Revista UIS Ingenierías
ISSN: 1657-4583
ISSN: 2145-8456
revistaingenierias@uis.edu.co
Universidad Industrial de Santander
Colombia

Sistema de votación electrónico con características de seguridad SSL/TLS e IPsec en Colombia

Bareño - Gutiérrez, Raul; Cardenas - Urrea, Sonia Elizabeth; Navarro - Nuñez, William; Sarmiento -Osorio, Hugo; Forero-Paez, Nelson

Sistema de votación electrónico con características de seguridad SSL/TLS e IPsec en Colombia
Revista UIS Ingenierías, vol. 16, núm. 1, 2017
Universidad Industrial de Santander, Colombia
Disponible en: http://www.redalyc.org/articulo.oa?id=553757254007

PDF generado a partir de XML-JATS4R por Redalyc
Proyecto académico sin fines de lucro, desarrollado bajo la iniciativa de acceso abierto

Sistema de votación electrónico con características de seguridad SSL/TLS e IPsec en Colombia

Electronic voting system with features of SSL / TLS and IPsec security in Colombia

Raul Bareño - Gutiérrez raulbare@misena.edu.co
Servicio Nacional de Aprendizaje SENA, Colombia
Sonia Elizabeth Cardenas - Urrea
secardenas9@misena.edu.co
Servicio Nacional de Aprendizaje SENA, Colombia
William Navarro - Nuñez williamnm2@misena.edu.co
Servicio Nacional de Aprendizaje SENA, Colombia
Hugo Sarmiento -Osorio
Servicio Nacional de Aprendizaje SENA, Colombia
Nelson Forero-Paez nelson.forero@docentes.umb.edu.co
Universidad Manuela Beltrán, Colombia

Revista UIS Ingenierías, vol. 16, núm. 1, 2017

Universidad Industrial de Santander, Colombia

Recepción: 05 Noviembre 2016
Aprobación: 27 Diciembre 2016

Redalyc: http://www.redalyc.org/articulo.oa?id=553757254007

Resumen: Colombia continúa debatiendo la implementación del voto electrónico evidenciando que existen temores en el acceso al sistema y en la transferencia de datos, esta investigación busca minimizar vulnerabilidades ante ataques informáticos por medio de un prototipo para el análisis de ataques y protección del envió de información durante la votación dando confianza en la transmisión, además verificando el acceso físico del sufragante mediante lecturas biométricas, la herramienta usa los protocolos SSL/TLS para la autenticación del elector y el protocolo IPSEC para validar el sitio, los datos y proteger las comunicaciones de operaciones no autorizadas. Este sistema propone el primer modelo integrado seguro para transporte y acceso de datos de votación, garantizando la confiabilidad a los electores; los protocolos SSL/TLS complementados con IPSEC y los nuevos sistemas electrónicos de validación de electores durante transmisión en los puntos de votación beneficiaran la democracia nacional soportada en nuevas tecnologías.

Palabras clave: Lector óptico y biométrico, Seguridad, Sistemas electrónicos de acceso, Transmisión, Voto electrónico.

Abstract: Colombia continues to debate the implementation of electronic vote showing that there are fears in system access and data transfer, this research seeks to minimize vulnerability to cyber attacks by means of a prototype for the analysis of attacks and security of information sent during the giving confidence vote in the transmission, besides verifying voter physical access by biometrics, the tool uses the SSL / TLS protocols for authentication of the voter and the IPSEC protocol to validate the site, data and secure communications of unauthorized transactions . This system proposes the first integrated transportation lock and polling data access model, ensuring reliability voters; SSL / TLS protocols supplemented with IPSEC and new electronic systems for transmission validation of voters in polling stations benefit national democracy supported by new technologies.

Keywords: Optical and biometric readers, Security, Electronic data systems access, Transmission, Electronic voting.

PDF generado a partir de XML-JATS4R por Redalyc
Proyecto académico sin fines de lucro, desarrollado bajo la iniciativa de acceso abierto

1. INTRODUCCIÓN

Con las nuevas tecnologías de la información y comunicación TIC, de amplio uso, y masificación en diferentes escenarios académicos, productivos también se pueden integrar hacia nuevos sistemas de votación electrónica que minimice algunas vulnerabilidades del sistema tradicional. Colombia debate el uso o inclusión de estas tecnologías [1], en su sistema electoral con serias dudas en el acceso al sistema y en la transmisión de los datos, con altos niveles de desconfianza y temor, entre los diferentes actores involucrados; a pesar de ello ha adelantado pilotos en algunas regiones [2], con resultados satisfactorios. El uso de las TIC hace fácil, sencillo y seguro la implementación de un sistema electrónico de votación; muchos países y universidades lo usan en diferentes procesos como Grecia, Noruega, México, España, Argentina, Estonia [3], [4], [46], entre otros usan investigan e implementan a sus sistemas de nuevas características de autenticación del elector con biometría en el acceso físico, con periféricos como lectores de código de barras, de huella dactilar [5], [6], [7] de rostro. En la actualidad países donde ya se aplica el voto electrónico presencial son Australia, Bélgica, Brasil, Francia, Alemania, India, Noruega, Venezuela, Paraguay, Argentina [8], [9], [14], y más de 30 países [12], [13] [43], con exitosa aplicación de estos sistemas algunos utilizan la validación biométrica, pero de forma independiente, no integrado a un único sistema.

Este prototipo [16], se diseña e implementa basado en la pregunta ¿Será el prototipo e-vote el sistema que garantiza la fiabilidad en la transmisión de información entre el punto de votación y los centro de datos? aplicado y necesario al contexto en Colombia que constituye una alternativa viable, que identifica una persona utilizando sistemas de identificación diferentes a los tradicionales minimizando vulnerabilidades durante la transferencia de los datos con poca probabilidad de ser sustraídos, o descifrados [9]. Estos lectores ópticos de identificación integrados entre la huella dactilar, y la autenticidad del documento de identificación entregan un alto porcentaje de validación, de transferencia de información hacia grandes centros de datos permitiendo el acceso al sistema del sufragante. Además de los protocolos de autenticación y de seguridad como secure sockets layer/transport layer security SSL/TLS que usa certificados de validación entre nodos si la solución opera de manera local; o si requiere comunicación externa el protocolo Internet Protocol security IPSEC ambos integrados en este prototipo minimizan muchas de las vulnerabilidades y ataques a los sistemas de votación tradicionales como DoS, DDoS y hombre en el medio (MITM) siendo los más referentes.

Finalmente se analiza el uso y funcionamiento de la tecnología para procesos de votación electrónica bajo ambientes TIC, la herramienta integra en un solo sistema parámetros de seguridad en cuanto al acceso físico o remoto de los electores, y protege la información desde la capa de aplicación y hasta la capa de red; los protocolos SSL/TLS y IPSEC [10], [11],[13] entrelazados aportan seguridad a cualquier sistema de votación electrónico.

PDF generado a partir de XML-JATS4R por Redalyc
Proyecto académico sin fines de lucro, desarrollado bajo la iniciativa de acceso abierto

2. PROCEDIMIENTO EXPERIMENTAL

2.1. Materiales

Se efectuó una investigación descriptiva experimental con énfasis cuantitativo, sobre una muestra controlada con diferentes electores, y pruebas durante la autenticación al sistema electoral, con ataques en el envío de datos entre uno y diez atacantes. Los ataques escogidos fueron: Denegación de servicio (DOS), denegación de servicio distribuido (DDOS), y de hombre en el medio (MITM) [20]. Se aplican estos ataques por ser los más reiterativos en sistemas de comunicación electrónicos según las estadísticas de empresas desarrolladoras de antivirus como Cert Kaspersky del año 2016. Todas las pruebas se validaron con los protocolos SSL/TLS e IPSEC [10],[11] con algunos parámetros adicionales de seguridad.

La instalación del prototipo E-vote se realizó bajo un escenario controlado con los dispositivos ópticos como el lector de código de barras y el lector de huella dactilar, además de la siguiente infraestructura: Configuración de los periféricos lector de código de barras [14] y lector de huella dactilar [15],[42],[45], en el PC, un servidor WEB apache con la base de datos MYSQL con los servicios SSL/TLS e IPSEC bajo el sistema operativo Linux. Además de la configuración de dispositivos activos de capa 3 y 2 como routers, switch (ver Figura 1). los escenarios de pruebas fueron: 1. En una intranet. 2. En una extranet. 3. Finalmente se integró el prototipo E-vote [16], bajo internet usando los protocolos SSL/TLS e IPSEC

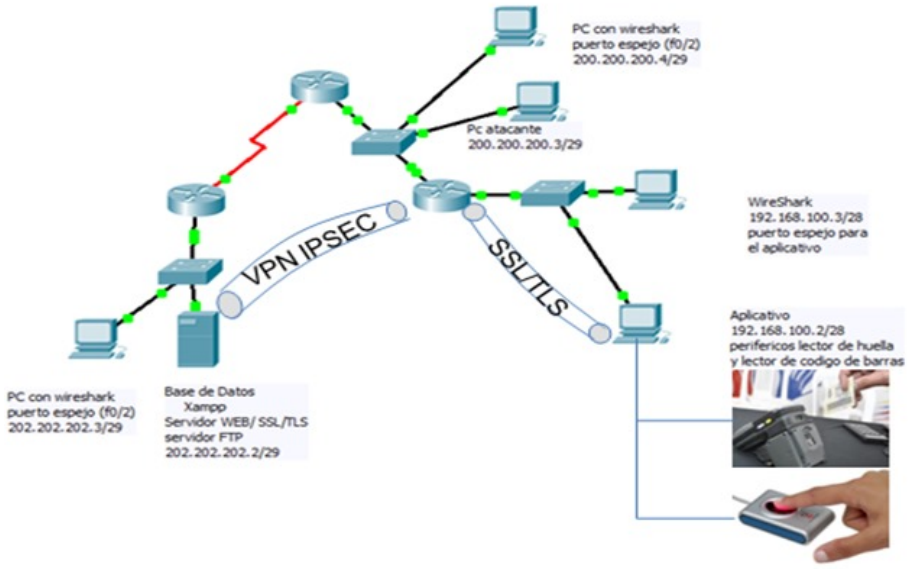

Figura 1
Transmisión de los datos
Fuente. Elaboración propia.

IPSEC: IPSec is an industry standard set of protocols and services based on cryptography, used to encrypt data so that it cannot be read or

PDF generado a partir de XML-JATS4R por Redalyc
Proyecto académico sin fines de lucro, desarrollado bajo la iniciativa de acceso abierto

tampered with during its journey across an IP network.Es un conjunto de estándares basados en criptografía utilizado para cifrar datos que mitigan su lectura o manipulación durante la trayectoria usando una red IP; se implementa There are a number of RFCs that provide specifications for IPSec and its protocols, as defined by the Internet Engineering Task Force (IETF).Good starting points are RFC 1825 and 2401, which deal with the security architecture for IP (http://www.ietf.org/rfc/rfc1825.txt and http://rfc.sunsite.dk/rfc/rfc2401.html).IPSec can be used with the current IPv4, and is built into the next generation of IP, IPv6.tanto en IPv4 o IPv6 [17], funciona en la capa de red del modelo OSI y permite privacidad y autenticación máxima de los datos. Ofrece tres funcionalidades: Una de autentificación con (AH) [18]. Otra mixta de autentificación y encriptamiento (ESP) [19], [20]. La última de intercambio de llaves por el protocolo de gestión de claves (IKE) [21], [22]. Funciona de dos formas: en modo transporte o túnel para las pruebas se implementó en modo túnel [23], [24]. En cuanto al protocolo SSL (secure sockets layer capa de sockets seguro) [25], provee privacidad y confiabilidad a la comunicación entre aplicaciones cliente-servidor vía web para autenticar los equipos. En cuanto a TLS surge de la necesidad de estandarizar un protocolo que provea seguridad entre el cliente y el servidor a través de internet debido a que SSL es un protocolo creado y patentado por Netscape. Siendo una evolución del protocolo SSL el cual establece una conexión segura por medio de un canal cifrado entre el cliente y el servidor [26]. SSL/TLS entrega seguridad en navegadores web y servidores protegiendo la transferencia de los datos [27]. Sus características son: seguridad criptografía, interoperabilidad, extensibilidad y eficiencia [28].

El sistema de código de barras [29], [30], [31] aporta beneficios, al prototipo E-vote en: velocidad en la identidad del elector, exactitud, integridad, y fácil implementación. Los lectores biométricos de huellas dactilares [32], [33], [34], ofrecen parámetros de identidad que son difíciles de falsificar, haciendo que la tecnología sea viable como sistema de identificación en los puestos de votación. Estos lectores hacen dos tareas: 1) Obtiene una imagen de la huella digital del elector; 2) la compara el patrón de valles y crestas de dicha imagen con los patrones de huellas ya almacenadas en la base de datos. Aportando ventajas en la identificación de los atributos físicos de una persona.

2.2. Métodos

Las pruebas se efectuaron para los 3 escenarios controlados y los ataques escogidos fueron: Denegación de servicio (DoS), denegación de servicio distribuido (DDoS) [35], y de hombre en el medio (MITM) [36]. Las pruebas para él envió del archivo en los escenarios 1 y 2 fueron: Prueba 1: envió con seguridad SSL/TLS, sin ataques, Prueba 2: envió con seguridad SSL/TLS, con ataques (DoS), Prueba 3: envió con seguridad SSL/TLS, con ataques (DDoS), Prueba 4: envió con seguridad SSL/TLS, con ataques. (MITM), Prueba 5: envió con seguridad IPSEC, sin ataques,

PDF generado a partir de XML-JATS4R por Redalyc
Proyecto académico sin fines de lucro, desarrollado bajo la iniciativa de acceso abierto

Prueba 6: envió con seguridad IPSEC, con ataques (DoS), Prueba 7: envió con seguridad IPSEC, con ataques (DDoS), Prueba 8: envió con seguridad IPSEC, con ataques (MITM). En el escenario 3 se transmitió con seguridad SSL/TLS e IPSEC; por los mecanismos de seguridad que tienen estos protocolos.

2.2.1. Escenario General

El procedimiento efectuado fue: primero el elector se reporta en la mesa de votación con su documento de identificación con hologramas. El sistema valida el documento usando el lector de código de barras, verificando los campos de nombres, apellidos y numero de cedula, fecha de expedición del mismo con los registrados previamente. (Figura 2).

Figura 2
Primera validación
Fuente: Autores

Segundo: Se activa la siguiente fase del elector utilizando el lector de huella dactilar. El sistema E-vote valida al elector comprobando que su huella concuerda con la registrada en la base de datos. (Figura 3).

PDF generado a partir de XML-JATS4R por Redalyc
Proyecto académico sin fines de lucro, desarrollado bajo la iniciativa de acceso abierto

Figura 3
Segunda validación
Fuente: Autores

Tercero: el sistema E-vote permite al elector su proceso de votación, y finaliza con él envió del archivo; en cuanto a la transmisión de los datos hacia los centros de cómputo ubicados en la intranet o extranet.

3. RESULTADOS Y ANALISIS

Son muchos los análisis y proyectos acerca de la seguridad en y durante el voto electrónico en América Latina que específicamente se pueden aplicar para el caso colombiano [37], Venezuela, Brasil, Paraguay y Perú [38]; que a pesar de sus barreras en términos de acceso a internet y a las TIC lo aplican y prueban en algunas regiones. En la actualidad se adicionan nuevos dispositivos ópticos que miden más características biométricas y permiten la identificación de las personas, como es rostro y voz entre otros, ahora en cuanto a transmisión de los datos los protocolos IPSEC y SSL/TLS se pueden implementar de manera integrada para su uso en Colombia, en otros países estos protocolos garantizando él envió de información de manera segura [39],[40],[41], pero independiente del sistema de votación, algunas características específicas para cada protocolo son: (Tabla I).

PDF generado a partir de XML-JATS4R por Redalyc
Proyecto académico sin fines de lucro, desarrollado bajo la iniciativa de acceso abierto

Tabla 1
Características de SSL/TLS e IPSEC para el prototipo e-vote

SSL/TLS	IPSEC
Específico para la aplicación, opera entre TCP y HTTP.	Protege el tráfico IP del equipo, opera en la capa de red
Se escoge SSL/TLS en cada conexión (desde la aplicación del cliente).	Configuración del equipo no admite el cifrado de conexión de red especifica
Vinculado a la aplicación E-vote	Transparente para el E-vote, con seguridad para IP
Su implementación depende de la aplicación. Transparente al usuario	Es complejo de implementar. No es transparente al usuario
Usa tecnología embebida en los navegadores WEB	Solución propietaria con VPN el cliente se necesita instalar software adicional
Aplica el modelo cliente/servidor	Une puestos de votación a data center.
Cifrado fuerte	Cifrado fuerte encripta y da integridad
Autentica el servidor al cliente, pero no el cliente al servidor	No protege las comunicaciones entre los PC y la puerta de enlace

Fuente: Autores

Es evidente que día a día es necesario contar con redes de telecomunicaciones y sistemas de votación electrónicos seguros y SSL/TLS por su universalidad en cuanto a calidad y fortaleza en los aspectos relacionados con el envió de información cifrada por canales inseguros. Fácil pensar que en el terreno de las comunicaciones seguras pueda ser desplazado por IPSEC sobre todo en el terreno específico de las aplicaciones de comercio electrónico y de E-vote [6]. Por el momento SSL/TLS e IPSEC son funcionales para aplicaciones específicas como el voto electrónico.

3.1. Resultados

Para el análisis de resultados las variables consideradas son (Tabla 2):

PDF generado a partir de XML-JATS4R por Redalyc
Proyecto académico sin fines de lucro, desarrollado bajo la iniciativa de acceso abierto

Tabla 2
Variables analizadas

Variables	**Paquetes recibidos por la BD**	**% de ocupación del canal PC1**	**% de procesamiento BD**
Tiempo de envió	Bytes enviados por PC1	% de ocupación del canal BD	% de disponibilidad del canal
Paquetes enviados aplicativo (PC1)	Bytes recibidos por la BD	% de procesamiento PC1	Archivos enviados

Fuente: Autores

Las pruebas efectuadas se llevaron a cabo enviando entre uno y tres archivos 10 veces por escenario, los atacantes entre 1 y 10 y el tamaño del archivo tipo PDF enviado era de 21 Kbyte, como máximo.

3.1.1 Pruebas escenario 1 intranet

Bajo este escenario (Figura 4) basado en la infraestructura de telecomunicaciones instalada se configuraron los switch, la base de datos y los PC para efectuar el análisis de trafico respectivo.

PDF generado a partir de XML-JATS4R por Redalyc
Proyecto académico sin fines de lucro, desarrollado bajo la iniciativa de acceso abierto

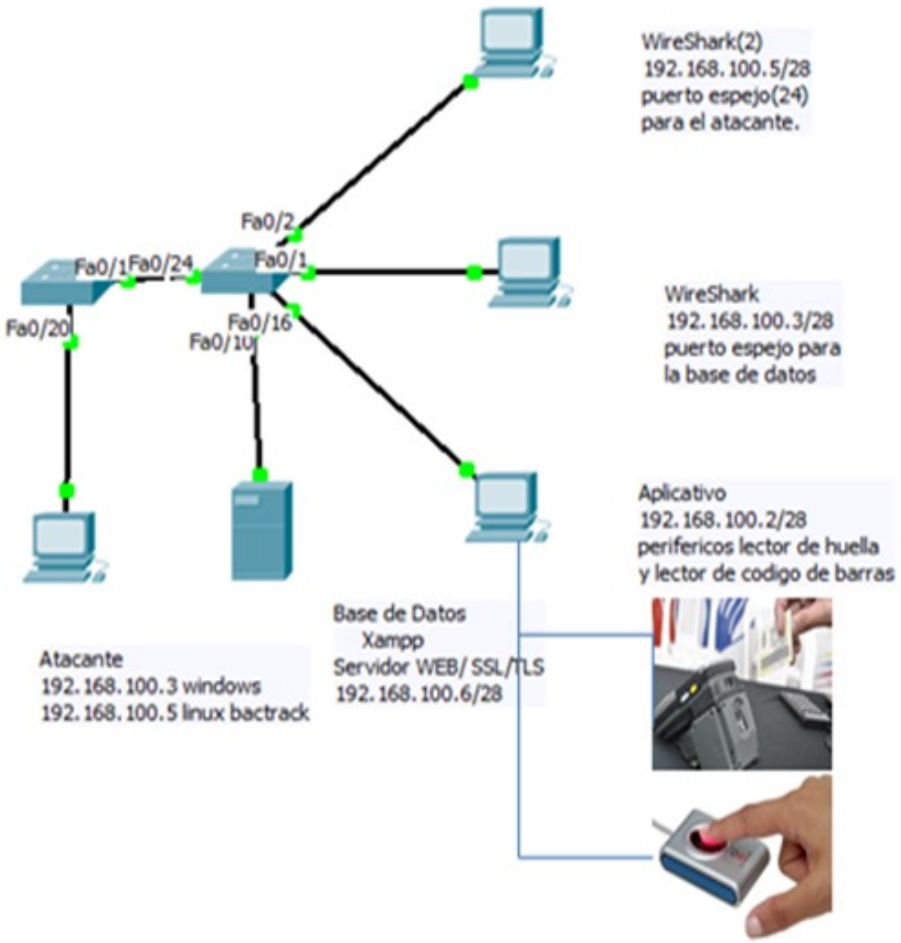

Figura 4
Escenario intranet
Fuente: Autor

Debido a la cantidad de variables consideradas (Tabla 3) se tabularon y basados en sus promedios arrojó lo siguiente:

PDF generado a partir de XML-JATS4R por Redalyc
Proyecto académico sin fines de lucro, desarrollado bajo la iniciativa de acceso abierto

Tabla 3
Escenario 1

Escenario 1	DoS	DDoS	MITM	Sin Ataques
Tiempo ENVIO	32	28	30	27
Paquetes enviados PC1	160	170	129	100
Paquetes Recibidos BD	231496	285678	127	114
Bytes PC1	30004	34043	54943	52994
Bytes BD	2190620	7906355	86544	53112
% Ocupación canal PC1	1,8	2,1	1,2	2
% Ocupación canal BD	77	92,5	2	2
% Procesamiento PC1	2,1	3,9	4,3	5,2
% Procesamiento BD	85,6	94,1	4,8	6,1
% Disponibilidad del Canal	23,1	7,5	98,5	97,70
Archivos	1,2,3	1,2,3	1,2,3	1,2,3
Atacantes	1,5,10	1,5,10	1,5,10	1,5,10

Fuente: Autores.

Basados en los paquetes recibidos en la base de datos durante los ataques de DoS y DDoS efectivamente se incrementan con relación a los enviados por el aplicativo (Figura 5); incrementando el procesamiento de la base de datos y limitando el ancho de banda del canal de manera notoria (Figura 6). Si se mantiene el ataque por más de 5 minutos continuos congestiona el canal al punto de deshabilitar el servicio de votación.

PDF generado a partir de XML-JATS4R por Redalyc
Proyecto académico sin fines de lucro, desarrollado bajo la iniciativa de acceso abierto

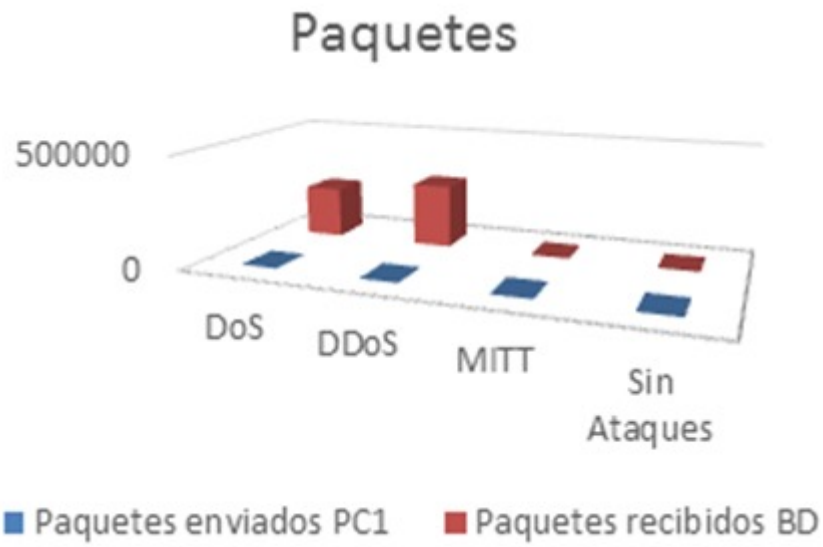

Figura 5
Cantidad de paquetes
Fuente: Autor

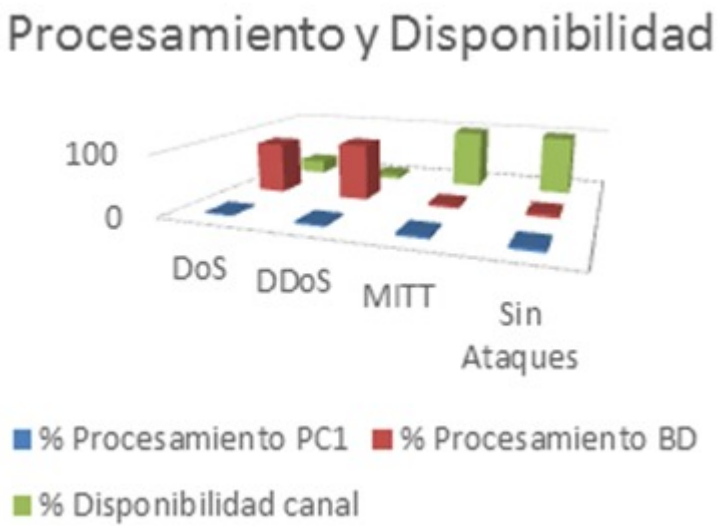

Figura 6
Procesamiento y disponibilidad del canal
Fuente: Autor

Durante los cortos tiempos de envió a pesar de los ataques; y por su tamaño 21 Kbyte permite la llegada de los datos al destino sin contratiempos.

Los altos consumos de ancho de banda durante los ataques disminuyen la disponibilidad del canal para DoS a 23,1%, para DDoS a 7,5%. Y Para el ataque de MITM puede interceptar el tráfico entre el puesto de votación y la base de datos, pero el protocolo TLS/SSL encripta con cierto grado de seguridad (Figura 7).

PDF generado a partir de XML-JATS4R por Redalyc
Proyecto académico sin fines de lucro, desarrollado bajo la iniciativa de acceso abierto

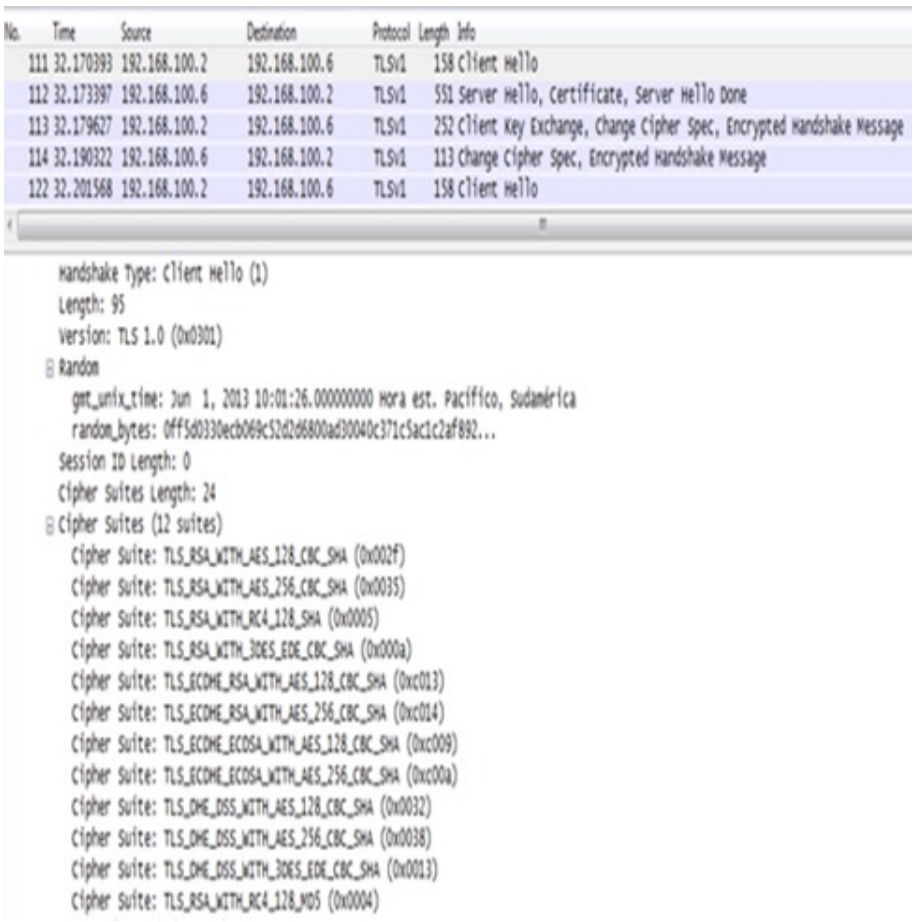

Figura 7
Trafico con TLS/SSL
Fuente: Autor.

3.1.2 Pruebas escenario 2 extranet con SSL/TLS

Es este escenario se amplía la cobertura y se diseña la infraestructura de telecomunicaciones configurando routers, switch, la base de datos y los pc (Figura 8) para efectuar el análisis.

PDF generado a partir de XML-JATS4R por Redalyc
Proyecto académico sin fines de lucro, desarrollado bajo la iniciativa de acceso abierto

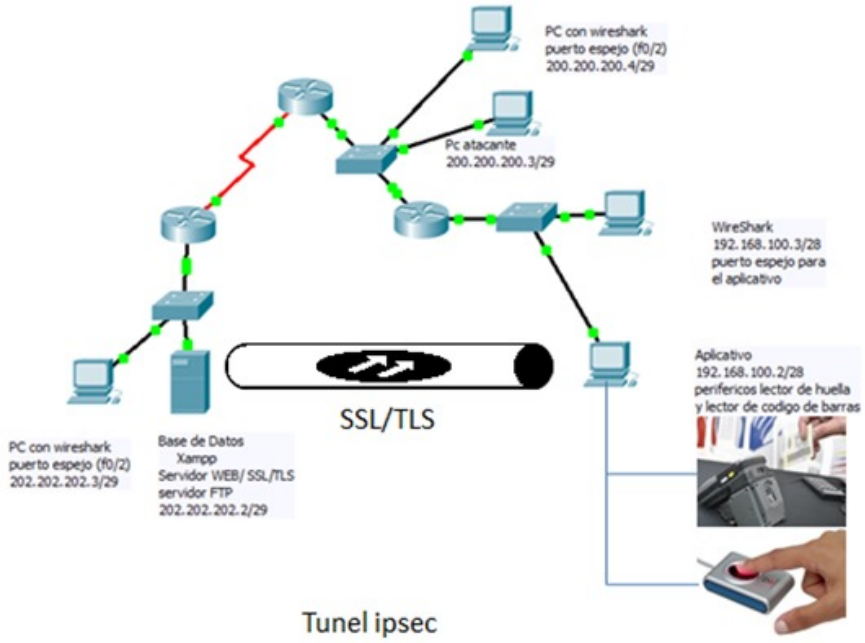

Figura 8
Escenario 2 extranet con SSL/TLS
Fuente: Autor

Se refieren las mismas variables ahora bajo el análisis del protocolo SSL/TLS (ver tabla 4) con sus promedios arrojando lo siguiente:

PDF generado a partir de XML-JATS4R por Redalyc
Proyecto académico sin fines de lucro, desarrollado bajo la iniciativa de acceso abierto

Tabla 4
Extranet con SSL/TLS

ESC 3 extranet con SSL/TLS	DoS	DDoS	MITM	Sin Ataque
Tiempo ENVIO	26	30	29	36
Paquetes enviados PC1	250	248	200	242
Paquetes Recibidos BD	72876	122059	176	245
Bytes PC1	62385	62385	73045	62385
Bytes BD	3929692	4028534	76201	63889
% Ocupación canal PC1	0,0259	0,0259	0,0188	0,0227
% Ocupación canal BD	66,1	86	0,0193	0,021
% Procesamiento PC1	1,9	1,9	4,4	2,9
% Procesamiento BD	68,5	68,1	4,8	4,1
% Disponibilidad del canal	33,9	14	99,98	99,98
Archivos	1,2,3	1,2,3	1,2,3	1,2,3
Atacantes	1,5,10	1,5,10	1,5,10	1,5,10

Fuente: Autor.

Durante esta prueba los paquetes aumentan de tamaño en relación a los enviados por el ataque pero el sistema de votación se mantiene lento garantizando él envió de los datos. El procesamiento en la base de datos aumenta disminuyendo la disponibilidad del canal para el ataque de DoS a 33,9%, para DDoS a 14%, y para MITM a 99,98%. (Tabla 4 y Figura 9). Si el ataque permanece más de 7 minutos para DDoS satura el canal y el procesamiento de la base de datos.

PDF generado a partir de XML-JATS4R por Redalyc
Proyecto académico sin fines de lucro, desarrollado bajo la iniciativa de acceso abierto

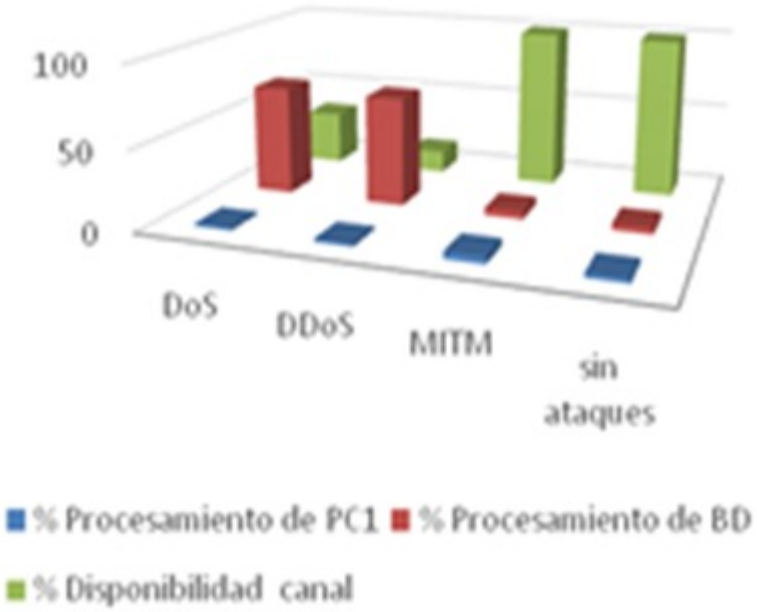

Figura 9
Cantidad de paquetes
Fuente: Autor

3.1.3 Pruebas escenario 2 extranet con IPSEC

Durante la prueba se crea una red privada virtual con parámetros de autenticación, encriptamiento y seguridad con listas de control de acceso y otros parámetros propios de IPSEC en modo túnel con AH. Con las mismas variables bajo IPSEC (ver tabla 5) así:

PDF generado a partir de XML-JATS4R por Redalyc
Proyecto académico sin fines de lucro, desarrollado bajo la iniciativa de acceso abierto

Tabla 5
Escenario 3 con IPSEC

ESCENARIO 3 CON IPSEC	DoS	DDoS	MITM	Sin Ataque
Tiempo ENVIO	22	24	31	35
Paquetes enviados PC1	270	282	263	239
Paquetes Recibidos BD	86675	86674	272	245
Bytes PC1	62385	63841	66559	62385
Bytes BD	4096875	4377308	80620	63889
% Ocupación del canal PC1	0,0402	0,0402	0,0188	0,0227
% Ocupación canal BD	72,3	74,3	0,0193	0,021
% Procesamiento PC1	4,4	4,4	4,4	2,9
% Procesamiento BD	74,9	75,4	4,8	4,1
% Disponibilidad del canal	27,7	25,7	99,98	99,98
Archivos	1,2,3	1,2,3	1,2,3	1,2,3
Atacantes	1,5,10	1,5,10	1,5,10	1,5,10

Fuente: Autor

En esta fase se crea un túnel entre el puesto de votación y el data center se ubica el atacante dentro del sistema congestionando y limitando la disponibilidad del canal para DoS a 27,7% para DDoS a 25,7% y para hombre en el medio MITM a 99,98%. (Figura 10).

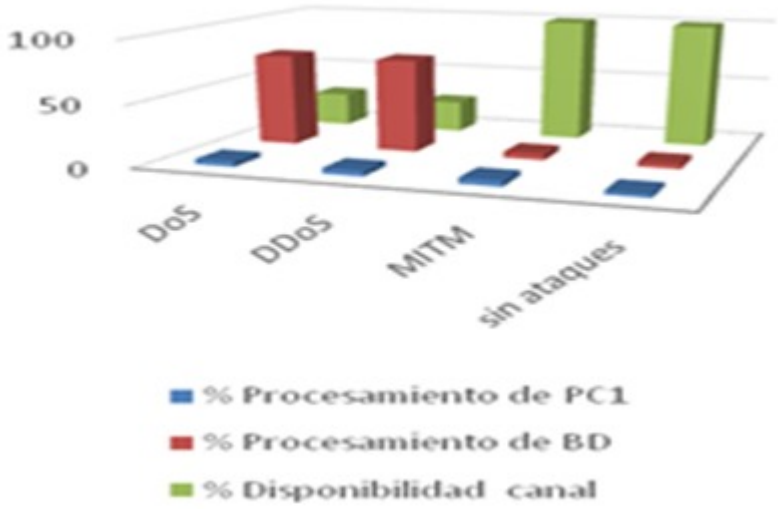

Figura 10
Procesamiento y disponibilidad del canal
Fuente: Autor

PDF generado a partir de XML-JATS4R por Redalyc
Proyecto académico sin fines de lucro, desarrollado bajo la iniciativa de acceso abierto

El atacante en la trayectoria no congestiona el canal, ni el procesamiento, solo ve las direcciones IP del túnel (Figura 11).

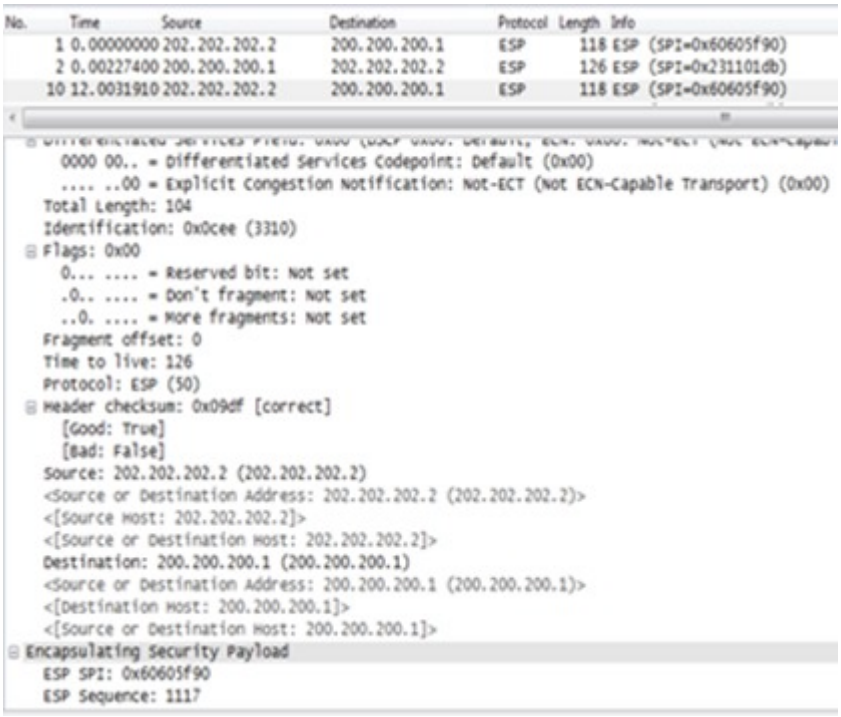

Figura 11
Visualización túnel
Fuente: Autor

Propuesta: finalmente se configura parametros adicionales de seguridad con mejores condiciones comparandola con los anteriores asi: Durante esta fase no se valoran los escenarios con ataques porque es dificil que el atacante conozca los criterios basicos para hacerlo como: no conocer las IP de origen y destino, el tunel se crea entre el dispositivo de origen y la base de datos de destino y a pesar que el atacante pueda capturar el trafico, por politicas de seguridad configuradas en los dispositivos intermedios como routers y switches no tiene interconexion con los mismos debido a los protocolos SSL/TLS y sus algoritmos protegen el aplicativo hasta el dispositivo intermedio en un extremo y desde el router de borde que conecta a internet con IPSEC llevando la información segura a la base de datos.

Se comparo por escenario durante el envio con SSL/TLS e IPSEC se carga mayor trafico (Figura 12) que en los demas escenarios debido a las politicas de encapsulamiento.

PDF generado a partir de XML-JATS4R por Redalyc
Proyecto académico sin fines de lucro, desarrollado bajo la iniciativa de acceso abierto

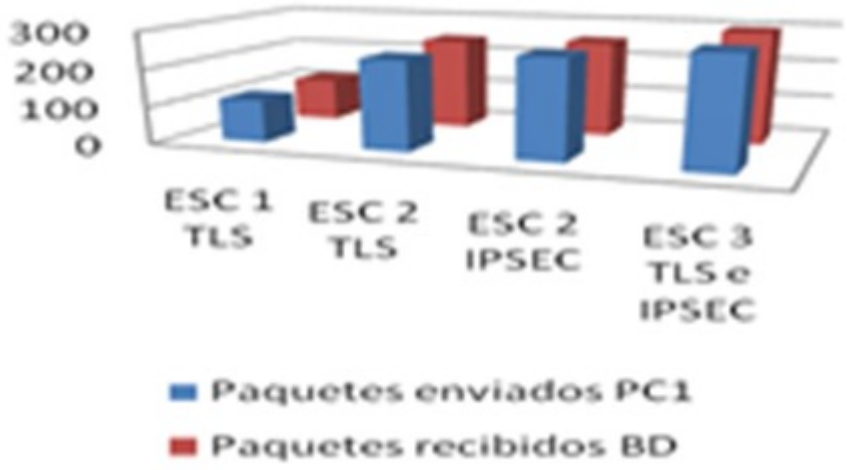

Figura 12
Paquetes Enviados
Fuente: Autor

Tabla 6
Comparativo por escenarios

Escenario Propuesto	ESC 1 TLS	ESC 2 TLS	ESC 2 IPSEC	ESC 3 TLS e IPSEC
Tiempo	26	35	20	38
Paquetes enviados PC1	114	239	263	290
Paquetes Recibidos BD	114	245	255	297
% Ocupación del canal PC1	2,4	1,227	1,227	2,3124
% Ocupación del canal BD	2,3	1,021	1,021	3,7
% Procesamiento en PC1	5,2	2,9	5,1	8
% Procesamiento en BD	6,1	4,1	6,4	6
% Disponibilidad del canal	97,7	99,977	99,97	96,3

Fuente: Autor.

Referente a la ocupación del canal durante el envio de datos no es relevante aunque operan los dos protocolos de seguridad SSL/TLS e IPSEC el consumo de ancho de banda disponible es del 96,3% (Figura 13).

PDF generado a partir de XML-JATS4R por Redalyc
Proyecto académico sin fines de lucro, desarrollado bajo la iniciativa de acceso abierto

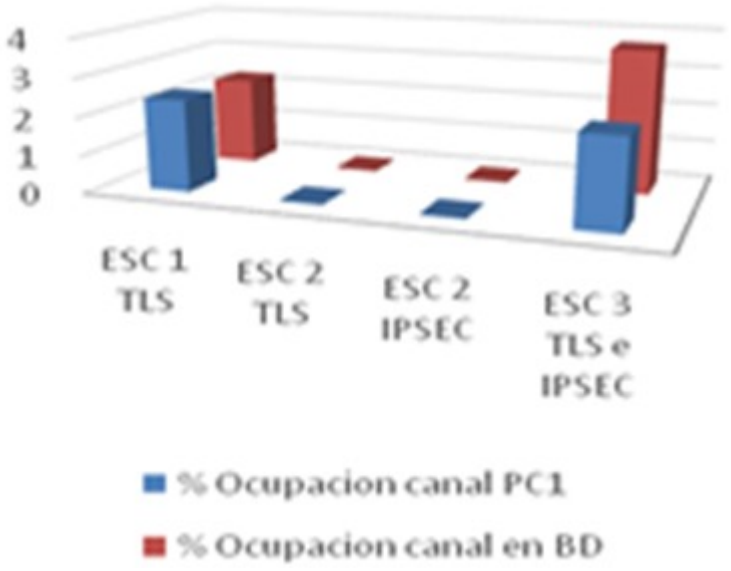

Figura 13
Ocupación del canal
Fuente: Autor

4. CONCLUSIONES

La seguridad en el acceso físico o remoto hacia los datos en sistemas de votación electrónico son fundamentales en todo proceso electoral, las nuevas posibilidades que ofrecen las telecomunicaciones y dispositivos bajo ambientes TIC fortalecen, dan confianza y transparencia a la democracia con ayuda de la tecnología; hoy existen usuarios maliciosos que pueden identificar y visualizar fácilmente el tráfico y redirigirlo, introducir paquetes falsos, modificarlos, diseñar diferentes tipos de ataques; esta investigación fortalece procesos electorales en las fases de identificación física del elector y la transmisión de los datos, y asegura la trayectoria de los mismos de manera fiable mediante los protocolos SSL/TLS entre el origen y destino hacia la intranet y se integra con el protocolo IPSEC para la protección hacia la extranet minimizando errores comunes de todo proceso electoral en cuanto a identificación de electores, y las transmisiones voz a voz.

También se revisan aspectos técnicos y de seguridad de un sistema de votación electrónico específico para el contexto colombiano que implica la confiabilidad del sistema además de permitir validar el proceso de identificación del ciudadano, el acto del voto, el escrutinio y la transmisión de los datos con características biométricas integradas en uno solo. Por ser una herramienta que integra software y hardware permite su implementación en diferentes fases del proceso electoral. Finalmente, este mecanismo puede ser tan seguro o incluso más seguro que el voto tradicional en papel ya que identifica el votante en un 90% por medio de lectores biométricos y garantía de transmisión en un 90% con algoritmos criptográficos fuertes usando circuitos virtuales por donde viajan los datos. Es una solución real pero no suficiente para garantizar los requisitos

PDF generado a partir de XML-JATS4R por Redalyc
Proyecto académico sin fines de lucro, desarrollado bajo la iniciativa de acceso abierto

de seguridad específicos en el contexto colombiano. a pesar de ello se debe plantear dar por terminada la etapa de pruebas piloto y empezar a usar el voto electrónico de forma vinculante, paralelo al sistema tradicional.

4.1 Trabajos futuros

Se recomienda la aplicación de nuevos algoritmos de seguridad como HSTS que permitan mejorar la confianza de los votantes en la integridad del proceso electoral de un país. Por lo tanto, las nuevas tecnologías si se planifican y diseñan perfectamente minimizan muchas de las preocupaciones de los sistemas electorales tradicionales.

REFERENCIAS

[1] C. Suarez, "El voto electrónico en Colombia: análisis de viabilidad de su implementación", 2014.

[2] L. F. Cepeda, "Implicaciones de la adopción del voto electrónico en Colombia", Departamento Nacional de Planeación, 2003. Disponible en: https://colaboracion.dnp.gov.co/CDT/Justicia%20Seguridad%20y%20Gobierno/Trabajo%20voto%20%20electr%C3%B3nico%20final.pdf

[3] V. M. Morales, "Seguridad en los procesos de voto electrónico: registro, votación, consolidación de resultados y auditoria", Universidad politécnica de Cataluña, 2009.

[4] S. Kremer, and M. Ryan, "Analysis of an electronic voting protocol in the applied pi calculus. In Programming Languages and Systems", Springer Berlin Heidelberg 2005. pp. 186-200.

[5] R. Sehr, U.S. Patent No. 5,875,432. Washington, DC: U.S. Patent and Trade Office. 1999.

[6] G. Regivaldo, A. Santin, and C. Maziero. A Three iBalloti Based Secure Electronic Voting System. IEEE security &privacy, 2008-3, pp.14-21.

[7] R. Glauss, Patent No. 6,553,494. Washington, DC: U.S. Patent and Trade Office. 2003.

[8] S. Hof, "E-Voting and Biometric Systems. En Electronic Voting in Europe", Technology, Law, Politics and Society 2004. p. 63-72.

[9] M. Oostveen, and b. Van den, "Security as belief: user's perceptions on the security of electronic voting systems. Electronic voting in Europe", Technology, law, politics and society, 47, 2004. Pp. 73-82.

[10] A. Jorba, and J. Roca, "Secure remote electronic voting system and cryptographic protocols and computer programs employed." U.S. Patent No. 7,260,552. 21 Aug. 2007.

[11] N. Hoffman, and p. Lapsley. U.S. Patent No. 7,613,659. Washington, DC: U.S. Patent and Trade Office. 2009.

[12] P. Pesado, A. Pasini, E. Ibáñez, et. al, "E-government: el voto electrónico sobre Internet". In XIV Congreso argentino de ciencias de la Computación. 2008

PDF generado a partir de XML-JATS4R por Redalyc
Proyecto académico sin fines de lucro, desarrollado bajo la iniciativa de acceso abierto

[13] J. Xu, and C. Shen-meng, "Comparison and analysis of Ipsec-based and SSL-based VPN [J]." Computer Engineering and Design, 2004, vol. 4, p. 586-588.

[14] O. Adebayo, D. Ugiomoh, and M. AbdulMalik, "The Design and Development of Real-Time E-Voting System in Nigeria with Emphasis on Security and Result Veracity." International Journal of Computer Network and Information Security 5.5 2013. vol. 5, no 5, p. 9.

[15] J. M. Huidobro, "RFID. Etiquetas Inteligentes". BIT Digital, (146), 2004.

[16] J. Pomares, I. Levin, R. Álvarez, G. Mirau, et al. "From piloting to roll-out: voting experience and trust in the first full e-election in argentina." En Electronic Voting: Verifying the Vote (EVOTE), 2014 6th International Conference on. IEEE, 2014. pp. 1-10.

[17] G. Aguilar, G. Sánchez, k. Toscano, M. Nakano, M, et al, "Reconocimiento de Huellas Dactilares Usando Características Locales". Revista Facultad de Ingeniería, (46), 2013. pp. 101-109.

[18] R. Espinosa, G. Morales, "Una arquitectura de seguridad para IP." (2007). Sección de Computación. 2006. México, D.F.

[19] P. Tripathi, S. Niraj, "Overview of Security Protocol for Network Layer." Journal of Android, IOS Development and Testing, 2017, vol. 1, no 3.

[20] D. Chung, M. Bishop, S. Peisert. "Distributed Helios-Mitigating Denial of Service Attacks in Online Voting". 2016.

[21] D. Harkins, and D. carrel. The Internet Key Exchange. RFC 2409.

[22] S. Kent and R. Atkinson. IP Authentication Header. RFC 2402.

[23] S. Kent and R. Atkinson. IP Encapsulating Security Payload (ESP). RFC 2406.

[24] S. Pérez, "Análisis del protocolo Ipsec: el estándar de seguridad en IP". Telefónica Investigación y Desarrollo 2008.

[25] S. Kent and R. Atkinson: Security Architecture for the Internet Protocol. RFC 2401.

[26] T. Dierks and C. Allen. The TLS Protocol Ver. 1.0.

[27] M. Riffo. "Vulnerabilidades de las redes TCP/IP y principales mecanismos de seguridad". Chile. 2009.

[28] J. Aguilar, J. Castellanos. "Estándares para Cloud Computing: estado del arte y análisis de protocolos para varias nubes". Puente, 2017, vol. 9, no 2, p. 33-40.

[29] N. Prakash, and N. Venkatram, "Establishing efficient security scheme in home IOT devices through biometric finger print technique". Indian Journal of Science and Technology, 2016, vol. 9, no 17.

[30] J. Alegretti, "Aplicación Actual de los Sistemas Biométricos". Revista Skopein, 2014, vol. 1, no 5.

[31] F. Tola, and D. Elizabeth. "Implementación de un Sistema de Gestión de Seguridad de la Información para una empresa de consultoría y auditoría, aplicando la norma ISO/IEC 27001", 2015.

[32] C. González, J. Madrigal, et. al. "Diseño de un sistema biométrico de identificación usando sensores capacitivos para huellas dactilares". Revista Facultad de Ingeniería, 2014, no 39, p. 21-32.

[33] P. Hernández, "Diseño e implementación de un sistema de asistencia basado en RFID". 2012.

PDF generado a partir de XML-JATS4R por Redalyc
Proyecto académico sin fines de lucro, desarrollado bajo la iniciativa de acceso abierto

[34] C. Medina, "RFID vs. Código de barras, procesos, funcionamiento y descripción". 2009.

[35] L. González, et al. "Seguridad en Redes Sociales: problemas, tendencias y retos futuros." 2014.

[36] P. Rodríguez, "Implementación de un prototipo de laboratorio para el estudio de ataques de seguridad en redes". Doctoral dissertation, Quito, 2016.

[37] L. Fandiño, et al. "Análisis de los alcances y limitaciones de la implementación del voto electrónico en América Latina, lecciones para Colombia". 2013. Doctoral dissertation, Universidad del Rosario.

[38] J. Thompson, "Algunas notas acerca del uso de la tecnología y del voto electrónico en la experiencia electoral de América Latina". Revista IIDH, 2013, no 58, p. 101-130.

[39] N. Goodman, and J. Pammett, "The patchwork of internet voting in Canada. In Electronic Voting: Verifying the Vote (EVOTE)", 2014 6th International Conference on (pp. 1-6). IEEE.

[40] S. Heiberg, and J. Willemson, "Verifiable internet voting in Estonia. In Electronic Voting: Verifying the Vote (EVOTE)", 2014. 6th International Conference on (pp. 1-8). IEEE.

[41] J. Chungata, E. López, and O. Granizo. "Confiabilidad y consideraciones del voto electrónico, una visión global." Journal of Science and Research: Revista Ciencia e Investigación 2.5 (2017): 26-38.

[42] L. Macías, and R. Alejandro. "Sistema de votación electrónico con mecanismo biométrico de autentificación para las elecciones de dignidades de la Pontificia Universidad Católica Del Ecuador Sede Esmeraldas (PUCESE)". Diss. Ecuador-PUCESE-Escuela de Sistemas y Computación, 2016.

[43] M. Montes, D. Penazzi, and N. Wolovick. "Consideraciones sobre el voto electrónico." X Simposio de Informática en el Estado (SIE 2016)-JAIIO 45. 2016.

[44] R. Araújo, et al. "Remote Electronic Voting Can Be Efficient, Verifiable and Coercion-Resistant." International Conference on Financial Cryptography and Data Security. Springer Berlin Heidelberg, 2016.

[45] K, Ranjitha, et al. "Biometric Based Secured Electronic Voting System." Biometrics and Bioinformatics 8.5 (2016), pp. 107-112.

[46] K. Gjosteen, and S. Anders. "An experiment on the security of the norwegian electronic voting protocol." Annals of Telecommunications 71.7-8 (2016), pp. 299-307.

PDF generado a partir de XML-JATS4R por Redalyc
Proyecto académico sin fines de lucro, desarrollado bajo la iniciativa de acceso abierto