Metodología para el Desarrollo de una Infraestructura de Claves Públicas orientado al Análisis de Riesgo

Marcelo Invert Palma Salas, Member, IEEE

***Resumen*—Los avances tecnológicos y la alta penetración que están teniendo los dispositivos electrónicos traen consigo ataques más sofisticados y difíciles de detectar, este reto cada día es más complicado de enfrentar, tanto para asegurar la información como las tecnologías de protección de información.**

Este artículo discute el desarrollo de una Plataforma de Claves Públicas más conocida como PKI (*Public Key Infrastructure*) para administración de firmas digitales y certificados digitales como una alternativa de sistemas de seguridad adecuados para la protección de la información haciendo uso del Sistema Asimétrico-Simétrico PGP (*Pretty Good Privacy*) y su aplicación en instituciones gubernamentales donde sus objetivos se centran en Tecnologías de la Información y desarrollamos una metodología para analizar su riesgo frente a ataques internos y externos.

***Índices*— Análisis de Riesgos, PKI, Infraestructura de Clave Pública, Firmas Digitales, Certificados Digitales, Criptografía, Seguridad, ATT, PGP, Pretty Good Privacy.**

I. Introducción

Los controles criptográficos son herramientas que aseguran la integridad (salvaguardar la exactitud y totalidad de la información y los métodos de procesamiento), disponibilidad (garantizar que los usuarios tengan acceso a la información y a los recursos relacionados con ella toda vez que se requiera) y autenticación de la información (garantizan que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a ella) a través de medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando [1].

La Seguridad de la información no está orientada al aprovechamiento de los recursos disponibles mediante la utilización de diversas herramientas y técnicas para asegurar la información, al respecto el *International Communication Union* (ITU) [17] [19] e *International Standard Association* (ISO) [23] analizaron que más de la mitad de los ataques informáticos el 2010 fueron realizados dentro de las empresas y organizaciones (ataques internos) como robo de paquetes de información para ser vendida a la competencia, violación de la seguridad física y lógica, fraude a los sistemas, entre otros (Figura 1) [2] [3].

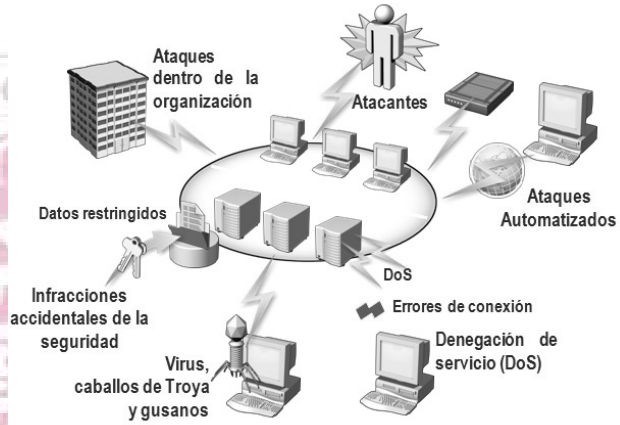

Figura 1. Tipos de Ataques Informáticos.[24]

Las Normas Internacionales y los Sistemas de Gestión de Seguridad de la Información (SGSI) como la NB ISO/IEC 27000[18] y Information Systems Audit and Control Association (ISACA) con la Norma COBIT (*Control Objectives for Information and related Technology*)[5] hacen hincapié al uso de herramientas criptográficas que coadyuvan al control por riesgos internos en la seguridad de la información en la empresas, evitando que los mismos se materialicen en amenazas que pongan en riesgo la continuidad del negocio de las organizaciones.

En este artículo, propongo el uso de una Plataforma de Claves Pública (*PKI*) para asegurar la información. Esta tecnología permite proteger la información de ataques internos y externos mediante el uso de claves simétricas y claves asimétricos. Estas técnicas de criptografía son unas poderosas herramientas que son usadas para encriptar la información, firmar todo tipo de documentos y asegurar la integridad y autenticidad del origen del emisor del mensaje [2], [5]. Convencionalmente se analiza los tipos riesgos a que son susceptibles toda organización. En este artículo mediremos los riesgos y como pueden ser mitigados sobre un escenario real.

El PKI también es una herramienta que nos permite reemplazar el uso de la firma manuscrita por la firma digital.

Este trabajo fue apoyado en parte por la Escuela Militar de Ingeniería de la ciudad de La Paz y la Superintendencia de Telecomunicaciones (SITTEL) a través del Departamento de Tecnologías de información y Comunicación.

M. I. Palma Salas colaboró en la Escuela Militar de Ingeniería (EMI) de La Paz, Bolivia y al Instituto de Computação da Universidade Estadual de Campinas (UNICAMP). CEP 13083-280, Campinas, São Paulo (e-mail: marcelopalma@ieee.org)

Con una Ley que sustente su funcionamiento puede contribuir al no repudio del origen del mensaje, aspecto que protege al receptor del documento, garantizando que el documento ha sido generado por el emisor. Además de reducir el costo de utilizar papel, contribuye al desarrollo de transacciones virtuales y desburocratiza los trámites gubernamentales [23] [24].

Su posibilidad para almacenar diferentes tipos de Sistemas Criptográficos nos permite tener una gran infraestructura con la posibilidad ampliar sus usos. Zheng Gou, Tohru Okuyama y Marion R. Finley. Jr [1] en su artículo investigativo nos explican la posibilidad de interactuar como una plataforma global comunicada por el medio de comunicación más inseguro, el internet y tener una conectividad entre diferentes tecnologías PKI. Hoh Peter In, Young-Gab Kim, Taek Lee, Choang-Joo Moon, Yoonjung Jung y Injung Kim [2] realizan el modelo de una técnica de Análisis de Riesgos para Sistemas de Información, donde analizan las amenazas y vulnerabilidades para mitigar los riesgos. La novedad de mi investigación se base en desarrollar una Metodología de Desarrollo de una Plataforma de Claves Públicas analizando los riesgos de la perdida de información para una Entidad Certificadora.

Se realiza un acercamiento a las vulnerabilidades y amenazas de la organización, a través del desarrollo de una auditoria de sistemas, catalogando los posibles ataques y procesos que participan. Aprovechamos la flexibilidad del Modelo de Auditoria PHVA (Planificar, Hacer, Verificar y Actuar) [8] para descubir los riesgos y el nivel de protección que debe administrar el PKI.

Entre otras contribuciones se tiene:

- Evaluar Sistemas de Encriptación.
- Explicar el procedimiento de una auditoria de sistema.
- Obtener los principales riesgos en la seguridad de la información.
- Obtener métodos que puedan contrarrestar riesgos de la seguridad de la información en la organización.

El resto del artículo está estructurado de la siguiente forma. La Sección 2 continúa la descripción de la Metodología y los pasos para su realización. La sección 3 muestra un caso de estudio donde se aplica la metodología y describimos los resultados de los experimentos, y la Sección 4 cierra el presente documento con conclusiones y futuros trabajos.

II. La Infraestructura de Claves Públicas

Una infraestructura de Clave Pública (*Public Key Infrastructures*) o PKI (Figura 1) es una combinación de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución de procesos con garantías de operaciones criptográficas como el cifrado, la firma digital o el no repudio de transacciones electrónicas [7] [8].

El término PKI se utiliza para referirse tanto a la autoridad de certificación y al resto de componentes, como para referirse, de manera más amplia al uso de algoritmos de clave pública.

Una de las dificultades al desarrollar un PKI es la colección de ataques. Los ataques pueden obtenerse de diferentes recursos (Internet, libros, normas, etc). De todas formas, es muy dificultoso hallar ataques relevantes y tomar un tiempo para verificar si el ataque es reproducible bajo ambientes y dependiendo del negocio de la organización. El objetivo es proveer un análisis de riesgo a la información importante para la organización. Se propone una metodología compuesta por nueve pasos para determinar el nivel de riesgos y mitigación de los mismos (figura 2) con un PKI.

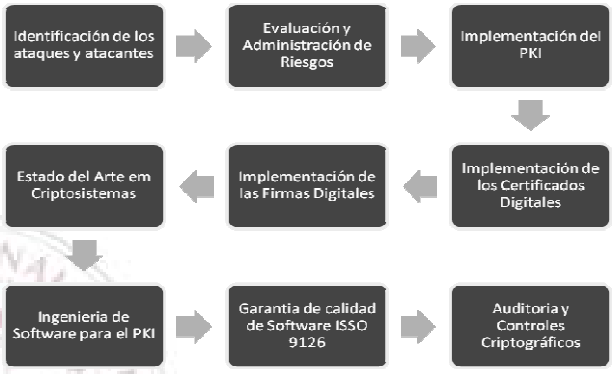

Figura 2. Metodologia para el Desarrollo de un PKI orientado al Análisis de Riesgo

A. *Identificación de los Ataques y Atacantes*

Actualmente tenemos muchos recursos que almacenan los diferentes tipos de ataques (ejemplo: *OWASP Top Ten, NIST – National Vulnerability Database, SANS Institute*, artítulos, etc,). Estos recursos nos brindan una gran colección de clases de ataques. Analizando los posibles ataques en una institución por pérdida de confidencialidad, integridad, disponibilidad, OWASP Ton Ten 2010 [4] nos entrega una lista de amenazas:

- Inyección de fallas.
- Secuencia de Comando de Sitios Cruzados (XSS).
- Pérdida de Autenticación y Gestión de Sesiones.
- Referencia Directa Insegura a Objetos.
- Falsificación de Peticiones en Sitios Cruzados (CSRF).
- Defectuosa Configuración de Seguridad.
- Almacenamiento Criptográfico Inseguro.
- Falla de Restricción de Acceso a URL.
- Protección Insuficiente en la Capa de Transporte.
- Redirecciones y reenvíos no validos.

B. *Evaluación y Administración de Riesgos*

El segundo paso es identificar los riesgos que puede comprometer la continuidad del negocio y las capacidades que tiene el atacante para consagrar el ataque. En este modelo, el atacante tiene completo control sobre la red.

Dado la complejidad que podemos tener, usamos la Norma Boliviana ISO/IEC 27000 para Sistemas de Gestión de la Seguridad de la Información que cubre diferentes controles de seguridad [18]. Estos controles servirán como base para desarrollar el MODELO P.H.V.A. (Figura 3) ideado

originalmente por Shewhart [23], fue adaptado a la Norma ISO 9001.

Figura 3. Circulo de Deming – Modelo PHVA [18].

Fuente: Microsoft, ©2004

Usa un ciclo PHVA básico que se conoce comúnmente como el Circuito Deming. Consiste en cuatro fases: Planificar, Hacer, Verificar y Actuar, donde:

- Planificar: establecer los objetivos y procesos necesarios para conseguir resultados de acuerdo con los requisitos del cliente (ya sea interno o externo) y las políticas de la organización.
- Hacer: implementar los procesos o actividades, considerando la educación y capacitación como requisito para seguir adelante con el ciclo.
- Verificar: realizar el seguimiento y la medición de los procesos y los productos respecto a las políticas, los objetivos y los requisitos para el producto, e informar sobre los resultados.
- Actuar: ejecutar acciones para mejorar continuamente el desempeño de los procesos.

C. Implementación del PKI

Obtenido los riesgos de la institución, debemos determinar la estructura del PKI. Los componentes más habituales de una infraestructura de clave pública son:

- La autoridad de certificación (*CA, Certificate Authority*): En este caso el ATT, 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 (*RA, Registration Authority*): En este caso ADSIB 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: Estructuras encargadas de almacenar la información relativa a la PKI.
- La autoridad de validación (*VA, Validation Authoirty*): encargada de comprobar la validez de los certificados digitales.
- La autoridad de sellado de tiempo: encargada de firmar documentos con la finalidad de probar que existían antes de un determinando instante de tiempo.
- Los usuarios y entidades finales son aquellos que poseen un par de claves (privada y pública) y un certificado asociado a su clave pública.

D. Estado del Arte en Criptosistemas

Es de suma importancia determinar cuáles serán los criptosistemas a utilizarse en nuestra PKI. La seguridad de la infraestructura PKI depende en parte de cómo se guarden las claves privadas como las políticas de uso. Dada la importancia de la información, en muchos de los algoritmos asimétricos ambas claves sirven tanto para cifrar como para descifrar [7].

E. Implementación de las Firmas Digitales

El concepto de firma digital nació como una alternativa tecnológica para optar por la autentificación de documentos legales en el marco de lo que se ha dado en llamar el ciberespacio. La firma digital ayuda a mantener la autentificación e integridad en la información, dos conceptos muy importantes en los sistemas de gestión de seguridad de la información.

Consiste en la transformación de un mensaje utilizando un sistema de cifrado asimétrico de manera que la persona que posee el mensaje original y la clave pública del firmante, pueda establecer de forma segura, que dicha transformación se efectúa utilizando la clave privada correspondiente a la pública del firmante, y si el mensaje es el original o fue alterado desde su concepción.

En el quinto paso nuestra misión es desarrollar el Sistema de Firmas Digitales y almacenar las claves públicas y privadas de manera segura.

1) La Seguridad en las Firmas Digitales

Para hacer uso de la firma digital, tenemos que satisfacer los siguientes aspectos de seguridad [17]:

- **Integridad de la información:** es una protección contra la modificación de los datos en forma intencional o accidental.
- **Autentificación del origen del mensaje:** Este aspecto protege al receptor del documento, garantizándole que dicho mensaje ha sido generado por la parte identificada en el documento como emisor del mismo, no pudiendo alguna otra entidad suplantar a un usuario del sistema.
- **No repudio del origen:** Protege al receptor del documento de la negación del emisor de haberlo enviado.
- **Imposibilidad de suplantación:** El hecho de que la firma haya sido creada por el signatario mediante medios que mantiene bajo su propio control (su clave privada protegida, por ejemplo, por una contraseña, una tarjeta inteligente, etc.) asegura, además, la imposibilidad de su suplantación por otro individuo.

Auditabilidad: permite identificar y rastrear las

operaciones llevadas a cabo por el usuario dentro de un sistema informático cuyo acceso se realiza mediante la presentación de certificados [9].

F. Implementación de los Certificados Digitales

Si bien las firmas digitales aseguran que los datos proceden de una parte que tiene acceso a una clave privada, no garantizan la identidad de dicha parte. Por ejemplo, un atacante podría haber obtenido una clave privada perteneciente al usuario A. Entonces podría utilizar esa clave junto con un algoritmo de hash estándar para firmar unos datos, lo que daría a entender que el origen de los datos es del usuario A [3]. Un certificado digital impide este robo de la identidad electrónica al comprobar que la firma pertenece sin duda alguna al emisor del mensaje.

Ahora es posible comprobar los datos y la firma como pertenecientes al emisor autorizado porque la entidad emisora de certificados (CA) de confianza ha comprobado que el emisor posee tanto la clave pública como la clave privada.

G. Ingeniería de Software para el PKI

El método más utilizado para desarrollo de software es el Modelo Lineal Secuencial o Ciclo de Vida Clásico. Su facilidad y alta prestación nos ayudara a desarrollar el software con mucha facilidad junto a los analistas, diseñadores y programadores para un PKI; además que brinda la posibilidad de mejorar los productos dentro de un proyecto de Seguridad [6].

Este modelo está compuesto por las siguientes fases:

- Investigación Preliminar.
- Determinación de los requisitos del sistema.
- Diseño del sistema (diseño lógico).
- Desarrollo de Software (diseño físico).
- Implementación y evaluación.

H. Garantía de calidad de Software

Las métricas del software proporcionan una manera cuantitativa de valorar la calidad de los atributos internos del producto, permitiendo por tanto al ingeniero valorar la calidad antes de construir el producto [6]. Las métricas proporcionan la visión interna necesaria para crear modelos efectivos de análisis y diseño, un código solidó y pruebas minuciosas.

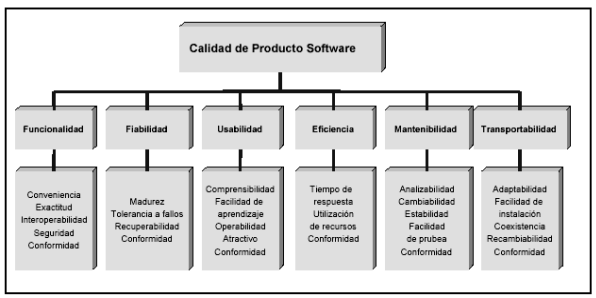

Figura 4. Calidad de un producto software (modelo ISO 9126) [6].

Para que sea útil en el contexto del mundo real, una métrica de software debe ser simple y calculable, persuasiva, consistente y objetiva. Debería ser independiente del lenguaje de programación y proporcionar una realimentación eficaz para el desarrollo del software.

El estándar ISO 9126 que se define [6] como la totalidad de características relacionadas con su habilidad para satisfacer necesidades o implicadas.

Los atributos de calidad se clasifican según seis características, las cuales a su vez se subdividen en subcaracterísticas (Figura 4).

Consecuentemente al uso de métricas para mejorar la calidad del software a ser implantado en SITTEL, se utilizara las herramientas Case para disminuir el tiempo de producción, el cual es desarrollado a continuación.

I. Auditoria y Controles Criptográficos

Una de las principales preocupaciones de las Entidades Públicas y Privadas que han realizado ingentes esfuerzos en la implementación de tecnologías de información, es la probabilidad de sus inversiones que han realizado no den soluciones inmediatas, tangibles y medibles; y allí donde se veía una oportunidad de mejora, realmente están creando un problema difícil de administrar, controlar y costos de mantener.

La Auditoria de Seguridad de Sistemas se constituye en una herramienta que gestiona la tecnología de la información en las entidades, a través de auditorias internas y externas.

Se tiene que proponer una metodología de auditoria informática con la finalidad de medir los riesgos y evaluar los controles en el uso de las tecnologías de información, haciendo uso de técnicas y estrategias de análisis, que permitan que la auditoria informática se convierta en una real y eficiente herramienta de gestión de tecnologías de información, a disposición de la organización.

III. Aplicación de la Propuesta

En esta sección presentamos la aplicación de nuestra propuesta al mundo real de la seguridad de la información.

Nuestro caso de estudio es la Autoridad de Fiscalización y Control Social de Telecomunicaciones y Transporte o ATT (ex Superintendencia de Telecomunicaciones o SITTEL) que tiene la potestad otorgada por el gobierno para administrar las telecomunicaciones y el transporte en Bolivia desde 2009 [11].

Uno de los objetivos del ATT es garantizar la provisión de servicios de calidad de transportes y telecomunicaciones, preservar la seguridad, y garantizar el ejercicio de los derechos de usuarios y/o consumidores.

Coadyuvado por la Agencia para el Desarrollo de la Sociedad de la Información en Bolivia (ADSIB), el ATT fue adquiriendo nuevas tareas en pro de la Sociedad de la Información Boliviana, participando de proyectos que proponen políticas, implementación de estrategias y coordinan acciones tendientes a lograr un uso y aprovechamiento de las Tecnologías de la Información y Comunicación en contextos como la Estratégica Bolivia de Reducción de la Pobreza y Bases para un Plan Nacional de Banda ancha de Internet entre otros [11].

Uno de los resultados fue el Desarrollo de la 1ra Ley de Documentos, Firmas y Comercio Electrónico aprobado por la ley 080/2007, quien otorga al ADSIB la función de entidad Acreditadora junto al ATT para regular las telecomunicaciones y proteger la seguridad de la información en Bolivia [22].

A. Análisis de Gestión y Riesgos de Seguridad

Según la Organización Internacional de Estandarización (ISO) [23] define a los riesgos como las amenazas, impactos y vulnerabilidades relativos a la información y a las instalaciones de procesamiento de la misma, y a la probabilidad de su ocurrencia, existiendo en cualquier actividad la contingencia implícita asociada al medio de trabajo y las tecnologías exigentes.

La gestión de riesgos hace procesos de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a los sistemas de información. A través de la gestión de riesgos se determinan las vulnerabilidades, amenazas y las posibles contramedidas, los cuales son:

- Vulnerabilidad: Representan las debilidades, aspectos factibles o atacables en el sistema informático.
- Amenaza: Posible peligro del sistema. Puede ser una persona, un programa o un suceso natural o de otra índole. Existen dos tipos de amenazas.
- Y las Contramedidas: Técnica de protección del sistema contra las amenazas, por el cual se determino que más de la mitad de los mismos son ataques intencionados por Hackers.

B. Evaluación y Administración de Riesgos

La Auditoria de Seguridad de Sistemas se constituye en una herramienta que gestiona la tecnología de la información en las entidades, a través de auditorías internas y externas, la finalidad de esta es determinar cuál será el impacto del PKI en la entidad que desarrollará la plataforma, por razones de seguridad llamaremos a la entidad PKI_CA de Certificadora Autorizada para claves públicas.

El auditor de sistemas debe tener la capacidad de definir las etapas y las técnicas que serán necesarias para la realización de la auditoria de manera óptima y cumpliendo las Normas de Auditoria de Sistemas y el Código de Ética Profesional descritos en la NB ISO/IEC 27000 para los puntos que tienen relación con las firmas y certificados digitales [18].

Los dominios a ser evaluados en la entidad PKI_CA para mejorar los niveles de seguridad mediante el modelo PHVA (Planificación, Hacer, Verificar y Actuar) son los siguientes:

PS1: Politicas de la seguridad de la información
OS1: Infraestructura de la Seguridad de la Información
CCA2: Clasificación de la Información
SP2: Capacitación al usuario
SP3: Respuesta a incidentes y anomalías en materia de seguridad
SFA3: Controles Generales
GCO3: Protección contra el software malicioso
GCO6: Gestión y seguridad de los medios de almacenamiento
CGO7: Intercambios de información y software
CA3: Responsabilidades del usuario
CA6: Control de acceso a las aplicaciones
DMS1: Requerimientos de seguridad de los sistemas
DMS3: Controles Criptográficos
DMS4: Seguridad de los archivos del sistema
GCN: Aspectos de la gestión de la continuidad de los negocios
C3: Consideraciones de auditoría de sistemas

Se realizó dos actividades relevantes en la entidad PKI_CA con el fin de determinar el nivel de riesgo de seguridad de la información, la primera es la revisión de la documentación para la seguridad de la información y la segunda es el cuestionario obtenido en base a la administración de riesgos (Tabla 1.).

					1-5	1-5	
N	**CR**	**Objet.**	**Debilidad y Recom.**	**Acción**	**Probab. de Riesgo (PR)**	**Impacto En ent_PKI (IS)**	**R=PR*IS**
1	4	PS1	PS1	-	2	2	**4**
2	3	OS1	OS1	-	3	4	**12**
3	5	CCA2	CCA2	-	2	2	**4**
4	**2**	**SP2**	**SP2**	**A3**	**3**	**5**	**15**
5	3	SP3	SP3	-	3	3	**9**
6	5	SFA3	SFA3	-	3	2	**6**
7	4	CGO3	CGO3	-	2	3	**6**
8	5	CGO6	CGO6	-	2	2	**4**
9	5	CGO7	CGO7	-	2	2	**4**
10	3	CA3	CA3	-	2	4	**8**
11	4	CA6	CA6	-	2	2	**4**
12	**1**	**DMS1**	**DMS1**	**A1**	**5**	**4**	**20**
13	**1**	**DMS3**	**DMS3**	**A2**	**5**	**5**	**25**
14	3	DMS4	DMS4	-	5	3	**15**
15	4	GCN1	GCN1	-	2	3	**6**
16	4	C3	C3	-	0	3	**0**

Tabla 1. Tabla de Riesgos.

Donde clasificamos el impacto de los riesgos según la Norma Bolivia ISO/IEC 27000 en la Tabla 2:

Evaluación de Riesgo en ATT	**1**	**Muy Bajo**
	2	**Bajo**
	3	**Medio**
	4	**Alto**
	5	**Muy Alto**

Tabla 2. Impacto de los Riesgos.

En la anterior tabla 2 se realiza una multiplicación de la Probabilidad del Riesgo del dominio determinado en la Auditoria a la entidad PKI_CA cuando el riesgo se materialice, además se adjunto una tabla con la valoración del Riesgo (R) descrito en la tabla 3.

Con los resultados obtenidos se analizo la probabilidad de ocurrencia y el cumplimiento de objetivos, llegando a las siguientes conclusiones en la tabla 3 donde describimos los posibles problemas, se determino por colores siendo el rojo el de Mayor Riesgo y el Verde Claro el de Menor Riesgo.

IMPACTO \ Riesgos	5	4	3	2	1
5	DMS3		SP2		
4	DMS1		OS1	SGO3-CA3	
3	DMS4		SP3	GCN1	
2			SFA3	PS1-CCA2-SGO6 SGO7-CA6	
1					C3

Tabla 3. Valoración de Riesgos.

A fin de desarrollar con mayor eficiencia la auditoria, se realizó acciones frente a los riesgos presentados en la anterior sección, descritos a continuación:

A1. Acción frente al riesgo de la Seguridad de la Información en los Requerimientos de Seguridad de los Sistemas: Protección por Backups y revisión semestral de los controles de seguridad.

A2. Acción frente al Riesgo de la Seguridad de la Información en los Controles Criptográficos: Protección de la información (Integridad y Confidencialidad) por Firmas Digitales, Administración de Claves y Certificados Digitales.

Comprobada la pertinencia del proyecto en la entidad PKI_AC, se procedió a desarrollar el proyecto en sus fases de Ingeniería de Software para el Desarrollo del PKI.

C. Implementación del PKI

Dada la organización del PKI determinamos que su estructura tiene que estar compuesta por (Figura 5):

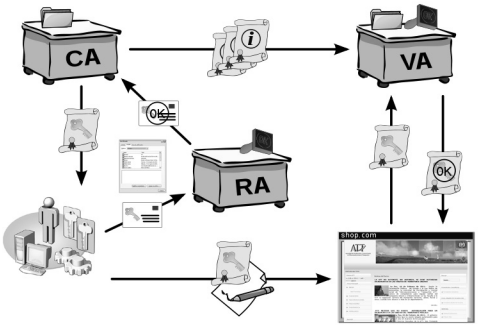

Figura 5. Infraestructura de Claves Públicas o PKI [12].

- La entidad emisora de certificados (CA) genera un par de claves para el usuaria A, quien tienen la potestad de la clave privada.
- A través de un certificado digital, la identidad del usuario es única frente al dominio de CA.
- La autoridad de registro (RA) aseguro esta unión entre el usuario y el CA.
- Para cada usuario, la identidad del usuario, la clave pública, las condiciones de validez y otros atributos se hacen infalsificables, estos datos se encuentran en el Certificado Digital otorgado por el CA.
- Ahora el usuario está listo para usar su firma digital en sus transacciones electrónicas mientras el VA comprueba su firma digital [10].

D. Estado del Arte en Criptosistemas

Dada la importancia de la información, se realizó un estado del arte de la criptografía asimétrica para el PKI para cinco algoritmos de encriptación RSA, Diffie-Hellman, Rabin, DSA y PGP. En muchos de los algoritmos asimétricos ambas claves sirven tanto para cifrar como para descifrar, para lo cual se revisan a continuación los algoritmos más robustos:

RSA: Debe su nombre a sus tres inventores: Ronald Rivest, Adi Shamir y Leonard Adleman [12] [13]. Tiene las siguientes características:

- Fácil de implementar.
- Sus claves sirven indistintamente tanto para decodificar como para autentificar.
- Uno de los más seguros en el mundo.
- La dificultad de desencriptar se base en la factorización de grandes números.
- Su utilización e implementación tiene costo de patente, por lo tanto no es un algoritmo asimétrico libre.
- Aunque el algoritmo RSA es bastante seguro conceptualmente, existen algunos puntos débiles en la forma de utilizarlo que pueden ser aprovechados por un atacante:
  - Claves o llaves débiles en RSA
  - Claves demasiado cortas
  - Ataques de Texto en Claro Escogido
  - Ataques de Módulo en Común
  - Ataques de Exponente Bajo
  - Ataque de Firma y Decodificar

Algoritmo de Diffie-Hellman: Lleva el nombre de sus creadores [12]. Tiene las siguientes características:

- Basado en el Problema de Diffie-Hellman de transmisión segura de la información.
- No son necesarias llaves públicas en el sentido estricto, sino una información compartida por los dos comunicantes en canales de comunicación seguras.
- Parte del protocolo de comunicación que son el factor X, Y no pueden ser trasmitidos por canales de comunicación públicos.
- Dificultad de ser utilizados para Firmas y Certificados Digitales por su estructura. Para lo cual se debe implementar una estructura de Firmas Digitales de ElGamal.

Algoritmo de Rabin: Las características del algoritmo son las siguientes [12] [14]:

- Basado en el problema de calcular raíces cuadradas de módulo de un número compuesto.
- Genera cuatro posibles respuestas.
- No existe mecanismos para decidir cuál de las cuatro es la auténtica, por lo cual el mensaje deberá incluir algún tipo de información para que el receptor pueda distinguirlo de los otros.

Algoritmo DSA: El algoritmo *Digital Signature Algorithm (DSA)* es parte del estándar *Digital Signature Standard (DSS)* [12]. Este algoritmo es una variante del método asimétrico ELGAMAL. Por lo cual tiene los mismos beneficios y problemas que el algoritmo mencionado.

PGP: Debe su nombre a *Pretty Good Privacy* (Privacidad Bastante Buena) [12] [15] [16]. Tiene un similar funcionamiento al algoritmo MD5 y SHA-1 (Figura 6). Tiene las siguientes características:

- La licencia es abierta para su uso.
- Combina lo mejor de las claves asimétricas y simétricas.
- Soporte para aplicaciones en Internet
- Herramientas Sencillas, Potentes y Gratuitas.
- Convertido en un estándar internacional (RFC2440).
- Aplicación de codificación automática y transparente sobre TCP/IP (PGPnet).
- Trabajado sobre Estándares del ISO 14888 con Certificación Internacional.
- Debilidad con la utilización de contraseñas de 8 caracteres o menos.
- Emitir revocaciones de las claves al generarlas.

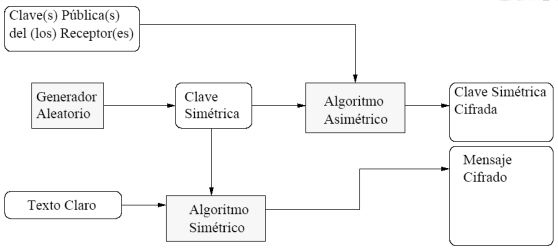

Figura 6: Codificación de un mensaje PGP [7].

1) Metodologia de selección del Algoritmo para el PKI

Para medir la efectividad (E) de los algoritmos, se analizó (ver tabla 4) cuan susceptible son los algoritmos [18]:

E1. Ataques de Denegación de Servicios
E2. Ataques de Fuerza Bruta
E3. Técnicas de Suplantación de Identidad
E4. Inyección de Fallas
E5. Licencias/patentes de uso
E6. Complejidad en la implementación y utilización

ALGORITMO	E1	E2	E3	E4	E5	E6
RSA	X	X	X		X	
Diffie-Hellman			X	X		X
Rabin	X	X	X	X		X
DSA	X	X	X	X	X	
PGP	X		X	X		

Tabla 4. Selección del algoritmo para el PKI.

Dado que no existe un algoritmo que cumpla todos nuestros objetivos, tomamos al algoritmo *Pretty Good Privacy* (PGP) por tener licencia libre y con un buen nivel de seguridad para un PKI.

E. Implementación de las Firmas Digitales

Las aplicaciones de la Firma Digital difieren según los requirentes del negocio, entre algunas aplicaciones tenemos:

- Transferencia de dinero de una cuenta a otra sobre redes no protegidas.
- Intercambio electrónico de Datos Privados.
- Intercambio de Documentación aprovechada en Sistemas Legislativo.
- Autentificación del emisor del E-mail por el receptor.
- Utilización en el E-Commerce para contratos electrónicos.
- Formas de procesamiento automatizado para autentificación de usuarios y empleados en empresas.

La funcionalidad puede ser orientada a corporaciones con plataformas PKI (Public Key Infraestructure), personal o servicio a terceras personas generando un modelo de mercado de ventas de firmas y certificados digitales, explotado principalmente por Verisign, empresa Certificadora principalmente en Certificados Digitales para Servidores y Páginas Web, Firmas Digitales Personales, etc.PGP combina algunas de las mejores características de la criptografía Simétrica y la criptografía asimétrica, siendo un sistema híbrido, tiene el siguiente funcionamiento como se describe en la figura 7:

1. El usuario envía un documento firmado por un medio de comunicación inseguro como el Internet.
2. El usuario emplea PGP para cifrar el texto plano, dicho texto es comprimido para aumentar una enorme resistencia al criptoanálisis.
3. Después de comprimir el texto, PGP crea una clave de sesión secreta que solo se empleará una vez. Esta clave es un número aleatorio generado a partir de los movimientos del ratón y las teclas que se pulsen durante unos segundos con el propósito específico de generar esta clave.
4. Se obtiene el valor Resumen (HASH) del texto comprimido mediante MD5.
5. Este valor HASH es cifrado por la clave asimétrica del usuario (clave simétrica).
6. La clave cifrada se adjunto al texto cifrado y el conjunto es enviado al receptor por un medio de comunicación inseguro como el internet.

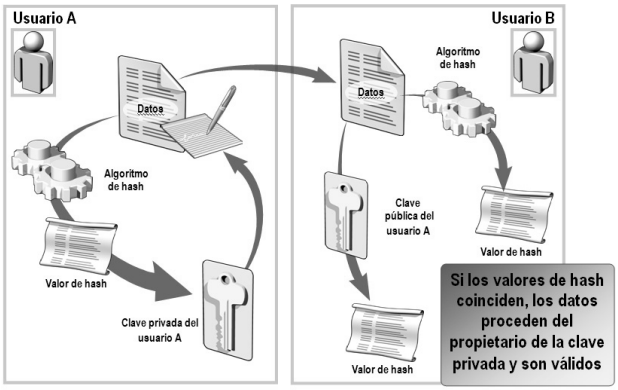

Fig. 7. Proceso de cifrado y descifrado por Firma Digital mediante uso del Criptositema PGP [24].

El descifrado sigue el proceso inverso. El receptor usa su clave privada para recuperar la clave de sesión, que PGP luego usa para descifrar los datos.

Cuando el proceso de descifrado concluye, PGP compara los valores HASH obtenidos del mensaje comprimido y el valor HASH recibido del emisor del mensaje, si estos valores son idénticos, entonces el mensaje esta integro y autentificado por el programa.

F. Implementación de los Certificados Digitales

Los certificados digitales colaboran a la seguridad de las firmas digitales y claves asimétricas de los usuarios de la siguiente forma (Figura 8):

1. Un usuario, equipo, servicio o aplicación crea el par de claves pública y privada.
2. La clave pública se transmite a la entidad emisora de certificados (CA) a través de una conexión de red segura.
3. El administrador certificado examina la solicitud de certificado para comprobar la información.

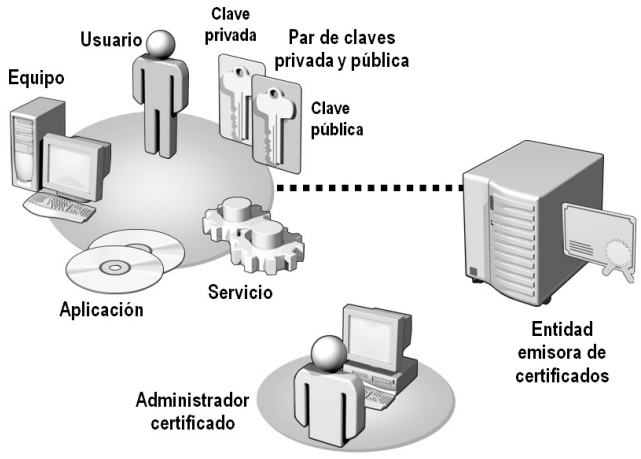

Fig. 8. Funcionamiento del Certificado Digital [24].

G. Ingeniería de Software para el PKI

El Modelo Lineal Secuencial conocido como Ciclo de vida Clásico se aplica al desarrollo de un proyecto de sistemas de seguridad para proyectar los riesgos en cada etapa, se determino que un PKI precisa de los siguientes casos:

- Ingreso al Sistemas, iniciar sesión y selección de opciones
- Inscripción y obtención de Claves Asimétricas
- Recuperación y Modificación de Datos de Contraseña de la Firma Digital
- Proceso de Firmado Digital
- Proceso de Autentificación de un mensaje por Firma Digital
- Gestión de Claves Públicas y Anillos Públicos
- Gestión de Usuarios
- Autentificación de Firma Digital por Certificado Digital
- Eliminar el servicio de Firmas y Certificados Digitales
- Cerrar Sesión del Programa

Dado la extensión del proyecto, solo describiremos el proceso de Autenticación de Firma Digital por Certificado Digital descrito en la Figura 9.

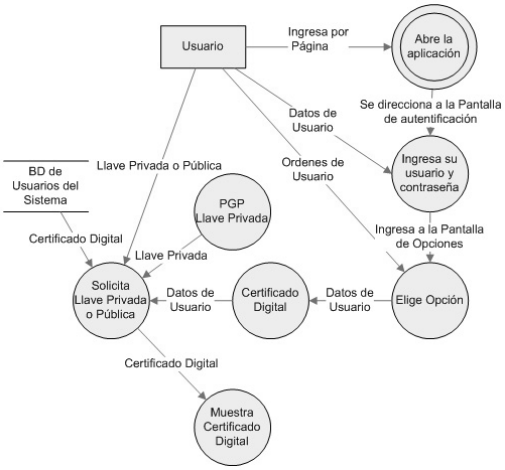

Figura 9. DFD de nivel 2 para la identificación de la Firma Digital por Certificado Digital.

-

H. Garantía de calidad de Software

Los factores que afectan a la calidad de software se concentran en tres aspectos: sus características operativas, su capacidad de cambios y su adaptabilidad a nuevos entornos (Figura 10).

Figura 10. Factores de Calidad de McCall.

Dentro del esquema presentado verificamos que el PKI cumple con los esquemas de calidad, comprobando su funcionalidad, fiabilidad, usabilidad, eficiencia, mantenibilidad y transportabilidad.

I. Auditoria y Controles Criptográficos

A fin de desarrollar con mayor facilidad la auditoria, se realizarán acciones frente a los riesgos presentados en la sección anterior, los cuales son descritos a continuación:

A1. Acción frente al Riesgo de la Seguridad de la Información en los Requerimientos de Seguridad de los Sistemas

Política de utilización de controles criptográficos:

- Las comunicaciones de requerimientos comerciales para nuevos sistemas o mejoras a los sistemas existentes deben especificar las necesidades de controles. Tales especificaciones deben considerar los controles automáticos a incorporar al sistema y la necesidad de controles manuales de apoyo. Se deben aplicar consideraciones similares al evaluar paquetes de software para aplicaciones comerciales. Si se considera adecuado, la administración puede querer utilizar productos certificados y evaluados en forma independiente.
- Los requerimientos de seguridad y los controles deben reflejar el valor comercial de los recursos de información involucrados y el potencial daño al negocio que pudiere resultar por una falla o falta de seguridad. El marco para analizar los requerimientos de seguridad e identificar los controles que los satisfagan son la evaluación y la administración de riesgo.
- Los controles introducidos en la etapa de diseño son significativamente más baratos de implementar y mantener que aquellos incluidos durante o después de la implementación.
- Se llego a la conclusión que dichos controles fueron revisados a la terminación del producto o software, determinándose el contra riesgo ante la perdida de seguridad/

A2. Acción frente al Riesgo de la Seguridad de la Información en los Controles Criptográfico.

Firma digital:

- Las firmas digitales proporcionan un medio de protección de la autenticidad e integridad de los documentos electrónicos. Por ejemplo, puede utilizarse en comercio electrónico donde existe la necesidad de verificar quien firma un documento electrónico y comprobar si el contenido del documento firmado ha sido modificado.
- Se den tomar recaudos para proteger la confidencialidad de la clave privada, esta clave debe mantenerse en secreto dado que una persona que tenga acceso a esta clave puede firmar documentos, por ej.: pagos y contratos, falsificando así la firma del propietario de la clave.
- Asimismo, es importante proteger la integridad de la clave pública. Esta protección se provee mediante el uso de un certificado de clave pública.
- Es necesario considerar el tipo y la calidad del algoritmo de firma utilizado (en el caso del proyecto de grado se hará uso del algoritmo PGP) y la longitud de las claves a utilizar (128 bits). Las claves criptográficas aplicadas a firmas digitales deben ser distintas de las que se utilizan para el cifrado.
- Al utilizar firmas digitales, se debe considerar la legislación pertinente que describa las condiciones bajo las cuales una firma digital es legalmente vinculante. Por ejemplo, en el caso del comercio electrónico es importante conocer la situación jurídica de las firmas digitales. Podría ser necesario establecer contratos de cumplimiento obligatorio u otros acuerdos para respaldar el uso de las mismas, cuando el marco legal es inadecuado. Se debe obtener asesoramiento legal con respecto a las leyes y normas que podrían aplicarse al uso de firmas digitales que pretende realizar la organización.

Administración de Claves y Certificado Digital:

- Decidir si una solución criptográfica es apropiada, deber ser visto como parte de un proceso más amplio de evaluación de riesgos, para determinar el nivel de protección que debe darse a la información. Esta evaluación puede utilizarse posteriormente para determinar si un control criptográfico es adecuado, que tipo de control debe aplicarse y con qué propósito, y los procesos de la empresa.
- Una organización debe desarrollar una política sobre el uso de controles criptográficos para la protección de su información. Dicha política es necesaria para maximizar beneficios y minimizar los riesgos que ocasiona el uso de técnicas criptográficas, y para evitar un uso inadecuado o incorrecto).

Se llego a la conclusión que los controles por Firmas Digitales, Administración de Claves y Certificados Digitales fueron revisados a la terminación del producto o software y con una periodizad de revisión cada seis meses.

IV. Conclusiones

En este trabajo se ha dirigido una perspectiva novedosa hacia la construcción de una Plataforma para la Administración de Firmas y Certificados Digitales en la Agencia para el Desarrollo de la Información en Bolivia (SITTEL) y la Autoridad de Fiscalización y Control Social de Telecomunicaciones y Transporte (ATT) bajo la visión de la NB ISO/EIC 27000 para la Gestión de la Seguridad de Sistemas de Información, esta reciente metodología implementa una combinación de herramientas y criptosistemas, dada la importancia de brindar seguridad a la

firma digital y el certificado digital a la firma digital.

Así mismo, se evaluó cinco criptosistemas, aplicándose el criptosistema PGP por su versatilidad ante ataques, además de asegurar la integridad de la información y la autenticidad del origen del mensaje ante la aparición de muchos casos de reproducción y suplantación de documentos físicos en las instituciones gubernamentales.

Como trabajos futuros serán analizadas la generación de una metodología para el desarrollo de proyectos que envuelvan los conceptos de protección de la información y seguridad de la información bajo modelos de desarrolla rápido de software (ejemplo: RAD, XP) y orientado a las tecnologías de información en e-goberment (Gobierno Electrónico) e e-commerce (Comercio Electrónico).

V. AGRADECIMIENTOS

El autor agradece la colaboración y revisión del MsC. Lic. Fernando Yañez Romero, por su constante apoyo en beneficio del presente trabajo. Al My. DIM. Álvaro Rios Oliver, por sus consejos y apoyo durante los cinco años de estudio en la Escuela Militar de Ingeniería. Al MsC. Ing. Guido Rosales Uriona por ser un amigo y consejero en el desarrollo del presente trabajo. A la MsC. Lic. Amparo Subieta por la confianza y colaboración para emprender esta propuesta en SITTEL. A PHD. Eliane Martins por ser mi guía durante la realización de mi Master in Science en la Universidade Estadual de Campinas.

VI. REFERENCIAS

Fuente: 1º Foro Latinoamericano de Seguridad Informática en Tecnologías de la Información

[1] Yukio Okada; Hiroaki Hazeyama; Youki Kadobayashi; , "Proposal of Constructing PKI on Overlay Network," Applications and the Internet Workshops, 2007. SAINT Workshops 2007. International Symposium on , vol., no., pp.64, Jan. 2007

[2] Haibo Yu; Chunzhao Jin; Haiyan Che; , "A Description Logic for PKI Trust Domain Modeling," Information Technology and Applications, 2005. ICITA 2005. Third International Conference on , vol.2, no., pp.524-528, 4-7 July 2005

[3] El Bakkali, H.; Kaitouni, B.I.; , "A logic-based reasoning about PKI trust model," Computers and Communications, 2001. Proceedings. Sixth IEEE Symposium on , vol., no., pp.42-48, 2001

[4] OWASP TOP TEN, Fundación OWASP, 3ra Edición, 2010.

[5] COBIT: Control Objectives for Information and Related Technology. ISACA, 5ta Edición, 2010.

[6] Pressman, Roger S. "Software Engineering", Editorial Mc Graw Hill, 6ta Edición. ©2004.

[7] Lucena, Manuel. "Criptografía y Seguridad en Computadoras", Departamento de Informática de la Escuela Politécnica Superior - Universidad de Jaén. ©2009.

[8] Tanenbaum, Andrew. "Computer Networks", Prentice Hall, S.A. 5ta Edición. ©2010.

[9] Microsoft Press. "Writing Secure Code". ©2003.

[10] Microsoft Press. "Building secure Microsoft ASP.NET Applications". ©2004. Disponible en Internet en: http://www.microsoft.com/downloads/release.asp?ReleaseID=44047

[11] Superintendencia de Telecomunicaciones. "Regulación de las Telecomunicaciones en Bolivia 1998 - 2001", La Paz, Bolivia. ©1998-2001.

[12] RED TEMATICA IBEROAMERICANA DE CRIPTOGRAFIA Y SEGURIDAD DE LA INFORMACION. Disponible en la Web: http://www.criptored.upm.es/

[13] RSA Security Sign On-Manager. Disponible en la Web: http://www.rsasecurity.com

[14] RED ESPAÑOLA DE I+D. Disponible en la Web. http://www.rediris.es/

[15] The International PGP. Disponible en la Web: http://www.pgpi.org/

[16] Organización de Software Libre Linux – PGP. Disponible en la Web: http://www.gnupgp.com/

[17] International Telecommunication Union o Unión Internacional de Telecomunicaciones (UIT). Disponible en la Web: www.itu.int/home/index-es.html

[18] IBNORCA NB-ISO-IEC 27000:2007

[19] Unión de Telecomunicaciones Internacional (ITU)

[20] ITU-T X.509:

[21] Information technology – Open systems interconnection – The Directory: Public-key and attribute certificate frameworks

[22] CEPAL. Conferencia "Los caminos hacia una Sociedad de la Información en América Latina y el Caribe". 2003 – http://www.alfa-redi.org

[23] IBNOCAR: Gestión de la Seguridad de la Información en la empresa Norma ISO/IEC 17799

[24] Microsoft Company. 1º Foro Latinoamericano de Seguridad Informática de Tecnologías de Microsoft. 2004 – http://www.microsft.com

VII. BIOGRAFÍAS

Marcelo Invert Palma Salas nació en la ciudad de La Paz, Bolivia el 14 de septiembre de 1982, recibió su grado de Ingeniero de Sistemas, en la Escuela Militar de Ingeniería (EMI) en 2005. Es becario (Convenio PEG-PG) del Programa en Ciencias de la Computación en la Universidade Estadual de Campinas (UNICAMP) en la ciudad de Campinas, estado de São Paulo, Brasil y miembro del Laboratorio de Sistemas Distribuidos del Instituto de Computação en la UNICAMP. Tiene diplomados en Gestión Universitaria y Administración Pedagógica del Aula Universitaria, ambos diplomados obtenidos en la Universidad Mayor de San Andrés. Desde 2004 colabora como investigador en la Administración de Seguridad de la Información y Auditoria de Sistemas en la Escuela Militar de Ingeniería y actualmente en el Grupo Internacional de Robust Web en Brasil. Postulante al grado de Master in Science en la Universidad Estadual de Campinas (UNICAMP) en Ciencias de la Computación con especialidad en Seguridad para Servicios y Criptografía. Especialista en DBA Oracle, CCNA Cisco, NB ISO/IEC 27000. Trabajo para empresas Gubernamentales y Multinacionales como PriceWater House Coopers, Superintendencia de Telecomunicaciones (SITTEL), Antalis-GMS Chile. Desde el 2007 fue docente de la Escuela Militar de Ingenieria, Miembro del Consejo de Carrera de Sistemas e investigador para el área de Seguridad de la Información. Miembro del Colegio de Ingeniero de Sistemas de la SIB La Paz, Presidente y fundador del Capítulo Profesional IEEE Computer Society Bolivia. Del 2006 al 2008 fue IEEE Student Section Activities Committe (SSAC) en la Sección Bolivia. El 2010 fue elegido como IEEE Student Regional Activities Committe (RSAC) para para América Latina y el Caribe. El 2009 Premio IEEE Theodore W. Hissey IEEE – USA / Región 9 América Latina y el Caribe. Miembro del MGA IEEE USA (marcelopalma@ieee.org).