PROPUESTA

"IMPLANTACIÓN DE UN SISTEMA DE CORREO ELECTRÓNICO SEGURO, EMPLEANDO CERTIFICADOS Y FIRMAS DIGITALES, PARA LAS INSTITUCIONES DEL ESTADO PERUANO"

Lima, Junio del 2002

Índice

1. DESCRIPCIÓN DEL PROBLEMA.

Actualmente existe un aumento creciente de la necesidad de transmitir información confidencial y sensitiva vía Correo Electrónico, entre las entidades del Estado y las compañías del sector privado; con la finalidad de reducir el uso de papel y agilizar los procesos en la toma de decisiones.

Así, en la mayoría de instituciones públicas, el correo electrónico se ha convertido en un medio de transmisión de información, prácticamente estándar a diferentes niveles de una organización; sin embargo existen aún una serie de "huecos de seguridad" al momento de efectuar una transacción electrónica, dado que no se toman las medidas necesarias para asegurar que se cumplan principios básicos de seguridad como son los de confidencialidad e integridad, entre otros de la información transmitida, así como el hecho de tener la plena seguridad de que la información recepcionada por medios electrónicos realmente ha sido enviada por la persona que dice que la está enviando (autenticación - no repudiación).

Después de lo sucedido el 11 de septiembre de 2001 en los Estados Unidos, y luego de los ataques de Ántrax contaminando el correo tradicional (basado en papel), la necesidad de correo electrónico seguro ha aumentado.

Un reciente reporte de MetaGroup menciona que un 47 % de los departamentos de seguridad entrevistados planean implementar en un año correo electrónico encriptado.

Todos los días, ejecutivos, profesionales y funcionarios, se basan en comunicaciones electrónicas para la entrega rápida de planes de negocio, contratos corporativos, patentes, registros de salud, sueldos, etc.

El correo electrónico es la forma de comunicación en Internet más antigua y común. Mientras que los protocolos de correo electrónico han evolucionado rápidamente en las últimas tres décadas, la arquitectura del sistema del mismo ha cambiado muy poco. Fundamentalmente, la arquitectura ofrece solo el servicio para la entrega de mensajes de correo electrónico.

El reconocer la fragilidad del correo electrónico de Internet es esencial para entender una característica importante de un sistema de correo electrónico seguro, el cual provee servicios de seguridad de punto a punto, pero ni aumenta ni disminuye la probabilidad de

que un mensaje será entregado a su destinatario. El correo seguro puede reducir el daño que podría resultar de un mensaje de correo electrónico mal direccionado o interceptado; más aún, los mensajes encriptados son protegidos de ser leídos aún si no llegan a su destinatario.

Un factor es el hecho de que el único punto de control garantizado en la entrega de un mensaje de correo electrónico es el software de usuario usado para crearlo y enviarlo. Desde el punto de vista del destinatario, el único punto de control es el software de usuario y el archivo de casilla de correo que lee para encontrar el mensaje. Debido a que los usuarios de origen y destino no controlan el sistema de transferencia que mueve los mensajes entre ellos, los únicos servicios de seguridad que se pueden implementar son aquellos que se pueden implementar en los software cliente de correo electrónico.

Se debe considerar además, que la probabilidad de que un mensaje de correo electrónico sea modificado en tránsito es de cerca del 50%. Se concluye entonces que existen serias dudas de que un mensaje recibido es idéntico al enviado. En este punto una modificación no tiene que ser necesariamente maliciosa o intencional para dañar la integridad del mensaje.

En el caso particular de entidades gubernamentales, se puede deducir, que existe un gran volumen de información de carácter no sólo crítico sino también confidencial, que viaja vía correo electrónico entre emisores y receptores, entre los cuales se pueden encontrar ministros, gerentes de área, jefes de área, entre otros; no resulta extraño pensar, que esta información esté siendo interceptada y por tanto accesada (“chuponeada”) por terceros no autorizados, con fines de simple “curiosidad”, o bien con objetivos maliciosos, pudiendo ser alterada o aprovechada para distintos fines, ocasionando daños de diferente proporción.

El uso de correo electrónico seguro se vuelve una necesidad aún mayor si se sabe que otros gobiernos tienen sofisticados sistemas de interceptación de mensajes como el sistema “Carnivore” del FBI (USA) y los sistemas “Echelon” y “Magic Lantern”. Algunos estiman que por ejemplo el sistema “Echelon” permite a la Agencia de Seguridad Nacional americana (NSA) obtener del 15% al 20% de información de inteligencia. Todos estos sistemas ofrecen a las agencias de inteligencia de gobiernos extranjeros la posibilidad de poder “ver” la actividad de mensajes de correo electrónico de cualquier persona o institución. Aún más, el sistema Echelon permitiría que se realice el monitoreo a cualquier usuario de correo electrónico (entre ellos nuestros funcionarios públicos) desde otro país sin tener que aplicar una orden judicial.

Así, si bien es cierto, el uso de medios electrónicos tiene una serie de beneficios, es necesario tomar las medidas de seguridad idóneas para que esos beneficios no sean mermados y se ocasionen además daños quizás irreparables. Teniendo en cuenta lo delicado de la información que es objeto de intercambio entre las entidades gubernamentales, se puede deducir que los daños a ocasionarse por negligencia o descuidos de seguridad pueden pasar no sólo por aspectos directamente tangibles o de índole monetaria, por ejemplo; sino también por pérdidas de imagen, prestigio, entre otros cuya valoración supera con creces la inversión que habría de realizarse para maximizar la seguridad de las transacciones electrónicas.

2. OBJETIVO.

El objetivo del presente proyecto consiste en la “Implantación de un Sistema de Correo Electrónico Seguro, empleando certificados y firmas digitales, para las Instituciones del Estado Peruano”.

3. SOLUCIÓN PROPUESTA.

El Instituto Nacional de Estadística e Informática, como ente rector del sistema informático estatal a nivel nacional, y por lo tanto, canalizador de soluciones informáticas al interior del Estado Peruano, propone, con la participación de la empresa privada, la realización de un proyecto de seguridad, con el objeto de llevar a cabo, en tres etapas, la “Implantación de un Sistema de Correo Electrónico Seguro, empleando certificados y firmas digitales, para las Instituciones del Estado Peruano”, que habilitará las facilidades de:

Firma Digital de Correo Electrónico.- para probar el origen y autenticidad, e integridad de un mensaje de correo electrónico enviado/recibido por las Instituciones del Estado Peruano.

Encriptación de Correo Electrónico.- para garantizar la confidencialidad de la información transmitida entre los funcionarios de las Instituciones del Estado Peruano.

Courier Electrónico Seguro.- para garantizar la entrega de la información transmitida electrónicamente entre los funcionarios de las Instituciones del Estado Peruano.

La solución propuesta de correo electrónico seguro ha considerado los siguientes aspectos:

- **Sistema Fácil de usar**, el requisito más importante para un sistema de correo seguro es la facilidad de uso, tanto para los usuarios que envían como para los que reciben. Si el envío de correo electrónico es moderadamente más complejo que el correo electrónico convencional, los usuarios no lo usarán.

- **Integración**, todo sistema de correo seguro debe ser capaz de integrarse con una infraestructura de seguridad existente, aún si la infraestructura de seguridad del que envía es diferente a la del que recibe. Tal integración puede preservar algunas de las inversiones realizadas en aseguramiento de las comunicaciones por las organizaciones. Similarmente, cualquier correo seguro debería integrarse fácilmente con la infraestructura de correo existente e imponer una sobrecarga adicional relativamente pequeña a los miembros del staff de tecnologías de información y otros recursos.

- **Transparencia Global**, un correo electrónico seguro debería ser transparente en su habilidad de comunicarse con usuarios de diferentes tipos, ya sea si son usuarios de un sistema de mensajería corporativo o usuarios externos como los clientes.

- **Seguimiento Automático de Auditoría**, la habilidad de mantener huellas de auditoria de cuándo los mensajes son recibidos está volviéndose muy importante debido a la regulación y otros requerimientos, y debería ser independiente de cualquier acción hecha por el destinatario.

- **Control de Envío**, una extensión del mantenimiento de huella de auditoría es el control de envío del correo hasta el punto que el usuario destino abra el correo, En otras palabras, el usuario origen debería poder recobrar un mensaje antes de que sea leído, controlar cuando la entrega se debe llevar a cabo o destruir el correo electrónico antes de su entrega.

- **Autenticación de dos vías**, la autenticidad garantizada del usuario origen vía una firma digital es un elemento crítico de cualquier sistema de correo electrónico seguro. Similarmente el usuario origen debería estar seguro de que el usuario destino es quien dice ser.

3.1. ALCANCES DE LA SOLUCIÓN PROPUESTA.

El proyecto propuesto tendrá los siguientes alcances:

- La solución se implementará para la PCM, el INEI y las Instituciones del Estado Peruano que se involucren en el presente proyecto.

Se propone la implementación de la solución en tres etapas:

Primera Etapa: Usar certificados digitales con los clientes del tipo S/MIME o compatible, de las entidades del Estado que las poseen.

Segunda Etapa: Estandarizar el software de correo de los usuarios con el estandar S/MIME

Tercera Etapa: Implementar un Sistema de Mensajería Segura, donde se implemente a mas usuarios de las entidades públicas (que garantice la entrega de documentos además de la seguridad). Este sistema permitirá además de firma digital y, encriptación y desencriptación de correo electrónico; la transmisión segura, seguimiento de cada entrega, y entrega segura de la información.

Luego de concluir esta etapa, se podrá contar con un sistema seguro y confiable para la entrega de documentos, archivos y mensajes electrónicos entre los usuarios de las instituciones seleccionadas. El sistema permitirá encriptar y asegurar entregas electrónicas (de mensajes, documentos, o archivos) antes de que éstas salgan de la computadora del usuario, otorgando además, a través de los canales de Internet, garantía de privacidad y entrega sólo a los recipientes indicados, además de realizar un seguimiento de las entregas en todos los puntos durante el proceso. Gracias a este sistema, se tiene además del cumplimiento de los principios de confidencialidad, integridad, autenticación y no repudiación, las pruebas de entrega de la información al destinatario indicado.

La primera etapa podría estar dirigida sólamente a los altos funcionarios (ministros, viceministros, etc.) de las entidades del estado, y sería un proyecto muy fácil de implementar y con un alto retorno de inversión. Al escoger una pequeña comunidad de usuarios se podría estandarizar el uso de clientes de correo electrónico y versiones de estos clientes garantizándose así la interoperabilidad de los sistemas de correo electrónico involucrados.

La segunda etapa tendría la finalidad de aumentar el número de usuarios del sistema para lo cual habría que estandarizar los posibles diferentes clientes de correo. El resultado de la implementación del sistema de correo seguro permitiría el uso seguro (con firma digital y/o encriptación) de los sistemas convencionales de correo electrónico que tengan las entidades del gobierno. Sin embargo para el envío de documentos que requieran características como garantía de entrega, acuse de recibo y seguimiento de éstos se requeriría implementar un sistema más complejo.

- Se llevará a cabo el Proceso de Identificación y Autenticación (I&A) en persona- previo a la emisión de certificados digitales-, por parte de Agentes Locales de Registro (LRA) que permitirá a la PCM, INEI y otras entidades, recibir certificados digitales de máximo nivel (nivel 3).

- La provisión y emisión de Certificados Digitales X.509 v3 se llevará a cabo por una Entidad Certificadora (CA) que cumpla con los estándares internacionales y las leyes peruanas .

- La provisión e instalación de dispositivos criptográficos externos de almacenamiento de llaves privadas como los smarts cards y/o ikeys.

- Se efectuará la configuración de los clientes de correo electrónico de los usuarios beneficiados con la solución, de manera que se habiliten las funciones de firma digital de los correos electrónicos y/o encriptación de los mismos, mediante el uso de certificados digitales.

- Se realizará la configuración de Clientes de Correo para la habilitación de los iconos respectivos de firma digital y encriptación de correo electrónico para los usuarios beneficiados con la solución.

- Pruebas de uso de correo/courier electrónico seguro y breve entrenamiento a los usuarios.

- Recomendaciones sobre Políticas de uso de los certificados.

3.2. FUNCIONALIDADES DE UNA INFRAESTRUCTURA PKI, CUMPLIMIENTO DE ESTÁNDARES.

A continuación se detallan aspectos sobre funcionalidades y requerimientos que la empresa proveedora deberá tener en consideración en su propuesta para el desarrollo de un sistema de correo electrónico seguro con tecnología PKI.

De la Entidad Certificadora (CA)

La empresa proveedora utilizará los servicios de la Entidad Certificadora con la que trabaja, como proveedor de servicios PKI reconocido internacionalmente y de acuerdo a las leyes del Perú y normas internacionales prevalecientes para la certificación digital y las firmas digitales.

La Entidad Certificadora, debe ofrecer los servicios de emisión, validación y revocación de los certificados digitales y firmas digitales. Los costos de los servicios de validaciones de firmas estarán cubiertos en la solución ofrecida en un periodo de un año.

De la Entidad de Registro (RA)

Identificar una Autoridad de Registro (RA), la cual se encargará de la autenticación e identificación de los usuarios y de completar el protocolo definido.

Una autoridad o entidad de registro o verificación, es aquella que se encarga del levantamiento de datos, así como de la comprobación de los mismos respecto a un solicitante de certificado digital y cuyos servicios son patrocinados por una autoridad de certificación

Una vez creado el certificado, el usuario podrá obtenerlo tantas veces como sea oportuno a través del repositorio de certificados asociado con la Autoridad de Certificación emisora de la credencial digital.

De los Requerimientos de Seguridad y Estándares Internacionales

La solución planteada deberá contar con una completa conformidad de certificado digital con el estándar x.509v3, que será almacenado en un medio de seguridad trasladable pero que no podrá ser copiado, lo cual se ajusta a la norma ISO 7816-4

para las Llaves Inteligentes USB (llamada ikey). Las entidades del estado también pueden evaluar el empleo de smart cards (tarjetas inteligentes) que cumplan también con la norma ISO 7816; y que tienen Lectora de la Tarjeta Inteligente o Smart Card, que es el dispositivo que actúa como interfase entre el usuario y el sistema, y permite conectarse a la PC del cliente a través del puerto serial, o USB, y soporta los estándares PC/SC y SCM SCR 100.

El proveedor de Certificación Digital deberá utilizar certificados X.509v3, que puedan ser almacenados en un directorio accesible LDAP.

La solución que plantee la empresa proveedora debe tener en cuenta lo siguiente:

- **Estándares de los Certificados**.- la solución debe tener en cuenta un 100% de conformidad con las normas de la estructura de los certificados, lo que asegure la aceptación y utilidad dentro de las aplicaciones de terceras partes, se trabajará entonces con los estándares X.509v3 (incluyendo todas las extensiones regularizadas) y S/MIME.

- **Estándares Criptográficos.-** además, la solución debe cumplir con las normas que manejan las estructuras criptográficas dentro de los certificados para los métodos de generación de claves, algoritmos hash y algoritmos de encriptación: RSA , DSA, RC2, DC4, SHA-1, DES, 3DES, MD5.

- **Normas de Comunicación.-** Las normas deben manejar las sesiones del navegador requeridas para el registro del cliente y para las respuestas del OCSP: TCP/IP, HTTP y HTTPS.

  Estas normas también validarán el certificado en tiempo real: CRL, OCSP.

- **Estándares Comerciales**.- La solución debe cumplir con las normas ISO 7816-4, que manejan los aspectos físicos de los componentes de seguridad; y con la Certificación FCC/CE. Además, la solución se adhiere a la norma ISO 15408, que maneja la seguridad lógica y física de la CA.

3.3. CONSIDERACIONES DE UN SISTEMA DE CORREO ELECTRÓNICO SEGURO

Con la finalidad de que el sistema de correo electrónico seguro funcione de manera óptima entre las distintas Instituciones del Estado peruano, se considera necesario tener en cuenta los siguientes aspectos:

De la Estandarización de los Sistemas de Correo Electrónico para el Estado Peruano

Como producto de la solución que se busca implementar, los usuarios de la PCM, INEI y de las Instituciones del Estado involucradas en el proyecto, podrán enviar correo electrónico seguro, esto es, firmado digitalmente y encriptado, gracias a la aplicación del estándar S/MIME (Secure Multipurpose Internet Mail Extension), el cual está basado en PKI.

Sin embargo, cabe destacar que uno de los problemas para implementar la solución es el hecho de que mientras existen varios software cliente de correo electrónico (Eudora, Microsoft Outlook, Netscape Messenger), existen muy pocos sistemas de transferencia de mensajes (Sendmail). Así, el número de aplicaciones correo electrónico que son totalmente compatibles con los estándares de Internet es muy pequeño.

Como resultado de lo anterior, la interoperabilidad se mantiene como una problemática, y la probabilidad de que un mensaje recibido es idéntico al enviado es dudosa.

Como lo vemos las ventajas de que el Estado estandarice sus sistemas de correo electrónico, o por lo menos sus clientes de correo electrónico, se ven en términos de costos de administración, performance, y servicio al ciudadano.

Aunque existe una variedad de productos de correo electrónico en el mercado, se observa que Microsoft que ofrece su Exchange Server y su cliente Outlook, y Lotus con su cliente Notes y su servidor Domino dominan el mercado.

De la Confianza del Sistema de Correo Electrónico

La gran barrera que afronta un sistema de correo seguro es la confianza. Este problema se manifiesta asimismo de dos formas principales; el primer tema tiene que ver con el uso – en particular en cómo las claves públicas son usadas y administradas; y el segundo tema es confiar en el contenido de un mensaje seguro.

S/MIME usa certificados X.509 V3. Esto requiere certificados que sean emitidos por una Entidad Certificadora (CA) de una de las dos siguientes formas: (1) a través de un proveedor de servicios de CA o (2) vía una comunidad de usuarios que hayan

implementado su propio CA comprando software de empresas como Entrust (http://www.entrust.com/) o RSA Security (http://www.rsasecurity.com/).

De acuerdo al alcance del presente proyecto, la solución propuesta maximiza la seguridad existente en cuanto a la transmisión de correo electrónico, solucionando el problema tanto para los usuarios de la PCM, INEI, así como de las instituciones del Estado involucradas en el proyecto.

Importante

La elección de un CA y su correspondiente RA es un tema de CONFIANZA en las empresas que cumplirán esos roles. A fin de tener certificados de mayor nivel (categoría 3), es indispensable para este proyecto, que busca implementar en la PCM, INEI y otras Instituciones de Estado que implementen un sistema de correo electrónico seguro; contar con una RA local, para que esta realice los procedimientos de autenticación e identificación en la modalidad conocida como "en persona" o "cara-a-cara" como aspecto previo a la emisión de certificados digitales.

Así, como la fuente de emisión del certificado es importante, el proceso de validación del certificado es también un tema crítico. El usuario origen debe validar un certificado digital del usuario de destino a fin de asegurarse que la clave pública usada para encriptar un mensaje es la correcta. Y el usuario destino debe validar el certificado digital del usuario origen a fin de confirmar la identidad del origen.

Un mito del correo seguro es que el instalar la tecnología es suficiente para comenzar a enviar y recibir mensajes seguros. La realidad es que los usuarios necesitarán claves públicas, que requiere una administración de infraestructura de clave publica (PKI), con las políticas y procedimientos adecuados.

Así, como en todos los temas de seguridad, la inversión en un sistema de correo electrónico seguro es tanto una inversión tecnológica como una inversión cultural.

De la Seguridad en la Transmisión de Correo Electrónico

La solución a implementarse brinda un sistema de correo electrónico seguro, para lo cual se ha tenido en cuenta la garantía de los siguientes principios de seguridad en la transmisión de información por Internet:

- Autenticación: Asegurarse que en una transacción ambas partes sean quienes dicen ser.
- Confidencialidad: Nadie podrá leer la información transmitida de manera encriptada salvo las personas que emiten y reciben el mensaje.
- Integridad: Asegurar que los mensajes transmitidos que han sido firmados digitalmente no sufran ninguna modificación en el camino entre el emisor y receptor, sin que esta sea percibida.
- No Repudiación: Deberá asegurar que el emisor del correo electrónico firmado digitalmente no pueda negar posteriormente el envío del mismo.

De los Certificados Digitales

Para este proyecto se plantea la adquisición por parte del INEI y demás Instituciones del Estado involucradas, certificados digitales de Categoría o Nivel "3" (es decir, con autenticación “face to face” o en persona), estándar X.509v3.

El certificado digital permitirá el cifrado de texto y la firma digital del correo electrónico, el cual utilizará una clave pública y una clave privada. El certificado digital garantizará, como se indicó anteriormente, los cuatro aspectos fundamentales en una transacción electrónica: Autenticidad, Integridad, Confidencialidad y No Repudiación.

Es importante señalar que la Entidad Certificadora, valiéndose de la Entidad de Registro verificarán la identidad de las personas a quien se le otorgará la licencia de uso del certificado digital.

Los Certificados Digitales ofrecidos permitirán además su uso en futuras aplicaciones diferentes a la que es objeto de la presente propuesta (por ejemplo, autenticación y realización de transacciones seguras en sistemas

propietarios, VPNs, firma y encriptación de documentos en diferentes formatos, etc.)

De la Generación y Grabación de las Firmas Digitales en las Llaves Inteligentes USB

La Autoridad de Registro se hará cargo de la instalación de los componentes de seguridad del tipo llave inteligente USB, y del procedimiento de generación y grabación de las llaves privadas en las tarjetas inteligentes, luego de que la Autoridad Certificadora y Autoridad de Registro hayan verificado y confirmado la identidad de la institución y del usuario al que se le entregará un componente de seguridad.

De la Distribución e Instalación de los Componentes de Seguridad

La Autoridad Certificadora se encargará de distribuir e instalar los certificados digitales y los componentes de seguridad. Cada institución beneficiada con componentes de seguridad deberá firmar un acta de conformidad de la instalación de los dispositivos de seguridad, para ello la Autoridad Certificadora entregará una guía de instalación y uso en idioma español.

4. BENEFICIOS DE LA SOLUCIÓN PROPUESTA.

- Se habilitarán las facilidades técnicas para que funcionarios de la PCM, INEI y de las Instituciones del Estado involucradas en el proyecto, puedan enviar y recibir correo electrónico firmado digitalmente, es decir, el receptor tendrá la certeza de que quien le envió el correo es quien dice ser. En otras palabras, el usuario que envió un correo electrónico firmado digitalmente no podrá negar que fue él el emisor (principio de no repudiación).

- En la PCM, el INEI y las Instituciones del Estado involucradas en el proyecto, sólo la persona que posee un certificado digital y su correspondiente llave privada puede haber creado la firma digital que la vincula al documento. Cualquier persona que tenga acceso a la correspondiente llave pública puede verificar la firma digital.

- Se habilitarán las facilidades técnicas para que funcionarios de la PCM, INEI y de las instituciones del Estado involucradas en el proyecto puedan enviar y recibir correo electrónico encriptado, los cuales, si son “chuponeados”, no podrán ser leídos (gracias a las técnicas criptográficas utilizadas para encriptar el mensaje, la persona que

"chuponee" el correo electrónico sólo verá un conjunto de caracteres sin sentido); sólo el destinatario a quien está dirigida la información enviada podrá tener acceso a ésta haciendo uso de su llave privada.

✍✍Cualquier cambio en la información contenida en el correo electrónico que fue firmado digitalmente por algún funcionario de la PCM, INEI y de las instituciones del Estado involucradas en el proyecto, será inmediatamente percibido por el receptor a quien va dirigido el correo, mediante un mensaje de advertencia que es proporcionado por el sistema al momento que el receptor accede al correo electrónico, que le indica que el contenido del correo electrónico fue alterado después de efectuada la firma digital por parte del emisor, y por lo tanto el mensaje ha dejado de ser válido. Cualquier modificación en la información (inclusive el cambio de un simple bit en un extenso mensaje) invalida la firma digital.

✍✍De acuerdo al alcance del presente proyecto, si se llega a concretar la solución en sus dos primeras etapas, se estaría maximizando la seguridad existente en cuanto a la transmisión de correo electrónico, y, al implementarse la tercera etapa, se tendría un sistema completo de correo electrónico seguro, que contemple además, seguridad de entrega de la información.

✍✍La implementación de la solución completa de correo electrónico seguro en las diferentes instituciones del Estado, brindarán las facilidades técnicas de encriptación y firma digital; y además, se cubriría también el aspecto legal de la validez de la firma digital, gracias a que la solución plantea la integración de una CA de acuerdo a los estándares de la industria y que luego podrá registrarse ante la Autoridad Administrativa Competente que define la ley, lo que significa que se estaría trabajando con una CA que cumplirá no sólo con estándares fijados por la industria, sino también, que se encontrará sometida a continuas auditorías internacionales. Gracias a lo anterior, la firma digital aplicada tendrá la validez y peso legal de una firma manuscrita de acuerdo a la Ley 27269 - Ley de Firmas y Certificados Digitales, que señala textualmente en su artículo 1°:"*Entiéndase por firma electrónica*[1] *a cualquier símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención precisa de vincularse o autenticar un*

[1] La firma digital se encuentra dentro de este tipo de firmas, la Ley 27269 señala también en su artículo 3°*:"La firma digital es aquella firma electrónica que utiliza una técnica de criptografía asimétrica, basada en el uso de un par de claves único; asociadas una clave privada y una clave pública relacionadas matemáticamente entre sí, de tal forma que las personas que conocen la clave pública no puedan derivar de ella la clave privada".*

documento cumpliendo todas o algunas de las funciones características de una firma manuscrita".

✍✍Los certificados digitales a ser generados, teniendo en cuenta que se propone una solución de máxima seguridad, se almacenarán en dispositivos de hardware seguro, como son las llaves inteligentes USB, que cuentan con un chip criptográfico especial, donde es almacenada e inclusive generada la llave privada, y que además es portátil, es decir, el dueño lo puede llevar consigo a donde vaya.

5. METODOLOGÍA.

La metodología y plan de trabajo a utilizar en la "Implantación de un Sistema de Correo Electrónico Seguro, empleando certificados y firmas digitales, para las Instituciones del Estado Peruano", constará de los siguientes pasos:

ETAPA 1.

1. Levantamiento de información.
   - ✍✍Verificación de cumplimiento de pre-requisitos para la implementación de la solución.
   - ✍✍Políticas de seguridad de transacciones vía correo electrónico.
   - ✍✍Plataforma actual de transmisión de correo electrónico.
   - ✍✍Diagnóstico de seguridad de correo electrónico de las instituciones del Estado involucradas en el proyecto.
2. Diseño de Seguridad de Correo Electrónico.
3. Registro de información de usuarios solicitantes de certificados digitales.
4. Proceso de identificación y autenticación de usuarios solicitantes de certificados digitales.
5. Generación de llaves pública y privada – Grabación de llave privada en componente de seguridad (llave inteligente USB).
6. Emisión de certificados digitales.
7. Instalación y configuración de Servicios de Seguridad de Correo Electrónico.
8. Pruebas de Uso Seguro de Correo Electrónico.
9. Entrenamiento a los usuarios.

ETAPA 2.

10. Estandarización de clientes de correo electrónico.

11. Instalación y configuración de Servicios de Seguridad de Correo Electrónico en clientes de correo que han cambiado sus características.
12. Pruebas de uso Seguro de Correo Electrónico.
13. Entrenamiento a los usuarios.

ETAPA 3.

14. Análisis de Requerimientos de sistema de courier electrónico seguro, para las instituciones del Estado peruano.
15. Desarrollo o outsourcing de sistema de courier electrónico seguro para las instituciones del Estado peruano.
16. Implantación del sistema de courier electrónico seguro.
17. Pruebas de uso del sistema de courier electrónico seguro.
18. Entrenamiento a los usuarios.

6. PLAN DE TRABAJO.

Para el desarrollo del presente proyecto, se seguirá un plan de trabajo que se diseñará especialmente, con la finalidad de cumplir con éxito el objetivo trazado. De acuerdo a la organización y al alcance del proyecto, se planificarán los tiempos y recursos necesarios para la implementación de la solución completa.

7. RECURSOS PARA EL PROYECTO.

7.1. RECURSOS DEL INEI E INSTITUCIONES DEL ESTADO INVOLUCRADAS EN EL PROYECTO

Para lograr el éxito en el desarrollo de las actividades del presente proyecto se propone el siguiente personal, con la dedicación indicada:

Responsable del Proyecto	Jefe de Sistemas, Quien proporcionará o designará a quienes proporcionen información para el buen desarrollo de la consultoría.

Jefe de Proyecto– Profesional INEI	?? Dar soporte a labores de personal técnico de la empresa proveedora. ?? Proveer la información requerida, en forma oportuna al personal de la empresa proveedora. ?? Tener disponibilidad durante el tiempo que dura la consultoría.

7.2. RECURSOS EXIGIBLES AL PROVEEDOR

Para lograr el éxito del proyecto, el proveedor deberá asignar el siguiente personal, con la dedicación indicada:

Ejecutivo de Cuenta	1 persona tiempo parcial
Jefe de Proyecto	1 persona tiempo parcial
Ingenieros e-Security	3 personas a tiempo completo durante el desarrollo del proyecto. 4 personas a tiempo parcial durante el desarrollo de la consultoría

8. ENTREGABLE.

El entregable del presente proyecto constituye un documento impreso, que consolide todos los aspectos contemplados en el alcance del mismo, dejando constancia de la implantación de la solución.

9. TIEMPO.

El tiempo se deberá estimar de acuerdo al tamaño del proyecto.

10. COSTOS ESTIMADOS.

Se presentan costos unitarios para efectos de evaluación y determinación de la cantidad a requerirse como SOLUCIÓN. El costo del proyecto, de acuerdo a la información disponible, se estimará en base a la distribución y cantidad de Certificados a requerirse:

Descripción Certificados Digitales	Canti- dad	Precio Unitario

		US$
Certificados Digitales **La Solución incluye:**	**01**	**95.00 ***
LatinSignID Certificate		
Duración del Certificado: 01 Año renovable		
CIP ikey 2000 Authentication Solution for PKI Kit de Seguridad compuesto por: Token Criptográfico iKey-2000 y Software de configuración.		
Servicio de Autenticación, Identificación, Validación, Instalación, Configuración. **(Precio Referencial estimado para una cantidad de 100 usuarios a nivel de Lima Metropolitana)**	**01**	**1,500.00**
Servicio de Soporte Técnico Anual Servicio en modalidad 8 x 5 con tiempo de respuesta máximo de 02 horas para incidentes graves. **(Precio Referencial estimado para una cantidad de 100 usuarios a nivel de Lima Metropolitana)**	**01**	**2,000.00**

Nota : Son precios referenciales de un proveedor local (*)

- Se estipula que el costo de los certificados es por un año, teniendo que considerarse la renovación para un segundo año por aproximadamente **$25.00 + IGV** por certificado.
- Es necesaria una actividad de capacitación, que se dimensiona de acuerdo a la cantidad de Certificados (usuarios) y lugares donde se instalarán.

11. PROPUESTA DE PILOTO PARA EVALUACIÓN.

El INEI plantea realizar un piloto de evaluación de Intercambio de Correo electrónico seguro entre INEI y Presidencia del Consejo de Ministros (PCM). Para realizar el piloto se ha dimensionado a implementar la solución propuesta con Certificados en una cantidad de, mínimo 05 y un máximo de 10 usuarios por institución.

Esta propuesta para el realizar el presente piloto debe incluir todos los servicios, lo cual servirá para demostrar cómo es el proceso de Registro e Identificación a seguir en un Proyecto de mayor envergadura. También se incluirán los servicios de un ingeniero para

apoyar en el piloto de pruebas durante el tiempo de duración del Piloto que no debe exceder de los 45 días.

Descripción Piloto de Evaluación	Cantidad	Precio Unitario US$
Propuesta de Implementación de Piloto de Evaluación de Intercambio de Correo Seguro entre dos Instituciones: **El piloto incluye:**		**3,000.00**
LatinSignID Certificate	**Máximo 10 por institución**	
Duración del Certificado: 1 año		
CIP ikey 2000 Authentication Solution for PKI Kit de Seguridad compuesto por: Token Criptográfico iKey-2000 y Software de configuración.	**Máximo 10 por institución**	
Servicio de Autenticación, Identificación, Validación, Instalación, Configuración. **(Para una cantidad máxima de 10 usuarios)**		
Servicios de un Ingeniero asignado al Plan Piloto Disponibilidad de dos (02) días a la semana, 03 horas por día.		
	Total US$	**3,000.00**

Nota : Estos precios han sido obtenidos de un proveedor local