladas en los indicadores de control denota la reducción en la pérdida de documentos legalizados, además mejoras en la gestión realizada entre operador y autoridad departamental al mantener un indicador equitativo.

Antes de evaluar si existen o no ventajas en el procesos de adquisiciones, se observa el cuadro comparativo siguiente que determina si los objetivos se alcanzan o existen diferencias para cumplirlos.

Tabla 23 COMPARATIVO DE VENTAJAS Y DESVENTAJAS POR OBJETIVO

CUADRO COMPARATIVO POR OBJETIVO ESPECIFICO		
OBJETIVO ESPECIFICO	**VENTAJA**	**DESVENTAJA**
Garantizar y mantener la confidencialidad e integridad de documentos transaccionales.	Empleando el algoritmo de HASH SHA256 con RSA, permite generar valores apropiados para el par de clave pública y privada, se añade el uso del dispositivo de almacenamiento, este a su vez permite mantener privado de acceso externo alguno, y resguardado con el uso de clave de protección. En cuanto a la comunicación que se establece mediante el uso de TLS, medio de comunicación cifrado. Se brinda confidencialidad, integridad en la información, además del no repudio.	Pérdida o daño del dispositivo de almacenamiento. Vulnerabilidad de seguridad en cuanto a futuras exploraciones de protocolos de cifrado (se debe mejorar continuamente).
Reducir tiempos en procesos operativos, administrativos con la incorporación de la seguridad en los mismos.	El indicador de control que mide la gestión operador / autoridad demuestra la interoperabilidad del mecanismo, promoviendo su uso principalmente por la agilidad en el tramite operativo.	Pérdida de comunicación en los equipos, que retrasarían la gestión. Se vuelve dependiente de la red de datos o internet. Se deben mantener servicios en alta disponibilidad.
Agilitar trámites administrativos para el pago de proveedores, mediante la aprobación de	El indicador de resultado presenta una continua tendencia que a pesar de las innovaciones tecnológicas para la legalización, cuenta con mecanismos externos	Pérdida de comunicación en los equipos, que retrasarían la gestión. Se vuelve dependiente de la red de datos o internet.

documentos.	que determinan tiempos. El mantener la trazabilidad de los documentos permite llevar un mejor control con respecto a la labor operativa.	Se deben mantener servicios en alta disponibilidad.
Legalizar documentos transaccionales mediante el registro de firmas digitales.	Confiabilidad, seguridad en la realización del trámite administrativo,	Cambios tecnológicos e innovaciones modernas pueden presentar vulnerabilidades que determinen una oportunidad de mejora, como por ejemplo: implementar firma digital con la huella dactilar empleando tablets o telefonía móvil. Donde los dispositivos deban guardar registros de archivos.
Reducir insumos de papelería, previniendo la contaminación y beneficiando al cuidado del medio ambiente, garantizado mediante tecnología segura.	No se requieren de documentación física para la gestión administrativa, por lo que ayuda en la reducción de insumos de oficina.	Se debe mantener un servicio operativo con capacidad de almacenamiento amplio, previniendo posible colapso o pérdida de información. La tecnología de hoy permite salvaguardar información a través de respaldos constantes o planificados, se debe tener servidores en alta disponibilidad.
Beneficiar al usuario final mejorando su desempeño.	Se reduce el tras papeleo o pérdida de documentación legalizada, que se vuelve en caos al momento de dar seguimiento o control al proceso.	Dependencia de la tecnología, si el usuario se complica en el uso tecnológico no visualiza el beneficio. Se requiere una constante

	Se reduce tiempo en la espera de legalizar. Menor esfuerzo en la labor operativa.	inducción y socialización para captar la atención de usuarios.

El resumen anterior, expone temas para mejorar, a su vez se considera por mantener: la innovación constante tecnológica, la inducción permanente al personal que se relaciona con la tecnología y la labor administrativa; visualizando estos temas no únicamente como desventajas sino como oportunidades de mejora, exponiendo los temas de seguridad, disponibilidad de la información en un trabajo constante.

Luego de observar que existen ventajas y desventajas en la implementación de tecnologías por objetivo de estudio, se determina las bondades y repercusiones que se presentan en el proceso de adquisición de la cadena logística. Se utiliza el cuadro de los documentos legalizables para establecer los cambios.

Tabla 24 CUADRO COMPARATIVO EN EL PROCESO DE ADQUISICIÓN Y PAGO

Procesos de Adquisición, Ingreso, Despacho y Pago		
Documento	Desventaja	Ventaja
Solicitud de Compra	**Antes:** El operador debía elaborar el documento y gestionar la legalización del mismo a cada autoridad.	**Ahora:** El operador elabora el documento, pero el sistema permite la gestión para que cada autoridad firme lo que le corresponde.
Orden de Compra	**Antes:** La solicitud de compra iniciaba el trámite	**Ahora:** El documento de solicitud no se envía a la

	de compra sin completar la etapa de legalización, para iniciar la orden de compra.	unidad de compra, hasta que se encuentre completamente legalizada.
Certificación Presupuestaria	**Antes:** no era obligatorio el envió de la Solicitud de Compra, únicamente mediante oficio se solicitaba la certificación presupuestaria.	**Ahora:** se obliga el uso del envió de solicitud de compra para el trámite de certificación presupuestaria, la solicitud debe ser estar legalizada.
Acta de Inspección del Bien, Traspaso de Material, y Tramite de Pago	**Antes:** La orden de compra sin ser elaborada y legalizada, el operador realizaba ingresos a bodega en físico, sin tener la aprobación de la unidad de compras. Esto conlleva a la imposibilidad de pagar al proveedor por la ausencia de documentación en el sistema, y peor realizar el despacho correspondiente del material no registrado en existencias.	**Ahora:** La orden de compra no se realiza sin la solicitud de compra fielmente legalizada, una vez que la orden de compra es aprobada por la unidad de compra, esta es enviada al departamento de contabilidad para tramitar los pagos, de esta manera habilita el ingreso del material a bodegas para el registro de existencias.

Cabe mencionar que el exponer antes y ahora en el cuadro no significa que únicamente se cometían falencias en los procesos, se usa para describir las mejoras con la implementación de la firma digital y sus respectivas necesidades; se establecen diferencias en ambos contextos.

Al inicio se vio la reacción negativa del personal por la implementación del cambio, sin embargo se observó la eliminación de inconsistencias en los procesos y con ello se pudo tener mejor aceptación. Esta observación no solo se presenta como

desventaja por negatividad del personal, sino se presenta como correctivo de las deficiencias en el proceso. Entre otras observaciones se eliminan tiempos perdidos en los procesos, retraso en entregas, eliminación de pérdida de documentación legalizada.

La operatividad del sistema se vuelve pieza fundamental para la ejecución de la cadena logística, el mismo que avizora la necesidad inmediata de planes de contingencia que mitiguen el riesgo a la disponibilidad de su uso.

CONCLUSIONES Y RECOMENDACIONES.

1. Conclusión: Se mejoran procesos y procedimientos en la cadena logística, se deben auditar constantemente para mantener la calidad del servicio.

2. Conclusión: Los objetivos planteados con respecto a reducción del tiempo en los procesos se vuelve dependiente de mecanismos externos tales como los dispuestos por el organismo de control de compras, los mismos que nos deja exentos de reducirlos en su totalidad.

3. Conclusión: El objetivo de reducir el uso de suministros de oficina se garantiza, sin embargo como plan de contingencia debe mantenerse.

4. Recomendación: El uso del sistema transaccional se vuelve primordial durante la ejecución de la cadena logística, se debe mantener plan de contingencia ante riesgos de pérdida de conexión, perdida de servicio, etc.

5. Recomendación: El cumplimiento de normas y policitas de gobierno se debe mejorar; la ley de comercio electrónico debe ser rigurosa en el uso de la firma digital, mencionando la obligatoriedad en todas las organizaciones gubernamentales, garantizando el nivel tecnológico a través de la Secretaria Nacional de Información o ente competente, generando los siguientes beneficios.

- Protección jurídica (Ley de comercio electrónico)
- Protección tecnológica (ECIBCE)
- Trámites Ágiles y seguros
- Ayuda al medio ambiente

6. Conclusión: Como se indica en la implementación de la solución. El procedimiento de firmar digitalmente un documento en un canal de comunicación cifrado empleando TLS, no graba o guarda archivo temporal alguno en la sesión del computador antes ni durante la ejecución del proceso, sin embargo una mejora a la realización de la implementación seria emplear SANDBOX o **aislamiento de procesos**, una técnica que permita aislar la memoria de cualquier intento de filtración al momento de firmar.

7. Conclusión: El manejo de navegadores o browser modernos que soporten tecnología HTML5 se vuelve relevante a la solución propuesta, se debe emplear Google Chrome, Firefox para su funcionalidad.

BIBLIOGRAFÍA

[1] CONTRALORIA GENERAL DEL ESTADO, Normas de Control Interno para las Entidades, Organismos del Sector Público y de las Personas Jurídicas de Derecho Privado que Dispongan de Recursos Públicos, Quito: CGE, 2009.

[2] REAL ACADEMIA DE LA LENGUA ESPANOLA, «REAL ACADEMIA ESPANOLA,» 2015. [En línea]. Available: http://www.rae.es/.

[3] ENTIDAD DE CERTIFICACIÓN DE INFORMACIÓN Y SERVICIOS RELACIONADOS (ECIBCE), «CERTIFICACIÓN ELECTRONICA,» [En línea]. Available: https://www.eci.bce.ec/.

[4] SECRETARIA NACIONAL DE INFORMACION SNI, «SECRETARIA NACIONAL DE INFORMACION,» 2014. [En línea]. Available: http://sni.gob.ec/inicio.

[5] SECRETARIA NACIONAL DE ADMINISTRACION PUBLICA SNAP, «SECRETARIA NACIONAL DE ADMINISTRACION PUBLICA,» 2014. [En línea]. Available: http://www.administracionpublica.gob.ec/.

[6] CGE, Dirección de Investigación Técnica, Normativa y de Desarrollo Administrativo, NORMAS DE CONTROL INTERNO PARA LAS ENTIDADES, ORGANISMOS DEL SECTOR PÚBLICO Y DE LAS PERSONAS JURÍDICAS DE DERECHO PRIVADO QUE DISPONGAN DE RECURSOS PÚBLICOS, CGE, Ed., 2009, p. 86.

[7] SERVICIO NACIONAL DE CONTRATACION PUBLICA, «SERVICIO NACIONAL DE

CONTRATACION PUBLICA,» 2015. [En línea]. Available: http://portal.compraspublicas.gob.ec/incop/.

[8] PrimeKey Solutions EJBCA.ORG, «EJBCA.ORG,» 12 Marzo 2015. [En línea]. Available: http://www.ejbca.org/index.html. [Último acceso: 2012].

[9] CONGRESO NACIONAL, Ley 2002-67 (Registro Oficial 557-S, 17-IV-2002)., Quito: CONGRESO NACIONAL, 2002.

[10] PrimeKey Solutions EJBCA.ORG, «EJBCA Installation,» 2014.

ANEXOS

1. MANUAL DE PROCEDIMIENTOS PARA LOS USUARIOS DEL PKI (BANCO CENTRAL DEL ECUADOR)

2. Ley de comercio electrónico, firmas electrónicas y mensajes de datos (Ley No. 2002-67)

3. DECRETO 867 1-SEP-2011 - Reformas al Reglamento-empresa pública

4. Acuerdo Ministerial 181 del Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL)

5. Instalar y Configurar EJBCA 6