UNIVERSIDAD TECNOLÓGICA ISRAEL
FACULTAD DE SISTEMAS INFORMÁTICOS
CARRERA DE SISTEMAS INFORMTICOS

Propuesta de una solución alternativa para contrarrestar actividades delincuenciales informáticas en instituciones bancarios en la web, por medio de Cryptomathic Signer.

Estudiante:

Nancy Yambay Valla

Tutor:

Ing. Pablo Tamayo

Quito – Ecuador

Noviembre 2011

AGRADECIMIENTO

Ante la dicha de haber culminado mi tesis de grado, solo me queda el placer de agradecer por ello, ante todo a Dios por haberme dado vida y fuerza para vencer todos los obstáculos que se me presentaron en el camino, a mis padres, finalmente tengo que mencionar de manera muy especial al Ing. Pablo Tamayo quien me brindo su sabiduría en todo el tiempo y por su confianza

DEDICATORIA

Este trabajo va dedicado a mis padres, porque siempre depositaron su confianza en mi todo este tiempo y por último a todas las personas que me brindaron su apoyo desinteresado

INDICE

RESUMEN

El trabajo está enfocado a conocer la herramienta de Cryptomathic Signer, que nos ayudará de forma segura que la información se mantenga de manera confidencial.

Es una ayuda de forma sencilla y fácil de usar,porque ofrece la posibilidad de cifrar y descifrar la información,poruna comunicación segura entre los miembros de las unidades de organización y sus socios de negocios.

Además se realizará un análisis de la herramienta de Cryptomathic firmante donde almacena una clave privada en una base de datos segura y genera la firma digital.

El usuario puede realizar transacciones electrónicas y pedir una firma en cualquier momento y desde cualquier PC a través de un navegador web.

Finalmente se da a conocer a fondo como elemento de una infraestructura de una tecnología informática segura.

ABSTRACT

The work is focused on knowing the Cryptomathic Signer tool that will help us secure that information is kept confidential.

It helps in a simple and easy to use, because it offers the ability to encrypt and decrypt the information, secure communication between members of organizational units and business partners.

In addition, an analysis tool which stores a signatory Cryptomathic private key in a secure database and generates the digital signature.

The user can perform electronic transactions and get a signature at any time from any PC via a web browser.

Finally, fully disclosed as part of an information technology infrastructure in a safe.

CAPITULO I

INTRODUCCIÓN

1. Tema de investigación

Propuesta de una Solución alternativa para contrarrestar actividades delincuenciales informáticas en la web en instituciones bancarios en línea, por medio de Cryptomathic Signer.

1.1 Planteamiento del problema

La Cooperativa de Ahorro y Crédito "Juventud Ecuatoriana Progresista" Ltda., es una entidad dedicada a las finanzas sociales, creada mediante acuerdo Ministerial 3310, del 31 de diciembre de 1971 y calificada por la Superintendencia de Bancos y Seguros.

Creada en la parroquia de Sayausi, del cantón Cuenca, provincia del Azuay, el proyecto se enfoca a la sucursal 2 de la 9 de octubre, ha incursionado en un sostenido apoyo crediticio a los segmentos poblacionales que no tienen acceso al crédito de la banca tradicional, aspecto que ha estimulado la aceptación y confianza de la gente.

El análisis de la puesta en marcha en nuestro país de una modalidad de negocio bancario, con un soporte innovador y relativamente reciente, como es Internet.

Se trata, pues, de los bancos independientes, que operan principalmente a través de la red, de cómo éstos resuelven el dilema sobre la adquisición de las nuevas tecnologías de la información.

Las firmas digitales permiten la confianza y actuar en consecuencia las transacciones electrónicas, como si estuviesen impresos en papel y firmada por un socio de confianza.

El Phishing comenzó en AOL durante los años 1990 solían obtener cuentas para usar los servicios de la compañía a través de números de tarjetas de crédito válidos, generados utilizando algoritmos para tal efecto.

En 1995 AOL tomó medidas para prevenir este uso fraudulento de sus servicios, la técnica utilizada del atacante enviaba un mensaje a una víctima potencial haciéndose pasar por un empleado de AOL, solicitando usuario y contraseña de acceso, con la excusa de que debían verificar la cuenta o confirmar los datos de la factura, conseguía la cuenta de la víctima, podía suplantar al usuario legítimo en el servicio y llevar a cabo cualquier acción fraudulenta como el envío de spam o ataques indiscriminados.

“El aspecto más importante de la informática radica en que la información a pasado a convertirse en un valor económico de primera magnitud, desde siempre el hombre ha buscado guardar información relevante para usarla después”, (Magliona, 1999)

En la actualidad las empresas necesitan comunicarse, siendo más dependientes de sus redes informáticas, la falta de medidas de seguridad en las redes es un problema que está en crecimiento, especialmente la privacidad.

Los bancos deben tomar las iniciativas pertinentes, para no ser víctima de robo de información, al momento de hacer transacciones online, los usuarios

previamente debe estar capacitados y tener la debida seguridad en las páginas web al momento de ingresar, deben proveerse al usuario de una solución seguro al momento de realizar sus transacciones en la web.

En el entorno social se conoce poco de Cryptomathic Singer, dado el desconocimiento de la herramienta para contrarrestar a ser víctimas de robo de dinero y que el usuario final, que no tiene ningún interés en aprender nada de seguridad informática, se ve cada vez más indefenso.

La solución para satisfacer esta necesidad de comunicación, es un servidor central que almacena la clave privada del usuario en una base de datos segura y genera firmas digitales a petición del usuario.

En el estudio aprenderemos que mediante el Cryptomathic Singer brindar la solución alternativa para contrarrestar actividades delincuenciales informáticas en la web, en instituciones bancarios.

1.2 Diagnóstico

1.2.1 Causas y efectos

Las instituciones bancarias no tienen una innovación tecnológica en la Protección de claves, causando cambio a la adaptación del sistema financiero.

Los bancos no conocen de los avances de la tecnología, si las instituciones no tienen una Seguridad mejorada en las claves, no tendrán la agilidad de sus servicios, ocasionando reducción de costes.

La limitación de los servidores en instituciones bancarias, hace que no sea rápida en la solicitud de la clave y no sea confiable.

En los servidores de almacenamiento no existe la renovación y aplicación de políticas de seguridad al enviar datos bancarios en la web, ocasionando al usuario el uso de software.

1.2.2 Pronóstico

Los usuarios están expuestos con las claves a terceras personas, quienes pueden llegar a saber la contraseña y modificar los datos perjudicando al usuario y a la institución.

Debe haber una inversión inmediata del software para contrarrestar la seguridad en las claves, por lo que la perdida de información ocasionaría perdida para el cliente y la institución bancaria en la web, y ocasionando estafas al momento de hacer transacciones en línea,

La restricción de los servidores para instituciones bancarias en la web, ocasiona perdida de costes por que no existe la rapidez de entregar clave pública, ocasionando desconfianza al hacer transacciones en la web.

Los usuarios no se actualizan en los conocimientos de la tecnología acerca de las transacciones bancarias en la web, al momento de enviar datos ocasionando almacenamiento de claves inseguras, para proteger información frente a delincuentes organizados.

1.2.3 Control del pronóstico

La protección mejorada de claves privadas se genera mediante un servidor de alta seguridad.

La seguridad mejorada de una clave privada, está protegida por la contraseña del usuario en todo momento, lo que significa que ni siquiera el proveedor de servicios puede acceder a la clave.

La movilidad siempre se puede llegar a través de Internet y no requerir instalación de software en el cliente secundario.

El servidor de almacenamiento de claves, se encarga de la administración central de llaves, simplifica la renovación de la clave y la aplicación de políticas.

1.3 Formulación de la problemática específica

1.3.1 Problema principal

¿ Permitirá el Análisis de la herramienta Cryptomathic Signer, ayudar a proteger la seguridad web mediante las firmas digitales, para contrarrestar las actividades delincuenciales en la web, en las instituciones bancarias en crecimiento como la “Cooperativa JEP de Cuenca”, determinando el impacto de éstas en dichas instituciones?.

1.3.2 Problemas Secundarios

¿Análisis de fortalezas y debilidades de Cryptomathic Signer, frente a la firma de seguridad para servicios web y banca online, en la “Cooperativa JEP de Cuenca.”?

¿Análisis de la funcionalidad de la Herramienta Cryptomathic Singer?

¿Elaborar el documento de implementación de Cryptomathic Signer, para las instituciones Bancarias en crecimiento “Cooperativa JEP de Cuenca.”?

1.4 Objetivos

1.4.1 Objetivo General

Análisis de la herramienta Cryptomathic Signer, para contrarrestar las actividades delincuenciales en la web, en instituciones bancarias en crecimiento que piensen implementar autenticación y firmas digitales, como cooperativas en crecimiento “Cooperativa Jep de Cuenca”. determinando el impacto de éstas en dichas instituciones.

1.4.2 Objetivos Específicos

- Análisis de fortalezas y debilidades de Cryptomathic Signer, frente a la firma de seguridad para servicios web y banca online, en la “Cooperativa JEP de Cuenca”.
- Análisis de la funcionalidad de la Herramienta Cryptomathic Singer.
- Elaborar el documento para implementar Cryptomathic Signer, en las instituciones Bancarias en crecimiento “Cooperativa JEP de Cuenca.”

1.5 Justificación

1.5.1 Justificación Teórica

“En todas las facetas de la actividad humana existen el engaño, las manipulaciones, la codicia, el ansia de venganza, el fraude, en definitiva, el delito. Desgraciadamente es algo consustancial al ser humano y así se puede constatar a lo largo de la historia”, (Laura, 1987)

Una organización bancaria es un intermediario financiero que se encarga de captar recursos en la forma de depósitos, así como la prestación de servicios financieros.

El Phishing y correos falsos permiten pasar a un atacante por una organización, banco o empresa verdaderos para obtener información que garantice acceso a algún recurso que usted utilice en esa organización.

Las manipulaciones informáticas, en cuanto a la fase entrada de datos en la cual se introducen datos falsos o se modifican los reales añadiendo otros o se omiten datos, las manipulaciones en el programa que contiene las órdenes precisas para el tratamiento informático.

La fase salida de datos, donde no se afecta el tratamiento informático, sino la salida de los datos procesados al exterior, cuando van a ser visualizados en la pantalla, se van a imprimir o registrar.

“La Cryptomathic Firmante ofrece la firma de seguridad para servicios Web, para banca electrónica, se combina autenticación fuerte, con la firma digital sin comprometer la seguridad, el usuario puede pedir una firma en cualquier

momento a través de Internet, por ejemplo, desde un navegador web o un cliente de correo electrónico”, (Copyright, 1986)

Con los usuarios del firmante están en condiciones de firmar las transacciones electrónicas legalmente vinculante de forma segura desde cualquier parte del mundo.

1.5.2 Justificación Metodológica

Cryptomathic firmante ofrece la firma de seguridad para servicios Web, la banca por Internet y los servicios públicos, se combina autenticación fuerte, con las firmas digitales móviles sin comprometer la seguridad.

Herramientas necesarias para la elaboración de una seguridad mediante la Cryptomathic Singer, Web Browser, Cliente de Correo Electrónico, Aplicación, Internet, Firma de Servidor y Servidor de Autenticación.

La Planeación estratégica mediante el Diagnóstico y Análisis Institucional Busca solucionar el problema de la brecha entre la situación inicial, la identificará mediante un Diagnóstico y la situación futura deseada para la empresa.

Cryptomathic Signer genera las firmas RSA con longitud de clave de 512 a 2048 bit.

1.5.3 Justificación Práctica

Es un mecanismo de estudio, por lo que se entregará un manual de las delincuencias informáticas en sistemas bancarios, con la solución de

Cryptomathic Signer, con sus procedimientos para la seguridad de la información.

Cryptomathic Signer, ayudará que los datos vayan al servidor central de forma segura, creando firmas digitales en nombre de un usuario, siendo un diseño único y está patentado en todo el mundo, para que no roben datos personales del usuario.

Brindando al usuario la protección de claves seguras y la autenticación de mensajes, fácil movilidad para el usuario, pretende defendernos contra todas las formas de ataque, garantizar una comunicación segura, incluso en redes abiertas como puede ser Internet.

Cryptomathic Signer es una solución centrada en servidor para la creación, gestión y el uso de claves privadas dentro de una infraestructura de clave pública (PKI),

El almacenamiento de las claves del usuario de la firma en una central segura servidor reduce el riesgo de seguridad, y al mismo tiempo aumenta el uso de la clave como el usuario está en condiciones de acceder y utilizar la clave de cualquier navegador Web.

1.6 Marco de Referencia

1.6.1 Marco Teórico

“El Phishing consiste en el envío de correos electrónicos aparentando provenir de fuentes fiables como entidades bancarias, intentan obtener datos confidenciales del usuario” (Wales, Jimmy, 2011)

Posteriormente son utilizados para la realización de algún tipo de fraude, con la “Firmante Cryptomathic podemos contrarrestar y brindar seguridad en la web, permitiendo autentificar los datos en una base de datos confiable, mediante claves legalmente autorizadas solo para el usuario principal” , (Wales, Jimmy, 2011)

Para no ser víctima de robo de identidad y datos confidenciales, esto provocaría pérdidas económicas para los usuarios o incluso impedirles el acceso a sus propias cuentas ocasionando pérdida de productividad.

Cryptomathic Firmante ofrece un método para el desarrollo de firmas digitales, permite al receptor de un mensaje verificar la autenticidad del origen de la información

La firma digital se basa en un mensaje cifrado utilizando la clave privada de un usuario, sólo puede ser descifrado utilizando la clave pública asociada, a través de la clave privada.

1.6.2 Marco Espacial

Análisis de la herramienta Cryptomathic Signer, para contrarrestar las actividades delincuenciales en la web, en instituciones bancarias en crecimiento que piensen implementar autenticación y firmas digitales, como cooperativas en crecimiento “Cooperativa Jep de Cuenca”.

1.6.3 Marco Temporal

El tiempo para elaborar proyecto es seis semanas.

1.7 Metodología

La metodología de la investigación cuantitativa analiza diversos elementos que pueden ser medidos y cuantificados, toda la información se obtiene a base de resultados, con un determinado nivel de error y nivel de confianza, se visualiza de números y métodos estadísticos, partiendo de casos concretos para llegar a una descripción general o comprobar hipótesis, a diferencia de la cualitativa que se encarga de dar la credibilidad de la comunicación, permiten observar al individuo encuestado y el objeto de la investigación, se sirve de entrevistas en profundidad o de análisis de materiales históricos.

El método Deductivo se infiere en los hechos observados basándose en la ley general, comienzan con el planteamiento del conjunto cierto de partida, donde los supuestos deben incorporar sólo las características más importantes de los fenómenos, con coherencia entre los postulados y continúan con el proceso de deducción lógica partiendo siempre de los postulados iniciales.

La Técnica Encuesta se encarga de recoger la información, por medio de preguntas escritas organizadas en un cuestionario impreso, se emplea para investigar hechos o fenómenos de forma general y no particular, sin la intervención directa de persona, que colaboran en la investigación.

Los mensajes enviados se representan mediante números, y el funcionamiento se basa en el producto, conocido, de dos números primos grandes elegidos al azar y mantenidos en secreto.

Cuando se quiere enviar un mensaje, el emisor busca la clave pública del receptor, cifra su mensaje con esa clave, y una vez que el mensaje cifrado llega al receptor, este se ocupa de descifrarlo usando su clave privada.

La Planeación estratégica mediante el Diagnóstico y Análisis Institucional Propone integrar el aporte de la técnica de planificación con las expectativas, intereses, necesidades y problemas de las personas involucradas.

1.7.1 Cronograma

CRONOGRAMA DE ACTIVIDADES	SEMANAS						
	1	2	3	4	5	6	7
1. Tema de investigación	*						
2. Planteamiento del problema	*						
2.1 Antecedentes	*						
2.2 Diagnóstico o planteamiento de la problemática general.	*						
2.2.1 Causa – Efecto	*						
2.2.2 Pronóstico y control del pronóstico	*						
2.3 Formulación de la Problemática Específica	*						
2.3.1 Problema Principal	*						
2.3.2 Problema Secundarios	*						
2.4 Objetivos	*						
2.4.1 Objetivo General	*						
2.4.2 Objetivos Específicos	*						
2.5 Justificación	*						
2.5.1 Justificación Teórica	*						
2.5.2 Justificación Metodológica	*						
2.5.3 Justificación Práctica	*						
2.6 Justificación	*						
2.6.1 Marco Teórico	*						
2.6.2 Marco Espacial	*						
2.6.3 Marco Temporal	*						
2.7 Metodología y Cronogramas	*						
2.8 Plan Analítico	*						
2.8.1 Análisis de fortalezas y debilidades de Cryptomathic Signer, frente a la firma de seguridad para servicios web y banca online, en la "Cooperativa JEP de Cuenca".		*	*				
2.8.2 Análisis de la funcionalidad de la Herramienta Cryptomathic Singer.				*	*		
2.8.3 Elaborar el documento para implementar Cryptomathic Signer, en las instituciones Bancarias en crecimiento "Cooperativa JEP de Cuenca.						*	
3. Sustentación del Proyecto							*

Tabla 1 Cronograma de Actividades

1.8 Plan Analítico (capítulos en base de los objetivos)

CAPITULO I

Análisis de fortalezas y debilidades de Cryptomathic Signer, frente a la firma de seguridad para servicios web y banca online, en la “Cooperativa JEP de Cuenca”.

CAPITULO II

Análisis de la funcionalidad de la Herramienta Cryptomathic Singer.

CAPITULO III

Elaborar el documento para implementar Cryptomathic Signer, en las instituciones Bancarias en crecimiento “Cooperativa JEP de Cuenca.

CAPITULO II

MARCO TEÓRICO

El objetivo de este trabajo es conocer cómo actúa el Phishing en la red, al momento de realizar transacciones en línea, donde el usuario se ve indefenso por no tener algún conocimiento de la seguridad informática, por lo que es necesaria una educación personal, para no tener pérdidas económicas.

Los diferentes medios y métodos informáticos que utilizan los estafadores para robar datos personales, al realizar pagos bancarios en línea, lo realizan mediante la suplantación de instituciones bancarias, donde se busca aumentar soluciones especializadas para enfrentar las amenazas actuales y futuras.

Por las grandes opciones en el mercado en cuanto a soluciones de seguridad de datos en la red, el trabajo se enfoca a una solución del servidor central, que almacena las claves privadas de los usuarios en una base de datos segura, generando así firmas digitales solo cuando el usuario lo solicite.

Además con la introducción del conocimiento de firmas digitales, permitirá al usuario dar la debida confianza de actuar frente a las transacciones electrónicas y no ser víctima de fraude.

La empresa de seguridad desarrolla soluciones de software como Cryptomathic, enfocado a industrias financieras y gubernamentales localizadas en Aartus, Dinamarca fundada en 1986 hace 25 años, siendo el presidente Peter Landrock.

2.1 Phishing.

Mediante la suplantación de sitios web que se encarga de capturarlos datos personales, siendo un delito que debe ser vigilada, porque mediante los mensajes de correo electrónico se hacen pasar por comunicados de bancos o tiendas de Internet, donde se debe hacer un llamado a los clientes a que actualicen o cambien continuamente sus claves de acceso, para no ser victimas de paginas web falsas como hacer que los clientes confirmen su número de tarjeta de crédito y así robar los datos.

Se trata de una forma de spam como correos electrónicos no deseados, donde satura los buzones de basura, poniendo en peligro la integridad de la información y con el tiempo tendrá graves consecuencias.

2.1.1 Delincuenciales Informáticas en la Web en Instituciones Bancarios.

El fraude en nuestro medio a intensificado siendo un riesgo en las actividades comerciales en línea, los estafadores intentan embaucar a los consumidores para que les suministren información confidencial que después lo utilizarán para su propio beneficio.

El usuario debe ser precavido al realizar cualquier tipo de transacción en Internet, debe asegurarse que la información y las solicitudes de pagos debe ser legítimos, así como la identidad de quienes los soliciten, para asegurarse debe llamar a la organización beneficiada.

2.2 Cooperativa de Ahorro y Crédito Juventud Ecuatoriana Progresiva.

En la actualidad cuenta con más de 200 mil socios dueños de la Cooperativa, aproximadamente un 70% de los mismos son mujeres, vinculadas a diferentes actividades micro productivas, tanto de los sectores rurales y urbano.

Creada en la parroquia de Sayausi del cantón Cuenca, ha incursionado porque las personas no tiene la facilidad de acceso al crédito de la banca tradicional, aspecto que ha estimulado la aceptación y confianza de la gente.

Basada en el principio de la solidaridad cooperativista, poniendo en primer lugar el entorno social para la rentabilidad financiera, generando de este modo sustentabilidad.

2.2.1 La Cooperativa de Ahorro y Crédito "La Merced" Ltda.

Creada el 23 de Septiembre de 1964 fundada por un grupo de artesanos de la parroquia el Vecino de la ciudad de Cuenca, cuya motivación fue el consolidar una alternativa de financiamiento, mediante la cooperación o ayuda mutua a través del ahorro y crédito.

Es una entidad que promueve el desarrollo socio económico de sus asociados, y la comunidad en general, mediante la prestación de servicios financieros en: ahorros, créditos e inversiones con las mejores tasas del mercado, además de proporcionar seguros gratuitos, beneficios en salud, medicina y vivienda.

Actualmente cuenta con 16 agencias ubicadas en Azuay, Cañar, Morona Santiago y Loja.

2.3 Delitos Informáticos

2.3.1 Pesca u olfateo de claves secretas

Suelen engañar a usuarios nuevos en el Internet, para que revelen sus claves personales, haciéndose pasar por el proveedor del servicio, para así esconder su verdadera identidad y cometer sus fechorías.

2.3.2 Transferencias de fondo

La seguridad en banca online, permite que los phishing o estafadores en la web, se hagan pasar por una empresa de confianza y en una aparente comunicación oficial electrónica, hacen que el usuario este indefenso por no tener conocimiento y el interés en aprender de seguridad informática.

2.3.3 Tipo de transacciones

2.3.3.1 Teclados virtuales

Ilustración 1 Tipo de transacciones. Teclados virtuales

Los ataques con los keyloggers, es un programa que permite espiar en su equipo cada palabra escrita en el teclado, desde sus contraseñas del correo, textos confidenciales hasta números de tarjeta de crédito a través de virus, troyanos o cualquier ejecutable disfrazado que se pueda ocurrir.

Los atacantes utilizan el software para registrar las pulsaciones, en el teclado y así memorizarlas en un fichero y enviarlas a través de internet en lugar de usar su propio teclado.

2.3.3.2 Tarjetas de coordenadas

	A	B	C	D	E	F	G	H
1	212	635	253	432	198	236	149	325
2	113	228	339	446	555	662	774	888
3	212	635	253	432	198	236	149	325
4	953	565	113	228	339	446	555	662
5	212	635	253	432	198	236	149	325
6	953	565	113	228	339	446	555	662
7	212	635	253	432	198	236	149	325
8	953	565	113	228	339	446	555	662
9	212	635	253	432	198	236	149	325
10	953	565	113	228	339	446	555	662

Ilustración 2 Tipo de Transacciones: Tarjetas de coordenadas

Es una tabla alfanumérica que se le entrega al usuario en la oficina, siendo el titular de la cuenta el único poseedor de la tarjeta.

Con un poco de paciencia si el usuario va haciendo transacciones, al final tendremos suficientes valores para poder saltarnos el mecanismo, donde un troyano puede simplemente pedir todas las coordenadas.

En el caso del phishing eBankinter es una técnica para burlar las tarjetas de claves, para así robar información al introducir el usuario y contraseña, mediante la presentación de un formulario, donde pedirá que introduzca los

números de la tarjeta, además para mayor facilidad para el usuario envían un número de fax, donde enviarán la copia de la tarjeta de coordenadas.

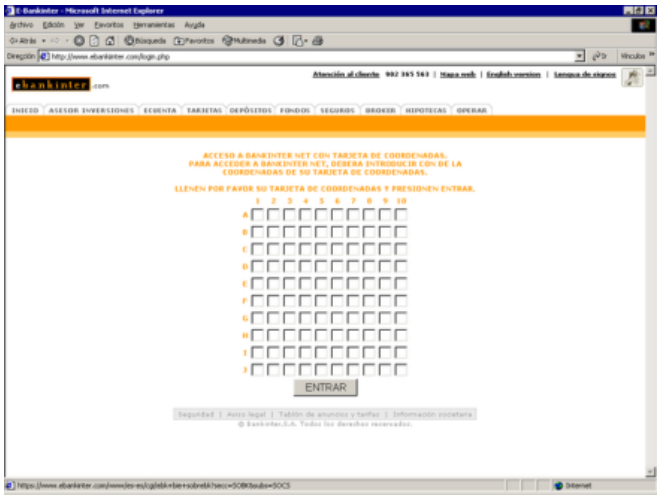

Ilustración 3 e-banking para robar información

2.3.3.3 Avisos por SMS

Ilustración 4 Tipo de Transacciones. Aviso por mensaje

En las instituciones bancarias se encargan de enviar un aviso por SMS, cada vez que se produce una transferencia de alta cantidad.

2.4 La criptografía

Es para garantizar la seguridad de la información hacia su destino, mediante el método de cifrado de texto, usada para enviar mensajes con información confidencial y sensible a través de medios no seguros.

2.5 Cifrado.

Es el tratamiento de un conjunto de datos o contenidos en un paquete, con el fin de impedir que ningún usuario no autorizado pueda dañar el archivo, sino el destinatario sea el único que pueda leerlo, siendo una base de seguridad que debe ser utilizada en la red.

2.5.1 Tipos de Cifrado de datos

- **Simétrico:** cuando utiliza la misma clave para cifrar y descifrar.
- **Asimétrico:** Usa claves diferentes privada y pública.

Clave Privada: Son aquellas que se usan tanto para el cifrado y descifrado de las clave secretas.

El punto fundamental de esta descomposición pública y privada es la imposibilidad práctica de deducir la clave privada a partir de la clave pública.

Clave pública: Es una mezcla de hardware y software, políticas y procedimientos de seguridad, que permiten la ejecución de operaciones criptográficas como el cifrado, permitiendo aumentar la seguridad de un mensaje, mediante la codificación del contenido para que usuarios maliciosos no puedan leer.

2.6 Métodos para la criptografía asimétrica RSA (Algoritmo de encriptación de clave pública)

Se basa en algoritmos matemáticos donde el encriptado y la autenticación se producen sin compartir ninguna clave secreta.

Cualquier persona puede enviar un mensaje encriptado o verificar un documento firmado por otra persona con las claves públicas, solamente el que posee la clave privada correcta puede desencriptar o firmar el mensaje y

con la seguridad del sistema RSA, que se basa en factorear números primos fuertes.

RSA: Es para realizar funciones administrativas en el gestor de bases de autenticación, mediante la incorporación de la administración llamada API en los servicios públicos, mientras que las tareas se puede lograr con el administrador de autenticación para la interfaz.

API: Interfaz de programación de aplicaciones

Representa la capacidad de comunicación entre componentes de software, el cual se encarga de llamar a ciertas bibliotecas que ofrecen acceso a servicios desde los procesos y representa un método para conseguir reducción en la programación, como dibujar ventanas, iconos en la pantalla así evitándose el trabajo de programar todo desde el principio.

2.7 Firma Digital

Es un medio que permite determinar con seguridad y confianza identificar al propietario de la firma y comprobar que los datos no hayan sido falsificados.

Ilustración 5 Firma Digital

Los requisitos para la validez jurídica de la firma digital son:

- Está unida de forma seguro a su firmante.
- La creación asegura que el firmante puede mantenerla sólo bajo su control.
- Está vinculada a los datos, si existe alteración en los mismos sería revelada.

2.8 Cryptomathic Signer

Es un servidor central que almacena las claves privadas de los clientes, de forma centralizada donde la seguridad física no reside en el usuario individual, sino está almacenada en una PC, ni siquiera el proveedor de servicios firmante puede acceder a la clave.

En la administración central de Key, se encarga de simplificar el complejo de tareas como la renovación de la clave y aplicación de políticas, donde todas las teclas son de hardware protegidos y las llaves son gestionados de forma encriptada en la base de datos.

La movilidad de servidor Signer se puede acceder mediante el Internet y no

requiere instalación de software en el cliente secundario.

2.8.1 Productos de Cryptomathic:

- ***EMV*:** Es un estándar de tarjetas con microprocesador para la autentificación de pagos mediante tarjetas de crédito y débito.
- ***Autenticacion Fuerte***: se encarga de verificar datos sin la transmisión de una contraseña.
- ***Firmante****:* es un servidor central de la firma con posibles tarjetas inteligentes.
- ***El HSM Portal****:* es un servicio que permite agrupar módulos de seguridad a través de aplicaciones como mantenimiento, soporte de sitios.

Los servicios que brinda a los clientes actuales y futuros incluyen los procesadores de tarjetas, sistemas de pago y proveedores de tecnología, ofreciendo un medio de seguridad para la banca electrónica.

La herramienta de Solución Firmante actúa cuando un cliente solicita una firma a través de Internet y están encargados de firmar transacciones electrónicas, que están legalmente seguras desde cualquier parte del mundo, ayudando a centralizar el almacenamiento y gestión de claves privadas, brindando seguridad con el fin de mantener un centro de datos.

2.9 Las Actividades de Cryptomathic Firmante.

La Solución Signer es servidor central, que sigue desarrollando innovadoras soluciones en cuanto a la firma digital.

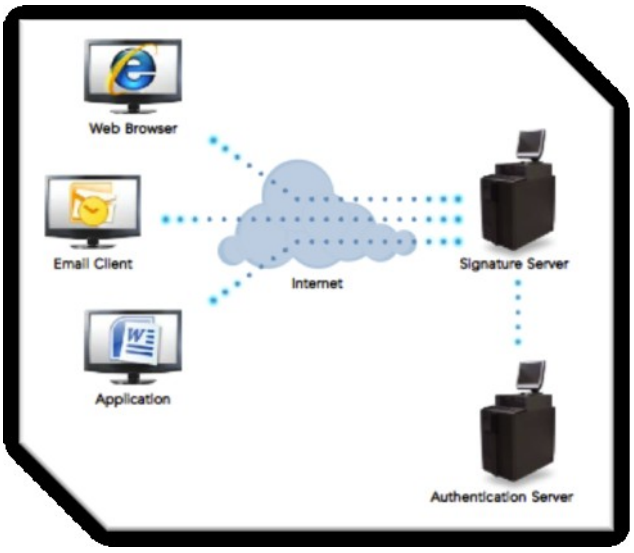

Ilustración 6 Actividades de Cryptomathic Singer

2.9.1 Web Browser:

Son programas clientes usados para navegar por la WWW, donde visualiza la información obtenida de los servidores, para que el navegador que proviene del visualizador Netscape Navigator, sea el encargado de incorporar un gestor de descargas, para incorporar nuevas mejoras en el gestor e-mail, avisando de los correos entrantes, para filtrarlos y así habilitar un gestor de mensajes instantáneos, siendo este compatible con Mozilla Firefox.

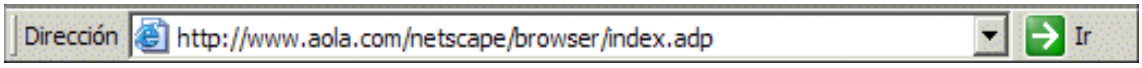

Ilustración 7 Web Browser

2.9.2 Cliente de correo electrónico:

Se encarga de enviar y recibir correo electrónico, donde precisa de un programa de gestión, en el que se redacta el contenido y se indican las direcciones del destinado, posteriormente el mensaje de correo electrónico

se envía a un servidor, que identifica al destinatario y lo remite al propio servidor de correo, quien se encargada de almacenarlo hasta que el propio destinatario se conecte con él y lo descargue en su terminal, donde los más comunes el SMTP (Simple Protocolo de Transferencia de Correo), se encarga de recibir y enviar el correo de la misma manera que recibe.

El POP3 (Protocolo 3 de Correo) es un protocolo estándar para recibir mensajes de mail, quienes son enviados a un servidor y almacenados.

El IMAP (Protocolo Interactivo de acceso a correo), permite al usuario interactuar con el Host para receptar los correos electrónicos y decidir que mensajes y archivos desea observar, es muy similar a los sistemas de correos Hotmail y Yahoo-Mail.

2.9.3 Documento de Aplicación:

Al codificar un sitio web en algún programa y subir luego al servidor web, donde se encargará de traducir a formato html, para que se traduzca al lenguaje que los servidores traducen la salida.

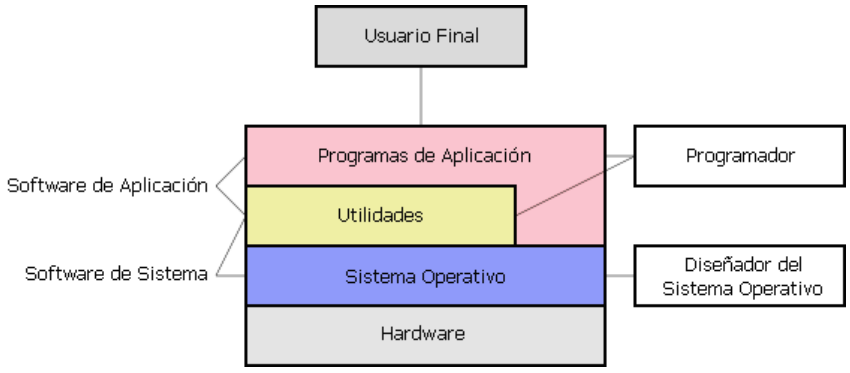

Ilustración 8 Documento de funcionamiento de Aplicación

2.9.4 Internet:

Cada ordenador de la red puede conectarse a cualquier otro ordenador, permitiendo el intercambio de la información.

2.9.5 Firma del servidor:

Es una entidad responsable de emitir y revocar los certificados digitales, donde se emplea criptografía de clave pública.

El Certificado Digital es utilizado para empresas que comercializan por Internet, siendo un sistema de seguridad ideado para acceder a un servidor que brinda confiabilidad de la información, mediante técnicas de encriptación.

Protocolo SSL (protocolo de capa de conexión segura) proporciona autenticación y privacidad de los datos en el internet mediante la Criptografía.

- **Confiabilidad:** Mediante el uso de encriptación garantiza que los datos enviados y recibidos, no se puedan modificar por otra persona que no sea el emisor o el receptor.
- **Integridad**: Los datos recibidos sean iguales a los datos enviados, permite que el receptor no modifique la información que recibe.
- **Autenticación:** Utiliza un certificado digital emitido por una empresa llamada Autoridad Certificadora de confianza, este documento es totalmente infalsificable que garantiza a la empresa que presta los servicios sea los mismos.

2.9.6 La autenticación del servidor:

La mayoría de los servidores web permiten verificar las credenciales, donde ayudará a autenticar y autorizar el acceso de usuarios mediante el servidor.

2.10 Formato soportados de la firma

- **PKCS # 1:** Versión 2.1, Es un estándar criptográfico RSA, sistema criptográfico de clave pública, este algoritmo permite cifrar para firmar digitalmente.
- **PKCS # 7:** Versión 1.5, Es un estándar sobre la sintaxis del mensaje criptográfico, que es usado para firmar o cifrar mensajes en PKI.
- **ISO 9796-1:** Es una norma que utiliza la función de redundancia para resistir a los ataques, que aprovechan de la propiedad multiplicativa del criptosistema RSA.

2.10.1 Métodos de autenticación compatibles

- **HOTP**: (Un tiempo Contraseñas Algoritmo) utilizado para autenticar a un usuario en un sistema a través de un servidor de autenticación.
- **TOTP**: Es utilizada para autenticar a un usuario a través de un servidor de autenticación.

2.10.2 Integración con la Autoridad de Certificación (X509v3 base)

Norma PKCS # 10: versión 1.7, es un estándar de solicitud de certificación, el formato de los mensajes enviados a una Certificadora Autorizada para solicitar la certificación de una clave pública.

2.10.3 Integración con el proveedor de aplicaciones Web.

Java basado SDK (kit de desarrollo de software) es un conjunto de herramientas de desarrollo que permite a un programador crear aplicaciones para un sistema concreto, con la integración brinda la autenticación y la firma de los propósitos del usuario.

API es el conjunto de funciones y métodos en la programación orientada a objetos, para ser utilizado por otro software como una capa de abstracción.

2.10.4 Integración con estaciones de trabajo cliente

- **Microsoft CryptoAPI:**se utiliza para firmar digitalmente los archivos, para confirmar las firmas en los archivos y crear archivos de catálogo, se integra como proveedor de servicios criptográficos para el diseño de software para sistemas fiables y seguridad delicado.
- **API:** Trabaja con certificados digitales, servicios de certificados, y el control de inscripción de certificados.

2.11 Entorno operativo

2.11.1 Windows XP

Dispone de versiones para varios entornos informáticos, para computadoras domésticos, negocios y portátiles.

A diferencia de versiones anteriores de Windows, al estar basado en la arquitectura de Windows NT, proveniente del código de Windows 2000, por mejoras en estabilidad y rendimiento.

Tiene una Interfaz gráfica de usuario, la primera versión de Windows que utiliza la activación del producto, para reducir la piratería del software.

2.11.2 Base de datos

- **Oracle 8:** Soporta aplicaciones de procesamiento de transacciones en línea y data warehousing, almacenado en una base de datos diseñada para favorecer el análisis y la divulgación eficiente de datos.
- **Microsoft SQL Server 7**: Tiene una gran escalabilidad, integración, rendimiento, inteligencia de negocios y fiabilidad.

2.11.3 Los módulos de hardware de seguridad.

- **IBM**: Licencias en uso por todos los módulos disponibles y Mantenimiento del Software.
- **nCipher:** Son módulos de Conexión a Hardware que brinda seguridad siendo dispositivo criptográfico que genera, almacena y protege las claves mediante las operaciones criptográficas y gestión de claves.

2.11.4 Protección mejorada de claves.

Las claves privadas se generan y nunca deja el entorno del servidor de alta seguridad.

Las normas europeas utilizadas:

- **TS 101 733:** para firmar datos o recursos de cualquier tipo, como documentos XML, pero cualquier cosa que sea accesible a través de una URL, puede firmarse especificada.
- **W3C**: (Consorcio Word Wide Web), se encarga de guiar la Web hacia su máximo potencial a través del desarrollo de protocolos que aseguren el crecimiento de la Web.

2.11.5 Establecen dos modalidades de firma que incluyen sellado de tiempo:

- La variante firma electrónica con sello de tiempo: añade el sellado de tiempo a una firma básica avalado por una fecha y hora de la autoridad, con el fin de situar el tiempo en que se firma un documentoy el formato de firma con la información completa.
- La variantefirma electrónica con validación de datos completa: la firma añade un conjunto de referencias a los certificados de la cadena de certificación y estado.

a) CRL (Lista de certificados revocados)

Es una lista con firma digital emitida por una Certificadora Autorizada que contiene los certificados que han sido revocada, incluye el número de serie del certificado, fecha que fue revocada y razón para la revocación.

Hay dos variantes de CRL:

- **Base / CRL completa:** contiene una lista de certificados revocados y publicados de forma automática, en intervalos definidos por el administrador de la Certificadora Autorizada.
- **Delta CRL**: contiene una lista de certificados revocados desde la última base.

b) OCSP (línea Certificado Status Protocolo) funciona con una configuración de respuesta y Repetidor.

Una organización utiliza el servidor como punto de contacto para la revocación de un certificado, permitiendo que las aplicaciones cliente obtenga una información oportuna, sobre el estado de revocación de un certificado, las dos normas CRL y OCSP son modalidades de firma avanzada y reconocida.

Además estas normas prevén formato de firma para la modalidad.

2.12 Ley 59/2003 sobre la firma electrónica, Artículo 8

"Son causas de extinción de la vigencia de un certificado electrónico:

a) Expiración del período de validez que figura en el certificado.

b) Revocación formulada por el firmante, la persona física o jurídica representada por éste, un tercero autorizado o la persona física solicitante de un certificado electrónico de persona jurídica.

c) Violación o puesta en peligro del secreto de los datos de creación de firma del firmante o del prestador de servicios de certificación o utilización indebida de dichos datos por un tercero.

d) Resolución judicial o administrativa que lo ordene.

e) Fallecimiento o extinción de la personalidad jurídica del firmante; fallecimiento, o extinción de la personalidad jurídica del representado; incapacidad sobrevenida, total o parcial, del firmante o de su representado; terminación de la representación; disolución de la persona jurídica representada o alteración de las condiciones de custodia o uso de los datos de creación de firma que estén reflejadas en los certificados expedidos a una persona jurídica.

f) Cese en la actividad del prestador de servicios de certificación salvo que, previo consentimiento expreso del firmante, la gestión de los certificados electrónicos expedidos por aquél sean transferidos a otro prestador de servicios de certificación.

g) Alteración de los datos aportados para la obtención del certificado o modificación de las circunstancias verificadas para la expedición del certificado, como las relativas al cargo o a las facultades de representación, de manera que éste ya no fuera conforme a la realidad.

1. El período de validez de los certificados electrónicos será adecuado a las características y tecnología empleada para generar los datos de creación de firma.

En el caso de los certificados reconocidos este período no podrá ser superior a cuatro años.

2. La extinción de la vigencia de un certificado electrónico surtirá efectos frente a terceros, en los supuestos de expiración de su período de validez, desde que se produzca esta circunstancia y, en los demás casos, desde que la indicación de dicha extinción se incluya en el servicio de consulta sobre la vigencia de los certificados del prestador de servicios de certificación" (R, 2003)

ANÁLISIS DE FORTALEZAS Y DEBILIDADES DE CRYPTOMATHIC SIGNER, FRENTE A LA FIRMA DE SEGURIDAD PARA SERVICIOS WEB Y BANCA ONLINE, EN LA "COOPERATIVA JEP DE CUENCA."

Análisis de como contrarrestar los Delitos Informáticos en transacciones en línea.

2.13 Keylogger.

- Se debe tener instalado un buen firewall, como el zone-alarm, que se encarga de avisar si algún programa quiere acceder a internet.
- El otro método es cambiar de ventana varias veces mientras introducimos la contraseña de cada letra, de ese modo el keylogger capturará todas las teclas seguidas y hará que la contraseña pierda significado.
- En ciertos bancos no ofrecen este tipo de teclados virtuales, aunque existe una alternativa si estamos utilizando el sistema operativo Windows XP, los pasos es ir a inicio, todos los programas, Accesorios, Accesibilidad y teclado en pantalla, de esta manera no usaremos el teclado evitando ser victima.

2.14 Robo de tarjetas coordenadas

Toda entidad bancaria debería mandar por carta y por correo electrónico, una copia de las diferentes páginas o pantallas que aparecen en cualquier proceso de operación bancaria y con la indicación de la transacción bancaria falsa y que el usuario nunca deberá contestar a dicha petición.

Otra medida de prevención sería que los proveedores de correo electrónico, al igual que implantan antivirus en los servidores, implanten filtros anti-phishing etiquetando los correos, de la misma forma como trabajan los SPAM, enviando correo basura o mensajes no deseados.

2.15 Aviso por SMS

En el celular se puede personalizar, para que sólo reciba los SMS cuando le envían email desde direcciones indicadas por el usuario, evitando así recibir SMS por cada email que reciba.

2.16 La Cooperativa de Ahorro y Crédito “La Merced” Ltda.

Es una Cooperativa de Ahorro y Crédito confiable, segura y solvente con 47 años en el Austro Ecuatoriano, quienes se encargan del desarrollo social y económico de la comunidad.

Misión

“Es una cooperativa de ahorro y crédito sólida, confiable, solvente y segura que logra la fidelidad de los socios a través de la entrega de productos y servicios financieros de calidad, siempre a la vanguardia del avance tecnológico, social, cultural y económico, contribuyendo al bienestar de la comunidad y desarrollo del país.”, (La MERCED, 23)

Visión

Busca ser una cooperativa de ahorro y crédito con una diversidad de productos y servicios que contribuirán al bienestar de las personas emprendedoras, asegurando transparencia, eficiencia, buen servicio y rentabilidad a todos los socios.

Servicios que brinda la Cooperativa:

- Cuenta de ahorro "gana ahorro"
- Depósito Inicial de $20.
- Depósito a plazo fijo.
- Las mejores tasas de interés.

- El cliente elige el plazo.
- Monto de inversión desde $500 dólares.

2.17 La Cooperativa de Ahorro y Crédito "Juventud Ecuatoriana Progresista" Ltda.

Es una entidad dedicada a las finanzas sociales, como un aporte a la lucha contra la pobreza y al mejoramiento de la competitividad, con el apoyo individual y comunitario de la gente

Misión

La cooperativa brinda servicios financieros de calidad, basados en una organizacional de excelencia y valores sólidos para satisfacer las necesidades de la gente y así tener socios satisfechos.

Visión

Es liderar las finanzas sociales en el país, como un aporte a la lucha contra la pobreza y al mejoramiento de la competitividad, mediante el apoyo al desarrollo del potencial productivo individual y comunitario de la gente.

Beneficios de la Cooperativa JEP.

- Disponibilidad inmediata del dinero.
- Transacciones en línea, desde cualquier parte del mundo.
- Costos accesibles.
- Elimina el riesgo del uso de efectivo.
- Seguridad y confidencialidad de tus transacciones.
- Cero costos al momento de la contratación del servicio y de transacciones internas.

2.18 Cuadro Comparativo entre cooperativas de Cuenca

Cooperativa de Ahorro y Crédito "La Merced" Ltda.	Cooperativa de Ahorro y Crédito "Juventud Ecuatoriana Progresista" Ltda.
VENTAJAS	
✓ Seguridad ✓ Solvencia. ✓ Rentabilidad a su dinero. ✓ Los créditos son ágiles, fáciles y oportunos. ▪ Créditos Comerciales ▪ Créditos de Consumo ▪ Créditos para la Vivienda. ▪ Micro créditos	➢ No existe costos de mantenimiento de libreta. ➢ Dispone de ayuda por mortuoria por un monto de $500 dólares, con saldo de $30 dólares en la cuenta. ➢ Pago de servicios básicos, a través de débitos automáticos. ➢ Créditos en 24 horas y tasas de intereses bajos. ➢ Microcrédito Minorista =< 3000; Tasa Nominal 20,00%. ➢ Microcrédito de Acumulación Simple > 3.000 USD y < = 10.000 USD: Tasa Nominal 19,50%. ➢ Microcrédito de Acumulación Ampliada >10.000 USD y < = 20.000 USD: Tasa Nominal 16,00%. ➢ Transferencia de dinero a nivel nacional e internacional.
DESVENTAJAS	
o Necesita garantes para realizar algún préstamo. o No estan sólida como los bancos.	

Ilustración 9 Cuadro Comparativo entre la Cooperativa "MERCED y JEP"

Al realizar un análisis entre la cooperativa JEP y la Cooperativa de Ahorro y Crédito “La Merced” Ltda, se considera que La Cooperativa Jep, es una de las instituciones en crecimiento por los servicios web que presta, por lo que esta expuesto a ser victima a delitos informáticos, debido a las transacciones bancarias en línea que realizan los clientes, siendo una empresa en crecimiento y la trayectoria en el mercado nacional, donde se toma la medida de analizar la funcionalidad mediante el caso de uso.

2.19 Caso de uso de cooperativa JEP.

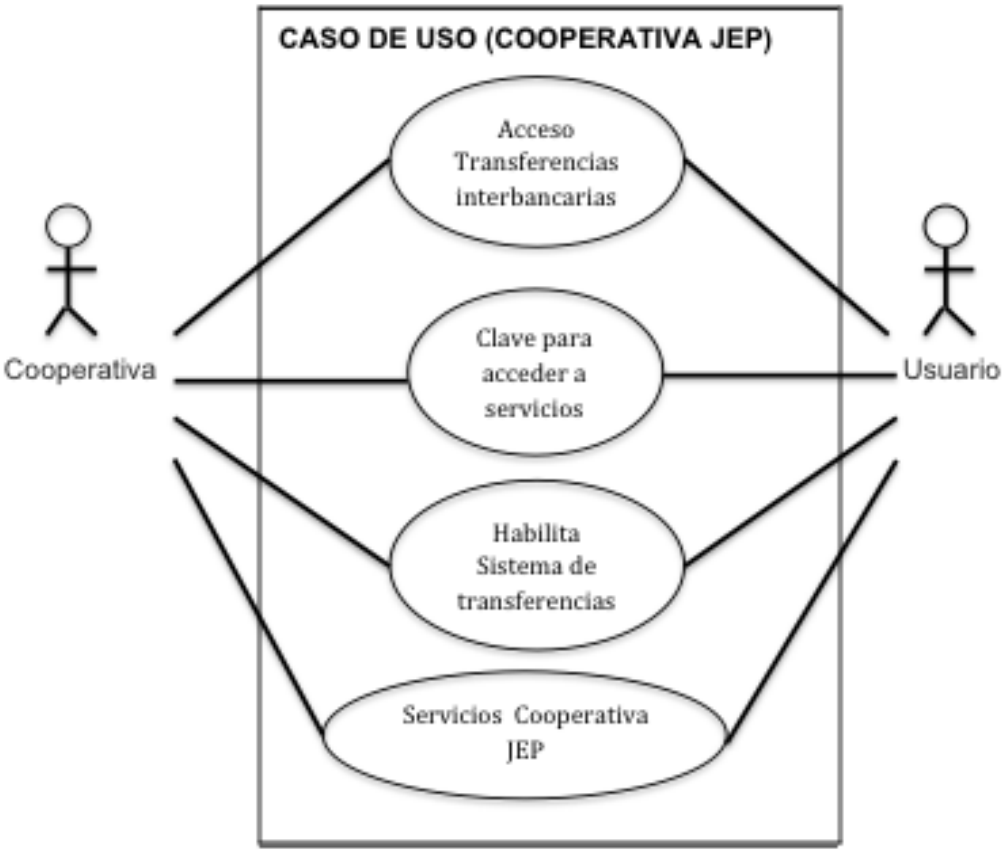

Ilustración 10 Caso de Uso para Cooperativa JEP

Caso de uso general:	Cooperativa JEP
Actores:	Cooperativa, Usuario.
Descripción:	La cooperativa se encargara de asignar un nuevo usuario para el acceso a las transferencias interbancarias en la web.
1. La Cooperativa Jep, le concede el acceso a los servicios de transferencias interbancarias mediante el Internet. 2. El usuario sera encargado de poner su clave para acceder a servicios de la cooperativa. 3. La Cooperativa habilitará el servicios del sistema de transferencias, y el usuario es el encargado de digitarlo para servicios deseado. 4. El usuario ingresa a los servicios en linea de la cooperativa JEP, para realizar consultas, transferencias entre otros servicios.	

Tabla 2 Funcionamiento de Cooperativa Jep

En la actualidad, la situación económica de nuestro país y frente a la inestabilidad y crisis que ha vivido el sistema bancario nacional, el cliente ha demostrado su total desconfianza especialmente con los bancos, es necesario buscar alternativas para demostrarle al cliente que existen opciones que le permite fomentar el ahorro y brindar créditos.

Los usuarios deben tener en secreto y no divulgar las contraseñas, porque la cooperativa no asume ninguna responsabilidad de cualquier daño o perjuicio, directo o indirecto, ocasionados por virus que infecten el sistema o el equipo informático del Usuario, es necesario poner una solución de seguridad de información.

2.20 Cryptomathic Signer

Es un software de seguridad para servicios web enfocada a la banca electrónica, donde los usuarios son capaces de firmar las transacciones electrónicas legalmente coordinadas de forma segura, desde cualquier lugar del mundo mediante el internet.

Características

- Fácil integración.
- Protección de claves seguras.
- Mejora de la seguridad.
- Gestión simplificada clave.
- Autenticación fuerte.
- Usuario y la autenticación de mensajes.
- No repudio.
- Movilidad para el usuario

2.21 COSIGN

Permite ayudar a reducir costes y agilizar los procesos de negocio automatizando sus aprobaciones formales de forma factible, donde añade la firma gráfica del firmante donde se coloca en el documento así como la justificación de la firma, donde esto asegura la aceptación intuitiva por sus socios externos que son los clientes.

Además, las firmas digitales son esenciales para las organizaciones en las industrias reguladas con los procesos de aprobación formal, así como las empresas que necesitan enviar documentos que requieren las autorizaciones de las oficinas múltiples o clientes y socios, debido a su perfecta integración con el flujo de trabajo y soluciones líderes de gestión de contenidos, permite

que los procesos automatizados de la aprobación formal de los sistemas de la organización del flujo de trabajo existente.

Características

- Utiliza contraseñas donde se envían al servicio web login centrales, para controlar el acceso individual a un sistema a través de SSL, donde se proporciona la autenticación y privacidad de la información por internet mediante el uso de criptografía.
- Los usuarios sólo necesitan autenticarse una vez por sesión para acceder a cualquier sitio protegido.
- Autenticación de múltiples factores.
- Sistemas de confianza pueden solicitar las credenciales de Kerberos desde un servidor central para la Nivel de autenticación (IMAP, LDAP, Oracle, etc.)
- Los usuarios pueden desconectarse de todos los servicios cosign protegidos por visitar una URL única.

2.22 Cuadro comparación de servidores centrales.

CRYPTOMATHIC SIGNER	COSIGN
VENTAJAS	
✓ Comodidad y movilidad mediante la conexión a Internet. ✓ Seguridad con el protocolo SSL, para el almacenamiento de claves. ✓ Rentabilidad ofrece servicios de autenticación y firma utilizable en entornos B2C. ✓ Los eventos están registrados en la base de datos. ✓ Base de datos protegidos con las claves privadas de los usuarios. ✓ Control de acceso para operadores mediante una autenticación segura.	➢ Firma digitalmente cualquier tipo de documento. ➢ Funciona con todos los formatos de archivo estándares: Microsoft Word, Excel, Outlook, Adobe PDF, AutoCAD. ➢ Podrá convertir cualquier documento en un PDF firmado y sellado. ➢ Puede añadir su firma gráfica y la justificación de su firma, se coloca en el documento junto con la razón para la firma. ➢ Se garantiza la permanencia del documento. ➢ Firma con la frecuencia que necesite, tiene la capacidad ilimitada de 500 documentos al año.

Tabla 3 Cuadro Comparación de Servidores Centrales

DESVENTAJAS	
○ Aún no se ha acreditado como un dispositivo seguro de creación de firma. ○ La solucion es orientada solo a Microsoft Windows .	○ La seguridad física y la clave reside en el usuario individual, porque está almacenada en un PC. ○ La congestión del tráfico ha sido siempre un problema en el

Tabla 4 Desventaja de Servidores Centrales

Para el presente informe se ha analizado varias características, que deben ser consideradas para la seguridad en las transacciones bancarias en línea, donde existen varios delitos informáticos en la web.

2.22.1 Cuadro comparativo para la seguridad de los datos.

Características	Cryptomathic Signer	Cosign Central
Integración del flujo de trabajo	✓	✓
Aplicaciones web	✓	✓
Mayor validez legal	✓	–
Mejor acreditación externa	✓	–
Protección de claves seguras	✓	✓
Seguridad Mejorada	✓	✓
Gestión simplificada clave	✓	–
Movilidad para el usuario	✓	✓
No repudio, servicio de seguridad (OSI ISO-7498-2) previene que un emisor niegue haber remitido un mensaje y que un receptor niegue su recepción.	✓	–

Tabla 5 Cuadro Comparativo

Características de Servidores Centrales

El análisis de Cryptomathic es una solución para sistemas bancarios en línea, que permite tener una integración en el grupo de trabajo, siendo uno de la

solución que tiene un peso grande en la validez legal, por la gran acogida en la acreditación externa en el mercado, y por los métodos de protección en las claves para el envió y recepción de la información y por la movilidad que se puede hacer a comparación con las soluciones tradicionales de almacenamiento de claves, Cryptomathic firmante ofrece una mayor protección de clave, mayor seguridad y una mejor gestión de claves central.

2.22.2 Perfil de la Empresa

Cryptomathic es una empresa de propiedad privada, que ha registrado un crecimiento de 74% y 86% para 2001 y 2002.

Es uno de los primeros en el mundo para la comercialización de algoritmos criptográficos, siendo unos de los principales mundiales de soluciones de seguridad.

2.22.3 Estrategia de cryptomathic firmante

Cryptomathic pretende enviar una nueva versión del producto cada 12 meses, para agregar soporte para nuevos dispositivos de autenticación y esquemas.

Los mercados de destino siguen siendo banca en línea, el Gobierno y gestión de identidades da acceso dentro de las grandes organizaciones.

Cryptomathic continúa ampliando sus asociaciones con proveedores que ofrecen productos y servicios complementarios: nCipher e IBM en el mercado de cripto procesador, y Vasco y Xiring en el mercado de autenticación.

La clave del éxito en este mercado será la visibilidad, de las series de empresas con perfiles altas en esta área y para Cryptomathic para tener éxito,

tiene que asociarse con algunos de los principales empresas de outsourcing más probable y los integradores de sistemas.

2.23 Comparación entre Clave Pública y Privada

Clave Pública	Clave Privada
Se puede darle la clave a cualquiera que quiera recibir mensajes cifrados o puede ponerla en un servidor de claves públicas, para que pueda mirar allí antes de escribirle.	Permite descifrar cualquier mensaje cifrado con su clave pública, nunca se da a nadie su clave privada.

Tabla 6 Cuadro Comparativo entre Clave Pública y Privada

Se ha realizado un análisis que la autenticación fuerte garantiza que la clave privada permanece bajo el control exclusivo del usuario, donde se utilizará desde cualquier dispositivo conectado.

2.24 Tiempo de Sellado de la Autoridad Cryptomathic

Es una marca de tiempo único e infalsificable pueden ser asignados a cualquier pedazo de datos digitales.

Existe una aplicación importante la firma digital de fecha y hora, se encarga de fijar el contenido de una transacción que lo vincula únicamente a la persona que firma.

2.24.1 Empleo del Sellado de tiempo en la firma electrónica

La variante ES-T: añade el sellado a una firma básica y la variante ES-C añade además del sellado de tiempo, información sobre la ruta en la que se puede verificar la validez del certificado obtenido de una consulta, que permite

proporcionar una información del estado de revocación de un certificado o CRL, donde indica la lista de números de serie de los certificados digitales revocados por una Autoridad Certificadora.

Además estas normas prevén la modalidad ES-XL, incluye información sobre el estado de revocación del certificado.

Cuando una Certificadora Autorizada emite un certificado digital, lo hace con un periodo máximo de validez que oscila entre dos y cuatro años máximo, la fecha de caducidad viene indicada en el propio certificado digital.

2.25 CASO DE USO DE TRANSACCIONES BANCARIAS EN LÍNEA

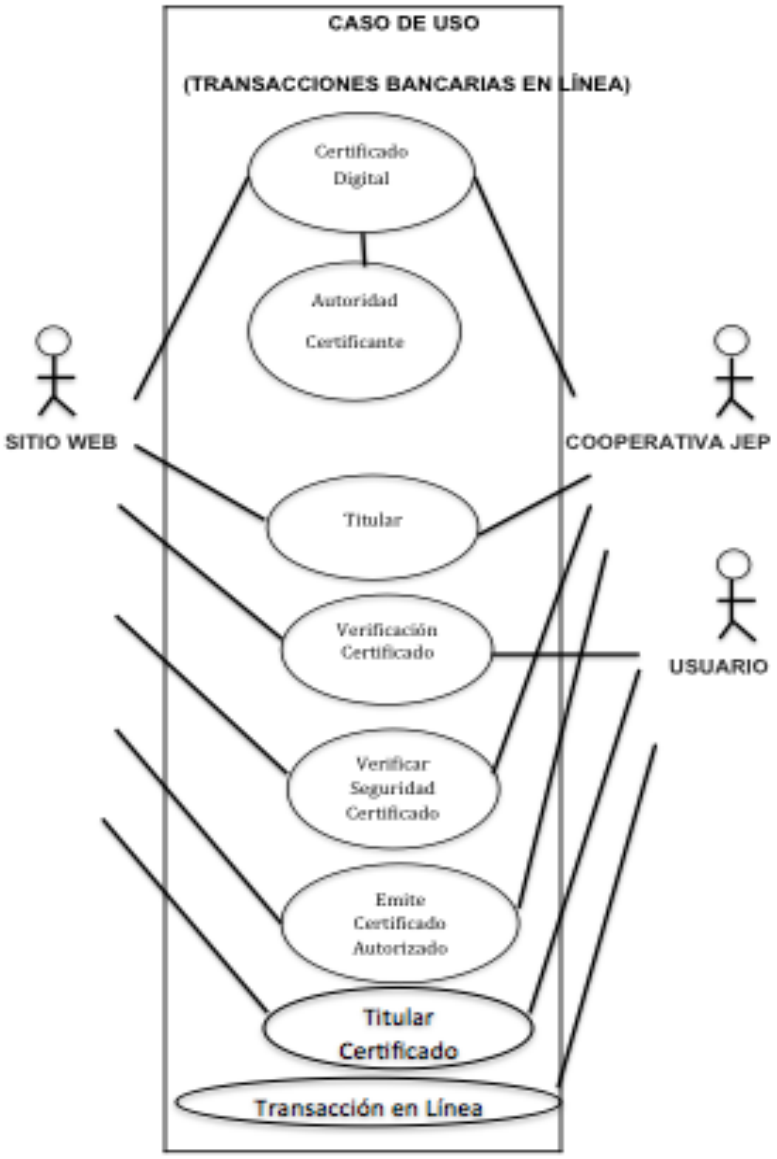

Ilustración 11 Caso de USO de transacciones bancarias en línea

Caso de uso general:	Transacción Bancaria en línea.
Actores:	Cooperativa, Usuario, Sitio Web.
Descripción:	El sitio web emite un certificado Digital, para afirmar que la Cooperativa es la quien dice ser, para dar crédito al usuario al momento de realizar las transacciones en línea.

1. El sitio Web posee un certificado digital válido.

   1.1 El certificado Digital se emite por una empresa de confianza como la Autoridad Certificante.
2. La Cooperativa Jep se registra para permitir la identificación del titular del sitio web.
3. El usuario verifica que el sitio web sea la correcta mediante un símbolo de un candado que estará en la parte inferior del navegador, permitiendo al usuario determinar que se encuentra conectado con un sitio web autenticado y que la comunicación se efectuará de manera encriptada.
4. El sitio Web solicita la verificación de la seguridad del Certificado a la Cooperaativa Jep.
5. La cooperativa emite el certificado Autorizado, asegurando que es seguro ingresar
6. El sitio Web indica que una página web segura, al usuario.
7. El usuario realiza la transaccion en línea de manera segura.

Tabla 7 Detalle de Caso de Uso Transacciones Bancaria en línea

El análisis se enfoca a la transacción en línea de la Cooperativa JEP, donde se verifica la importancia de la Certificadora Autorizada, Registro Autorizado y firmante en la transferencia de información.

2.26 ANÁLISIS DE LA FUNCIONALIDAD DE LA HERRAMIENTA CRYPTOMATHIC SIGNER

Cryptomathic Signer es una solución centrada en servidor para la creación, gestión y uso de claves privadas dentro de una Infraestructura de Clave Pública.

El almacenamiento de las claves del usuario es mediante una firma en un servidor central seguro, para reducir el riesgo de seguridad del uso de la clave en cualquier navegador Web.

Las grandes organizaciones, bancos y departamentos gubernamentales que se benefician, donde el no repudio juega un papel importante en el gobierno corporativo y cumplimiento.

2.26.1 Análisis de Funcionalidad de Firmante.

Es evidente que uno de los retos empresariales más importantes hoy en día es la preservación de la confidencialidad, integridad y disponibilidad.

La confidencialidad garantiza que la información sea accesible sólo para aquellos que han autorizado el acceso, mientras que la integridad salvaguardará la exactitud de la información, asegurando que los usuarios autorizados tengan acceso a la información cuando y donde sea necesario mediante la disponibilidad.

La Infraestructura de la Clave Pública (PKI) se puede confiar en el mundo del Internet.

Para abordar el tema de seguridad en los negocios, las organizaciones empiezan a considerar al cifrado de clave pública para firmas digitales, sin embargo al almacenar las claves del usuario y la firma en el ordenador PC o en una tarjeta inteligente no es una opción factible.

La vulnerabilidad de los ordenadores de PC y la complejidad de los costos con soluciones basadas en hardware, las organizaciones están buscando soluciones alternativas para la gestión de las claves privadas de los usuarios.

La solución de servidor Central Cryptomathic firmante, pasa de papel a una Clave Pública quien se encargada de generar y almacenar la clave de usuario en firma para un entorno de alta seguridad.

2.26.2 Operación de cryptomathic firmante

La solución de Firmante se enfoca a desempeñar un papel importante en una PKI, siendo un sistema de gestión de claves, que ayuda a generar y almacenar claves de usuario y las firmas digitales para cuando sea necesario, donde se realizará un análisis de la operación de la solución del servidor central.

2.26.3 Caso de uso operación de Cryptomathic Signer.

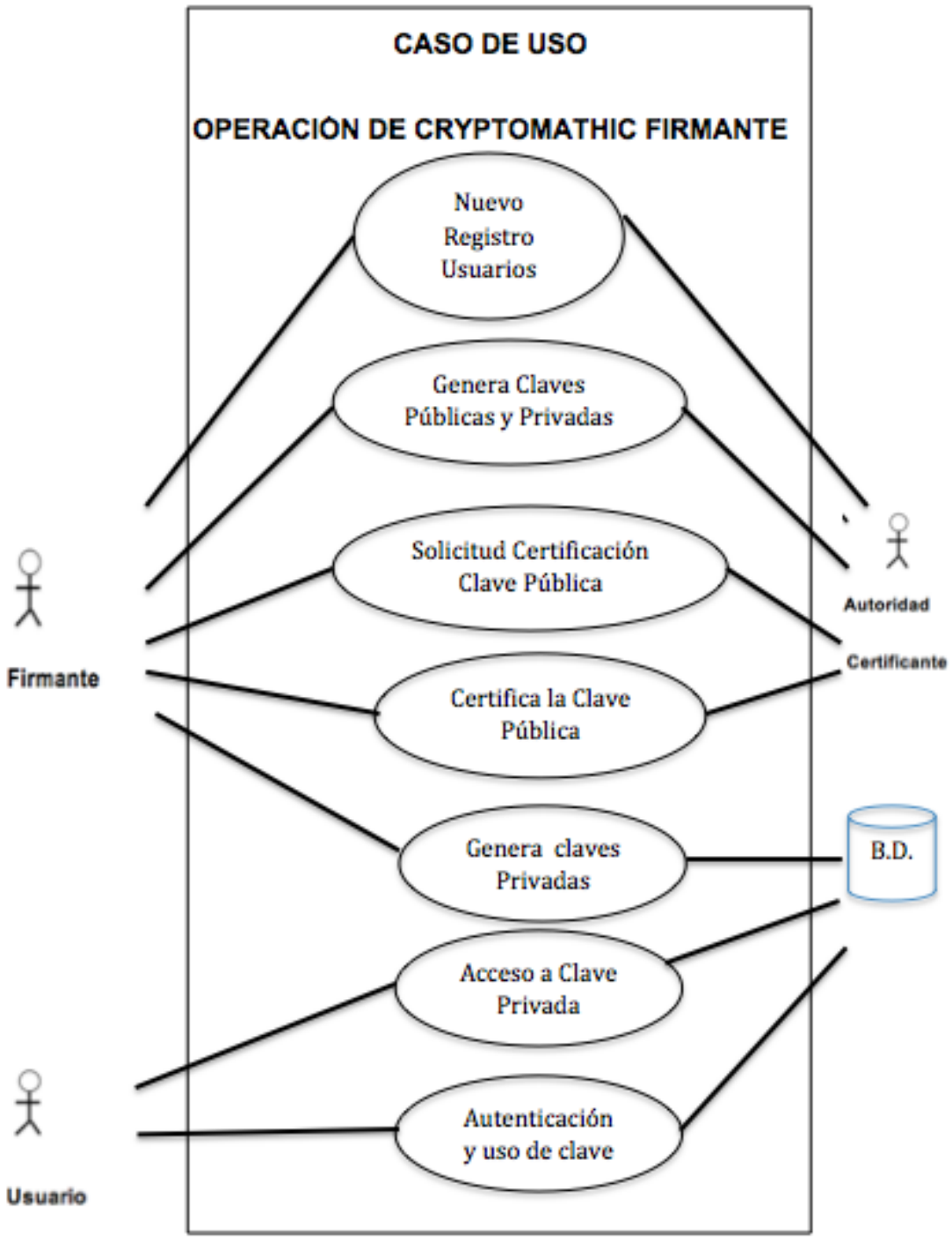

Ilustración 12 Caso de Uso de Operación de Cryptomathic Singer

Caso de uso general:	Operación de Cryptomathic Signer.
Actores:	Firmante, Autoridad Certificante, Base de Datos Central y Usuario.
Descripción:	Firmante es un servidor central donde almacena las claves públicas y privadas de forma segura.
1. Firmante interactúa con una autoridad de certificación (CA), tanto como Autoridad de Registro (RA) y propietario de la clave. 2. Firmante inicia el registro de usuarios con una C.A. 3. La C.A. genera claves públicas y privadas a Firmante. 4. Firmante realiza las solicitudes de certificación de la clave pública a la CA. 5. El C.A. luego de haber certificado la clave pública al firmante, se encarga de la gestión de certificados. 6. El firmante genera claves privadas para la protección de firma en una base de datos central. 7. La Base de Datos, proporciona al usuario el acceso a la clave privada en cualquier momento a través de un navegador Web. 1. El usuario autentica y hace uso de la clave privada donde se almacena ahora en un servidor central de alta seguridad.	

Tabla 8 Detalle Operación de Cryptomathic Singer

En el siguiente caso de uso se analiza, porque tiene un valor grande firmante por su desarrollo, para proporcionar una solución de transacción de firma de un sistema de banca por Internet, por lo tanto un requisito fundamental de la solución era la independencia del mecanismo de seguridad de la aplicación de banca central.

2.27 Funcionamiento de cryptomathic signer

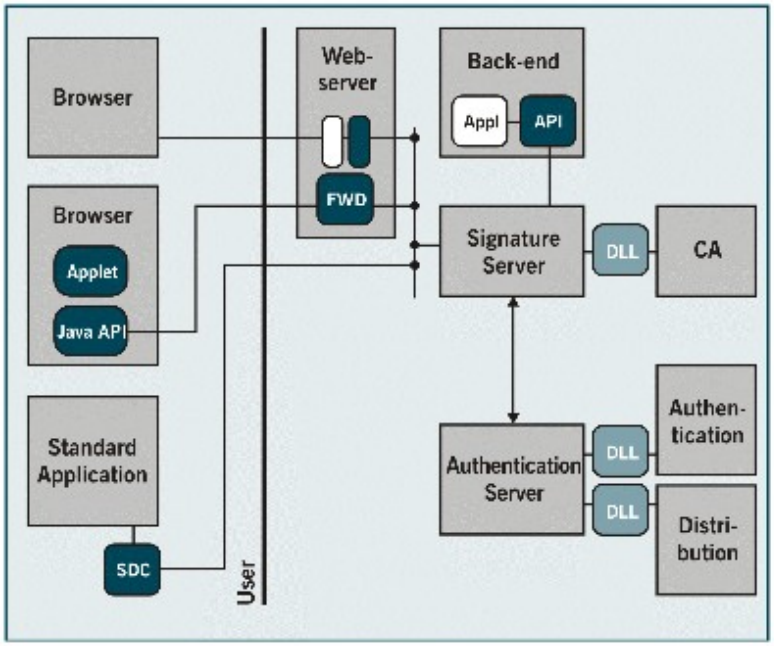

Ilustración 13 Funcionamiento de Cryptomathic Signer

La solución combina una contraseña estática conocida por el cliente, así como una contraseña de una sola vez en poder del cliente.

La contraseña de una sola vez puede ser entregado al teléfono móvil del usuario a través del sistema de (SMS), generada por un testigo o impresas en una tarjeta de cero, otras opciones de autenticación pueden ser acomodados en la arquitectura del producto.

Para acceder a la clave de la firma del cliente tiene que demostrar:

Debe conocer la contraseña, tiene el teléfono móvil.

2.27.1 Generación de funcionamiento de cryptomathic signer

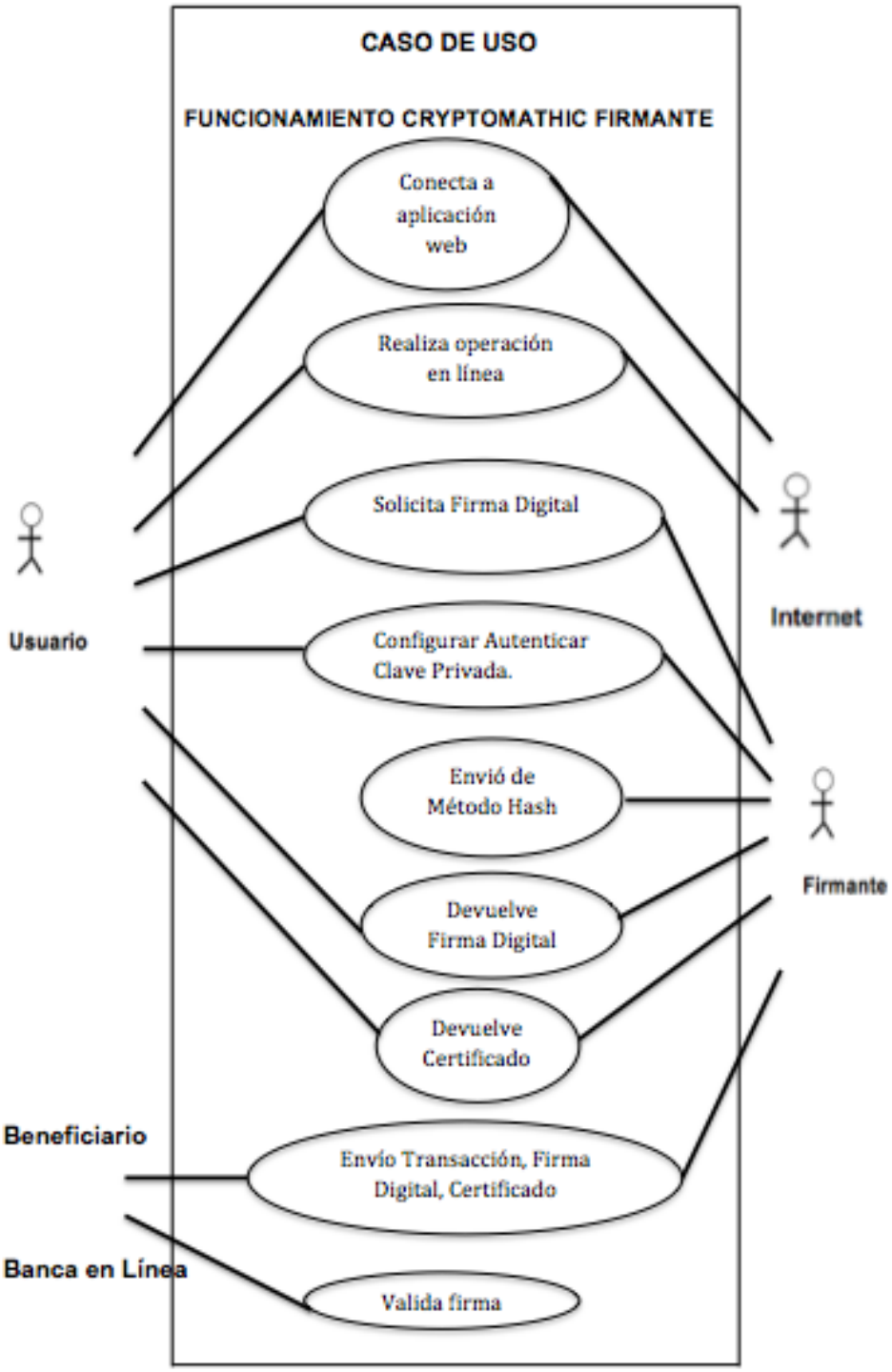

Ilustración 14 Generación de Funcionamiento de Cryptomathic Signer

Caso de uso general:	Funcionamiento De Cryptomathic Signer
Actores:	Usuario, Internet, Firmante, Beneficiario.
Descripción:	El usuario mediante la conexión a Internet puede acceder al firmante, y enviar la firma digital asegurando que los datos son seguros al destinatario.

1. El cliente de banca por Internet se conecta a la aplicación que utiliza su ordenador a través de Internet.
2. El usuario lleva a cabo una operación en internet.
3. El usuario solicita firma digital, donde el cliente se conecta a firmante con la contraseña privada.
4. Un túnel seguro se establece entre el servidor y el usuario para autenticar la clave privada.
5. El Método hash de la transacción se envía al firmante.
6. El Firmante devuelve una firma digital al Usuario.
7. El Usuario devuelve el certificado al Firmante.
8. La transacción, la firma digital y certificado de ahora se envían a la aplicación de banca por Internet.
9. La aplicación de banca por Internet ahora válida la firma del cliente. Si el certificado fue emitido al cliente por un tercero, entonces la aplicación de banca por Internet valida el certificado.

   9.1 No ve el contenido del firmante de la transacción, sólo su valor hash.

   9.2 La clave del cliente y la firma deja el entorno seguro del firmante.

Tabla 9 Detalle de Funcionamiento de Cryptomathic Singer

2.27.1.1 Caso de uso para funcionamiento de Cryptomathic Signer para conexión a aplicación Web.

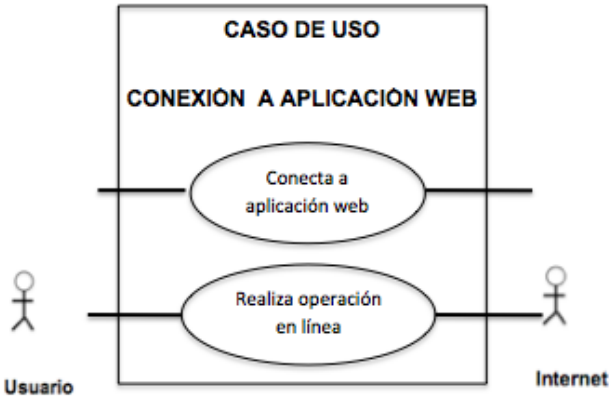

Ilustración 15 Caso de Uso de Conexión a Aplicación Web

Caso de uso:	Conexión a Aplicación Web.
Actores:	Usuario, Internet.
Descripción:	El usuario ingresa a una aplicación web, mediante el acceso a Internet y procede a realizar la operación.
1.1.1 El cliente se conecta a una aplicación web, mediante el Internet. **1.1.2** El Internet realiza la operación en línea de acuerdo a la necesitad del Usuario.	

Tabla 10 Detalle de Conexión a Aplicación Web

2.27.1.2 Caso de uso para funcionamiento de Cryptomathic Signer para solicita Firma Digital.

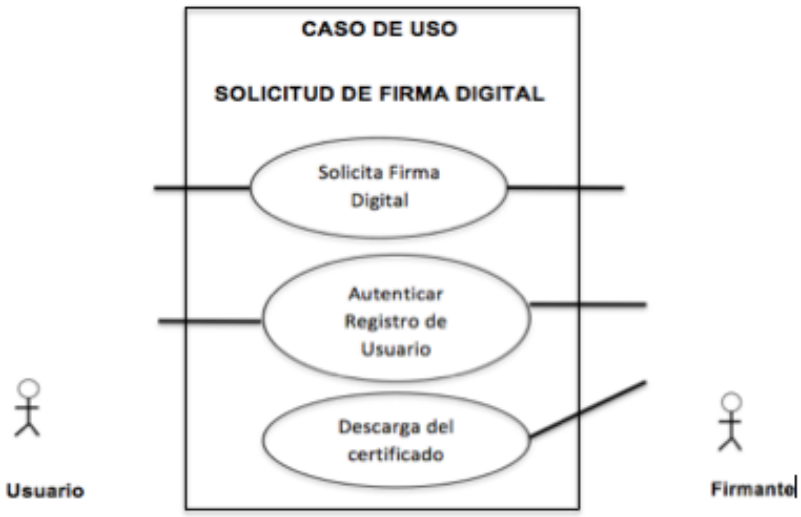

Ilustración 16 Caso de Uso de Cryptomathic Signer para solicitar Firma Digital

Caso de uso:	Solicitud Firma Digital
Actores:	Usuario, Firmante.
Descripción:	El usuario realiza solicitud de la Firma Digital al Firmante.
1.2.1	El usuario solicita la firma digital, mediante la cual se obtiene un código de solicitud del certificado, que se deberá facilitar en el momento de acreditar su identidad y en la obtención del certificado, que solicita al firmante.
1.2.2	El Firmante verifica que el Titular osea la Cooperativa JEP, donde deberá personarse en una oficina de registro para proceder a la acreditación de la identidad del usuario.
1.2.3	El Firmante se encarga de descargar el certificado, que se podrá obtener desde la página de Internet de la Autoridad de Certificación, donde se realizada desde el mismo equipo y navegador que realizó la solicitud.

Tabla 11 Detalle de Solicitud de Firma Digital

2.28 Caso de uso para funcionamiento de Cryptomathic Signer para Envió de Método Hash.

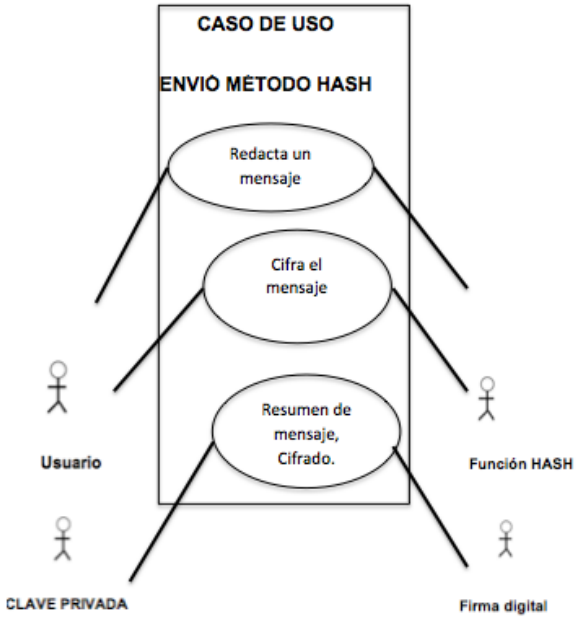

Ilustración 17 Funcionamiento de Envió de Datos Mediante Método Hash

Caso de uso:	Envió de Método Hash
Actores:	Usuario, Función Hash, Clave Privada y Firma Digital.
Descripción:	El usuario realiza la firma del mensaje por el emisor del mismo y la verificación de la firma por el receptor del mensaje.
1.3.1 El usuario redacta un mensaje electrónico, mediante la función Hash. **1.3.2** La función Hash envía un resumen del mensaje y aplica un I algoritmo para obtener una clave privada. **1.3.3** La Clave Privada envía un resumen cifrado y se obtiene la firma digital.	

Tabla 12 Detalle de envió de información mediante método HASH

2.28.1 Caso de uso para funcionamiento de Cryptomathic Signer para Verificación por el receptor de la firma del mensaje.

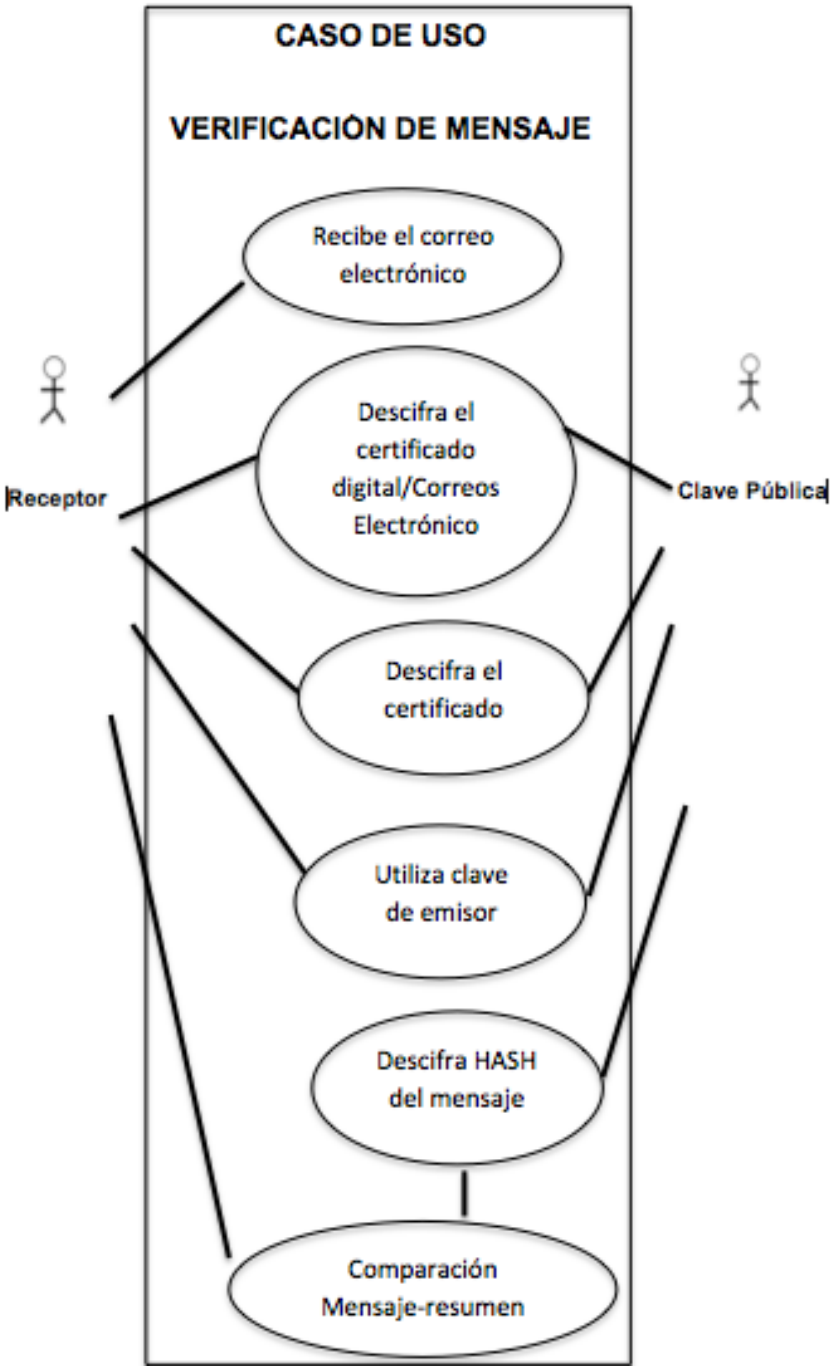

Ilustración 18 Caso de Uso para verificar el mensaje

Caso de uso:	Verificación del Mensaje
Actores:	Receptor, Clave Pública.
Descripción:	El Usuario verifica la firma digital se desencriptar de manera automática.

1.3.4.1 El receptor recibe el correo electrónico que contiene todos los elementos mencionados anteriormente.

1.3.4.2 El receptor descifra el certificado digital, incluido en el correo electrónico, utilizando para ello la clave pública.

1.3.4.3 La clave pública se encarga de enviar al receptor para descifrar el certificado.

1.3.4.4 El receptor descifrado el certificado, con el acceder a la clave pública en dicho certificado.

1.3.4.5 El receptor obtiene el certificado digital para descifrar con el método el hash o mensaje-resumen creado por el Usuario.

1.3.4.6 El receptor aplica al cuerpo del mensaje, y realiza la comparación del resumen del mensaje y verifica que el certificado es igual a la firma digital del usuario.

Tabla 13 Detalle para verificación el mensaje

2.28.2 Caso de uso Develve Firma Digital

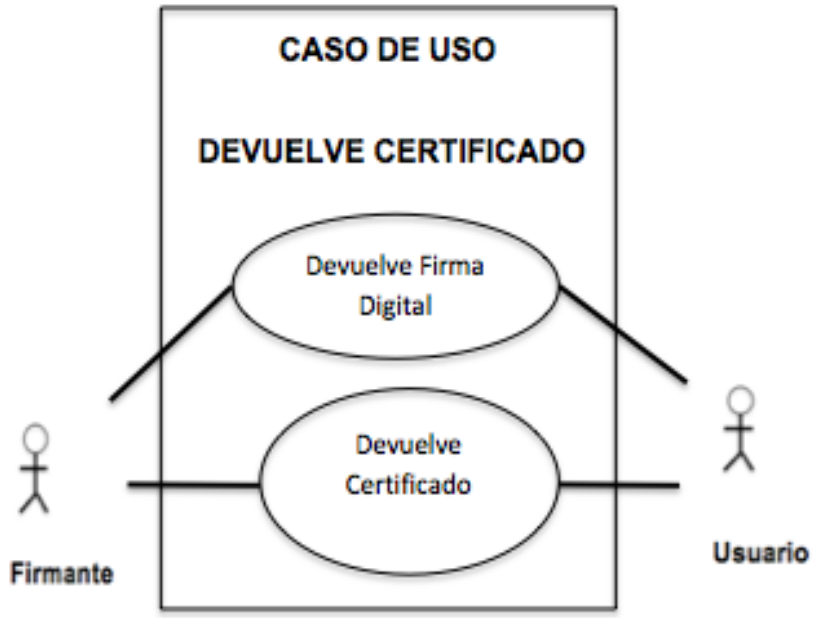

Ilustración 19 Caso de Uso para devolver el certificado Firma Digital

Caso de uso:	Devuelve Certificado
Actores:	Usuario, Firmante.
Descripción:	El Firmante devuelve la firma digital y el certificado envía el Usuario.
1. El Firmante devuelve la firma digital al usuario 2. El usuario envia el certificado autorizado al Firmante.	

Tabla 14 Detalle de Devolver el certificado

2.28.3 Caso de uso envió de transacción

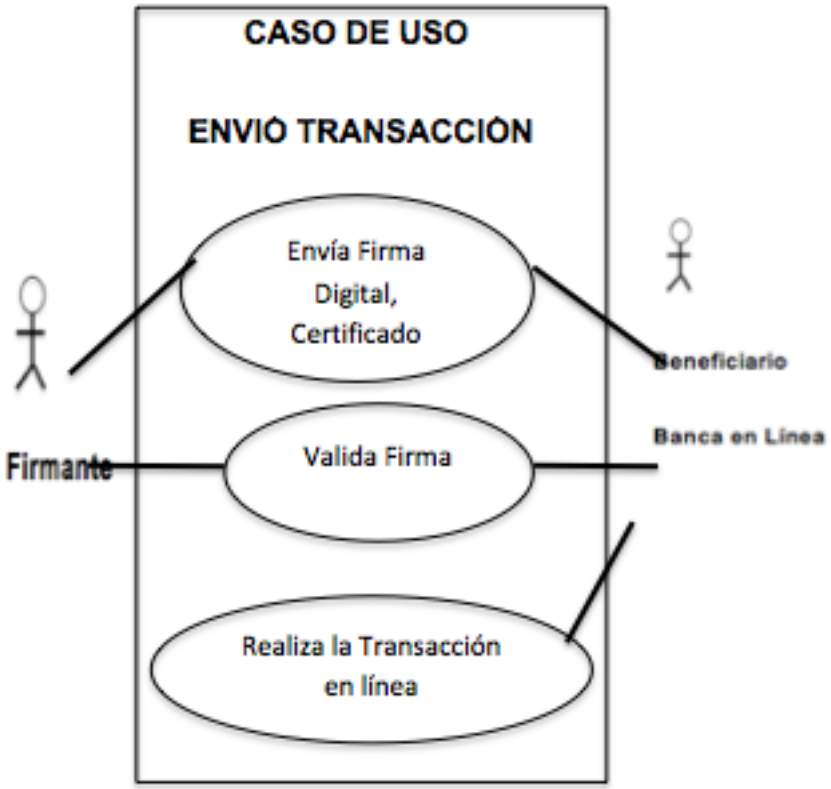

Ilustración 20 Caso de Uso devuelve Firma Digital

Caso de uso:	Envió de Transacción, firma Digital y certificado.
Actores:	Usuario, Firmante.
Descripción:	El Usuario envía la transacción al firmante.
1. El Firmante envía la firma digital con el certificado para realizar las transacciones en línea para el beneficiario. 2. El beneficiario valida la firma mediante el firmante. 3. La banca en línea realiza la trasacción del Usuario.	

Tabla 15 Detalle de envió de transacción

El análisis es una completa herramienta de encriptación que asegura la confidencialidad tanto de la información que almacenas en tu PC como de la que compartes con tus amigos.

Es una solución que utiliza un potente sistema de codificación que no deja ningún tipo de rastro una vez es encriptado el archivo.

Siendo un sistema simple y efectivo, que utiliza una sola contraseña compartida por ambas partes.

Cryptomathic siendo fácil de utilizar simplemente selecciona el archivo que desea codificar y escribe una contraseña, se puede codificar el archivo en un formato especial que sólo funcione con Cryptomathic puede ejecutarse donde pide la contraseña y decodifica el archivo original.

Además de archivos, esta aplicación permite proteger directorios completos, disco duro, una unidad compartida en red local o cualquier otra unidad de almacenamiento.

La licencia es gratuita sólo para uso personal, y shareware con caducidad a los 30 días para uso corporativo.

La seguridad de los datos está protegidos frente a revelaciones accidentales o intencionadas a usuarios no autorizados, frente a modificaciones indebidas o frente a destrucciones.

- Coste, rendimiento y usabilidad

2.29 Interpretación de resultados de la encuesta.

PREGUNTAS DE LA ENCUESTA

		SI	NO
1	¿Alguna vez ha sido víctima de algún delito informático?	9	1
2	¿Alguna vez ha trabajado con transacciones bancarias?	1	9
3	¿Con qué sistema Bancarios ha trabajado en sus transferencias?	8	2
6	¿Tiene algún mecanismo de protección en su PC, para contrarrestar delitos Informáticos en la red?	4	6
7	¿Conoce acerca de método de Protección de Firma de Criptografía?	4	6
8	¿Conoce otro tipo de mecanismo de protección para el envió de datos seguros?	3	7
9	¿Tiene usted la debida educación acerca de los delitos informáticos en los sistemas bancarios?	7	4
10	¿Considera Usted, que los Sistemas bancarios en la ciudad utilizan el método seguro de firma de Criptografía, para que la información llegue al usuario final, sin que usuarios no autorizados alteren su archivo?	9	1

Tabla 16 Preguntas para la Encuesta

2.29.1 ¿Alguna vez ha sido víctima de algún delito informático en la red?

SI 9 NO 1

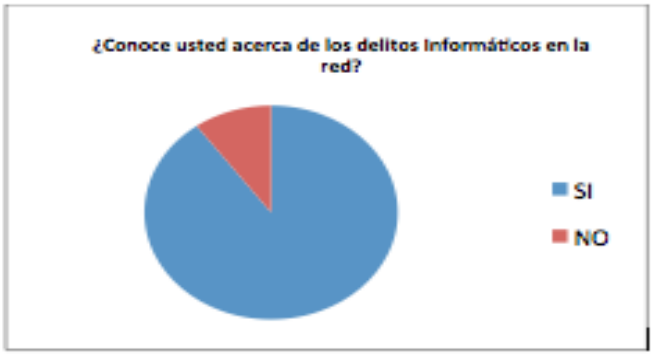

Ilustración 21 conocimiento sobre delitos informáticos en la red

Fuente: Encuesta aplicado a la Universidad de Israel y trabajadores de JEP

Fecha: Cuenca, 1 de septiembre del 2011

EL 90% conocen los delitos informáticos que existen en la red, indica que están actualizados en sus conocimientos informáticos.

El 10% siendo un porcentaje pequeño que desconoce y debe poner en práctica los conocimientos a cerca de los delitos informáticos.

“Las operaciones ilícitas realizadas por medio de Internet o que tienen como objetivo destruir y dañar ordenadores o medios electrónicos y redes de Internet.” (Wales , Jimmy;, 2011)

2.29.2 ¿Alguna vez ha trabajado con transacciones bancarias?

SI 8 NO 2

Ilustración 22 si han trabajado con transacciones bancarias

Fuente: Encuesta aplicado a la Universidad de Israel y trabajadores de JEP

Fecha: Cuenca, 1 de septiembre del 2011

El 80% Alguna han trabajado o realizado transferencias bancarias, aquellas personas que desean fácilmente las transferencias, sin saber el riesgo a la que están expuestos.

El 20% no han realizado transferencias bancarias por la red, quienes desconocen de los servicios bancarios que ofrecen los bancos.

“Acuerdo formal en el que participan muchas partes que acuerdan unas reglas comunes y estandarizadas para la transmisión y liquidación de obligaciones monetarias que surjan entre sus miembros.”

2.29.3 ¿Con qué sistema Bancarios ha trabajado en sus transferencias?

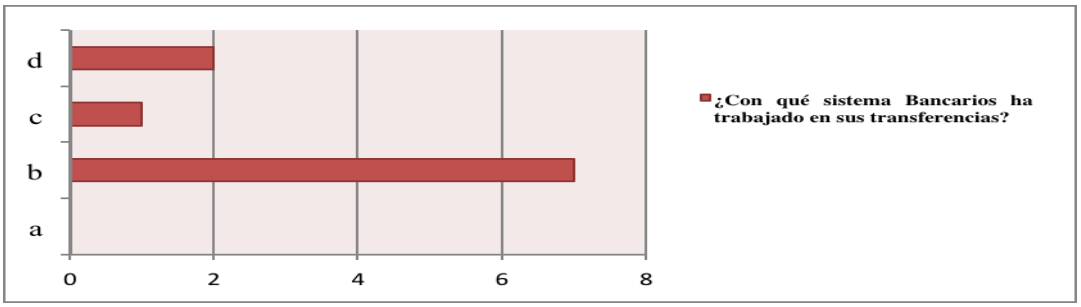

Ilustración 23 Distintos Sistemas Bancarias que han realizado transacciones

Fuente: Encuesta aplicado a la Universidad de Israel y trabajadores de JEP

Fecha: Cuenca, 1 de septiembre del 2011

El 70% han trabajado con algún sistema bancario en sus transacciones como el teclado virtual, El 10% han trabajado con algún sistema bancario en sus transacciones como es las tarjetas de coordenadas.

El 20% han trabajado con algún sistema bancario en sus transacciones como es el aviso por mensajes.

“Conéctese al sitio de su banco de forma segura, para ello asegúrese de que su red inalámbrica sea segura, nunca envíe información sensible a través de una red inalámbrica no segura, como un hotel o un café.

Las transacciones de su banco debe estar seguro de que está visitando el banco real cada vez, no una imitación del sitio, instale tecnología antirrobo y respalde sus datos, además configure su dispositivo para bloqueo automático después de un período de tiempo”.

2.29.4 ¿Conoce usted acerca de algún mecanismo para contrarrestar los Delitos Informáticos en los Sistemas Bancarios?

SI 4 NO 6

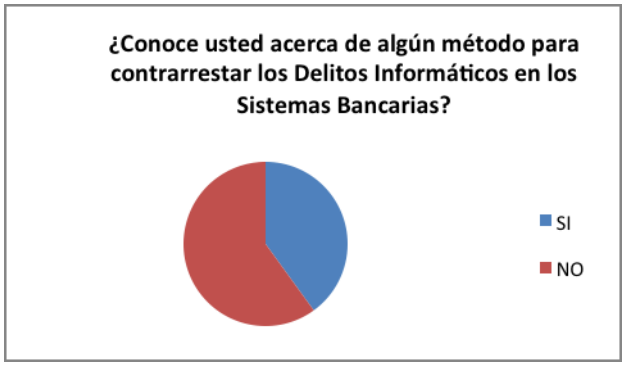

Ilustración 24 conocimiento de métodos para contrarrestar

Fuente: Encuesta aplicado a la Universidad de Israel y trabajadores de JEP

Fecha: Cuenca, 1 de septiembre del 2011

El 40% son aquellas personas que poseen los métodos para contrarrestar los delitos informáticos en los sistemas bancarios.

El 60% son aquellas personas que no poseen los conocimientos informáticos acerca de los métodos para contrarrestar quienes son más vulnerables a ser víctimas de un delito.

“La proliferación de nuevas tecnologías de la información y las comunicaciones en todo el mundo ha dado lugar a más formas de delitos informáticos, que amenazan no sólo a la confidencialidad, la integridad, o la disponibilidad de los sistemas de computadoras, sino también a la seguridad de la infraestructura”, (Bangkok, 2005)

2.29.5 ¿Tiene algún mecanismo de protección en su PC, para contrarrestar delitos Informáticos en la red?

SI 4 **NO 6**

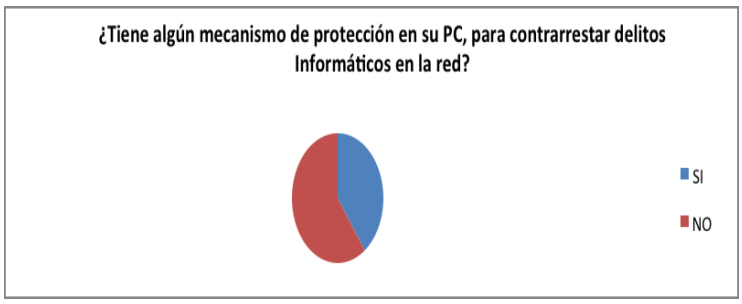

Ilustración 25 cuanto conocen sobre los mecanismos de protección para la PC

Fuente: Encuesta aplicado a la Universidad de Israel y trabajadores de JEP

Fecha: Cuenca, 1 de septiembre del 2011

El 40% de los usuarios tiene mecanismos de seguridad siendo un porcentaje bajo.

El 60% desconocen de la problemática de no tener mecanismos de seguridad en su PC, siendo expuestos a delitos informáticos

Es un compromiso de las instancias técnicas por estar preparadas para actuar y regular el efecto que dicho incidente puede ocasionar a la empresa.

“Administrar un incidente de seguridad requiere experiencia y habilidades técnicas para controlar las acciones del atacante, pero al mismo tiempo habilidad y pericia para establecer los rastros y registros de dichas acciones con las cuales relacionar las acciones y efectos ocasionados por el intruso dentro del sistema”. (Hadden Security)

2.29.6 ¿Conoce acerca de método de Protección de Firma de Criptografía?

SI 4 NO 6

Ilustración 26 método de protección de Firma Digital

Fuente: Encuesta aplicado a la Universidad de Israel y trabajadores de JEP

Fecha: Cuenca, 1 de septiembre del 2011

El 40% conocen que existe algún método de protección de firma criptográfica

El 60% desconoce del conocimiento de la firma criptográfica, siendo propenso a ser víctima de delitos informáticos en los sistemas bancarios.

“Es la técnica, bien sea aplicada a la ciencia, que altera las representaciones de un mensaje”.

CAPITULO III

DOCUMENTO PARA IMPLEMENTAR CRYPTOMATHIC SIGNER, EN LAS INSTITUCIONES BANCARIAS EN CRECIMIENTO "COOPERATIVA JEP DE CUENCA."

Cryptomathic Signer es una solución para instituciones bancarias ya que está centrada en Internet para garantizar la generación, almacenamiento y uso de las firmas digitales, además con el mantenimiento de la firma digital del usuario es un entorno seguro, por motivo que no estará en el disco duro de una computadora de escritorio, permitiendo a las organizaciones reducir los riesgos, aumentando la flexibilidad de información.

3. Implementación de Cryptomathic Signer.

a) Firmante sólo se ejecuta en Microsoft Windows NT y Microsoft Windows 2000.

b) Instalar y configurar la base de datos, Microsoft SQL Server 7 y 2000, siendo esta la plataforma de administración preferida.

c) Oracle (8 y 9), porque la mayoría de instituciones tiene un administrador de base de datos, firmante se limita a estas bases de bases de datos.

d) Instale la solución Firmante que constan de dos servidores físicos a través de una configuración de servidor único.

e) Servidor de firma Cryptomathic (CSS).

f) Servidor de autenticación Cryptomathic (CAS), se instalara el software del servidor, es preferible que se encuentra en una organización separada e independiente.

3.1 Esta configuración se separa por la operación de los dos servidores, para proteger el sistema contra los ataques de las personas con acceso a información privilegiada en una empresa, El CSS y el CAS para el intercambio de claves.

3.2 En el Asistente de instalación, en el cliente de administración, se Inicializará el sistema usando el asistente de inicialización.

3.3 Luego la carga de archivos para la definición de políticas y de archivos de configuración del sistema por el Oficial de Seguridad.

3.4 La función de administrador tiene derecho a crear otros administradores o para llevar a cabo relacionadas con la seguridad de gestión.

Firmante de administración generalmente se divide entre dos roles: el Oficial de Seguridad y el secretario, tiene derecho a administrar cuentas de usuario, mientras que el primero tiene control total sobre el sistema el CSS y CAS se implementan en la misma organización, e incluso luego se separan CSS y administradores CAS es preferible.

3.5 Los clientes de administración requieren una aplicación Java 2 Runtime Environment.

3.6 Firmante soporta procesadores criptográficos de hardware de IBM (4578) y nCipher (nForce y nShield), mediante el uso de estos productos resistentes

a la manipulación, ya que firmante proporciona cierto no repudio de firmas digitales.

Firmante genera firmas RSA con longitudes de clave desde 512 hasta 2048 bits.

a) Formatos firmados son ISO9796, PKCS # 1, y PKCS # 7.

b) Firmante usa X509v3 brinda certificados de clave pública, estos se pueden añadir a los mensajes firmados por ISO9796 y PKCS # 1 o incrustado en el mensaje PKCS # 7.

c) Los Protocolos PKCS # 10 para la emisión y PKIX-CMP revocación de los certificados de la CA, la renovación del certificado y la actualización no se utilizan.

3.7 CRYPTOMATHIC, Creamos algún documento ene cualquier formato y posteriormente guardamos

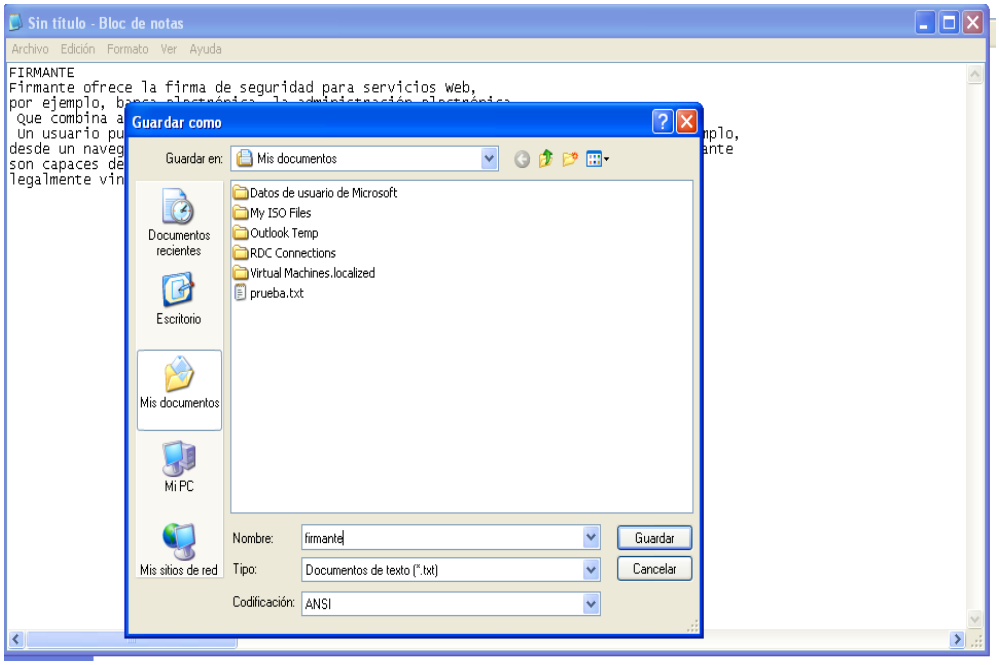

Ilustración 27 Crear documento en cualquier formato.

3.7.1 El formato que ahora visualizamo .txt

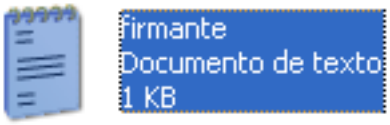

Ilustración 28 Archivo con formato Bloc de Notas

3.8 A continuación para encriptar el archivo nos vamos a posesionar en el Archivo click derecho y File 2 File y colocamos la contraseña privada.

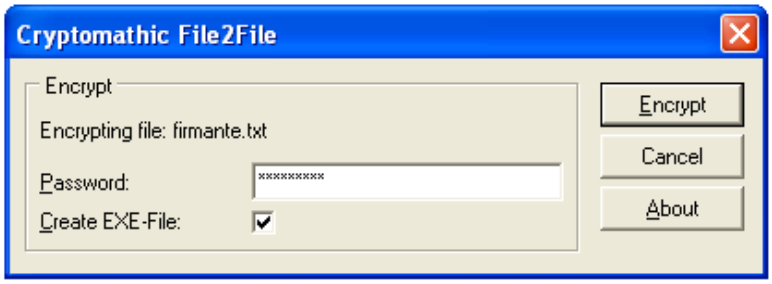

Ilustración 29 para encriptar el archivo

3.8.1 Después nos solicita que confirmemos la contraseña.

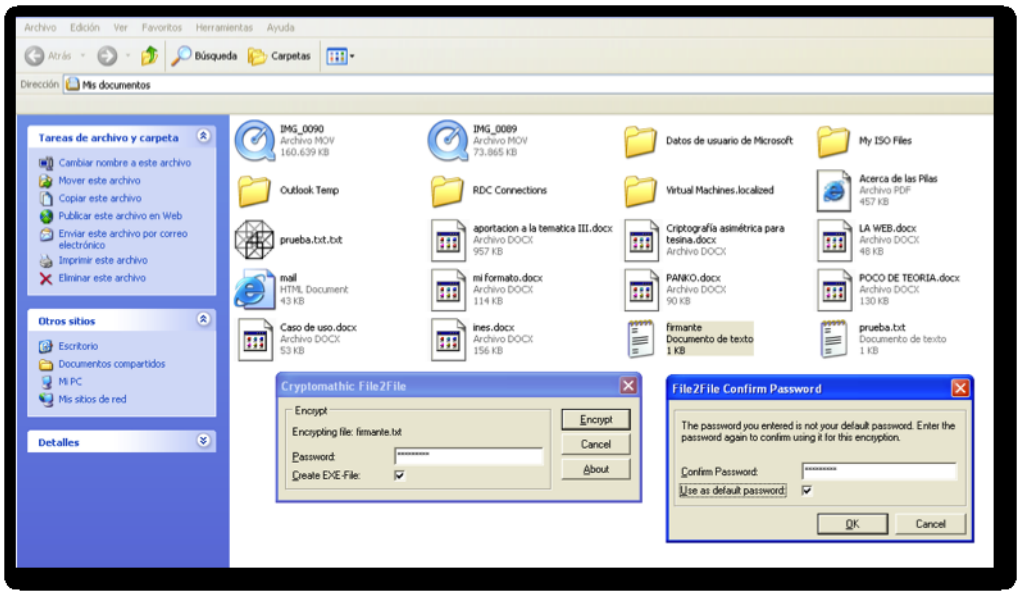

Ilustración 30 confirmar la contraseña

3.8.2 El archivo queda protegido o encriptado.

Ilustración 31 Imagen de Cryptomathic Seguro

3.9 Para desencriptar pulso con clic derecho abrir y escribo la contraseña que debe ser más de 7 dígitos.

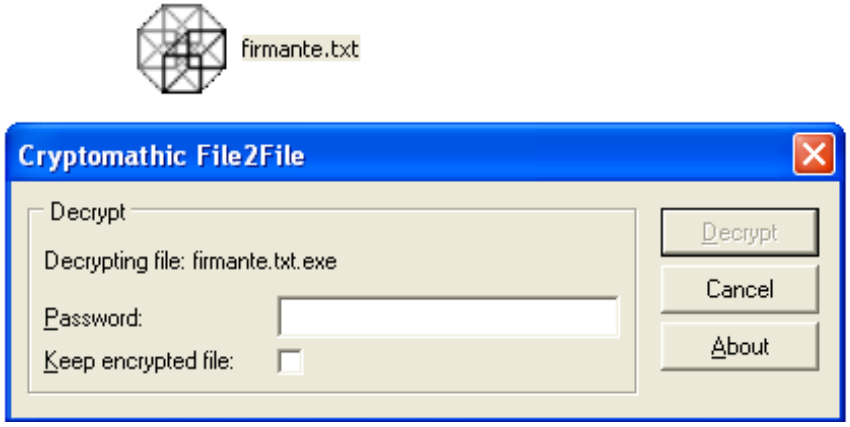

Ilustración 32 para modificar o realizar cambios debe colocar la contraseña

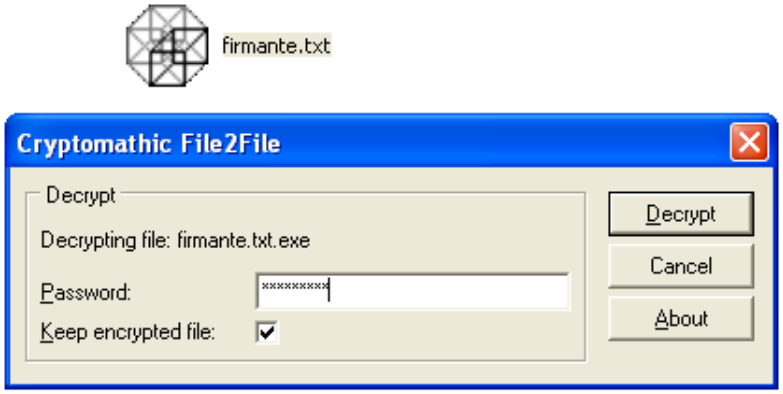

Ilustración 33 Para modificar el archivo presionas en abrir y tiene que colocar la contraseña correcta caso contrario no podrá abrir el archivo.

3.10 Para modificar el archivo presionas en abrir y tiene que colocar la contraseña correcta caso contrario no podrá abrir el archivo.

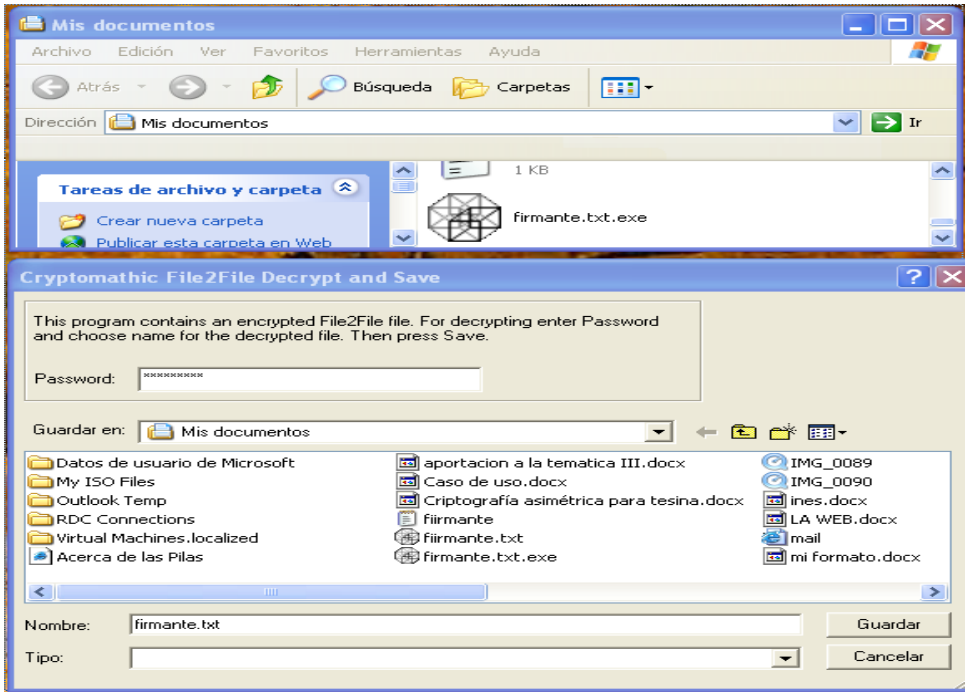

Ilustración 34 accederá al archivo

3.10.1 El archivo se modificará

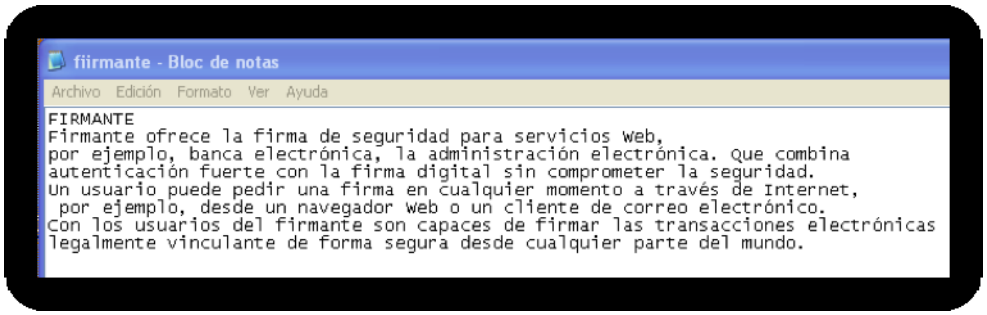

Ilustración 35 Accede al Texto

3.11 Especificaciones para el CLIENTE

El usuario puede utilizar firmante a través de un navegador.

a) Para la firma del formulario a través de aplicaciones como: Microsoft Outlook Express y Netscape Messenger, esta integración del lado del cliente se puede lograr a través de diversos medios:

b) PKCS # 11, Microsoft CryptoAPI se integra como un proveedor de servicios de Crypto.

3.12 Especificaciones de PC

- Pentium2.8GHz 19 "Monitor (pantalla táctil y no táctil)
- 2 GB Memoria RAM.
- 80 GB disco duro IDE

CAPITULO IV

CONCLUSIONES

1. Debe existir un debido tratamiento ante las actividades y tratamientos delincuenciales informáticas en Instituciones Bancarios, con el uso de criptografía fuerte, siendo este imprescindible para que los nuevos cripto sistemas puedan usars con facilidad
2. Firmante se integra con las soluciones PKI y aplicaciones de usuario final.
3. Soporta una gran variedad de técnicas de autenticación y escalable para múltiples servidores.

RECOMENDACIONES

1. Cryptomathic Firmante se ha centrado mucho en el mercado nacionales en el sector bancario, pero ahora la compañía está apuntando a sus productos a servicios en telecomunicaciones, los gobiernos y las grandes empresas, se debería trabajar mas en su publicación del software.

2. Realizar un análisis de actividades de usuarios para enviar datos y los debidos privilegios.
3. Monitoreo de Recursos Humanos que tienen acceso a información sensible a Sistemas de Control de Confianza, en la base de datos con la debida firma criptográfica.

Bibliografía

Bangkok*Naciones Unidas*

BOE

Copyright1986*Productos de Cryptomathic*

*El Délito Informático*1987EspañaMadrid

Hadden Security*cierterrorismo*

La MERCED. (2000 de 9 de 23). Recuperado el 12 de 10 de 2011, de Mision:

http://www.lamerced.fin.ec/seccion.aspx?sid=2

Magliona, P. (1999). *Delincuencia y Fraude Informático.* Jurídica de Chile.

Signer1986 *Cryptomathic* 2

Wales , Jimmy;*Wikipedia*

Wales, Jimmy. (22 de 11 de 2011). *Wikipedia.* Recuperado el 1 de 11 de 2011, de Phishing:

http://es.wikipedia.org/wiki/Phishing

Wales, Jimmy. (22 de 11 de 2011). *Wikipedia.* Recuperado el 12 de 10 de 2011, de Firma

Digital: http://es.wikipedia.org/wiki/Firma_digital

Anexo 1

ENCUESTA

Fecha: _____

La información recolectada sirve para conocer acerca del conocimiento, que tienen acerca de Cryptomathic Firmante, para la protección de los datos enviados por la red, siendo un método para protegerse de personas no autorizadas accedan a leer su información.

1. ¿Conoce usted acerca de los delitos Informáticos en la red?

Si ( )No ( )

2. ¿Alguna vez ha sido víctima de algún delito informático?

Si ( )No ( )

3. ¿Alguna vez ha trabajado con transacciones bancarias?

Si ( )No ( )

4 ¿Con qué sistema Bancarios ha trabajado en sus transferencias?

Acceso con NIF/DNI u otros datos personales ( )

Teclados virtuales ( )

Tarjetas de coordenadas ( )

Avisos por SMS ( )

5 ¿Conoce usted acerca de algún método para contrarrestar los Delitos Informáticos en los Sistemas Bancarias?

Si ( )No ( )

6 ¿Tiene algún mecanismo de protección en su PC, para contrarrestar delitos Informáticos en la red?

Si ( )No ( )

7. ¿Conoce acerca de método de Protección de Firma de Criptografía?

Si ( )No ( )

8. ¿Conoce otro tipo de mecanismo de protección para el envió de datos seguros?.

Si ( ) No ( )

9. ¿Tiene usted la debida educación acerca de los delitos informáticos en los sistemas bancarios?

Si ( ) No ( )

10. ¿Considera Usted, que los Sistemas bancarios en la ciudad utilizan el método seguro de firma de Criptografía, para que la información llegue al usuario final, sin que usuarios no autorizados alteren su archivo?

Si ( ) No ()

Anexo 2

Cuenca, 30 de noviembre de 2011

Señor:

Jefa de talento humano

En su Despacho,

De mis consideraciones:

Yo, Nancy Yambay Valla con CI. 0105294060, estudiante de la Universidad de Israel, realizó la entrega del Manual de Procedimiento para Implementación del Software Cryptomathic Singer, a la Cooperativa de Ahorro y Crédito Juventud Ecuatoriana Progresista. "JEP".

Reciba un cordial agradecimiento.

Atentamente

.....

Nancy Yambay Valla

Recibido
30/11/2011
JEFE DE TALENTO HUMANO
Coop. de Ahorro y Credito JEP Ltda.

CONCLUSIONES

1. Debe existir un debido tratamiento ante las actividades y tratamientos delincuenciales informáticas en Instituciones Bancarios, con el uso de criptografía fuerte, siendo este imprescindible para que los nuevos sistemas puedan usar con facilidad
2. Firmante se integra con las soluciones PKI y aplicaciones de usuario final.
3. Soporta una gran variedad de técnicas de autenticación y escalable para múltiples servidores.

RECOMENDACIONES

1. Cryptomathic Firmante se ha centrado mucho en el mercado nacionales en el sector bancario, pero ahora la compañía está apuntando a sus productos a servicios en telecomunicaciones, los gobiernos y las grandes empresas, se debería trabajar mas en su publicación del software.
2. Realizar un análisis de actividades de usuarios para enviar datos y los debidos privilegios.
3. Monitoreo de Recursos Humanos que tienen acceso a información sensible a Sistemas de Control de Confianza, en la base de datos con la debida firma criptográfica.

Bibliografía

Bangkok*Naciones Unidas*

BOE

Copyright1986*Productos de Cryptomathic*

*El Délito Informático*1987EspañaMadrid

Hadden Security*cierterrorismo*

La MERCED. (2000 de 9 de 23). Recuperado el 12 de 10 de 2011, de Mision: http://www.lamerced.fin.ec/seccion.aspx?sid=2

Magliona, P. (1999). *Delincuencia y Fraude Informático.* Jurídica de Chile.

Signer1986 *Cryptomathic* 2

Wales , Jimmy;*Wikipedia*

Wales, Jimmy. (22 de 11 de 2011). *Wikipedia.* Recuperado el 1 de 11 de 2011, de Phishing: http://es.wikipedia.org/wiki/Phishing

Wales, Jimmy. (22 de 11 de 2011). *Wikipedia.* Recuperado el 12 de 10 de 2011, de Firma Digital: http://es.wikipedia.org/wiki/Firma_digital

Anexo 1

ENCUESTA

Fecha: _____

La información recolectada sirve para conocer acerca del conocimiento, que tienen acerca de Cryptomathic Firmante, para la protección de los datos enviados por la red, siendo un método para protegerse de personas no autorizadas accedan a leer su información.

1. ¿Conoce usted acerca de los delitos Informáticos en la red?

   Si ( )No ( )

2. ¿Alguna vez ha sido víctima de algún delito informático?

   Si ( )No ( )

3. ¿Alguna vez ha trabajado con transacciones bancarias?

   Si ( )No ( )

4 ¿Con qué sistema Bancarios ha trabajado en sus transferencias?

   Acceso con NIF/DNI u otros datos personales ( )

   Teclados virtuales ( )

   Tarjetas de coordenadas ( )

   Avisos por SMS ( )

5 ¿Conoce usted acerca de algún método para contrarrestar los Delitos Informáticos en los Sistemas Bancarias?

   Si ( )No ( )

6 ¿Tiene algún mecanismo de protección en su PC, para contrarrestar delitos Informáticos en la red?

   Si ( )No ( )

7. ¿Conoce acerca de método de Protección de Firma de Criptografía?

   Si ( )No ( )

8. ¿Conoce otro tipo de mecanismo de protección para el envió de datos seguros?.

   Si ( ) No ( )

9. ¿Tiene usted la debida educación acerca de los delitos informáticos en los sistemas bancarios?

   Si ( ) No ( )

10. ¿Considera Usted, que los Sistemas bancarios en la ciudad utilizan el método seguro de firma de Criptografía, para que la información llegue al usuario final, sin que usuarios no autorizados alteren su archivo?

   Si ( ) No ()

Anexo 2

Cuenca, 30 de noviembre de 2011

Señor:

Jefa de talento humano

En su Despacho,

De mis consideraciones:

Yo, Nancy Yambay Valla con CI. 0105294060, estudiante de la Universidad de Israel, realizó la entrega del Manual de Procedimiento para Implementación del Software Cryptomathic Singer, a la Cooperativa de Ahorro y Crédito Juventud Ecuatoriana Progresista. "JEP".

Reciba un cordial agradecimiento.

Atentamente

.....

Nancy Yambay Valla

Recibido
30/11/2011
JEFE DE TALENTO HUMANO
Coop. de Ahorro y Crédito JEP Ltda.