UNIVERSIDAD SAN FRANCISCO DE QUITO

COLEGIO POLITECNICO

Estudio de factibilidad de la seguridad para voto electrónico

Juan Pablo Atiaga Oleas

Tesis de grado presentada como requisito para la obtención del título de Ingeniero de Sistemas

Quito

Julio de 2008

UNIVERSIDAD SAN FRANCISCO DE QUITO

Hoja de aprobación de Tesis

Estudio de factibilidad de la seguridad para voto electrónico

Juan Pablo Atiaga Oleas

Fausto Pasmay, M.S. ……

Director de Tesis

Vinicio Carrera, Ph.D ……

Miembro del Comité de Tesis

Fernando Romo, M.S. ……

Decano del Colegio Politécnico

Quito, Julio de 2008

© Derechos de autor

Juan Pablo Atiaga Oleas

2008

Dedicatoria

A todos los ecuatorianos.

Resumen

Este proyecto denominado “Estudio de factibilidad de la seguridad para voto electrónico” es un estudio que determina la posibilidad de aplicar las directrices de seguridad para la elaboración de sistemas de votación del estándar VVSG 2007 en el sistema de elecciones llamado mivoto.com.ec (también llamado votoecuador.com). El estudio consiste en analizar 57 directrices del estándar VVSG 2007 correspondientes a los servicios de seguridad: integridad, confidencialidad, autentificación y no repudiación. El análisis de las directrices mencionadas determinará si el sistema cumple actualmente con esas directrices; en caso de no cumplirlas se realizarán recomendaciones de posibles acciones para hacer que el sistema cumpla con ellas. Posteriormente se mejorará el sistema de elecciones con las recomendaciones establecidas en el análisis de las directrices del estándar VVSG que son posibles de implementar en el costo y tiempo establecido para este proyecto. Finalmente se realizará una implementación de prueba del sistema en un ambiente controlado para poder evaluar el cumplimiento de las directrices del estándar basado en el análisis antes realizado.

Abstract

This project, called “Feasibility study for electronic voting security” is a study that determines the possibility of applying the VVSG 2007 security standard guidelines for developing of voting systems in the voting system called mivoto.com.ec (also called votoecuador.com). This study is made of the analysis of 57 guidelines from the VVSG 2007 standard classified in the following security services: integrity, confidentiality, authentication and non-repudiation. The analysis of those guidelines will determine if the system currently complies with them; if it does not comply, recommendations on how to accomplish compliance will be made. Following that, the voting system will be improved using the recommendations made in the VVSG 2007 analysis that are possible to implement in the cost and time established for this project. Finally, a test implementation will be performed in a controlled environment for later determining the compliance of the VVSG 2007 guidelines based on the previously performed analysis.

Tabla de contenido

Índice de figuras

Reglas y convenciones para el uso de la tesis

Se incluyen los siguientes archivos como parte de esta tesis, que corresponden a los registros e historiales generados en la implementación de prueba. La descripción de los archivos se encuentra en la parte 5: Análisis de la implementación de prueba.

- application.log
- application.log.sign
- boot.msg
- boot.msg.sign
- electores.html
- electores.html.sign
- EMS TSCR.txt
- EMS TSCR.sign
- firewall
- firewall.sign
- messages
- messages.sign
- rs_referendum.html
- rs_referendum.html.sign
- TSC.txt
- TSC.txt.sign
- votos.html
- votos.html.sign
- warn
- warn.sign

Además se incluye el siguiente archivo, que corresponde a la base de llaves (keystore) que contiene la llave necesaria para comprobar las firmas digitales de los registros e historiales:

- votoecuador.com.key

También se incluye el documento “Voluntary Voting System Guidelines Recommendations to the Election Assistance Commission”, elaborado por Technical Guidelines Development Committee (TGDC). Este documento contiene las directrices VVSG 2007 sobre las cuales se elaboró esta tesis. El archivo de ese documento es: Final-TGDC-VVSG-08312007.pdf

Las directrices VVSG 2007 fueron elaboradas en inglés, sin embargo, se requiere que este documento de tesis sea escrito en español; por esta razón se han traducido las directrices que se analizaron. Debido a que la traducción puede cambiar el significado de los requerimientos, la mejor manera de entender las directrices es leerlas en su idioma original.

Muchas de las directrices VVSG 2007 incluyen un texto de discusión, el cual aporta información valiosa para aclarar el requerimiento. Se recomienda leer las discusiones de las directrices para entenderlas mejor.

Capítulo 1 – Antecedentes

1.1 Introducción

En el año 2006 se creó el sistema de elecciones por Internet llamado mivoto.com.ec. Uno de los objetivos de este sistema fue el utilizar el mejor nivel de seguridad posible. Por esta razón se utilizaron técnicas de programación, aplicaciones y ambientes de implementación que se consideraron seguros, como el uso de J2EE, Enterprise Java Beans, el desarrollo utilizando Oracle Database Release 2 Enterprise Edition y Oracle Toplink, Linux y SSL.

Para tener un nivel de seguridad que promueva confianza entre usuarios y organizaciones responsables de las elecciones no basta con utilizar elementos que se consideraron seguros. Por esta razón se buscó un estándar, VVSG 2007, que se pueda aplicar a sistemas de elecciones para asegurar que el diseño de este sistema cumple con dicho estándar y, de ser necesario, modificar el sistema y establecer recomendaciones para lograr que el sistema cumpla con el estándar.

1.2 Problemas de las elecciones actuales

Entre los problemas del actual proceso de elecciones están: costo, falta de transparencia, inexactitud e ineficiencia.

La transparencia no puede ser garantizada cuando:

- Físicamente no es posible controlar todas las juntas receptoras del voto.

- Durante el proceso de conteo de votos, la información pasa por muchas personas.
- Las urnas y actas pudieran ser saboteadas.

La exactitud no puede ser garantizada cuando:

- Los humanos cometen errores (especialmente en el conteo y paso de información).
- Por problemas causados por el proceso de elecciones no se puede votar por candidato, sino por lista, obligando a usar métodos de conteo inexactos.

La eficiencia no puede ser garantizada cuando:

- Hay demasiados pasos en el proceso de escrutinio.
- Se necesitan semanas o meses para preparar una elección; en esto está principalmente el tiempo de impresión y traslado de papeletas de votación.
- El escrutinio demora días o semanas.

1.3 Costo de las elecciones

Uno de los grandes motivadores del voto electrónico es la posibilidad de reducir el costo de las elecciones. Para las elecciones del año 2006 el Tribunal Supremo Electoral solicitó un presupuesto de 37,5 millones de dólares ("El proceso electoral costará…", n.p.). Dos de los principales rubros dentro de las elecciones que

el voto electrónico puede reducir drásticamente son: la impresión de papeletas y los gastos operativos.

Para impresión de papeletas electorales para la elección de asambleístas en el año 2007 se destinaron 3,2 millones de dólares ("TSE aprobó el diseño de las papeletas electorales", n.p.). El voto electrónico puede suprimir la necesidad de papeletas, pues las elecciones se pueden mostrar en una pantalla en lugar de en un papel impreso. Además, cada elección requiere la impresión de nuevas papeletas (es decir, repetir este millonario gasto en cada elección), lo cual no es necesario con un sistema de voto electrónico que permita diseñar las pantallas para selección de candidatos sin que sea necesario comprar un nuevo sistema para cada elección.

Los gastos operativos de las elecciones del año 2006 en el Ecuador tuvieron dentro del presupuesto 14 millones de dólares; estos gastos incluyen la logística y la contratación de alrededor de 7000 personas ("El proceso electoral costará…", n.p.). El voto electrónico puede desarrollar un sistema cuya ejecución sea más simple, sin la necesidad de contratar a tantas personas y el traslado y manipulación del material electoral. Por ejemplo, un sistema de elecciones que funcione a través de Internet envía y recibe toda la información desde un servidor central; de esta manera se elimina una gran parte de los costos de logística además de que el servidor ejecutará todo el trabajo de recepción del voto y conteo, sin que se necesite pagar a 7000 personas para que ejecuten estas tareas.

Capítulo 2 – Marco teórico

2.1 Voto electrónico (e-vote)

El voto electrónico, o e-vote por su nombre en inglés (electronic vote) es, en términos generales, el uso de equipos electrónicos en el proceso de elecciones.

Existe una gran cantidad de tecnologías disponibles, las cuales se pueden aplicar de distintas maneras y en conjunto con otras tecnologías para el proceso de elecciones.

El uso de tecnología en las elecciones debe tener como objetivo mejorar las elecciones. No se trata de introducir la tecnología por el simple hecho de ser modernos, sino de utilizar la tecnología para solucionar los problemas actuales de las elecciones.

La tecnología puede complementar o reemplazar una o más partes del proceso de elecciones, el cual básicamente se compone de tres partes:

Registro de los electores

El sistema, sea manual o automático, debe poder autentificar al elector; para esto se debe definir quiénes son aptos para votar y se los debe registrar como electores autorizados. En el Ecuador son electores autorizados todos los ecuatorianos mayores de edad y en goce de los derechos de ciudadanía.

Voto

El elector se autentifica con la autoridad, sea una persona o máquina, y realiza su voto. El elector debe poder votar si está registrado y solo debe poder votar una vez.

Conteo de los votos

Los votos de todos los electores se someten a conteo para determinar el o los ganadores de la elección.

El proceso descrito anteriormente está simplificado para representar a cualquier elección. El proceso completo de elecciones es mucho más amplio, involucra a más actores y depende de los reglamentos, procedimientos y más características únicas de cada elección.

La tecnología puede cambiar cualquiera de las partes del proceso antes mencionado independientemente de las otras partes o en conjunto.

1. Ejemplo de registro de electores electrónico:

Los electores se inscriben en una base de datos a través de terminales que introducen esta información. Las listas de electores se pueden imprimir o ser consultadas por las autoridades para autorizar a los electores para votar.

2. Ejemplo de voto electrónico:

Una vez que el elector es autentificado por la autoridad, éste inscribe su voto en una urna electrónica que imprime su voto en papel. El papel con el voto del elector es posteriormente ingresado en una urna para el conteo.

3. Ejemplo de conteo electrónico:

El voto puede ser recibido en hojas especiales donde el elector marca con un lápiz su voto. Luego, lectores de este tipo de hojas cuentan automáticamente los votos, leyendo la marca que el elector realizó.

Una solución que abarca las tres partes del proceso puede ser una aplicación Web. Esta aplicación contiene una base de datos en donde se inscriben a los electores. Los electores votan por medio de una página Web y su voto se registra en la base de datos. El conteo se realiza en la misma base de datos.

2.2 Voluntary Voting System Guidelines

La organización National Institute of Standards and Technology (NIST) de Estados Unidos es participa en el programa Help America Vote Act (HAVA).

HAVA es la ley 107-252 de Estados Unidos cuyo propósito es “establecer un programa para proveer fondos a los Estados para reemplazar los sistemas de tarjetas perforadas, establecer el U.S. Election Assistance Commission (EAC) para asistir en la administración de elecciones Federales y para de otra manera proveer asistencia con la administración de ciertas leyes y programas Federales de

elecciones, establecer estándares mínimos de administración de elecciones para los Estados y unidades de gobierno local con responsabilidad en la administración de elecciones Federales, y para otros propósitos." ("NIST and the Help America Vote Act of 2002", n.p.)

El rol de NIST en este programa es mejorar los sistemas de votación en los Estados Unidos, creando un conjunto de recomendaciones que los fabricantes deben seguir en la elaboración de sistemas de votación y que los equipos de pruebas y auditoría pueden seguir para revisar dichos sistemas.

Technical Guidelines Development Comité (TGDC) es la división de NIST que se encarga de de crear los estándares técnicos. TGDC creó el estándar Voluntary Voting System Guidelines (VVSG). VVSG es un conjunto de directrices voluntarias.

La razón por la que las directrices VVSG son voluntarias es porque en Estados Unidos el gobierno Federal no puede imponer criterios generales en las elecciones. Cada estado tiene sus propias leyes y decide qué es obligatorio en cuanto a sistemas de votación. De todas maneras, VVSG se ha vuelto una norma en varios estados que han acogido sus directrices voluntariamente y las han hecho obligatorias en su territorio.

VVSG es un estándar que ha evolucionado en los últimos años. La última versión completa del estándar es la VVSG 2005. Actualmente (febrero 2008) hay una nueva versión del estándar que no es definitiva, pero que está abierta al público. Estas nuevas directrices han sido propuestas al Election Assistance Commission

(EAC) para su revisión. Las directrices que fueron enviadas a EAC el 4 de septiembre del 2007 aún no han sido aprobadas como una versión final ni tampoco han sido tampoco devueltas a revisión a NIST.

Los requerimientos del estándar VVSG están clasificados en tres categorías:

- Parte 1, requerimientos para equipos: requerimientos específicos para equipos de elecciones.
- Parte 2, requerimientos de documentación: requerimientos para la documentación realizada por los constructores de los equipos y los laboratorios de prueba.
- Parte 3, requerimientos de pruebas: información y requerimientos de las pruebas; cómo probarán los laboratorios de pruebas; los tipos de pruebas que serán utilizadas para probar la conformidad con los requerimientos de las partes 1 y 2.

(TGDC, 4 – 5)

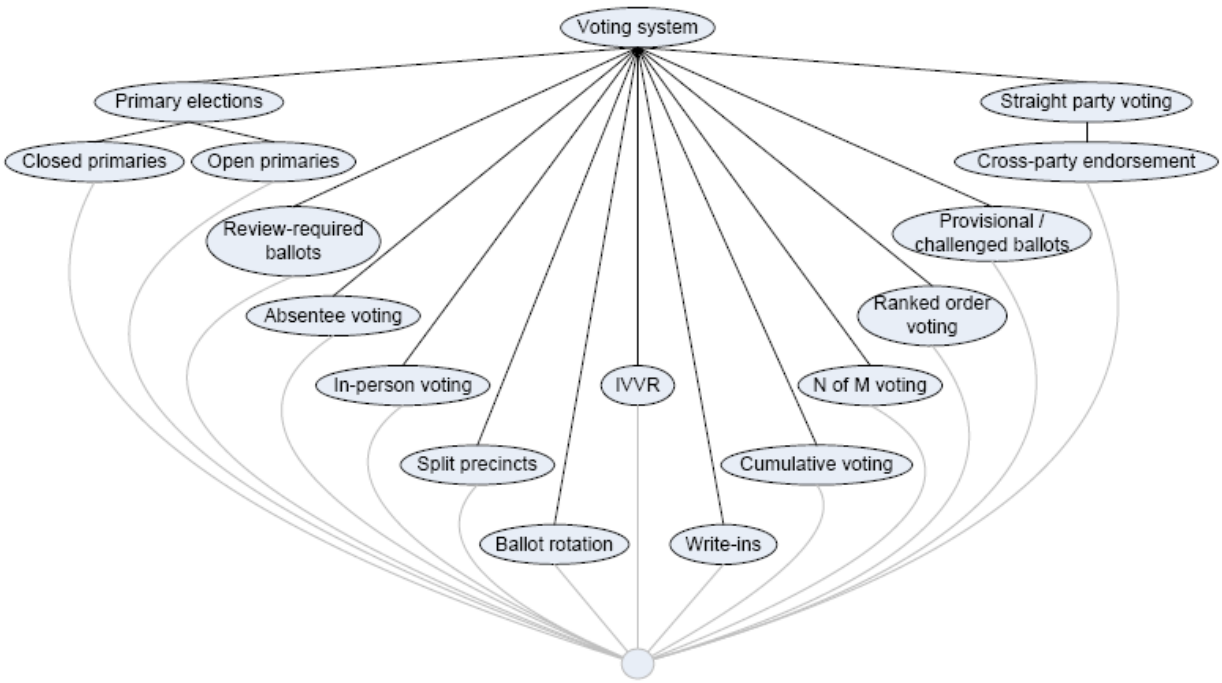
Los requerimientos de VVSG pueden ser de cuatro tipos:

- SHALL: Es obligatorio hacer algo.
- IS PROHIBITED: Es obligatorio no hacer algo.
- SHOULD, IS ENCOURAGED: Una acción opcional, recomendada.
- MAY: Una acción opcional, permisible.

En VVSG se separa a los sistemas de votación de los dispositivos de votación. El sistema es en conjunto la solución de elecciones; un dispositivo es el equipo con el cual los usuarios votan, y es parte del sistema de votación.

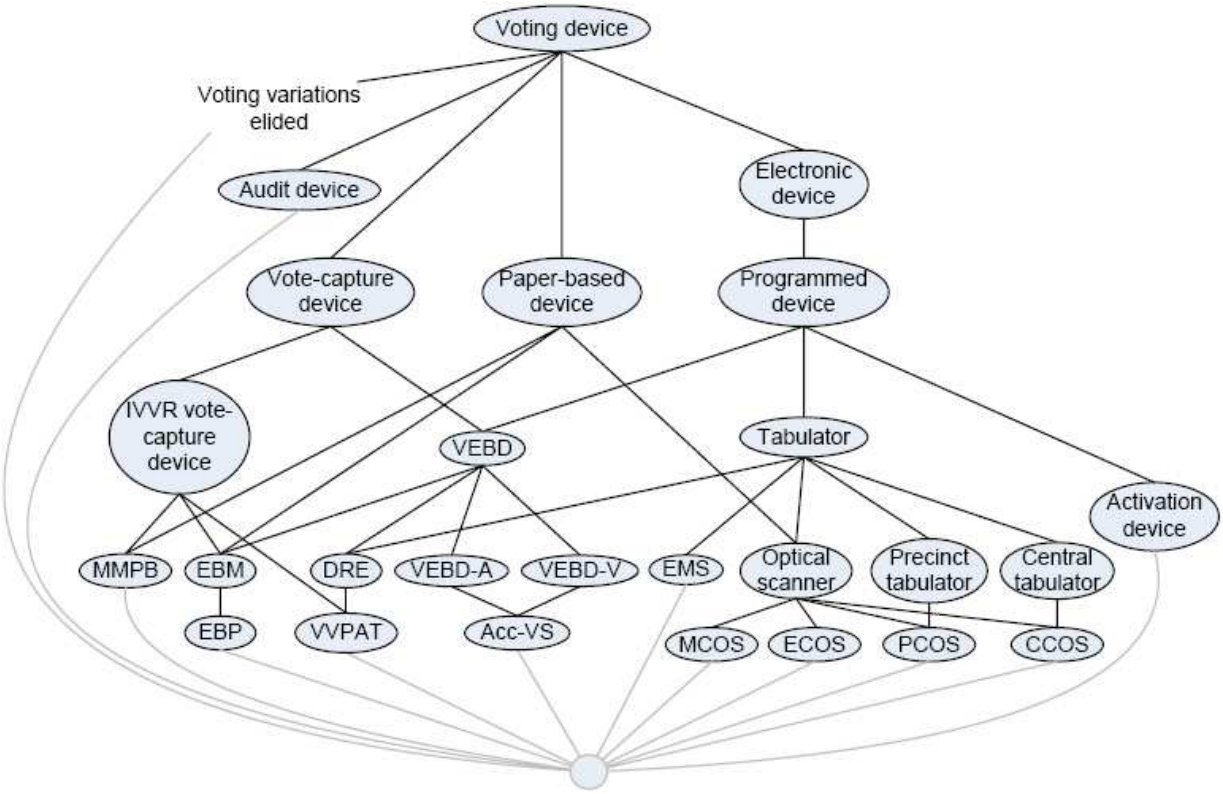
Tanto los sistemas de votación como los dispositivos de votación están separados en clases, las cuales tienen relaciones de jerarquía y herencia. La clase superior de sistemas de votación es Voting System. La clase superior de dispositivos de votación es Voting Device.

Sistemas de votación:



(TGDC, 90)

Dispositivos de votación:



(TGDC, 89)

2.3 mivoto.com.ec (votoecuador.com)

mivoto.com.ec es un sistema de elecciones. Este sistema es una aplicación Web que muestra al usuario las opciones para votar en un explorador Web y le permite votar; funciona en conjunto con una base de datos que guarda los registros de electores, candidatos y votos.

Este sistema fue desarrollado por Juan Pablo Atiaga y Humberto Guarderas en el año 2006.

Entre las características de este sistema están:

- Muestra las opciones de elecciones para diferentes dignidades (papeletas) en diferentes páginas, pero en la misma sesión de votación.
- Permite, al igual que las elecciones actuales en el Ecuador, votar por un candidato, por varios (dependiendo de la dignidad), anular el voto y votar en blanco.
- Permite al usuario revisar su voto y corregirlo antes de enviarlo.
- Al igual que las elecciones actuales, muestra nombres de los candidatos, fotografías de los candidatos, nombres de los partidos políticos e imágenes de los logotipos de los partidos políticos.
- Permite imprimir sus preferencias de voto.
- Tiene autentificación de usuario.
- No permite votar más de una vez; es decir, después de que el usuario ha revisado y confirmado su voto ya no se le permite tener una nueva sesión de votación (no podrá cambiar su voto).
- Genera un código de confirmación con el cual se puede verificar que el usuario sí ha votado, pero no indica cuál fue su voto.
- Utiliza HTML simple para máxima compatibilidad.

Los detalles del desarrollo de la aplicación son los siguientes:

- Fue desarrollado en ambiente Java 2 Enterprise Edition.
- Utiliza Enterprise Java Beans.
- Utiliza Java Server Faces.
- Utiliza la base de datos Oracle Enterprise Edition 10g.
- Se utilizó Oracle JDeveloper como herramienta de desarrollo del código.
- Este sistema de elecciones se desarrolló y probó sobre un ambiente Linux 64 bits (Fedora core 4 para la aplicación, Gentoo 2005 para la base de datos), JBoss, Oracle Enterprise 10g r2.

Fue probado como usuario en ambientes Windows, Linux y Mac usando los exploradores Web Internet Explorer, Firefox y Safari.

El nombre inicial de este sistema es mivoto.com.ec; sin embargo, se utilizó el nombre votoecuador.com para la implementación de prueba ejecutada entre el 2 de julio y el 9 de julio del 2008. Ambos nombres, mivoto.com.ec y votoecuador.com, se refieren al mismo sistema y se lo utilizan por igual.

Capítulo 3 – Estudio de factibilidad

3.1 Directrices VVSG 2007 analizadas

Los requerimientos de VVSG 2007 que se analizaron, clasificados por el servicio de seguridad al cual corresponden, son:

Integridad	
Num. de requerimiento	*Título*
4.2.1-A	Sistema de votación, soporte para auditoría del padrón electoral
4.2.2-A	IVVR, soporte para auditoría manual
4.3.1-A	Se puede exportar todos los registros
4.3.1-B	Se puede imprimir todos los registros
4.3.1-C	Protección criptográfica de los registros de dispositivos de votación
4.3.2-A	Tabulador, registro de resumen de conteo
4.3.2-B	Tabulador, manejo del registro de resumen de conteo
4.3.2-C	Tabulador, registro de colección de imágenes de papeletas
4.3.2-C.1	DRE, registro de colección de imágenes de papeletas
4.3.2-C.2	Tabulador, manejo de la colección de votos emitidos
4.3.2-D	Tabulador, manejo del registro del historial de eventos y registros electrónicos
4.3.3-A	EMS registro de resumen de conteo del tabulador
4.3.3-B	EMS, registros de resumen de conteo de recintos electorales
4.3.3-C	EMS, registro de ajuste de recintos electorales
4.3.4-A	Tabulador, verificación de registros firmados
4.3.5-A	Contador de papeletas
4.3.5-B	Contador de papeletas, disponibilidad
5.5.1-A	Proteger la integridad del proceso de arranque
5.5.1-B	Verificación de integridad de los binarios antes de ejecución o carga de memoria
5.5.1-C	Aislar aplicaciones
5.5.2-A	Restringir el uso de medios removibles
5.5.3-A	Restringir las capacidades de respaldo y recuperación
Confidencialidad	
Num. de requerimiento	*Título*
3.2.3.1-A	Soporte del sistema para privacidad
3.2.3.1-A.1	Privacidad visual
3.2.3.1-A.3	Privacidad de las advertencias
3.2.3.1-A.4	Sin recibos
3.2.3.2-A	No grabación de lenguajes alternativos

3.2.3.2-B	No grabación de características de accesibilidad
4.3.3-A.1	Tabulador, combinación del reporte para privacidad
5.1.1-A	Validación del módulo criptográfico
5.1.1-B	Fortaleza criptográfica
Autentificación	
Num. de requerimiento	*Título*
5.4.1-A	Mecanismos de control de acceso
5.4.1-A.1	Control de acceso al dispositivo de votación
5.4.1-B	Control de acceso para el software y archivos
5.4.1-C	Estados de votación de control de acceso
5.4.1-E	Permisos mínimos predeterminados
5.4.3-A	Mecanismo mínimo de autentificación
5.4.3-B	Mecanismo de autentificación múltiple
5.4.3-C	Autentificación multi-factor de grupo o rol administrador
5.4.3-D	Almacenamiento seguro de los datos de autentificación
5.4.3-G	Bloqueo de cuenta
5.4.3-H	Configuración del bloqueo de cuenta
No repudiación	
Num. de requerimiento	*Título*
5.7.1-A	Requerimiento de mecanismos de registro de eventos
5.7.1-B	Requerimiento de protección de integridad
5.7.1-C	Requerimiento de privacidad del elector y confidencialidad de la papeleta
5.7.1-D	Requerimiento de registro de características de eventos
5.7.1-D.1	Requerimiento de registro del tiempo
5.7.1-D.2	Requerimiento de precisión del tiempo
5.7.1-D.3	Requerimiento de datos de fecha y hora
5.7.1-D.4	Requerimiento de cumplimiento del tiempo
5.7.1-D.5	Requerimiento de ajuste del reloj
5.7.1-D.6	Requerimiento de mínima desviación del reloj
5.7.1-E	Requerimiento de mínimos eventos registrados
5.7.1-E.1	Requerimiento de deshabilitación mínima de los historiales
5.7.3-A	Requerimiento de protección general de los historiales
5.7.3-B	Requerimiento de protección de modificación
5.7.3-C	Requerimiento de protección de archivos de historiales de eventos

Tabla 1: Directrices VVSG 2007 que se analizaron

3.2 Análisis de las directrices de integridad

4.2.1-A

Número	4.2.1-A
Título	Sistema de votación, soporte para auditoría del padrón electoral
Aplica a	Sistema de votación
Descripción	El sistema de votación DEBE soportar una auditoría

	segura del padrón electoral que pueda detectar diferencias de conteo de papeletas entre el padrón electoral, dispositivos de captura de votos, dispositivos de activación y tabuladores.

Análisis

El sistema no soporta actualmente la verificación independiente de los registros de elecciones. En el anexo 1 se detalla el análisis de la verificación independiente que permitirá cumplir con este requerimiento.

Los dispositivos de votación (computadores personales) no generan registros de elecciones; son solo clientes que acceden a la información del sistema. Toda la información está en el servidor central, eliminando el riesgo de que los dispositivos de votación u otros dispositivos generen registros de elecciones con errores (intencionales y no intencionales).

Después de implementar las funciones de verificación independiente, este sistema de elecciones podrá demostrar si se han modificado los registros de votación, como indica este requerimiento.

Resultado

El sistema deberá implementar un soporte a verificación de registros como el detallado en el anexo 1.

4.2.2-A

Número	4.2.2-A
Título	IVVR, soporte para auditoría manual
Aplica a	Sistema de votación

Descripción	El sistema de votación DEBE soportar una auditoría manual de IVVR (registro independiente verificable por el elector) que pueda detectar diferencias entre el IVVR y la papeleta electrónica

Análisis

El sistema no soporta actualmente la verificación de los registros de elecciones mediante una auditoría manual. En el anexo 1 se detalla el análisis de la verificación independiente que permitirá realizar un conteo de los votos con la flexibilidad de que se lo realice de cualquier manera que sea requerido.

Después de implementar las funciones de verificación independiente, este sistema de elecciones tendrá la capacidad de ser verificado mediante una auditoría manual, como indica este requerimiento.

Resultado

El sistema deberá implementar un soporte a verificación de registros como el detallado en el anexo 1.

4.3.1-A

Número	4.3.1-A
Título	Se puede exportar todos los registros
Aplica a	Sistema de votación
Descripción	El sistema de votación DEBE proveer la capacidad para exportar sus registros electrónicos a archivos.

Análisis

Todos los datos se almacenan en las tablas de la base de datos. La base de datos Oracle 10g Release 2 permite exportar todos los datos a archivos como parte

de la función de respaldo y recuperación. Además se pueden crear registros con la información solicitada por el organismo regulador de las elecciones y guardarla como archivos.

Resultado

El sistema cumple actualmente con este requerimiento. No se necesitan ejecutar acciones.

4.3.1-B

Número	4.3.1-B
Título	Se puede imprimir todos los registros
Aplica a	Sistema de votación
Descripción	El sistema de votación DEBE proveer la habilidad para producir versiones impresas de todos sus registros electrónicos. a. Las versiones electrónicas DEBEN retener toda la información requerida como se especifica para cada tipo de registro que no sean firmas digitales. b. La impresión PUEDE realizarse en un dispositivo diferente que el dispositivo de votación. c. Debe ser posible imprimir los registros producidos por el tabulador central e EMS en un dispositivo diferente.

Análisis

Todos los datos se almacenan en las tablas de la base de datos; por esta razón es posible generar consultas que muestren todos los datos que se necesitan.

El organismo regulador de las elecciones será quien defina cómo se deben mostrar los registros impresos. La base de datos proporciona suficiente flexibilidad para extraer los datos necesarios. Se pueden generar los registros requeridos de varias maneras; una manera es generarlos mediante una página Web dinámica que

tome los datos de la base de datos y presente el registro como sea requerido; otra manera es simplemente generar una consulta a la base de datos e imprimir el resultado en forma de tabla.

Resultado

El sistema cumple con este requerimiento. Se podría añadir un generador de registros una vez que se conozcan las características y formato que necesita el organismo regulador de las elecciones.

4.3.1-C

Número	4.3.1-C
Título	Protección criptográfica de los registros de dispositivos de votación
Aplica a	Sistema de votación
Descripción	Los registros electrónicos DEBEN ser firmados digitalmente con la ESK (llave de firma de elecciones)

Análisis

Existen varias opciones para firmar digitalmente los registros de votación.

Una manera es agregar la firma a cada valor de los registros de votación. Esta se la puede crear en una columna adicional de la tabla que contiene el registro de voto de cada elector. Por ejemplo, se toman los datos de identificación del elector, su voto y la hora de votación; con esa cadena de texto se crea un código cifrado con la llave específica para esa instancia de elecciones. De esta manera se puede saber si cada voto está intacto o ha sido modificado repitiendo el proceso de obtener la firma y comparándola con la original. Otra ventaja de esta opción es que los datos

firmados se mantienen en la base de datos y siguen siendo útiles para cualquier propósito (por ejemplo, consultas) que el organismo regulador de elecciones requiera. El proceso de agregar firmas digitales a cada uno de miles de votos y entradas en los registros es muy costoso en tiempo y ocupación del procesador, por lo que no resulta conveniente realizarlo durante las elecciones para no afectar el rendimiento de la aplicación; es mejor realizarlo inmediatamente después de las elecciones, mientras nadie ha tenido acceso al servidor.

Otra manera es crear los registros de las elecciones con la cuenta de votos, una vez que las elecciones han finalizado, y firmar digitalmente cada registro completo (no cada valor del registro). De esta manera se puede saber si cada registro está intacto, pero no cuáles valores de los registros han sido modificados. La ventaja de esta opción es que el tiempo para obtener la firma digital es mucho menor a firmar cada registro independientemente.

Ambas opciones permiten cumplir con este requerimiento. Sin embargo se debería usar la opción de firmar los registros, no los valores de los registros; eso es suficiente para cumplir con el requerimiento y no requiere un excesivo uso de procesamiento y memoria.

También se estudió la opción de utilizar el paquete de seguridad Oracle Advanced Security, el cual permite cifrar la base de datos completa. Esto proporciona la seguridad necesaria para evitar que los registros sean modificados además de aprovechar otras características de seguridad. Sin embargo, con esta opción no se cumple exactamente lo que este requerimiento pide.

Resultado

El sistema puede cumplir el requerimiento creando los registros una vez finalizadas las elecciones y firmándolos digitalmente con la llave para la elección correspondiente.

4.3.2-A

Número	4.3.2-A
Título	Tabulador, registro de resumen de conteo
Aplica a	Tabulador
Descripción	Cada tabulador DEBE producir un registro de resumen de conteo que incluya lo siguiente: a. Identificador único del dispositivo de el certificado X.509; b. Fecha y hora del registro de resumen; c. Lo siguiente, en total y dividido por configuración de papeletas y recinto electoral: 1. Número de papeletas leídas; 2. Número de papeletas contadas; 3. Número de papeletas rechazadas; y 4. Por cada N-de-M (incluyendo 1-de-M) o elección de votación acumulativa que aparezca en cualquier configuración de papeleta manejada por el tabulador: I. Número de papeletas contadas que incluyó esa elección por la definición de K(j,r,t) de Part 1:Table 8-2; II. Total de votos para cada elección no escrita por la definición de T(c,j,r,t) de Part 1:Table 8-2; III. Número de votos escritos; IV. Número de sobre-votos por la definición de O(j,r,t) en Part 1:Table 8-2; y V. Número de sub-votos por la definición de U(j,r,t) en Part 1:Table 8-2. Al producir este registro de resumen de conteo, el tabulador DEBE asumir que no se aceptan papeletas provisionales o cuestionadas.

Análisis

En este sistema de elecciones existe un solo tabulador que es el servidor que maneja la base de datos y realiza el conteo; por lo tanto se necesita un solo registro de resumen de conteo (TSC, Tabulator Summary Count).

Los datos del registro que deben existir según este requerimiento se obtendrán de la siguiente manera:

- Cuando se utilice este sistema en elecciones se adquirirá un certificado digital de una compañía de seguridad conocida (por ejemplo, VeriSign). Este certificado tiene el identificador único especificado por el nombre de la compañía que lo emite y el número de certificado.
- Se incluirá la fecha y hora del registro.
- Se contará el total de votos ingresados.
- En este sistema no hay pérdida de votos por mala lectura, pero se puede contar el número de sesiones abiertas para compararlas con el número de votos ingresados.
- Para este sistema K(j,r,t) equivale al número de votos que se registraron en el sistema para cada elección r. En este sistema todo voto que ingresó es verdadero en A(t,v) a excepción de los votos nulos (votar por más de una opción cuando solo se debe votar por una) y los votos blancos.
- Se contarán los votos de cada candidato y cada opción. T(c,j,r,t) para este sistema son todos los votos ingresados a excepción de los votos nulos y blancos.
- En este sistema no existen votos escritos (write-in). Solo se permite votar por las opciones establecidas.
- En este sistema no existen sobre-votos de la manera en que se ha votado por un candidato más de una vez. Existen los votos nulos cuando se ha votado

por más opciones de las que se debe votar. Se contarán todos los votos nulos y en blanco.

- Se contarán los votos inferiores al número de opciones que se debe elegir (undervote).

Resultado

Se generará el reporte TSC como se ha especificado en el análisis de este requerimiento.

4.3.2-B

Número	4.3.2-B
Título	Tabulador, manejo del registro de resumen de conteo
Aplica a	Tabulador
Descripción	El tabulador DEBE manejar el registro de resumen de conteo de acuerdo a lo siguiente: a. El registro DEBE ser transmitido al EMS con los demás registros electrónicos; b. DEBE ser guardado en el repositorio de las elecciones, si está disponible; y c. DEBE ser guardado en el historial de eventos del sistema de votación.

Análisis

En este sistema el tabulador y el EMS son un solo equipo; no es necesario transmitir entre la una y la otra parte.

Se deberá almacenar el registro TSC al igual que los demás registros e historiales de la manera que requiera el organismo regulador de las elecciones. Por ejemplo, para hacer el repositorio (archive) de las elecciones se podrá exportar todos

los registros a archivos y guardarlos en un medio seguro; en este repositorio se incluirá el registro TSC.

El contenido del registro TSC puede ser incluido en el historial de eventos del sistema.

Resultado

Para cumplir con este requerimiento se ejecutarán las acciones que se mencionan en el análisis.

4.3.2-C

Número	4.3.2-C
Título	Tabulador, registro de colección de imágenes de papeletas
Aplica a	Tabulador
Descripción	Los tabuladores DEBEN producir un registro de imágenes de papeletas que incluya: a. Fecha y hora de creación del registro completo de imágenes de papeletas; y b. Imágenes de papeletas registradas en orden aleatorio por el DRE para la elección. Para cada papeleta votada, esto incluye: 1. Configuración de la papeleta y contexto de conteo; 2. Si la papeleta fue aceptada o rechazada; 3. Para cada elección: I. La opción registrada, incluyendo sub-votos y votos escritos; y II. Cualquier información recolectada electrónicamente por el dispositivo de captura de voto acerca de cada voto escrito; 4. Información especificando si la papeleta es provisional, y proveyendo un identificador único para la papeleta, así como información de categoría provisional requerida para soportar el Requerimiento Part 1:7.7.2-A.6.

Análisis

Este registro se puede crear con toda la información especificada en este requerimiento. Una consulta a la base de datos que incluya la fecha y hora, el voto (o el código del elector) y el estado de ese voto (si es válido, nulo o blanco) permitiría construir el registro para cumplir con el requerimiento.

Resultado

Se puede cumplir con este requerimiento opcional si se construye un registro con los datos mencionados en el análisis.

4.3.2-C.1

Número	4.3.2-C.1
Título	DRE, registro de colección de imágenes de papeletas
Aplica a	DRE
Descripción	Los DRE DEBEN producir un registro de imágenes de papeletas que incluya: a. Fecha y hora de cierre de las elecciones; y b. Imágenes de papeletas registradas en orden aleatorio por el DRE para la elección. Para cada papeleta votada, esto incluye: 1. Configuración de la papeleta y contexto de conteo; 2. Si la papeleta fue aceptada o rechazada; 3. Para cada elección: I. La opción registrada, incluyendo sub-votos y votos escritos; y II. Cualquier información recolectada electrónicamente por el dispositivo de captura de voto acerca de cada voto escrito; 4. Información especificando si la papeleta es provisional, y proveyendo un identificador único para la papeleta, así como información de categoría provisional requerida para soportar el Requerimiento Part 1:7.7.2-A.6.

Análisis

En este sistema los dispositivos de votación son computadores personales independientes que no califican como máquinas DRE (Direct Record Electronic)

según la definición de DRE en VVSG 2007, debido a que son solo interfaces del sistema que funciona en un servidor central (EMS).

Toda la información necesaria está en el EMS y es ahí donde se creará este registro, como se indica en el análisis del requerimiento 4.3.2-C.

Resultado

El sistema cumplirá con este requerimiento creando el registro de votos indicado en el requerimiento 4.3.2-C.

4.3.2-C.2

Número	4.3.2-C.2
Título	Tabulador, manejo de la colección de votos emitidos
Aplica a	Tabulador
Descripción	Los tabuladores que producen la colección de registros de imágenes de papeletas DEBEN manejar los registros de acuerdo a lo siguiente: a. El registro depe ser transmitido al EMS con los otros registros electrónicos; b. DEBE ser guardado en el repositorio de las elecciones, si está disponible; y c. DEBE ser guardado en el historial de eventos del sistema de votación.

Análisis

En este sistema el tabulador y el EMS son la misma máquina; por esta razón no hay necesidad de transmitir registros entre ambos.

Se deberá almacenar el registro de votos al igual que los demás registros e historiales de la manera que requiera el organismo regulador de las elecciones. Por ejemplo, para hacer el repositorio (archive) de las elecciones se podrá exportar todos

los registros a archivos y guardarlos en un medio seguro; en este repositorio se incluirá el registro de votos.

El contenido del registro de votos puede ser incluido en el historial de eventos del sistema.

Resultado

Para cumplir con este requerimiento se ejecutarán las acciones que se mencionan en el análisis.

4.3.2-D

Número	4.3.2-D
Título	Tabulador, manejo del registro del historial de eventos y registros electrónicos
Aplica a	Tabulador
Descripción	El tabulador DEBE firmar digitalmente el historial de eventos, transmitir el historial de eventos firmado al EMS, y retener un registro de la transmisión.

Análisis

Este sistema no tiene tabuladores que se comuniquen con un EMS. El servidor de la base de datos es el tabulador y es parte del EMS.

El historial (log) de eventos se puede exportar y firmarlo con la llave específica para esa instancia de elecciones. Esto se debería hacer inmediatamente al terminar las elecciones.

Resultado

Al terminar las elecciones se exportará el historial de eventos a un archivo y se lo firmará digitalmente usando la llave de esa instancia de elecciones.

4.3.3-A

Número	4.3.3-A
Título	EMS registro de resumen de conteo del tabulador
Aplica a	EMS
Descripción	El registro de resumen de conteo del tabulador DEBE incluir: a. Identificadores únicos de cada tabulador contenido en el resumen; b. Para tabuladores con llaves públicas: 1. La llave pública para cada tabulador en el resumen; 2. La certificación de la ESK y registro de cierre; y 3. El registro de resumen de conteo del tabulador firmado. c. Resumen de conteo de papeletas y totales de votos por tabulador, recinto electoral y sitio de votación. 1. Los totales de los recintos electorales incluyen subtotales de cada tabulador utilizado en el recinto.

Análisis

En este sistema de elecciones existe un solo tabulador que es el servidor que maneja la base de datos y realiza el conteo; por lo tanto se necesita un solo registro de resumen de tabulador.

Los datos del registro que deben existir según este requerimiento se pueden obtener de la siguiente manera:

- Cuando se utilice este sistema en elecciones se adquirirá un certificado digital de una compañía de seguridad conocida (por ejemplo, VeriSign). Se podrá incluir toda la información de este certificado en el registro.

- El sistema tiene la capacidad de reconocer a los electores de distintas provincias, cantones y parroquias. Se pueden añadir segmentos de electores. En el registro se podrá incluir resultados de cada segmento de electores.
- Se firmará digitalmente el registro.

Resultado

Se generará el reporte de resumen del tabulador que pide este requerimiento como se especifica en el análisis.

4.3.3-B

Número	4.3.3-B
Título	EMS, registros de resumen de conteo de recintos electorales
Aplica a	EMS
Descripción	El EMS DEBE producir un reporte por cada recinto electoral incluyendo: a. Cada tabulador incluido en el recinto electoral con su identificador único; b. Número de papeletas leídas; c. Número de papeletas contadas; d. Número de CVR electrónicos rechazados; y e. Por cada elección N-de-M (incluyendo 1-de-M) o elección acumulativa que aparezca en cualquier configuración de papeleta manejada por el tabulador: 1. Número de papeletas contadas que incluyeron esa elección, por la definición K(j,r,t) en Part 1:Table 8-2; 2. Total de votos para cada opción de votación no escrita por la definición T(c,j,r,t) en Part 1:Table 8-2; y 3. Número de votos escritos.

Análisis

El sistema tiene la capacidad de reconocer a los electores de distintas provincias, cantones y parroquias. Se pueden añadir segmentos de electores; por ejemplo, recintos electorales, juntas receptoras del voto y hasta mesas de votación.

Cualquier tipo de división que sea requerida por el organismo regulador de las elecciones será considerada un recinto (precinct).

Los datos del registro que deben existir según este requerimiento se pueden obtener de la siguiente manera, para cada recinto:

- En este sistema no existen casos de que se emita un voto y no pueda ser leído. En lugar de esto se pueden contar los electores que iniciaron una sesión de voto pero no emitieron un voto.
- Se obtendrá el total de votos.
- Se obtendrán el número de votos nulos y blancos (no válidos).
- Para este sistema K(j,r,t) equivale al número de votos que se registraron en el recinto para cada elección r. En este sistema todo voto que ingresó es verdadero en A(t,v) a excepción de los votos nulos (votar por más de una opción cuando solo se debe votar por una) y los votos blancos.
- Se contarán los votos de cada candidato y cada opción. T(c,j,r,t) para este caso son todos los votos ingresados en el recinto a excepción de los votos nulos y blancos.
- No existen votos escritos (write-in) en este sistema.

Resultado

Se generará el reporte de resumen de recintos de votación que pide este requerimiento como se especifica en el análisis.

4.3.3-C

Número	4.3.3-C
Título	EMS, registro de ajuste de recintos electorales
Aplica a	EMS
Descripción	El EMS DEBE producir un reporte que muestre los cambios hechos a cada votación basada en la resolución de papeletas provisionales, papeletas cuestionadas, opciones escritas, y la fecha y hora del reporte.

Análisis

Este requerimiento tiene como objetivo que no haya diferencias entre los votos procesados, aunque no sean válidos según A(t,v), y los votos contabilizados. La aplicación permite el ingreso solo a los usuarios que constan en la base de datos; además no existen votos escritos (write-in) ni votos provisionales (provisional ballot). Si la base de datos contiene solo a los electores calificados para votar, la aplicación no permitirá que un elector que no está calificado pueda emitir un voto; por esta razón no existirán votos de electores que sean procesados y no contabilizados.

Resultado

La base de datos deberá contener solo a los electores calificados para votar; de esta manera el objetivo de este requerimiento se cumple y la aplicación no necesita modificaciones.

4.3.4-A

Número	4.3.4-A
Título	Tabulador, verificación de registros firmados
Aplica a	EMS
Descripción	Por cada tabulador que produce registros electrónicos, el EMS DEBE verificar: a. El certificado de la llave pública de la elección asociada con el registro es válido para la elección

	actual, usando la llave pública del tabulador para verificar el certificado como se especifica en Part 1:5.1 “Cryptography”; b. El ID de la elección y la fecha y hora del registro coinciden con la elección actual y los valores en el certificado de la llave pública de la elección; y c. La firma digital en el registro es correcta, usando la llave pública de la elección para verificarla.

Análisis

Este requerimiento tiene la intención de verificar los registros que llegan al sistema (EMS) desde los tabuladores. Este sistema funciona con un servidor central, el cual es el único tabulador y a la vez es el EMS.

Resultado

Este requerimiento no aplica para este sistema porque no existen múltiples tabuladores; el único tabulador es el mismo EMS con su servidor central.

4.3.5-A

Número	4.3.5-A
Título	Contador de papeletas
Aplica a	Tabulador, dispositivo de captura de votos
Descripción	Los tabuladores y dispositivos de captura de votos DEBEN mantener un conteo del número de papeletas leídas todo el tiempo durante un ciclo de pruebas particular o elección.

Análisis

El sistema no cuenta actualmente con esta función.

Esta función puede ser añadida aumentando un contador cada vez que un voto es ingresado. Este contador no debería ser volátil; es decir, no debería ser una

variable que se pierde si el sistema deja de funcionar por cualquier razón. El contador puede ser un valor almacenado en la base de datos o en un archivo.

El valor debe ser calculado correctamente mediante una operación atómica; es decir, no deben existir problemas por accesos simultáneos a este valor.

Resultado

Para que el sistema cumpla con este requerimiento se debe agregar un contador que se incremente cada vez que se ingresa un voto mediante una operación atómica y cuyo valor se almacena en la base de datos o en un archivo.

4.3.5-B

Número	4.3.5-B
Título	Contador de papeletas, disponibilidad
Aplica a	Tabulador, dispositivo de captura de votos
Descripción	Los tabuladores DEBEN permitir que los jueces de la elección determinen el número de papeletas leídas todo el tiempo durante un ciclo de pruebas particular o elección sin interrumpir cualquier operación en progreso.

Análisis

Después de ejecutar la acción recomendada para cumplir con el requerimiento 4.3.5-A, se debe crear un método para que las autoridades de elección verifiquen el número de votos ingresados (el contador del requerimiento 4.3.5-A) sin interrumpir las operaciones en progreso.

Se puede revisar este contador en el mismo servidor o en un computador conectado remotamente al servidor. Revisarlo en el servidor crea un riesgo de

seguridad al permitir acceso a personas al sitio donde funciona el servidor y a la máquina en sí; por esta razón se debe descartar esta opción. Revisarlo en un computador conectado remotamente no debe incrementar riesgos de seguridad.

Este valor se podrá verificar en un computador que reciba esta información del servidor. El servidor transmitirá periódicamente el valor a un computador seleccionado donde se podrá verificar el contador, y no se permitirán conexiones “a demanda” al servidor. De esta manera se evita que al ofrecer un servicio adicional se pueda explotarlo para crear un riesgo de seguridad, como por ejemplo una sobrecarga de requerimientos a este servicio. El servidor solo enviará el valor y solo lo enviará al destino seleccionado.

Resultado

Para que el sistema cumpla con este requerimiento el servidor enviará periódicamente el valor del contador del requerimiento 4.3.5-A a un destino seleccionado. El destino puede ser el servidor adicional independiente que se menciona en la solución a IVVR en el anexo 1.

5.5.1-A

Número	5.5.1-A
Título	Proteger la integridad del proceso de arranque
Aplica a	Dispositivo electrónico
Descripción	Antes del arranque o inicialización, los dispositivos electrónicos DEBEN verificar la integridad de los componentes usados para arrancar o inicializar el dispositivo electrónico utilizando un módulo de hardware resistente a manipulación.

Análisis

Este requerimiento está pensado para los dispositivos electrónicos de votación que deben ser protegidos contra modificación de sus componentes de inicialización. Este sistema no necesita proteger a los dispositivos porque los dispositivos de votación son computadores personales que solo acceden a la interfaz del sistema.

El servidor del sistema sí se beneficia de la protección de sus componentes de inicialización, como el BIOS y el kernel del sistema operativo utilizando un chip TPM; esto servirá para ayudar a prevenir cualquier modificación no autorizada de esos componentes.

El chip TPM (Trusted Platform Module) es un chip que facilita la creación segura de llaves criptográficas, y además tiene de un generador seudo-aleatorio de números en hardware. También tiene la capacidad de guardar un código hash imposible de modificar por software, el cual tiene un resumen de la configuración de hardware y software; esto permite verificar que el software crítico no ha sido cambiado. (Wikipedia contributors, “Trusted Platform Module.”)

La manera de utilizar un chip TPM en el servidor del sistema sería instalar el sistema en un servidor que ya tenga esta característica, como por ejemplo el Dell PowerEdge R300.

Otros usos para el chip TPM que no se mencionan en el requerimiento pero que son útiles para el sistema son la autentificación al servidor y la criptografía para los datos de las elecciones.

Para que el chip TPM funcione, éste debe estar apoyado por el software. Las comprobaciones de arranque (BIOS) pueden estar integradas en el sistema (el servidor), pero hay funciones como la verificación de integridad de archivos del sistema que requieren de apoyo del sistema operativo. Si este sistema va a correr sobre Linux como está diseñado para el prototipo inicial se puede utilizar el software TrouSerS de IBM que implementa las funciones del chip TPM en Linux.

Resultado

El sistema podrá cumplir con este requerimiento si se lo instala en un servidor con chip TPM.

5.5.1-B

Número	5.5.1-B
Título	Verificación de integridad de los binarios antes de ejecución o carga de memoria
Aplica a	Dispositivo electrónico
Descripción	Los dispositivos electrónicos DEBEN verificar la integridad de los binarios (ej: controladores de dispositivos, archivos de librerías, aplicaciones, y utilidades) utilizando un módulo de hardware resistente a manipulación y confirmar que los binarios han sido especificados por el fabricante como es requerido para el estado del sistema de votación actual antes de ser ejecutados o cargados en memoria.

Análisis

Este requerimiento está pensado para los dispositivos electrónicos de votación que deben ser protegidos contra modificación de los archivos ejecutables. Este sistema no necesita proteger a los dispositivos porque los dispositivos de votación son computadores personales que solo acceden a la interfaz del sistema.

El servidor del sistema sí se beneficia de la protección de los archivos ejecutables, como por ejemplo los ejecutables del servidor de aplicaciones y las librerías Java de las que depende la aplicación, utilizando un chip TPM; esto servirá para ayudar a prevenir cualquier modificación no autorizada de esos archivos.

La manera de utilizar un chip TPM en el servidor del sistema sería instalar el sistema en un servidor que ya tenga esta característica, como por ejemplo el Dell PowerEdge R300.

Otros usos para el chip TPM que no se mencionan en el requerimiento pero que son útiles para el sistema son la autentificación al servidor y la criptografía para los datos de las elecciones.

Para que el chip TPM funcione, éste debe estar apoyado por el software. Las comprobaciones de arranque (BIOS) pueden estar integradas en el sistema (el servidor), pero hay funciones como la verificación de integridad de archivos del sistema que requieren de apoyo del sistema operativo. Si este sistema va a correr sobre Linux como está diseñado para el prototipo inicial se puede utilizar el software TrouSerS de IBM que implementa las funciones del chip TPM en Linux.

Resultado

El sistema podrá cumplir con este requerimiento si se lo instala en un servidor con chip TPM.

5.5.1-C

Número	5.5.1-C
Título	Aislar aplicaciones
Aplica a	Dispositivo electrónico
Descripción	Los dispositivos electrónicos que soporten arquitecturas de multi-procesamiento DEBEN separar lógicamente cada aplicación para que las aplicaciones solo puedan acceder a los recursos necesarios para su funcionamiento normal.

Análisis

El requerimiento indica que se debe separar lógicamente las aplicaciones en los dispositivos electrónicos de votación. En este sistema no se utilizan dispositivos de votación, sino computadores personales que solo despliegan la interfaz del sistema y permiten al elector que realice su voto.

El servidor que maneja a este sistema cumple con este requerimiento. El sistema está pensado para que se ejecute sobre un servidor UNIX o similar. Estos sistemas operativos separan los procesos de manera que tienen espacios de memoria separados. Los procesos en sistemas UNIX tienen dos segmentos: el segmento de texto y el segmento de datos. El segmento de texto contiene el código del programa; a éste se le asigna un espacio de memoria fijo y de solo lectura. El segmento de datos contiene las variables del programa; es un espacio de memoria variable y modificable. Solo el segmento de texto se puede compartir para que se puedan ejecutar varias instancias de un proceso utilizando el mismo código, en lugar de cargar en memoria el mismo código varias veces. Las aplicaciones están separadas lógicamente.

(Tanenbaum, p. 690 – 692, 710 – 714)

Resultado

El sistema cumple con este requerimiento si se lo instala en un sistema operativo UNIX o similar.

5.5.2-A

Número	5.5.2-A
Título	Restringir el uso de medios removibles
Aplica a	Dispositivo electrónico
Descripción	Los dispositivos electrónicos DEBEN deshabilitar todas las interfaces de medios removibles que no son necesitadas para cada estado del sistema de votación.

Análisis

El acceso al servidor será restringido a las personas autorizadas y que los accesos al sistema operativo y aplicaciones están protegidos por contraseña. A pesar de eso, restringir el uso de medios removibles es posible y puede agregar un elemento adicional de seguridad. De esta manera se ayuda a impedir que cualquier dato o código ingrese al servidor.

La aplicación correrá en un solo servidor; por lo tanto las restricciones se deberán efectuar en un solo computador (el servidor).

Los posibles medios removibles que pueden estar disponibles en el servidor son:

- Unidad de disquete

- Unidad de disco compacto
- Unidad de cinta magnética
- Puertos USB
- Puertos FireWire
- Puertos seriales
- Puertos paralelos

Los puertos USB, FireWire, seriales y paralelos tienen muchas funciones. La decisión de restringir el uso de estos puertos es debido a la posibilidad de que se utilicen medios de almacenamiento removibles en estos puertos, como por ejemplo unidades Flash que se conectan a los puertos USB.

Resultado

El resultado del análisis de este requerimiento es ejecutar las siguientes acciones como parte de los pasos de preparación del servidor para las elecciones:

- Retirar del servidor las unidades de disquete, disco compacto y cinta magnética.
- Deshabilitar los puertos de comunicación que no se necesitan para que la aplicación de elecciones funcione (USB, FireWire, serial, paralelo).

5.5.3-A

Número	5.5.3-A
Título	Restringir las capacidades de respaldo y recuperación
Aplica a	Dispositivo electrónico
Descripción	Los dispositivos electrónicos que no seam EMS NO DEBEN proveer capacidades de respaldo y recuperación.

Análisis

El requerimiento indica que solo los sistemas de elecciones (EMS) pueden tener capacidad de respaldo y recuperación.

El sistema utiliza la base de datos Oracle 10g Release 2 provee funciones de respaldo y recuperación. Estas funciones son útiles para guardar los datos de las elecciones y recuperarlos en caso de que los datos se pierdan por cualquier razón. Para evitar que existan consecuencias que afecten al proceso de elecciones no se deberá ejecutar respaldo o recuperación durante las elecciones.

También pueden existir funciones de respaldo y recuperación en el sistema operativo. Se deben deshabilitar esas funciones.

Los dispositivos clientes (computadores personales) no almacenan datos de las elecciones, y por lo tanto cualquier función de respaldo y recuperación que éstos tengan no almacenará datos de las elecciones. Además, lo que pueda suceder en el cliente (por ejemplo, bloqueo de archivos debido al proceso de respaldo) no afecta al sistema de elecciones debido a que el cliente es un computador independiente que únicamente recibe y envía información HTML con el servidor; por lo tanto no puede afectarlo.

Resultado

El resultado del análisis de este requerimiento es ejecutar las siguientes acciones como parte de los pasos de preparación del servidor para las elecciones:

- Deshabilitar cualquier función de respaldo y recuperación del sistema operativo.
- Deshabilitar la función de respaldo y recuperación de la base de datos Oracle 10g Release 2.

Proteger por contraseña el acceso de administrador al sistema operativo y a la base de datos.

3.3 Análisis de las directrices de confidencialidad

3.2.3.1-A

Número	3.2.3.1-A
Título	Soporte del sistema para privacidad
Aplica a	Sistema de votación
Descripción	El sistema de votación DEBE prevenir que otros determinen el contenido de una papeleta.

Análisis

El sistema no permite acceso alguno a los electores además del necesario para realizar su sesión de voto y, si ya ha votado, para ver una pantalla informándole que ya ha votado. Ningún elector puede ingresar al sistema para ver su voto, por lo que no puede demostrar a nadie cómo votó.

Resultado

El sistema cumple actualmente con este requerimiento. No se necesita ejecutar alguna acción.

3.2.3.1-A.1

Número	3.2.3.1-A.1
Título	Privacidad visual
Aplica a	Sistema de votación
Descripción	La papeleta, cualquier otro registro visible que contenga información de la papeleta, y cualquier otro control de ingreso de información DEBE ser visible solo para el votante durante la sesión de votación y presentación de la papeleta.

Análisis

El sistema está pensado, como prototipo inicial, para que se pueda acceder desde cualquier computador conectado al Internet. Será imposible que cualquier sistema, incluyendo este, sea visible únicamente para la persona que está votando si no hay el control necesario en el sitio de votación.

Este sistema tiene la ventaja de permitir al elector que se asegure de su privacidad si éste toma las medidas necesarias; por ejemplo, votar en su domicilio sabiendo que ninguna otra persona está mirando.

Al votar usando este sistema en un sitio público, como un café-net, es más difícil controlar la privacidad visual. Una solución para este problema sería permitir el acceso al sistema solo desde lugares de votación autorizados; para esto se puede utilizar el método de dos contraseñas descrito en el anexo 2.

Resultado

Si el sistema se aplica en elecciones reales para electores obligatorios será necesario tomar medidas para mantener la privacidad visual del elector. Para eso será necesario establecer sitios autorizados de votación, y por lo tanto autentificación del cliente.

Sin embargo, el objetivo inicial de esta aplicación es ser un prototipo accesible para que todas las personas que quieran probarlo lo puedan hacer; no existirá autentificación del cliente y por lo tanto se podrá acceder desde cualquier computador personal. Se podrá motivar a mantener la privacidad visual con una pantalla de bienvenida para recordar al elector que se asegure que ninguna otra persona puede ver la pantalla o el teclado del computador (similar a la información mostrada en cajeros automáticos).

3.2.3.1-A.3

Número	3.2.3.1-A.3
Título	Privacidad de las advertencies
Aplica a	Sistema de votación
Descripción	El sistema de votación DEBE emitir todas las advertencias en una manera que preserve la privacidad del votante y la confidencialidad de la papeleta.

Análisis

Toda alerta o advertencia es mostrada solo al elector y solo durante su sesión de voto. No existen alertas o advertencias que identifiquen al elector con su voto; no se almacenan en el computador cliente; la notificación de que el voto fue realizado no muestra cuál fue el voto del elector; la notificación de que el elector ya ha votado no

muestra el voto, solo dice que ese elector ya ha votado y no permite al elector ingresar a una nueva sesión de voto.

Resultado

El sistema cumple actualmente con este requerimiento. No se necesita ejecutar alguna acción.

3.2.3.1-A.4

Número	3.2.3.1-A.4
Título	Sin recibos
Aplica a	Sistema de votación
Descripción	El sistema de votación NO DEBE emitir un recibo para el votante que provea de una prueba para otros de cómo votó.

Análisis

Una vez que el elector ha escogido los candidatos y ha confirmado su voto, la única información que se despliega es una pantalla con información que indica que su sesión de voto ha concluido exitosamente y el código de confirmación con el cual puede comprobar que ya ha votado. No se indica cómo votó ni hay manera de que el elector ingrese nuevamente al sistema con ese código para ver cómo votó.

Resultado

El sistema cumple actualmente con este requerimiento. No se necesita ejecutar alguna acción.

3.2.3.2-A

Número	3.2.3.2-A

Título	No grabación de lenguajes alternativos
Aplica a	Sistema de votación
Descripción	Ninguna información DEBE ser mantenida en un CVR electrónico que identifique cualquier lenguaje alternativo utilizado por un votante.

Análisis

El sistema no soporta idiomas alternativos. Cada instancia de la aplicación contará con un solo idioma, por lo que no existe la posibilidad de que se mantenga información que identifique idiomas alternativos usados por un elector.

Resultado

El sistema cumple actualmente con este requerimiento. No se necesita ejecutar alguna acción.

3.2.3.2-B

Número	3.2.3.2-B
Título	No grabación de características de accesibilidad
Aplica a	Sistema de votación
Descripción	Ninguna información DEBE ser mantenida en un CVR electrónico que identifique alguna característica de accesibilidad usada por un votante.

Análisis

Este requerimiento protege al elector de que su voto sea identificado por usar funciones de accesibilidad. Ninguna función de accesibilidad que pueda tener un computador personal será almacenada en el sistema; el contenido es HTML estándar y no guarda datos del computador del cliente.

Resultado

El sistema cumple actualmente con este requerimiento. No se necesita ejecutar alguna acción.

4.3.3-A.1

Número	4.3.3-A.1
Título	Tabulador, combinación del reporte para privacidad
Aplica a	EMS
Descripción	El EMS debe ser capaz de combinar reportes de tabuladores para proteger la privacidad del votante en casos cuando hay tabuladores con pocos votos.

Análisis

El requerimiento no especifica cuántos son “pocos” electores; se asume que 10 electores son “pocos” electores porque con menos de 10 electores puede ser posible adivinar cómo han votado los electores. El ejemplo más claro es si existe solo un elector; en este caso el único voto pertenecerá a ese elector y se puede saber cómo votó.

Si un número de 10 o menos electores es poco, entonces no se aplica para este sistema. Este sistema está pensado para que sea utilizado por cientos y miles de electores. Es el mismo servidor único de base de datos el que funciona como tabulador (contador); no existen varios tabuladores que contengan resultados parciales. No conviene utilizarlo para 10 o menos electores porque el costo sería demasiado alto; este requerimiento no se aplica en este sistema al no utilizarlo para tan pocos electores.

Resultado

El requerimiento no aplica en este sistema mientras no sea utilizado en elecciones de 10 o menos electores si 10 o menos electores son “pocos”, como está explicado en el análisis.

5.1.1-A

Número	5.1.1-A
Título	Validación del módulo criptográfico
Aplica a	Dispositivo programado
Descripción	La funcionalidad criptográfica DEBE estar implementada en un módulo criptográfico validado para FIPS 140-2 operando en modo FIPS.

Análisis

FIPS 140-2 es un estándar de seguridad del gobierno de Estados Unidos usado para acreditar módulos criptográficos (Wikipedia, “FIPS 140-2”). Existen varios módulos acreditados que han recibido la certificación FIPS 140-2. Entre los módulos acreditados esta Oracle 10g Application Server, el cual será considerado como el servidor de aplicaciones sobre la cual correrá este sistema.

Para que Oracle 10g Application Server funcione como un módulo acreditado se necesita habilitar el modo FIPS. Esto, según el sitio Web de Oracle, no reduce funcionalidad. Para habilitar en modo FIPS solamente se debe cambiar un parámetro del archivo sqlnet.ora, que es un archivo de configuración.

(Oracle, “Oracle 10g Application Server…”)

Resultado

Para cumplir con este requerimiento se debe implementar la aplicación sobre un servidor de aplicaciones que esté acreditado para FIPS 140-2. La aplicación originalmente corre sobre el servidor JBoss, el cual no está acreditado. Oracle 10g Application Server es una opción adecuada para este sistema para mantener la interoperabilidad entre las partes del sistema, porque la base de datos utilizada es Oracle Database Enterprise Edition y se desarrolló utilizando Oracle JDeveloper.

5.1.1-B

Número	5.1.1-B
Título	Fortaleza criptográfica
Aplica a	Dispositivo programado
Descripción	Los dispositivos programados que aplican protección criptográfica DEBEN emplear algoritmos aprobados por NIST con una fortaleza de seguridad de por lo menos 112-bits para proteger información de elecciones y registros sensibles. MACs de 96-bits son convencionales en protocolos de comunicación seguros estandarizados, y aceptables para proteger registros de votos y sistemas; sin embargo, la llave utilizada con esos MACs DEBE también tener una seguridad de por lo menos 112 bits.

Análisis

El sistema funciona y depende de aplicaciones como la base de datos Oracle y el servidor de aplicaciones. Por esta razón no se puede escoger qué tipo de algoritmos va a usar el sistema en todos los casos. El caso más importante es la comunicación SSL, pues toda la comunicación entre el servidor y los clientes es a través del Internet y usando SSL. En lugar de escoger los algoritmos, es preferible escoger las aplicaciones correctas. Oracle 10g Application Server se puede ejecutar en modo FIPS, el cual utiliza los algoritmos 3DES, SHA-1, RSA y HMAC-SHA-1 que son aprobados para FIPS.

(Baker, Baker, Burr, Polk, Smith; p. 34 - 68)

Resultado

Para cumplir con este requerimiento se recomienda utilizar un servidor de aplicaciones como Oracle 10g Application Server, el cual utiliza algoritmos aprobados para FIPS.

3.4 Análisis de las directrices de autentificación

5.4.1-A

Número	5.4.1-A
Título	Mecanismos de control de acceso
Aplica a	Dispositivo de votación
Descripción	El dispositivo de votación DEBE proveer mecanismos de control de acceso diseñados para permitir acceso autorizado al sistema de votación y para prevenir acceso no autorizado al sistema de votación.

Análisis

Los dispositivos de votación son todas las computadoras con acceso a Internet. El sistema cuenta con autentificación del elector para que pueda realizar la única función que debe realizar, que es votar, y solo podrá utilizar su voto; no tendrá acceso a otras funciones ni a datos de los demás electores. Se cuenta con los puntos que establece la discusión:

1. Se autentifica al elector y se registra su voto. Se debería registrar también la fecha y hora del acceso.

2. El voto es confidencial. No se muestra el voto de un usuario a otro usuario. Los datos se guardan en el servidor central.
3. Los historiales, registros y reportes no están en el dispositivo de votación. El acceso al servidor desde un computador externo es solo para votar, no se puede consultar información.
4. La disponibilidad del sistema depende del servidor central y desde el dispositivo de votación no hay acceso a otras funciones. Por esta razón no es posible que un usuario pueda realizar acciones desde el dispositivo de votación que afecten la disponibilidad del sistema.

En el caso en que en el sistema se implementen los cambios necesarios para que solo se pueda votar desde sitios autorizados se aplicará el esquema de autentificación descrito en el requerimiento 5.4.1-A.1.

Resultado

El sistema, como prototipo inicial, no contará con sitios autorizados para votar. Todo computador conectado al Internet será un cliente (dispositivo de votación). Los clientes solo tienen y solo necesitan acceso como electores que votan, por lo que no se necesitan realizar cambios para cumplir con este requerimiento.

5.4.1-A.1

Número	5.4.1-A.1
Título	Control de acceso al dispositivo de votación
Aplica a	Dispositivo de votación
Descripción	Los mecanismos de control de acceso del dispositivo del votación DEBEN ser capaces de identificar y autentificar los roles de Part 1:Table 5-1 permitidos para realizar operaciones en el dispositivo de votación.

Análisis

La tabla Table 5-1 a la cual se refiere el requerimiento es la siguiente:

GROUP OR ROLE	DESCRIPTION
Voter	The voter role is a restricted process in the vote-capture device. It allows the vote-capture device to enter the Activated state for voting activities.
Election Judge	The election judge has the ability to open the polls, close the polls, handle fled voters, recover from errors, and generate reports.
Poll Worker	The poll worker checks in voters and activates the ballot style.
Central Election Official	The central election official loads ballot definition files.
Administrator	The administrator updates and configures the voting devices and troubleshoots system problems.

Figura 1: Table 5-1 Voting system minimum groups and roles
(TGDC, 209)

Este sistema utiliza como dispositivo de votación al computador cliente.

Utilizando la configuración pensada inicialmente, donde el computador cliente es cualquier computador con acceso a Internet, todas las funciones mencionadas para los grupos Election Judge, Poll Worker, Central Election Officer y Administrador se van a ejecutar en el servidor central, no en el dispositivo de votación. Por esta razón no se va a permitir otro acceso al sistema desde el dispositivo de votación que no sea el del elector para votar.

Si se vota solo desde sitios autorizados para votar y utilizando solo computadores autorizados se necesitará aplicar el esquema de autentificación que plantea este requerimiento. Los distintos roles deberán ser autentificados por el servidor central; no se almacenarían datos de los usuarios en el sistema. El único rol

que no sería necesario es Central Election Officer, porque de cualquier manera se toma la información de las elecciones desde el servidor central.

Todos los cambios necesarios para habilitar los roles en el dispositivo de votación se pueden realizar; sin embargo, los cambios son grandes, pues el sistema no está diseñado actualmente de esa manera. Se requieren varias pantallas distintas para que se puedan ejecutar todas las funciones, cambios en la lógica interna de la aplicación, cambios en la base de datos. Un ejemplo de modificación del sistema para utilizar estos roles está detallado en el anexo 2.

Resultado

El sistema, como prototipo inicial, no contará con sitios autorizados para votar. Todo computador conectado al Internet será un cliente (dispositivo de votación). Los clientes solo tienen y solo necesitan acceso como electores que votan, por lo que no se necesitan realizar cambios para cumplir con este requerimiento.

5.4.1-B

Número	5.4.1-B
Título	Control de acceso para el software y archivos
Aplica a	Dispositivo de votación
Descripción	El dispositivo de votación DEBE proveer controles que permitan o nieguen acceso al software y archivos del dispositivo.

Análisis

Los dispositivos de votación son todas las computadoras con acceso a Internet. El requerimiento se refiere a permitir o negar acceso al software y archivos del dispositivo.

El sistema solo permite acceder a las funciones de voto a través del Web. Sin importar si el usuario accede al software y archivos del dispositivo, ninguna función será comprometida y ningún dato al que el usuario no deba acceder será accesible. Todas las funciones son realizadas desde el servidor, presentando al usuario las pantallas para poder votar. Todo el software y archivos del sistema están en el servidor. No existe acceso al software y archivos desde un dispositivo de votación.

Resultado

El sistema está diseñado para cumplir con este requerimiento. Se recomienda asegurarse que el único acceso externo al servidor sea para votar; es decir, se debe deshabilitar todo tipo de acceso remoto que no sea Web (por ejemplo: telnet, ssh, isqlplus).

5.4.1-C

Número	5.4.1-C
Título	Estados de votación de control de acceso
Aplica a	Dispositivo de captura de votos
Descripción	Los mecanismos de control de acceso del dispositivo de captura de votos DEBEN distinguir por lo menos los siguientes estados de votación de Part 1:Table 5-2: a. Pre-votación; b. Activado; c. Suspendido; y d. Post-votación.

Análisis

La tabla Table 5-2 a la que se refiere este requerimiento es la siguiente:

STATE	DESCRIPTION
Pre-voting	Power-on, loading and configuring device software, maintenance, loading election-specific files, preparing for election day usage.
Activated	Activating the ballot, printing, casting, spoiling the ballot.
Suspended	Entered when an election official suspends voting.
Post-voting	Closing polls, tabulation, printing records, power-off.

Figura 2: Table 5-2 Vote-capture device minimum states
(TGDC, p. 210)

Actualmente el sistema puede distinguir tres de los cuatro estados mencionados:

- Pre-votación: En este estado el sistema está inactivo; el elector no puede acceder a votar.
- Activado: El elector puede acceder, ve las pantallas para ingresar y puede realizar su voto.
- Post-votación: El elector ha votado y no puede votar nuevamente; el sistema está apagado y no se puede acceder a votar.

Se puede mejorar el estado de pre-voto, incluyendo una pantalla que muestre al usuario que el sistema está en línea, pero que no está en la fecha y hora cuando estará autorizado a votar. Si se incluyen funciones de información al usuario, como por ejemplo, mostrar las listas de candidatos para que los electores las conozcan antes del día de votación, esto también será parte del estado de pre-voto.

Durante el estado de activado no deben existir otras funciones que no sean las elecciones.

Se debe manejar el estado de suspendido. Actualmente el sistema no tiene este estado. Se puede realizar una pantalla que informe al usuario que el sistema está en línea, pero que ha sido suspendido.

Para cambiar entre estados se deberá incluir una pantalla de administración donde se permita realizarlos.

Resultado

Para cumplir con este requerimiento se deberán realizar las siguientes acciones:

- Manejar el estado de suspendido.
- Crear un panel de administración para cambiar entre estados.
- Mostrar al usuario información del estado en el que se encuentra el sistema.

5.4.1-E

Número	5.4.1-E
Título	Permisos mínimos predeterminados
Aplica a	Dispositivo de votación
Descripción	Los permisos de control de acceso predeterminados del dispositivo de votación DEBEN implementar los permisos mínimos necesarios para cada rol o grupo.

Análisis

Durante las elecciones, los dispositivos de votación solo permiten al elector votar; no tienen otra función. Como se discute en el requerimiento 5.4.1-A.1, el único rol que se implementa en el dispositivo de votación es el del elector. Además, para que el acceso sea solo para la función de votar y solo a la información necesaria para votar, se recomienda la misma acción que para el requerimiento 5.4.1-B.

Resultado

El sistema está diseñado para cumplir con este requerimiento. Se recomienda asegurarse que el único acceso externo al servidor sea para votar; es decir, se debe deshabilitar todo tipo de acceso remoto que no sea Web (por ejemplo: telnet, ssh, isqlplus).

5.4.3-A

Número	5.4.3-A
Título	Mecanismo mínimo de autentificación
Aplica a	Dispositivo de votación
Descripción	El dispositivo de votación DEBE autentificar usuarios mediante los métodos mínimos de autentificación descritos en Part 1:Table 5-4.

Análisis

En el dispositivo de votación solo se autentifica el elector. Los roles descritos en la tabla Table 5-4 no están implementados en el sistema, como se describe en el análisis del requerimiento 5.4.1-A.1.

La autentificación del elector está diseñada actualmente como nombre de usuario y contraseña; esto es, el número de cédula de ciudadanía y una contraseña

asignada por el sistema. El sistema cuenta con una función para generar contraseñas para los electores.

En el caso de que se cambiaría el sistema al modo de voto en sitios autorizados, se necesitaría implementar la autentificación como indica la tabla Table 5-4:

GROUP OR ROLE	MINIMUM AUTHENTICATION METHOD
Election Judge	User name and password
Poll Worker	N/A – poll worker does not authenticate to voting system
Central Election Official	User name and password
Administrator	Two-factor authentication
Application or Process	Digital certificate or signature

Figura 3: Table 5-4 Minimum authentication methods for groups and roles

(TGDC, 216)

Se puede modificar las función de generar contraseñas del sistema para los electores para que también se generen contraseñas para los roles Election Judge y Central Election Official. La generación de contraseñas para administrador se puede hacer en dos partes: una contraseña generada por este sistema y otra generada por un sistema independiente del organismo regulador de las elecciones; así se consiguen dos factores distintos de autentificación. Se necesitará modificar también la base de datos para almacenar la información referente a estos roles.

La autentificación de la aplicación con el dispositivo de votación es a través de un certificado digital. La comunicación se realiza con SSL y se autentifica de la manera estándar como lo hace un navegador Web, verificando el certificado digital

que le envía el servidor. Para la ejecución en elecciones reales se debe adquirir un certificado digital de una compañía de seguridad conocida como por ejemplo VeriSign.

Resultado

El sistema cumple con el requerimiento de autentificación de la aplicación, y no necesita cumplir con los roles que no se utilizan en el dispositivo de votación. Si se llegaran a implementar los roles adicionales se deberán ejecutar los cambios que se mencionan en el análisis de este requerimiento.

5.4.3-B

Número	5.4.3-B
Título	Mecanismo de autentificación múltiple
Aplica a	Dispositivo de votación
Descripción	El dispositivo de votación DEBE proveer múltiples mecanismos de autentificación para soportar la autentificación multi-factor.

Análisis

En el requerimiento 5.4.3-A se analiza que para tener dos factores de autentificación se puede generar una contraseña en este sistema y otra en un sistema independiente. Si se llega a utilizar el rol de administrador en los dispositivos de votación se deberá cumplir con este requerimiento.

Este requerimiento pide que se tengan múltiples métodos de autentificación para soportar la autentificación de múltiples factores. La autentificación de dos factores requerida para el rol de administrador puede ser con dos contraseñas como

se analizó en el requerimiento 5.4.3-A, y para que sea un método distinto de autentificación se puede variar el ingreso de las contraseñas. Se puede crear una pantalla para que una persona distinta al administrador habilite el ingreso de administrador utilizando una de las dos contraseñas; una vez que se ha habilitado este ingreso el administrador podrá ser autentificado con su contraseña, que es la otra de las dos generadas.

Resultado

Si se utiliza el rol de administrador se deberán realizar los cambios mencionados en el análisis para soportar la autentificación del administrador utilizando los dos factores por separado.

5.4.3-C

Número	5.4.3-C
Título	Autentificación multi-factor de grupo o rol administrador
Aplica a	Dispositivo de votación
Descripción	El dispositivo de votación DEBE autentificar el grupo o rol administrador con un mecanismo de autentificación multi-factor.

Análisis

Si se llega a utilizar el rol de administrador en los dispositivos de votación, este requerimiento estará cubierto con los cambios mencionados en el análisis de los requerimientos 5.4.3-A y 5.4.3-B.

Resultado

Se deben realizar los cambios indicados para los requerimientos 5.4.3-A y 5.4.3-B en caso de que se utilice el rol de administración para los dispositivos de votación.

5.4.3-D

Número	5.4.3-D
Título	Almacenamiento seguro de los datos de autentificación
Aplica a	Dispositivo de votación
Descripción	Cuando datos privados o secretos de autentificación son almacenados en el dispositivo de votación, los datos DEBEN ser protegidos para asegurar que la confidencialidad e integridad de los datos no sean violadas.

Análisis

En ningún caso se almacenará información privada o secreta de autentificación en el dispositivo de votación. En ambos casos, cuando cualquier computador funciona como dispositivo de votación o cuando solo se permite votar en sitios autorizados, toda la información de autentificación estará en el servidor central.

Resultado

El sistema cumple con este requerimiento. No se necesita realizar alguna acción.

5.4.3-G

Número	5.4.3-G
Título	Bloqueo de cuenta
Aplica a	Dispositivo de votación
Descripción	El dispositivo de votación DEBE bloquear grupos, roles o individuos después de un número especificado de intentos de autentificación fallidos consecutivos dentro de un período de tiempo predefinido.

Análisis

El único rol que puede ingresar por medio de los dispositivos de votación es el elector.

Esta función es importante para evitar acceso no autorizado que intente ingresar como elector intentando varias contraseñas hasta acertar. Además, con esto se puede evitar que máquinas generadoras de contraseñas ingresen automáticamente al sistema generando contraseñas aleatorias para distintos electores.

Existe el problema de negar a un elector su derecho al voto e impedir que cumpla con esta obligación, especialmente si el elector no es el culpable de que haya sido bloqueado del sistema. El organismo regulador de las elecciones deberá decidir si utiliza esta función, qué muestra al usuario en caso de que sea bloqueado y después de cuántos intentos fallidos es bloqueado. Esta razón podría ser menos importante si se utiliza solo para el voto opcional.

El sistema no cuenta actualmente con esta función.

Resultado

Se deberá implementar la función que pide este requerimiento. Para esto se creará una pantalla accesible al administrador del sistema (no accesible desde el

dispositivo de votación) que permita especificar si se habilita o deshabilita esta función y después de cuántos intentos errados se bloquea a un usuario (elector).

5.4.3-H

Número	5.4.3-H
Título	Configuración del bloqueo de cuenta
Aplica a	Dispositivo de votación
Descripción	El dispositivo de votación DEBE permitir que el grupo o rol administrador configure la política de bloqueo de cuenta, incluyendo el período de tiempo en el cual los intentos fallidos deben ocurrir, el número de intentos de acceso fallidos consecutivos permitidos antes del bloqueo, y la longitud de tiempo que la cuenta está bloqueada.

Análisis

Este requerimiento extiende al requerimiento 5.4.3-G, especificando parámetros adicionales que deben ser configurables para la función de bloqueo de usuario después de varios intentos fallidos.

Resultado

Se deben adicionar los parámetros que este requerimiento indica a la pantalla de control que se creará por el requerimiento 5.4.3-G.

3.5 Análisis de las directrices de no repudiación

5.7.1-A

Número	5.7.1-A
Título	Requerimiento de mecanismos de registro de eventos
Aplica a	Dispositivo programado
Descripción	El dispositivo de votación DEBE proveer mecanismos de registro de eventos designados para registrar las

	actividades del dispositivo de votación.

Análisis

En este sistema los dispositivos de votación no generan eventos, solo muestran la interfaz del sistema. El sistema tiene la capacidad de generar registros de las actividades de votación descrita en el requerimiento 5.7.1-E.

Resultado

El sistema cumplirá con este requerimiento al registrar las actividades de votación como se describe en el requerimiento 5.7.1-E.

5.7.1-B

Número	5.7.1-B
Título	Requerimiento de protección de integridad
Aplica a	Dispositivo programado
Descripción	El dispositivo de votación DEBE habilitar la protección de integridad de los archivos para archivos de historial almacenados como parte de la configuración inicial.

Análisis

Los historiales pueden ser guardados y almacenados en archivos.

Para mantener la integridad de los historiales se puede firmarlos digitalmente o realizar una operación hash sobre el archivo y guardar el resultado para compararlo cuando sea necesario hacer una comprobación de integridad.

Resultado

Para cumplir con este requerimiento se firmarán digitalmente los historiales o se creará un código de comprobación para mantener su integridad.

5.7.1-C

Número	5.7.1-C
Título	Requerimiento de privacidad del elector y confidencialidad de la papeleta
Aplica a	Dispositivo programado
Descripción	Los historiales del dispositivo de votación NO DEBEN contener información que, si se publica, viole la confidencialidad de la papeleta o la privacidad del elector o que comprometa a la seguridad del sistema de cualquier manera.

Análisis

Los votos de los electores se guardan en el sistema con el código único asignado al elector, pero no vinculado a éste de ninguna manera lógica. Las contraseñas de acceso se guardan en manera de código hash. Ningún dato almacenado en el sistema compromete la confidencialidad y privacidad de los electores.

Actualmente el sistema carece de varios historiales que se requieren en este estándar. Para crear los historiales que le faltan a este sistema se deberá mantener esta condición y se debe procurar no registrar datos que comprometan a la seguridad del sistema.

Resultado

El sistema cumple actualmente con este requerimiento. Todo nuevo historial que se cree deberá mantener la confidencialidad y privacidad del elector y no deberá comprometer la seguridad del sistema.

5.7.1-D

Número	5.7.1-D
Título	Requerimiento de registro de características de eventos
Aplica a	Dispositivo programado
Descripción	El dispositivo de votación DEBE registrar como mínimo las siguientes características de datos para cada tipo de evento: a. ID del sistema; b. ID único de evento y/o tipo; c. Fecha y hora; d. Éxito o fracaso del evento, si aplica; e. ID del usuario que inicia el evento, si aplica; f. Recursos solicitados, si aplica.

Análisis

En este sistema no hay dispositivos de votación con identificación única o que generen eventos. Todo evento sucede en el servidor principal y será registrado en este.

La necesidad de registrar los eventos mencionados en este requerimiento está cubierta por el requerimiento 5.7.1-E.

Resultado

Debido a que no existen dispositivos de votación con identificación única que generen eventos, el sistema cumplirá con este requerimiento al cumplir con el requerimiento 5.7.1-E.

5.7.1-D.1

Número	5.7.1-D.1
Título	Requerimiento de registro del tiempo
Aplica a	Dispositivo programado
Descripción	Los mecanismos de registro del tiempo DEBEN generar valores de hora y fecha.

Análisis

Este sistema corre sobre computadores (servidores) capaces de generar valores de fecha y hora.

Resultado

El sistema cumple actualmente con este requerimiento. No se necesita ejecutar alguna acción.

5.7.1-D.2

Número	5.7.1-D.2
Título	Requerimiento de precisión del tiempo
Aplica a	Dispositivo programado
Descripción	La precision del mecanismo de registro del tiempo DEBEN tener la capacidad de distinguir y ordenar adecuadamente todos los registros de auditoría.

Análisis

Este sistema corre sobre computadores (servidores) capaces de generar valores de fecha y hora con precisión de segundos, milisegundos y hasta microsegundos. Esto permitirá distinguir y ordenar apropiadamente los registros auditables.

Resultado

El sistema cumple con este requerimiento al ser instalado sobre un servidor contemporáneo. Se puede comprobar revisando los valores de fecha y hora de los historiales generados.

5.7.1-D.3

Número	5.7.1-D.3
Título	Requerimiento de datos de fecha y hora
Aplica a	Dispositivo programado
Descripción	Los valores de tiempo DEBEN incluir la fecha y hora, incluyendo horas, minutos, y segundos.

Análisis

Los registros generados actualmente por el sistema contienen fecha, hora, minuto y segundo. Los registros e historiales que el sistema no tiene actualmente se deberán crear con valores de fecha, hora, minuto y segundo.

Resultado

Se debe incluir valores de fecha, hora, minuto y segundo en los nuevos registros e historiales que se incluirán en el sistema.

5.7.1-D.4

Número	5.7.1-D.4
Título	Requerimiento de cumplimiento del tiempo
Aplica a	Dispositivo programado
Descripción	Los valores de fecha y hora DEBEN cumplir con ISO 8601 y proveer todos los cuatro dígitos del año e incluir la zona horaria.

Análisis

Los registros generados actualmente por el sistema contienen el año con cuatro dígitos. Se deberá agregar la información de la zona horaria. Se puede utilizar el formato estándar de ISO 8601: YYYY-MM-DDThh:mm:ss, donde YYYY es el año con cuatro dígitos, MM es el mes con dos dígitos, DD es el día con dos dígitos, T es el separador de fecha y hora, hh es la hora con dos dígitos, mm es el minuto con dos dígitos y ss es el segundo con dos dígitos.

(ISO, “ISO – FAQs…”)

Resultado

Se debe incluir la información de zona horaria en los registros actuales. Se deben usar valores del año con cuatro dígitos e incluir la información de zona horaria en todos los nuevos registros e historiales del sistema.

5.7.1-D.5

Número	5.7.1-D.5
Título	Requerimiento de ajuste del reloj
Aplica a	Dispositivo programado
Descripción	Los dispositivos de votación DEBEN permitir solo a administradores a ajustar el reloj.

Análisis

Todas las fechas y horas registradas en el sistema corresponden a la fecha y hora del reloj del servidor. La fecha y hora del servidor solo se pueden cambiar por el administrador del sistema operativo.

Resultado

El sistema cumple actualmente con el requerimiento, no se necesita ejecutar alguna acción.

5.7.1-D.6

Número	5.7.1-D.6
Título	Requerimiento de mínima desviación del reloj
Aplica a	Dispositivo programado
Descripción	El dispositivo de votación DEBE limitar la desviación del reloj a un minimo de 1 minuto dentro de un período de 15 horas después de que se ha ajustado el reloj.

Análisis

Los servidores se construyen para tener desviaciones de hora menores a 1 minuto por cada 15 horas.

De cualquier manera, se toma en cuenta que una desviación importante es perjudicial para las elecciones, por lo que se recomienda realizar una prueba para comprobar la desviación del reloj del servidor en condiciones de trabajo como las que soportará durante las elecciones.

Resultado

Se deberá comprobar la desviación del reloj del servidor antes de utilizarlo para las elecciones.

5.7.1-E

Número	5.7.1-E
Título	Requerimiento de mínimos eventos registrados
Aplica a	Dispositivos programados
Descripción	El dispositivo de votación DEBE registrar como mínimo los eventos de sistema descritos en Part 1:Table 5-5.

Análisis

La tabla 3 muestra los eventos mínimos que se deben mantener en historiales según VVSG 2007. Se muestran las funciones del sistema que generan los eventos, clasificados por tipo de evento y por tipo de dispositivo.

Todos los eventos mencionados a excepción del evento “Backup and restore” son eventos de los dispositivos de votación. En este sistema de elecciones los dispositivos de votación son los computadores personales que solo muestran la interfaz de usuario del sistema, por lo que no necesitan monitorear y registrar eventos. De todas maneras, este requerimiento es útil para monitorear los eventos que ocurren en el servidor del sistema de elecciones.

Este sistema depende de algunos elementos: el sistema operativo, el servidor de aplicaciones, la base de datos y la aplicación. Todos estos elementos generan eventos que se mencionan en la tabla Table 5-5 de VVSG 2007.

Los eventos del sistema operativo están en historiales propios. El sistema está pensado para un sistema operativo UNIX o similar. Se lo ha desarrollado en Linux, y en Linux los historiales están en archivos dentro de /var/log. Además existen herramientas como dmesg y ksymoops que pueden generar entradas en los historiales tan detalladas desde emergencias del kernel hasta llegar a mensajes de corrección de código (debug), como muestra la siguiente tabla de niveles de alertas de syslog:

0> system is unusable

1> action must be taken immediately
2> critical conditions
3> error conditions
4> warning conditions
5> normal but significant condition
6> informational
7> debug-level messages

Tabla 2: Niveles de alertas del sistema operativo

(die.net, p.1)

La base de datos tiene extensas funciones de auditoría. Existen controles e historiales para acceso a las diferentes tablas de la base de datos, acciones de los usuarios (por ejemplo, añadir o eliminar registros de las tablas), eventos de la base de datos (por ejemplo, inicio de la base de datos o creación de nuevas tablas) y más funciones configurables.

El sistema fue desarrollado en el servidor de aplicaciones JBoss, el cual despliega en la consola de salida estándar (standard output de Linux) todos los mensajes de estado, eventos, información, alertas y errores de JBoss y las aplicaciones que ejecuta; además muestra los mensajes escritos por la aplicación usando la llamada System.print y System.println. El servidor de aplicaciones recomendado para la aplicación es Oracle Application Server; este servidor de aplicaciones lleva registros de todo lo que sucede con el sistema.

Los productos Oracle Enterprise Database y Oracle Application Server pueden ser monitoreados con Oracle Enterprise Manager. Oracle Enterprise Manager ya fue utilizado en este sistema de elecciones desde el desarrollo.

La aplicación actualmente no envía mensajes de estado a algún historial. Mensajes como el inicio de la aplicación, finalización de la aplicación, ingreso de un elector, registro de un voto, inicio de las elecciones y fin de las elecciones son algunos que deben ser registrados en un historial. Esta es una característica que se debe incluir en la aplicación.

A continuación se presentan los eventos de la tabla Table 5-5 y la manera en que se obtiene esa información en el sistema de elecciones.

FUNCIONES GENERALES DEL SISTEMA

Mensajes de errores y excepciones generados por los dispositivos	Este tipo de mensajes se pueden ver en los logs del kernel ubicados en /var/log
Mensajes de estado críticos del sistema	El sistema actualmente no envía mensajes de estado a algún historial. Se deben registrar mensajes de estado crítico como el estado de la conexión con el servidor de la base de datos y la verificación de “conteo cero” antes de las elecciones.
Mensajes de estado no críticos	El sistema actualmente no envía mensajes de estado a algún historial. Se deben registrar mensajes de estado no críticos (informativos).
Eventos que requieren intervención de un oficial de elecciones	El sistema actualmente no envía mensajes de estado a algún historial. Se deben registrar mensajes de eventos que requieran la intervención humana, sea de un oficial de elecciones (si hay alguno) o del administrador del sistema.
Apagado y reinicio de dispositivos	No hay dispositivos de votación. El apagado y reinicio del servidor se registra en los historiales del sistema operativo.
Cambios a la configuración del sistema	Existen herramientas en los sistemas UNIX y Linux que monitorean a los archivos de configuración. Una de estas herramientas es RPM, que viene incluido en las principales distribuciones de Linux.
Verificación de integridad de ejecutables, archivos de configuración, datos e historiales	Se puede obtener una firma digital de los ejecutables y archivos compilados de la aplicación. Así se puede comparar las versiones iniciales con las versiones en ejecución.
Agregar o eliminar archivos	En un servidor existen muchos eventos del sistema de archivos durante el funcionamiento normal del sistema. A pesar de que este requerimiento está enfocado en dispositivos simples de votación que no generarán muchos eventos de este tipo, se puede monitorear todo cambio en el

	sistema de archivos con herramientas como inotify, que se incluye en el kernel de Linux versión 2.6 y superior.
Resultados de la comprobación inicial	El sistema no hace actualmente una comprobación inicial que muestre que el sistema está listo para ser utilizado. Se deberá incluir esta función.
Eventos de medios removibles	Estos eventos deben estar visibles en los historiales del kernel del sistema operativo.
Respaldo y recuperación	Cada operación de respaldo y recuperación de la base de datos Oracle Enterprise 10g crea un historial detallado de los datos procesados.
AUTENTIFICACIÓN Y CONTROL DE ACCESO	
Eventos relacionados con la autentificación	El sistema actualmente no registra este tipo de eventos. Se deberán registrar eventos como el ingreso de usuarios y cambio de contraseñas.
Eventos relacionados con el control de acceso	La base de datos Oracle permite registrar todo tipo de acceso; se puede habilitar la opción AUDIT_SYS_OPERATIONS para este propósito.
Manejo de cuentas de usuarios y roles (o grupos)	Los eventos como creación de usuarios (electores) y modificación de esas cuentas no son registrados actualmente y se deben registrar. Los eventos de modificación de usuarios de la base de datos Oracle son registrados automáticamente y guardados en $ORACLE_HOME/RDBMS/AUDIT.
SOFTWARE	
Instalación, actualización, instalación de parches o modificación de software o firmware	El sistema operativo puede monitorear estos eventos con herramientas como RPM que se incluye en la mayoría de las distribuciones de Linux.
Cambios a las opciones de configuración	La configuración de las elecciones está programada en el sistema. Todo cambio en el esquema de la base de datos Oracle es auditado.
Finalizaciones anormales de procesos	Estos eventos deben estar visibles en los historiales del kernel del sistema operativo.
Intentos de conexión a la base de datos exitosos y fallidos	La base de datos Oracle permite auditar los accesos a la base de datos; además se puede auditar los accesos a objetos específicos (por ejemplo, tablas) con el comando AUDIT.
FUNCIONES DE VOTACION	
Definición y modificación de papeletas	La configuración de las elecciones está programada en el sistema. Todo cambio en el esquema de la base de datos Oracle es auditado.
Eventos de votación	El sistema actualmente no registra este tipo de eventos. Se deberán registrar eventos como ingreso de un voto y el inicio

y cierre de las elecciones.

Tabla 3: Registros e historiales

La sección 5.7 de VVSG 2007 contiene una una explicación completa de todo lo que representa el tema de eventos, registros e historiales para la seguridad de un sistema de elecciones y los objetivos de estos requerimientos. Se recomienda leer esta sección para analizar las directrices de eventos e historiales.

Una buena descripción general de los eventos e historiales está en la introducción de la sección 5.7 de VVSG 2007 y se presenta a continuación:

“Un *evento* es algo que ocurre en un dispositivo de votación y un *historial* es un registro de estos eventos que han ocurrido. Cada registro de un historial contiene información relacionada a un evento específico. Los historiales son utilizados para reportar errores, auditoría, solución de problemas, optimizar el rendimiento, registrar las acciones de los usuarios, y proveer datos útiles para investigar actividad maliciosa”. (TGDC, 235)

La descripción de cada uno de los eventos mínimos de la tabla 3 se encuentra en la sección 5.7 de VVSG 2007 (páginas 240 – 241). El documento que contiene el estándar VVSG 2007 está citado en la bibliografía de esta tesis y además se incluye en formato digital como archivo adjunto a este documento de tesis.

Es necesario señalar que todas estas funciones de auditoría consumen recursos del sistema. Algunas funciones consumen tantos recursos que pueden afectar considerablemente el rendimiento de la aplicación, como por ejemplo el

monitoreo del sistema de archivos. Si el rendimiento de la aplicación se ve afectado, se deberá alcanzar un balance entre funciones de auditoría y rendimiento.

Resultado

Los diferentes componentes del sistema (sistema operativo, servidor de aplicaciones, base de datos y aplicación) tienen funciones y herramientas que permiten monitorear y registrar los eventos. Se pueden realizar las acciones recomendadas en la tabla de eventos que aparece en el análisis de este requerimiento para cumplir con el mismo.

5.7.1-E.1

Número	5.7.1-E.1
Título	Requerimiento de deshabilitación mínima de los historiales
Aplica a	Dispositivo programado
Descripción	El dispositivo de votación DEBE asegurar que el mínimo de registro de eventos en Part 1:Table 5-5 no pueda ser deshabilitado.

Análisis

Mientras no se permita acceso al sistema diferente al acceso Web a la aplicación desde clientes externos, los historiales no se pueden deshabilitar sin tener acceso físico al servidor y a la cuenta de administrador del sistema operativo y a la cuenta de administrador (SYSDBA) base de datos.

No es factible impedir que el administrador deshabilite los historiales por el diseño del sistema operativo.

Resultado

Se debe deshabilitar todo acceso externo al servidor a excepción del acceso Web durante las elecciones. Se debe asegurar cualquier acceso del administrador al sistema sea autorizado.

5.7.3-A

Número	5.7.3-A
Título	Requerimiento de protección general de los historiales
Aplica a	Dispositivo programado
Descripción	El dispositivo de votación DEBE proteger la información de los historiales de eventos de acceso, modificación y eliminación no autorizados.

Análisis

Mientras no se permita acceso al sistema diferente al acceso Web a la aplicación desde clientes externos, los historiales no se pueden ver, modificar ni borrar sin tener acceso físico al servidor y a la cuenta de administrador del sistema operativo y a la cuenta de administrador (SYSDBA) base de datos.

No es factible impedir que el administrador vea, modifique o borre los historiales por el diseño del sistema operativo.

Resultado

Se debe deshabilitar todo acceso externo al servidor a excepción del acceso Web durante las elecciones. Se debe asegurar cualquier acceso del administrador al sistema sea autorizado.

5.7.3-B

Número	5.7.3-B
Título	Requerimiento de protección de modificación
Aplica a	Dispositivo de votación
Descripción	El dispositivo de votación DEBE proteger los historiales de modificación no autorizada.

Análisis

Mientras no se permita acceso al sistema diferente al acceso Web a la aplicación desde clientes externos, los historiales no se pueden modificar sin tener acceso físico al servidor y a la cuenta de administrador del sistema operativo y a la cuenta de administrador (SYSDBA) base de datos.

No es factible impedir que el administrador modifique los historiales por el diseño del sistema operativo.

Resultado

Se debe deshabilitar todo acceso externo al servidor a excepción del acceso Web durante las elecciones. Se debe asegurar cualquier acceso del administrador al sistema sea autorizado.

5.7.3-C

Número	5.7.3-C
Título	Requerimiento de protección de archivos de historiales de eventos
Aplica a	Dispositivo programado
Descripción	Si el dispositivo de votación tiene capacidad para archivar los historiales, DEBE asegurar la integridad y disponibilidad de los historiales archivados.

Análisis

Los historiales pueden ser guardados en archivos y almacenados en un repositorio (archive) de las elecciones.

Para mantener la integridad de los historiales se puede firmarlos digitalmente o realizar una operación hash sobre el archivo y guardar el resultado para compararlo cuando sea necesario hacer una comprobación de integridad.

El repositorio de elecciones se puede mantener en el servidor o también puede ser guardado en otros medios físicos; esta última opción puede ayudar a la disponibilidad de la información. Lo que se haga con el repositorio de las elecciones será decidido por el organismo regulador de las elecciones.

Resultado

Para cumplir con este requerimiento se firmarán digitalmente los historiales o se creará un código de comprobación para mantener su integridad; además se podrá mantener el repositorio de las elecciones en medios de almacenamiento para mantener su disponibilidad, de acuerdo a la decisión del organismo regulador de las elecciones.

Capítulo 4 – Mejoras al sistema

4.1 Registro independiente verificable por el elector

Descripción

Se separó la información del elector de su voto. La información del voto consiste en el código de confirmación del elector y su voto, lo cual puede ser auditado independientemente por cualquier sistema independiente.

Se creó la función de envío de la información de los votos recibidos a un servidor independiente. El sistema recibe el voto del elector y, además de registrarlo en la misma base de datos del sistema, lo envía tal y como lo recibe en forma de un datagrama a un destino especificado por el administrador de la base de datos.

Aplica a:

- 4.2.1-A
- 4.2.2-A
- 5.7.1-C

Estado anterior del sistema

El sistema no incluía algún tipo de verificación independiente.

Los votos en el sistema se registraban en una tabla llamada VOTO de la siguiente manera:

Columna	Descripción
CI	Cédula de identidad del elector
IDCANDIDATO	Número único de identificación del candidato
FECHAHORA	Fecha y hora en la que se ingresa el voto

Tabla 4: Tabla VOTO anterior

El número de cédula (CI) identifica al elector. El número de identificación del candidato (IDCANDIDATO) identifica al candidato por el cual el elector ha votado. En este esquema se vincula al elector con su voto y esto es visible para quien tenga acceso a ejecutar consultas en la base de datos; de esta manera se pierde la confidencialidad del voto.

Además, el código de confirmación (CODICONF) se almacenaba en la tabla ELECTOR, vinculando el código de confirmación al elector al cual pertenece.

Cambios realizados

Se modificó la tabla VOTO de la siguiente manera:

Columna	Descripción
IDCANDIDATO	Número único de identificación del candidato
CODICONF	Código de confirmación de 25 caracteres (letras y números) generado de manera aleatoria
FECHAHORA	Fecha y hora en la que se ingresa el voto

Tabla 5: Tabla VOTO actualizada

Para elecciones de tipo consulta o referéndum se ha cambiado la estructura de la base de datos para que en lugar de almacenar el número de identificación de un candidato almacene el identificador único de la pregunta y el voto que ha realizado en ésta:

Columna	Descripción
IDPREGUNTASINO	Número único de identificación de la pregunta
VOTO	Voto realizado (0 = blanco; 1 = SI; 2 = NO; 3 = nulo)
CODICONF	Código de confirmación de 25 caracteres (letras y números) generado de manera aleatoria
FECHAHORA	Fecha y hora en la que se ingresa el voto

Tabla 6: Tabla VOTO para preguntas y consultas

Como se puede observar, se elimina la referencia del elector en las tablas que contienen los votos.

El código de confirmación no se almacena en algún otro lugar y solo es mostrado una vez y solo al elector; el código se muestra una vez que el usuario ingresa su voto desde la pantalla que muestra el voto con la opción de regresar y modificarlo o ingresarlo definitivamente. De esta manera solo el elector puede conocer su código de confirmación; debido a que el código de confirmación es generado de manera aleatoria, no se puede conocer a quién corresponde el código, manteniendo la confidencialidad del voto.

Se creó la tabla CONTROL y en ella un registro llamado INDEPENDENT1 que contiene un valor correspondiente a una dirección IP (v4) y otro valor

correspondiente a un número de puerto. El sistema envía a la dirección especificada un datagrama construido con el código de confirmación y el número de identificación del candidato, separados por una coma “,”. El número de puerto especifica el puerto desde donde se envía el datagrama y donde se recibe.

Se crea un registro en el historial por el ingreso de un voto y por cada envío de información.

4.2 Advertencia de privacidad visual

Descripción

El sistema advierte al usuario que se debe mantener la privacidad visual antes de ingresar a votar.

Aplica a:

- 3.2.3.1-A.1

Estado anterior del sistema

El sistema no mostraba advertencias sobre privacidad visual.

Cambios realizados

El sistema tiene una pantalla de inicio donde se pide al usuario que ingrese su número de cédula de identidad y la contraseña. En esta pantalla se ha agregado un texto de advertencia para indicar al usuario que debe continuar solo si no hay alguna persona observándolo.

Esto es similar al mensaje de advertencia que se muestra al utilizar un cajero automático. El objetivo es recordar que la privacidad del usuario es importante y que el usuario debe tomar las precauciones necesarias para mantener la privacidad.

4.3 Estado del sistema

Descripción

El sistema debe manejar 4 estados como especifica el requerimiento 5.4.1.C: pre-elecciones (apagado), activo, suspendido y post-elecciones (finalizado).

Aplica a:

- 5.4.1-C

Estado anterior del sistema

El sistema no utilizaba los estados. Los únicos posibles de estados eran activo, si el sistema estaba funcionando, y apagado, si el sistema no estaba funcionando.

Cambios realizados

Para poder manejar diferentes estados en el sistema, lo primero que se hizo fue agregar una entrada denominada ESTADO en la tabla CONTROL con los siguentes valores:

- 0 - apagado
- 1 - activo
- 2 - suspendido
- 3 - finalizado

El administrador del sistema puede establecer el estado del sistema modificando esta entrada y colocando el valor numérico correspondiente al estado.

El código de la aplicación comprueba el estado del sistema antes de presentar la pantalla de inicio y antes de registrar un voto. De esta manera se asegura que un usuario no pueda ingresar a votar en un estado en el que no se puede votar, y que si ya había ingresado mientras el sistema estaba activo (1) y el estado cambió antes de que ingrese su voto, que no se registre el voto.

Durante el estado activo (1) el sistema funciona normalmente. Los otros estados muestran una pantalla informativa al elector. Para el estado finalizado (4) se muestra la hora actual además de la información del estado, debido a que las

elecciones finalizan a una hora específica y es útil mostrar al elector que la hora límite para las elecciones ya ha pasado.

En el código se comprueba que la entrada ESTADO tenga un valor válido. En el caso de que el valor no sea válido, no se permite que los electores voten.

4.4 Bloqueo de la cuenta de un usuario por exceso de intentos

Descripción

Las cuentas de los usuarios (electores) se deben bloquear después de un número indicado de intentos para prevenir que personas o máquinas realicen ataques con el objetivo de ingresar al sistema como algún elector adivinando su contraseña.

Esta función se ha agregado al sistema, pero su uso dependerá del organismo regulador de las elecciones debido a las implicaciones que pueda tener (por ejemplo, negar el derecho de votar a cualquier persona, sin importar la razón).

Aplica a:

- 5.4.3-G

Estado anterior del sistema

El sistema no bloqueaba las cuentas de usuarios.

Cambios realizados

La validación de la cuenta del usuario y su contraseña ahora adicionalmente verifica el número de intentos de ingreso que se han realizado con la contraseña incorrecta.

Se agregó en la tabla ELECTOR la columna INTENTOS, la cual almacena el número de intentos con la contraseña incorrecta. Cada vez que el usuario intenta entrar y su contrasena es incorrecta se suma 1 al contador del usuario.

Todos los electores deben iniciar con sus cuentas creadas con el contador de intentos en cero. Esto se puede verificar en la comprobación inicial del sistema (requerimiento 5.7.1-E).

Cada intento con una contraseña incorrecta es registrado en el historial del sistema.

Se agregó el registro INTENTOSELECTOR en la tabla CONTROL, la cual especifica el número máximo de intentos erróneos permitidos.

Se creó una página informativa que se muestra al usuario cuando su cuenta ha sido bloqueada.

4.5 Registros e historiales

Descripción

El sistema debe mantener registros e historiales de todos los eventos relacionados al sistema y a las elecciones para: permitir auditorías, anticipar problemas, diagnosticar y corregir errores, controlar posibles ataques al sistema y almacenar la información requerida por el organismo regulador de las elecciones.

Aplica a:

- 5.7.1-A
- 5.7.1-D
- 5.7.1-E

Estado anterior del sistema

No se registraban eventos en la aplicación. Los eventos del sistema operativo se registran independientemente.

Cambios realizados

Se habilitaron diferentes tipos de registros e historiales que indica el requerimiento 5.7.1-E:

Mensajes de errores y excepciones generados por los dispositivos; eventos de medios removibles

Se habilitaron los mensajes del sistema operativo hasta el nivel 7; esto permitirá registrar todo tipo de evento. Estos registros estan en la ubicación /var/log dentro del sistema operativo linux.

Este tipo de registros dependen del sistema operativo. Cada vez que se implemente la aplicación en un nuevo servidor se deberá volver a habilitar este registro.

Autentificación

Se registran los siguientes eventos de autentifiación en el sistema:

- El usuario ingresa al sistema exitosamente
- El usuario no está registrado en el sistema
- El usuario ha intentado ingresar con una contraseña incorrecta
- El usuario ha excedido el número de intentos de ingreso
- El usuario finaliza su sesión

Mensajes de estado críticos y no críticos del sistema; inicio y apagado del sistema; eventos de votación

El sistema registra ahora tres tipos de mensajes de estado:

- 1 – Informativos
- 2 – Alertas

- 3 – Errores

Los mensajes son enviados al standard input, el cual puede ser capturado y almacenado de diferentes maneras, como sea necesario. Por ejemplo, en Oracle Application Server el standard input es almacenado como parte de los historiales de la aplicación y está disponible en la herramienta Oracle Enterprise Manager; otra manera es ejecutar el servidor (JBoss, OC4J, etc) desde la consola de linux y capturar el standard input hacia un archivo.

En este sistema de elecciones cada página y cada managed bean tienen una lógica definida. La tabla 7, en el anexo 3, muestra todos los mensajes registrados por el sistema, organizados por la página o managed bean donde se generó el mensaje.

Los mensajes de estado críticos (errores y excepciones) y el inicio y apagado de la aplicación están en el historial de OC4J, que es el servidor de aplicaciones que maneja la aplicación. En este historial se puede ver el inicio del sistema, el stack trace completo de errores y excepciones, y la finalización del sistema. Se modificó a la aplicación para que todo error o excepción devuelva el stack trace hacia el standard output.

Cambios a la configuración del sistema; cambios a las opciones de configuración

El sistema operativo Linux sobre el cual funciona este sistema de elecciones tiene varios archivos de configuración. La protección y el registro de cambios de estos archivos dependerán de cada implementación.

Para esta implementación se trabajó con el programa *changetrack*, el cual es gratuito y está disponible en SourceForge.net. Este programa mantiene una base de datos similar a SVN donde se almacenan cada cierto período los archivos de configuración; el usuario define cuánto dura ese perídodo y cuáles son los archivos que se deben monitorear. En esta implemetación se especificó que la base de datos se actualiza todos los días a las 12h00 y que se monitorean los siguientes archivos de configuración:

- Todos los archivos con extensión ".conf" en el directorio /etc, los cuales tienen la configuración del sistema operativo linux
- Los archivos con extensión ".xml" en el directorio OC4J_HOME/j2ee/home/config, los cuales tienen la configuración del servidor de aplicaciones y de la aplicación de elecciones
- Los archivos con extensión ".ora" en el directorio ORACLE_HOME/network/admin, los cuales tienen la configuración de la base de datos

El programa changetrack permite, además de ver las modificaciones a los archivos, restaurar versiones anteriores de los mismos.

Resultados de la comprobación inicial del sistema

Se añadió primero una comprobación inicial del sistema. Esta comprobación hace consultas a la base de datos y obtiene la siguiente información:

Código	***Mensaje***	***Valor***
I010	Fecha y hora de la comprobacion del sistema	Fecha y hora (ej: 2008-07-02T16:29:40 -0500)
I011	Estado del sistema	[Apagado; Activo; Suspendido; Finalizado]
I012	Numero total de electores	Total calculado
I014	Electores habilitados para votar	Total calculado
I015	Electores que no disponen de una contrasena	Total calculado
I016	Electores que han sido inhabilitados por sobrepasar el numero de intentos de ingreso	Total calculado
I017	Numero maximo de intentos de ingreso permitidos	Parámetro de la aplicación
I018	Electores que ya han votado	Total calculado
I019	Electores que no han votado	Total calculado

Tabla 7: Comprobación del sistema

Esta comprobación se la puede hacer, además de antes de iniciar las elecciones, durante las elecciones y al final de las elecciones, de ser requerido.

La lógica de esta comprobación y la interfaz que despliega los resultados están en la página ad_test.jsp. Se puede imprimir los resultados a un archivo o documento físico para mantenerlo como registro. Además, se envía al standard output los resultados de todos estos valores con fecha y hora, como todos los demás registros; así se puede saber cuándo se hizo la comprobación del sistema y cuáles son los valores, evitando posibles modificaciones a los resultados.

Instalación, actualización, instalación de parches o modificación de software o firmware

Esto depende de la implementación. En RedHat se utiliza la herramienta RPM para instalar software y parches. En SuSE se utiliza la herramienta YAST para instalar software y parches. Ambas herramientas generan historiales de todas las modificaciones.

4.6 Uso de criptografía

Descripción

La comunicación entre el cliente y el servidor debe utilizar criptografía. La criptografía debe ser generada en un módulo aprobado para FIPS 140-2 operando en modo FIPS.

Aplica a:

- 5.1.1-A
- 5.1.1-B
- 5.4.3-A

Estado anterior del sistema

No se utilizaba criptografía usando la certificación FIPS 140-2.

Cambios realizados

Se instaló la aplicación sobre el servidor de aplicaciones Oracle Application Server. Esto requirió de cambios en la manera de acceder a los EJB, pues el modelo es distinto a Jboss, que es el servidor de aplicaciones donde se desarrolló la aplicación.

Se agregó el parámetro SQLNET.SSLFIPS_140=TRUE al archivo de configuración sqlnet.ora. De esta manera, Oracle Application Server funciona en modo FIPS, operando de acuerdo a la certificación FIPS 140-2.

Se instaló un certificado SSL otorgado por una autoridad de certificación (CA), permitiendo la autentificación del servidor, y se habilitó la comunicación por SSL entre los clientes y el servidor.

El certificado SSL se lo obtuvo de la compañía COMODO con los siguientes datos:

- Common Name [CN]: votoecuador.com
- Organizational Unit [OU]: Unknown
- Organization [O]: votoecuador.com
- Location [L]: Quito
- State [ST]: Pichincha
- Country [C]: EC

De la autoridad de certificación se obtuvieron los siguientes archivos de certificación:

- AddTrustExternalCARoot.crt – El certificado raíz

- EssentialSSLCA.crt – El certificado de la compañía

- votoecuador_com.crt – El certificado del sitio

El pedido de certificación y el keystore donde se almacenan los certificados se generaron utilizando la herramienta keytool de la máquina de Java JRockit, sobre la cual es ejecutado el servidor de aplicaciones OC4J.

El certificado instalado es reconocido por los principales navegadores de Internet, incluyendo Microsoft Internet Explorer y Mozilla Firefox.

Capítulo 5 – Análisis de la implementación de prueba

5.1 Características de la implementación

Servidor	Notebook HP Pavillion
Procesador	Intel Celeron Core Duo 2
Memoria RAM	1 GB
Sistema operativo	Novell SuSE Linux Enterprise Server 10 (Kernel 2.6.16.46-0.12-smp)
Base de datos	Oracle Database 10g Release 2 Enterprise Edition
Servidor de aplicaciones	Oracle Containers for Java (OC4J)
Java JDK	Oracle JRockit R27.5 (JDK 1.5.0_14)
Conexión a Internet	sDSL 1 Mbps
Dominio	votoecuador.com
Autoridad de certificación (CA)	InstantSSL (COMODO)
Ubicación	Quito, Ecuador (GMT-5)
Fecha y hora de inicio	2 de julio de 2008, 16h30
Fecha y hora de finalización	9 de julio de 2008, 16h30
Número de personas que participaron	467

Tabla 8: Características de la implementación

Para esta implementación se habilitó el envío del código de confirmación a la dirección de correo electrónico especificada por el usuario. Esta característica es única de esta implementación y no se habilitará en una elección real sin un estudio previo de riesgos de seguridad.

5.2 Antes de las elecciones

Retirar unidades removibles y deshabilitar puertos de comunicación

La única unidad de medios removibles en este computador es la unidad de CD/DVD. Se desmontó la unidad y se deshabilitó el montaje automático de este medio en /etc/fstab.

Se eliminó el montaje automático de unidades USB en /etc/fstab.

El único usuario que puede montar unidades de medios removibles es root, el cual está protegido por contraseña.

Deshabilitar funciones de respaldo y recuperación del sistema operativo y base de datos

El sistema operativo no tiene activada alguna función de backup automático.

La base de datos dispone de funciones de respaldo y recuperación. Se verificó que estas funciones no estén habilitadas. Solo los administradores de la base de datos, que son los usuarios SYS y SYSMAN, pueden iniciar o hablilitar las funciones de respaldo, y estos usuarios están protegidos por contraseña.

Deshabilitar todo acceso al sistema a excepción del acceso Web

Se está usando el cortafuegos (firewall) de SuSE Linux Enterprise para permitir la comunicación solo en puertos que proporcionen los servicios de la aplicación. Se dejaron habilitados los siguientes puertos:

- 22 – Secure Shell (SSH)

  Este puerto permite conectarse a una terminal remota segura para monitorear el servidor, ver los registros e historiales y corregir posibles problemas.

- 80 – HTTP

La única comunicación HTTP necesaria es para acceder a la página /index.html que es la página que el explorador busca al acceder al sitio sin especificar una página (www.votoecuador.com). Esta página redirecciona al sitio seguro, usando SSL.

También se podría utilizar este puerto en caso de que sea necesario acceder a las herramientas iSQLPlus y Oracle Enterprise Manager para solucionar problemas. Ambas herramientas tienen protección por contraseña.

- 4443 – HTTPS

  Se utiliza el puerto 4443 para la comunicación entre el navegador de Internet y el servidor utilizando SSL.

- 4011

  Se envían datagramas con la información de los votos al servidor de verificación independiente por el puerto 4011. No se establecen ni se reciben conexiones TCP por este puerto.

- 110 – POP3; 25 – SMTP

  El servidor se utiliza por esta ocasión también como servidor de correo para enviar y recibir correo con el dominio votoecuador.com. Esto es una excepción por no disponer de otro servidor que cumpla esta función; para una implementación real se deberá utilizar otro servidor para este propósito.

Además de permitir la comunicación solo por los puertos especificados, se han controlado las aplicaciones y servicios que operan en estos puertos.

- sshd

  sshd proporciona el servicio SSH

- oc4j

  oc4j es el servidor de aplicaciones Oracle Containers for Java

- smtp, pop3

  smtp y pop3 pertenecen al servidor de correo Merak y proporcionan los servicios de correo. Esto es una excepción por no disponer de otro servidor que cumpla esta función; para una implementación real se deberá utilizar otro servidor para ejecutar estos procesos.

Estado inicial del sistema

Parámetro	***Valor***
Fecha y hora de la comprobacion del sistema	2008-07-02T16:29:40 -0500
Estado del sistema	Activo
Numero total de electores	0
Electores habilitados para votar	0
Electores que no disponen de una contrasena	0
Electores que han sido inhabilitados por sobrepasar el numero de intentos de ingreso	0
Numero maximo de intentos de ingreso permitidos	5
Electores que ya han votado	0
Electores que no han votado	0

Tabla 9: Estado inicial del sistema para la implementación de prueba

Registro de electores

En esta implementación de prueba no se dispone de una base de datos de electores. Es por esta razón que el sistema muestra en la comprobación inicial un total de cero electores habilitados para votar. En una implementación real se deberá disponer de una base de datos con todos los electores registrados.

Para esta implementación se habilitó una página de registro donde, después de ingresar su número de cédula, los usuarios ingresan sus nombres y apellidos, su dirección de correo electrónico y una contraseña que pueden utilizar para ingresar al sistema. Una vez que el elector ingresa sus datos se lo registra en el sistema; es decir, se crea en la base de datos un registro con los datos de este elector.

A cada elector registrado se le permite votar una sola vez; esto se verifica con el número de cédula del elector. No se permite registrar más de un elector con el mismo número de cédula.

De esta manera no se dispone de un ambiente idéntico al verdadero al no tener una base de datos de electores. Sin embargo, se pudo evaluar todas las directrices VVSG 2007 a excepción de una (4.3.3-C), como se demuestra en la sección 5.5.

5.3 Durante las elecciones

El sistema se ejecutó desde el inicio de las pruebas, el 2 de julio del 2008 a las 16h30, hasta la finalización el 9 de julio del 2008 a las 16h30. El sistema funcionó sin interrupciones durante este período de tiempo de 10080 minutos.

El sistema fue monitoreado todos los días para verificar su disponibilidad, seguridad y desempeño.

Entre las acciones que se ejecutaron para comprobar la seguridad del sistema están:

Monitoreo del historial de la aplicación

Este historial se verificaba varias veces al día para controlar:

- Accesos a la aplicación, tanto exitosos como fallidos.
- Conexiones a la base de datos.
- Errores y excepciones en la aplicación.
- Terminaciones anormales del sistema.
- Resultados de la comprobación del sistema.
- Actividad en el sistema.

Monitoreo de los historiales del sistema

Se verificaron los historiales del sistema (/var/log) para controlar:

- Errores del sistema.
- Eventos de medios removibles.
- Accesos remotos al sistema.
- Eventos del cortafuegos (firewall).

Monitoreo de conexiones de red

Se verificó en tiempos aleatorios el estado de las conexiones activas utilizando la herramienta netstat para comprobar que solo los procesos permitidos tenían conexiones activas.

Monitoreo de los archivos de configuración

Los archivos de configuración se comparaban cada día para buscar posibles cambios utilizando la herramienta changetrack, como se detalla en la descripción de las mejoras al sistema.

5.4 Después de las elecciones

Se cerraron las elecciones el día 9 de julio del 2008 a las 16h30 cambiando el estado de la aplicación a Finalizado. De esta manera se impidió cualquier voto pasada la hora de finalización.

Se comprobó que no hubo más votos después de la hora de finalización.

Accesos al sistema

El proceso sshd, que proporciona el servicio SSH, reportó miles de intentos de ingreso incorrectos de las siguientes direcciones IP:

```
64.88.177.59
209.23.72.100
81.171.35.65
220.227.91.180
203.199.200.43
189.21.198.99
190.2.41.217
218.12.196.5
58.240.48.27
190.4.2.69
```

El listado completo de los intentos de conexión se encuentran en el archivo “messages”.

Las siguientes líneas son un ejemplo de los registros generados por estos intentos de conexión que, al parecer, intentaban ingresar al sistema adivinando el nombre de usuario y contraseña:

Jul 9 08:09:28 informate1now sshd[18047]: Invalid user staff from 58.240.48.27

Jul 9 08:09:31 informate1now sshd[18052]: Invalid user sales from 58.240.48.27

Jul 9 08:09:34 informate1now sshd[18057]: Invalid user recruit from 58.240.48.27

Jul 9 08:09:37 informate1now sshd[18062]: Invalid user alias from 58.240.48.27

Jul 9 08:09:41 informate1now sshd[18067]: Invalid user office from 58.240.48.27

Jul 9 08:09:45 informate1now sshd[18072]: Invalid user samba from 58.240.48.27

Jul 9 08:09:48 informate1now sshd[18077]: Invalid user tomcat from 58.240.48.27

Jul 9 08:09:52 informate1now sshd[18083]: Invalid user webadmin from 58.240.48.27

Ninguno de estos intentos de acceso fue exitoso. Los únicos accesos exitosos reportados por sshd corresponden a los accesos para el monitoreo del sistema.

Estos intentos de acceso no afectaron a la disponibilidad del sistema.

Estado del sistema al finalizar las elecciones

Parámetro	***Valor***
Fecha y hora de la comprobacion del sistema	2008-07-09T13:13:29 -0500
Estado del sistema	Finalizado
Numero total de electores	467
Electores habilitados para votar	459
Electores que no disponen de una contrasena	8
Electores que han sido inhabilitados por sobrepasar el numero de intentos de ingreso	0
Numero maximo de intentos de ingreso permitidos	5
Electores que ya han votado	430
Electores que no han votado	37

Tabla 10: Estado del sistema al finalizar la implementación de prueba

Registros e historiales

Se obtuvieron los siguientes registros e historiales al terminar las elecciones:

- EMS tabulator summary count record (EMS TSCR.txt): Registro de resumen de la información de todos los tabuladores en el sistema. Solo se utilizó un tabulador.

- Tabulator Summary Count (TSC.txt): Registro de la información de cada tabulador. Solo se utilizó un tabulador.

- Historial de la aplicación (application.log): Historial que contiene todo el standard output generado por Oracle Containers for Java, que contiene los mensajes de la aplicación, mensajes de OC4J, eventos de las elecciones, errores y excepciones.

- messages, warn: Registros de todos los eventos del sistema operativo.

- boot.msg, boot.omsg: Registro de los eventos de inicio del computador.

- firewall: Registro de todos los eventos del cortafuegos.

- electores.html: Registro de los números de cédula de identidad y nombres de todos los electores que participaron.

- rs_referendum.html: Registro de resultados del tabulador.

- votos.html: Registro de todos los votos (ballots), que contiene el código de confirmación y el número correspondiente al voto (0, 1, 2, 3).

Todos los registros fueron firmados digitalmente usando la llave privada obtenida de la autoridad de certificación COMODO InstantSSL para estas elecciones. Las firmas digitales de cada registro están en los archivos con el mismo nombre del registro y con extensión .sign (ejemplo: boot.msg.sign).

Todos los registros mencionados y sus archivos de firma digital se incluyen como parte de esta tesis como archivos adjuntos. Para análisis de esta tesis se

incluyen los archivos legibles, sin cifrado. En una elección real se almacenan estos registros cifrados y bajo control del organismo regulador de las elecciones.

Errores en el sistema

- El sistema no reconocía caracteres especiales al digitar la cédula de identidad; solo se aceptan números. Cuando los usuarios escribieron caracteres especiales se mostró una pantalla de error.
- Cuando el usuario dejaba el campo de correo electrónico en blanco, el sistema generaba una excepción NullPointerException al intentar enviar el mensaje.

Ningún error causó que un elector no pueda votar, que su voto se registre incorrectamente o que pueda votar más de una vez.

5.5 Directrices VVSG 2007

Las siguientes tablas muestran un resumen todas las directrices del estándar VVSG 2007 analizadas y el estado del cumplimiento de esta implementación basado en el estudio de factibilidad de aplicación de las mismas.

El estudio de factibilidad, la descripción de las mejoras y el análisis de la implementación contienen más detalles acerca del estado de los requerimientos.

Integridad

Num. de requerimiento	*Cumple*	*Estado*
4.2.1-A	Sí	Se implementó el método de verificación independiente descrito en este estudio.

4.2.2-A	Sí	Se implementó el método de verificación independiente descrito en este estudio.
4.3.1-A	Sí	Todos los registros se pueden exportar a archivos.
4.3.1-B	Sí	Todos los registros se pueden imprimir.
4.3.1-C	Sí	Se firmaron digitalmente todos los registros de las elecciones con la llave privada otorgada por la autoridad de certificación.
4.3.2-A	Sí	Se creó el reporte TSC.
4.3.2-B	Sí	Se exportó el reporte TSC y se lo incluyó junto a los demás registros del sistema.
4.3.2-C	Sí	Se creó un registro de todos los votos (ballots) recibidos por el sistema.
4.3.2-C.1	Sí	Se creó un registro de todos los votos (ballots) recibidos por el sistema.
4.3.2-C.2	Sí	Se exportó el reporte de todos los votos (ballots) y se lo incluyó junto a los demás registros del sistema.
4.3.2-D	Sí	Se exportó el historial de eventos de la aplicación, se lo firmó digitalmente y se lo incluyó junto con los demás registros del sistema.
4.3.3-A	Sí	Se creó el reporte de resumen de tabuladores.
4.3.3-B	N/A	No se dividieron a los electores por recintos electorales.
4.3.3-C	N/A	En esta implementación se permitió el voto a todas las personas; no existieron casos en que se niegue el voto a alguna persona por no estar calificada.
4.3.4-A	N/A	El sistema solo utiliza un tabulador.
4.3.5-A	Sí	El sistema tuvo un contador de votos no calculado.
4.3.5-B	Sí	El contador de votos era accesible a cualquier momento sin interrumpir las elecciones.
5.5.1-A	No	No se disponía del hardware necesario en esta implementación.
5.5.1-B	No	No se disponía del hardware necesario en esta implementación.
5.5.1-C	Sí	El sistema utiliza la protección de recursos entre procesos del sistema operativo.
5.5.2-A	Sí	Se inhabilitaron las unidades removibles y puertos de comunicación.
5.5.3-A	Sí	Ninguna función de respaldo y recuperación estuvo activa.

Tabla 11: Cumplimiento de las directrices de integridad

Confidencialidad

Num. de requerimiento	*Cumple*	*Estado*
3.2.3.1-A	Sí	El sistema no vincula el voto a la información identificable del elector y no se publicó informacion que permita al elector demostrar cómo votó.
3.2.3.1-A.1	Sí	Se incluyó la advertencia de privacidad en la pantalla inicial.
3.2.3.1-A.3	Sí	Los mensajes al usuario no revelan información confidencial.
3.2.3.1-A.4	Sí	El recibo (código de confirmación) no muestra cómo ha votado el elector.
3.2.3.2-A	Sí	El sistema no utiliza idiomas alternativos.
3.2.3.2-B	Sí	El sistema no tiene funciones de accesibilidad.
4.3.3-A.1	Sí	El número de electores no permite identificarlos o descubrir sus votos.
5.1.1-A	Sí	El sistema utiliza el módulo de criptografía de Oracle validado por FIPS.
5.1.1-B	Sí	El sistema utiliza el módulo de criptografía de Oracle validado por FIPS.

Tabla 12: Cumplimiento de las directrices de confidencialidad

Autentificación

Num. de requerimiento	*Cumple*	*Estado*
5.4.1-A	Sí	El acceso al sistema está protegido por contraseña.
5.4.1-A.1	N/A	No existen roles distintos para acceder al sistema, solo electores. El acceso al sistema está protegido por contraseña.
5.4.1-B	Sí	Se deshabilitó todo acceso remoto al sistema a excepción de los mencionados en el análisis de la implementación.
5.4.1-C	Sí	El sistema maneja los 4 estados que pide este requerimiento. Se muestra una pantalla de información para los estados no activos del sistema.
5.4.1-E	Sí	Se deshabilitó todo acceso remoto al sistema a excepción de los mencionados en el análisis de la implementación.
5.4.3-A	Sí	El acceso al sistema está protegido por contraseña.
5.4.3-B	N/A	No se utiliza el rol de administrador en el sistema; el acceso es solo para electores.
5.4.3-C	N/A	No se utiliza el rol de administrador en el sistema; el acceso es solo para electores.
5.4.3-D	No	El sistema no guarda información en los dispositivos de votación; sin embargo, algunos navegadores de Internet permiten guardar contraseñas.
5.4.3-G	Sí	Se deshabilitan las cuentas de usuarios que sobrepasan un límite de intentos de ingreso configurable.
5.4.3-H	No	No se especifica por cuánto tiempo se bloquea una cuenta de usuario.

Tabla 13: Cumplimiento de las directrices de autentificación

No repudiación

Num. de requerimiento	*Cumple*	*Estado*
5.7.1-A	Sí	El sistema registra los eventos de votación en el historial de la aplicación.
5.7.1-B	Sí	Se firmaron digitalmente todos los registros de las elecciones con la llave privada otorgada por la autoridad de certificación.
5.7.1-C	Sí	El sistema no tiene información que revele datos confidenciales de los electores.
5.7.1-D	Sí	El sistema registra los eventos de los electores en el historial de la aplicación.
5.7.1-D.1	Sí	El sistema puede generar valores de fecha y hora.
5.7.1-D.2	Sí	El sistema genera valores de fecha y hora con precisión de milisegundos.
5.7.1-D.3	Sí	Los historiales incluyen la fecha, hora, minuto y segundo de cada evento.
5.7.1-D.4	No	Las fechas se registran con el estándar ISO 8601, pero no se incluyó la zona horaria.
5.7.1-D.5	Sí	El cambio de la fecha y hora solo lo puede ejecutar el administrador del sistema.
5.7.1-D.6	Sí	El reloj del servidor cumple con el desvío máximo.
5.7.1-E	Sí	Se registraron los eventos que dicta esta directriz.

5.7.1-E.1	Sí	El acceso a los historiales está restringido solo al administrador del sistema.
5.7.3-A	Sí	El acceso a los historiales está restringido solo al administrador del sistema.
5.7.3-B	Sí	El acceso a los historiales está restringido solo al administrador del sistema.
5.7.3-C	Sí	Se firmaron digitalmente todos los registros de las elecciones con la llave privada otorgada por la autoridad de certificación.

Tabla 12: Cumplimiento de las directrices de no repudiación

Capítulo 6 – Conclusiones y recomendaciones finales

6.1 Conclusiones

Este estudio cumple con el objetivo de evaluar la factibilidad de aplicar las directrices de seguridad del estándar VVSG 2007 seleccionadas. Todas las directrices seleccionadas fueron analizadas para determinar si el sistema cumplía con ellas. En los casos en que el sistema no cumplía con una directriz, se hicieron recomendaciones para lograr que el sistema cumpla con la directriz.

Existen directrices simples cuyo cumplimiento se puede demostrar fácilmente; por ejemplo, la directriz 5.7.1-D.4 que establece el formato de la fecha y hora que se debe usar en los historiales. Otras directrices tienen varias formas de resolverse; por ejemplo, la directriz 4.2.1-A que requiere un método de verificación independiente realizado por el elector.

Algunas directrices se pueden cumplir con cambios en el código de la aplicación como, por ejemplo, la directriz 4.3.5-A que se resolvió creando un contador no calculado de votos. Otras directrices dependen del ambiente de instalación, conformado por el hardware y software donde se instala la aplicación; por ejemplo, la directriz 5.5.2-A requiere que se deshabiliten las unidades de medios removibles del servidor donde funciona la aplicación. Por esta razón el sistema debe considerarse como el conjunto de la aplicación y el ambiente donde se la instala.

Todos los sistemas de votación electrónica están en constante desarrollo. Este estándar provee una guía para el desarrollo de los mismos. Al utilizar un estándar como el VVSG 2007 se garantiza que se van a utilizar directrices que han sido elaboradas por un grupo respetado de estándares, como es NIST, y que están basadas en la experiencia de varios años de desarrollo de sistemas de elecciones. La responsabilidad de crear un sistema con un alto nivel de seguridad es del equipo de desarrollo del sistema.

Probablemente la mejor definición de un sistema seguro es que no existe un sistema seguro. Hay muchas causas que crean riesgos de seguridad en todos los sistemas electrónicos como, por ejemplo, los posibles errores de código y el desarrollo de hardware con más capacidad de procesamiento que permita descubrir contraseñas. Además, la aplicación de un estándar no garantiza que un sistema sea seguro. Los sistemas electrónicos son utilizados en la actualidad por los usuarios y organizaciones con la confianza de que se han realizado todas las acciones posibles para minimizar los riesgos de seguridad en dichos sistemas. Este esfuerzo de aplicar las directrices del estándar VVSG 2007 debe ser una de las acciones que se realicen para lograr un nivel de seguridad que minimice los riesgos de seguridad en este sistema de elecciones.

La implementación de prueba fue un éxito considerando que:

- Se contó con la participación de 467 personas, de las cuales solo 2 conocían el sistema antes de comenzar a utilizarlo; es decir, se logró realizar una prueba con usuarios reales.
- El sistema nunca dejó de funcionar desde el inicio hasta el final de las elecciones.
- Los registros e historiales muestran que los resultados de las elecciones no fueron modificados.
- Ningún usuario puede demostrar cómo votó a otra persona con la información que se le proporcionó.
- Se mantiene la confidencialidad del voto al ser imposible vincular a un elector con su voto en la base de datos del sistema.
- Todos los votos de los usuarios fueron registrados y contados para los resultados.
- No existió algún acceso no autorizado al sistema.
- El número de errores en la aplicación fue mínimo.
- Ningún error causó que un usuario esté impedido de votar.
- Esta fue la primera prueba abierta del sistema.

Este sistema de elecciones es un prototipo. Para que este sistema esté listo para utilizarse en una elección real se necesitará trabajar constantemente en la seguridad del mismo; esto además de otras posibles modificaciones necesarias para cumplir con las leyes vigentes, estándares de rendimiento, estándares de interfaz de usuario y la ejecución de pruebas paralelas a las elecciones reales, utilizando una

base de datos con los electores proporcionada por el organismo regulador de las elecciones.

Este estudio y las mejoras realizadas al sistema son un esfuerzo para minimizar los riesgos de seguridad. Los resultados de la implementación proporcionan son una prueba de que el sistema cuenta con un nivel de seguridad que permitió cumplir con todos los objetivos de integridad, confidencialidad, autentificación y no repudiación que establecen las directrices estudiadas del estándar VVSG 2007.

6.2 Recomendaciones finales

- Se deben monitorear constantemente los riesgos de seguridad y el cumplimiento de las directrices del estándar utilizado. Todo cambio de código, equipos, aplicaciones, infraestructura, tecnología y cualquier cambio que afecte directamente o indirectamente al sistema puede crear nuevos riesgos de seguridad y puede causar que se dejen de cumplir las directrices que antes se cumplían.
- Se debe incluir la zona horaria en los registros de los historiales (5.7.1-D.4)
- Se debe realizar una prueba verificando la integridad del código con hardware de criptografía resistente a cambios (5.5.1-A, 5.5.1-B)
- La autentificación del usuario no debe permitir que el dispositivo cliente guarde los datos de autentificación (5.4.3-D). Una alternativa es indicar al

usuario que deshabilite las funciones que guardan datos de autentificación del navegador Web.

- Se debe realizar una prueba que divida a los electores por recintos electorales (4.3.3-B)
- El registro de electores debe ser un servicio que no esté integrado en este sistema; solo los electores calificados para votar deben ser ingresados en la base de datos de este sistema (4.3.3-C)
- El estándar VVSG 2007 está siendo revisado y puede cambiar. Si el estándar es modificado, se deberá volver a evaluar el sistema.
- Se deben buscar constantemente formas de mejorar la seguridad del sistema, en todo sentido. Ejemplos: evaluar el sistema con otros estándares de seguridad, contratar auditores externos, realizar pruebas de ataques al sistema, etc.

Anexo 1: Registro independiente verificable por el elector

VVSG 2007 requiere que los sistemas de votación sean verificables independientemente por el elector. Esto tiene el objetivo de que, aunque un sistema sea electrónico, se pueda comprobar que los resultados son los mismos que el sistema dice haciendo las comprobaciones que el organismo regulador de las elecciones considere convenientes; por ejemplo, un conteo independiente (posiblemente manual).

Para esto se tienen dos registros de los votos separados: el registro del sistema de elecciones y el registro que tendrá un sistema independiente. El sistema es independiente porque es manejado por una organización distinta al organismo regulador de las elecciones. Por ejemplo, si las elecciones las maneja el Tribunal Supremo Electoral en Ecuador, la organización Participación Ciudadana puede ser quien tenga el control del sistema independiente. El registro independiente servirá para auditar al registro del sistema, comparando ambos registros. Así se podrá asegurar que no se han modificado, introducido o eliminado votos del sistema.

Los requerimientos de VVSG 2007 para la verificación independiente no dictan cómo se debe realizar la auditoría de los resultados; eso depende del organismo regulador de las elecciones. En lugar de eso, dicen qué debe tener el sistema de elecciones para estar listo para una auditoría de sus registros.

(TGDC, 151 - 154)

Una opción que se presenta en VVSG 2007 es Voter-Verifyable Paper Audit Trail (VVPAT). VVPAT es un recibo impreso en papel que tiene dos partes: la primera parte muestra el voto del elector; la segunda parte es un recibo que comprueba que el elector votó. La primera parte se muestra al elector y se queda en el sitio de votación. La segunda parte se la lleva el elector. De esta manera el elector mira que haya una prueba de cuál fue su voto, pero no se la puede mostrar a nadie.

VVPAT no es perfecto; tiene los siguientes defectos:

- No garantiza que el sistema haya guardado el mismo resultado que está mostrando en papel.
- Se asume que el papel que contiene el voto del elector será tratado confidencialmente.
- Se confía que quien haga el conteo manual de los papeles lo haga correctamente.

(Popoveniuc, p. 6 - 10)

Ningún sistema de verificación independiente es perfecto. Todo dependerá de la implementación.

Para este sistema se propone una alternativa de verificación independiente flexible que se puede adaptar a la forma requerida. Se basa simplemente en el envío de la información del voto tal y como será grabada en el sistema de elecciones al sistema independiente. Esta es la forma más abierta y flexible de permitir la auditoría

independiente de resultados que se puede lograr con este sistema. De esta manera no se indica cómo se debe manejar la información, ni qué se debe hacer con ella, ni cualquier limitación que haría que la información sea controlada o manipulada por este sistema; así se puede lograr la mejor apertura a verificación independiente posible de acuerdo a las características de este sistema.

En el sistema se registra un código único generado para cada elector. Este código no revela el nombre, número de cédula o cualquier otra información que pueda revelar la identidad del elector; el código no está basado en información del elector. Este código es mostrado al elector una vez que ha emitido su voto y sirve para mantener el registro de que ese elector ha votado. El voto se almacena en el sistema en conjunto con el código del elector.

El código de voto del elector y su voto se almacenan en tablas separadas. La razón para hacer esto es que en tablas separadas se asignan permisos distintos. De esta manera solo el sistema tiene acceso a ambos datos; en este sistema ninguna persona (a excepción del administrador del sistema) deberá tener acceso a la información en conjunto del código del usuario y su voto. Para evitar que el administrador del sistema pueda obtener esta información, cualquier acceso que realice es registrado en el historial y debe ser vigilado por delegados del organismo regulador de elecciones; además no existirán medios de almacenamiento removibles donde se pueda copiar la información de acuerdo al requerimiento 5.5.2-A.

La información que se envía es la misma que se registra en el sistema: el código del elector y su voto. El objetivo es que los electores puedan ver que su código está en los registros y que la auditoría independiente pueda contar los votos.

Existe una sola recomendación en cuanto a la información proporcionada. Se van a enviar tanto el código de voto del elector como su voto. Para que la información mantenga la integridad y sea verificable, se vincula el código del elector con su voto. El sistema de verificación independiente debe mantener oculto este vínculo para cualquier persona. El elector podrá ver que su código está en el registro, mostrándole que su voto ha sido recibido, pero no podrá ver su propio voto para mantener la confidencialidad y evitar que el elector pueda mostrar a otras personas cómo votó. Quien o quienes hagan el conteo independiente podrán ver los votos pero no deberán ver a qué código corresponde cada voto; aunque puedan ver el código no tendrán manera de saber a quién corresponde cada código, pero es información confidencial que no corresponde a la función de contar los votos. Un caso posible de que se muestre el código del elector y su voto sería si un elector accede a una verificación voluntaria de su voto y se verifica que su voto fue registrado correctamente; este tipo de verificaciones no se hacen en la actualidad pero es posible con este sistema y se menciona aquí como un ejemplo.

El manejo de la información enviada es responsabilidad del o de los verificadores independientes; solo así se mantiene la independencia completa de la verificación externa.

La información que llega al sistema independiente se la puede manejar de cualquier manera. Por ejemplo, puede almacenarse en una base de datos para posterior verificación; puede mostrarse en pantallas o ser impresa en papel en el sitio de votación para verificación inmediata del elector; puede ser impresa en un sitio asignado por el organismo regulador de las elecciones como registro verificable. Se pueden inventar muchas otras maneras de utilizar esta información como registro verificable.

Un ejemplo que se puede implementar fácilmente es almacenar esta información en una base de datos accesible desde el Internet. Se puede incluir un servidor configurado solo para recibir información desde el servidor de la aplicación. El servidor independiente no debe enviar información al servidor de la aplicación. El servidor de la aplicación no debe aceptar conexiones desde el servidor independiente. El servidor de la base de datos del sistema de elecciones (si es separado del servidor de la aplicación) no debe ser visible para el servidor independiente.

La única función accesible a cualquier persona por Web es que cada elector pueda verificar que su código ha sido registrado; así verifican que su voto está en el registro y será contabilizado. La información de los votos será accesible solo para el administrador del sistema independiente (con responsabilidad sobre la información) para realizar el conteo.

Se repite nuevamente que este ejemplo mencionado es solo una de las maneras en que se puede manejar la información enviada por el sistema.

Se incluye un diagrama de la comunicación entre los servidores de este ejemplo.

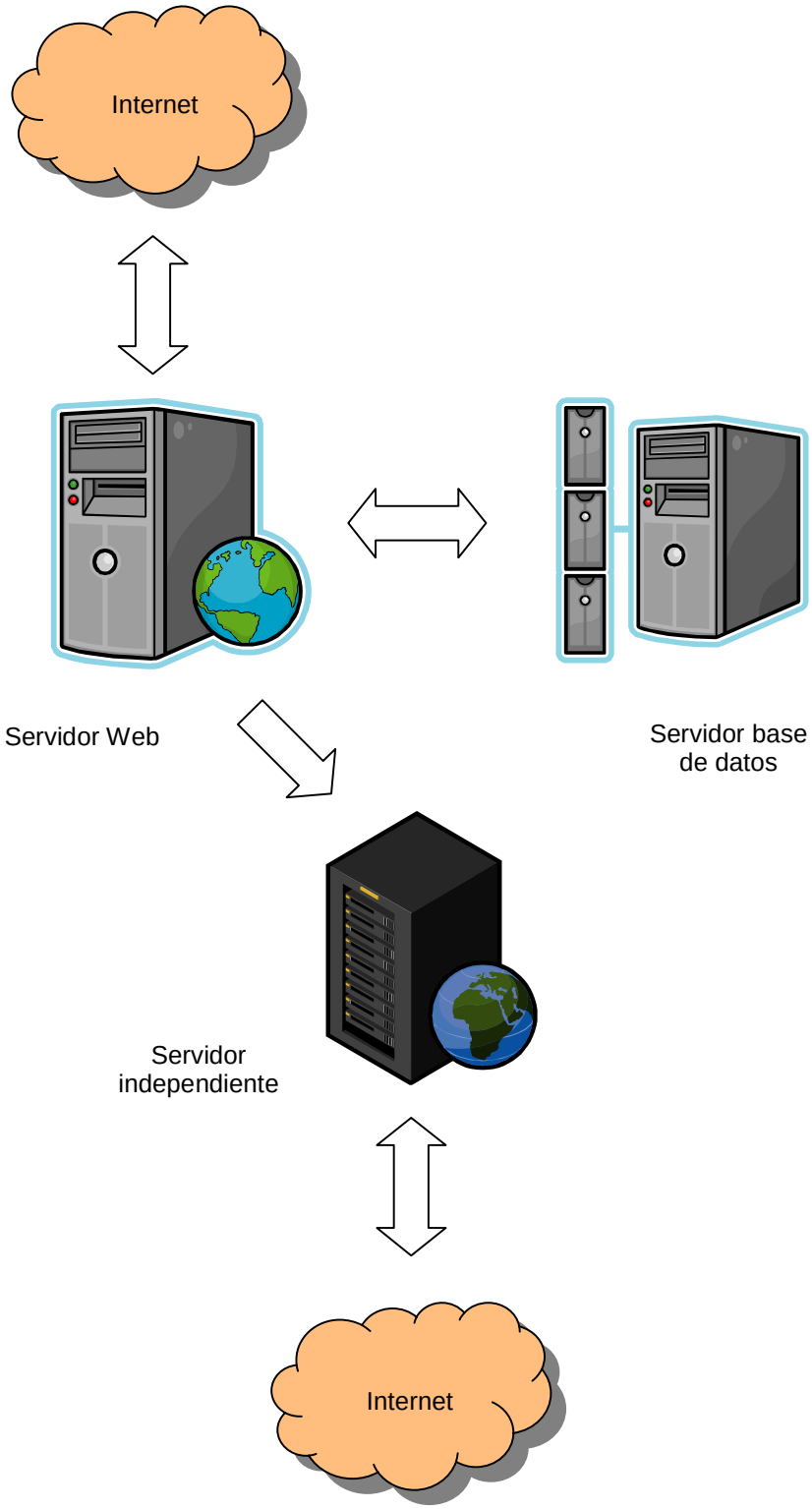


Figura 4. Diagrama de comunicación para implementación IVVR

Anexo 2: Autentificación del cliente – dos contraseñas

El sistema de elecciones denominado mivoto.com.ec es un sistema diseñado para tener un servidor central el cual soporta a la aplicación de elecciones. La aplicación es un servicio Web al que se conecta cualquier computador personal con acceso a Internet.

Varios requerimientos de VVSG 2007 están orientados a dispositivos de votación fabricados específicamente para el sistema de elecciones. Cambiar el sistema de elecciones mivoto.com.ec a un modelo con dispositivos de votación específicos para el sistema requiere rediseñar el sistema, y esto está fuera del alcance de esta tesis. Sin embargo, se analiza un posible diseño del sistema con la configuración mencionada con el objetivo de comparar ambos tipos de diseño y de poder incluir estos criterios en el análisis de algunos requerimientos.

La autentificación por parte del computador cliente con el servidor del sistema permite que sólo los computadores registrados puedan iniciar una sesión de votación; de esta manera, los electores no podrían votar desde cualquier computador personal.

Para utilizar autentificación del computador cliente se puede utilizar el método de contraseñas; esto funcionaría de la siguiente manera:

a) El sitio de votación tiene un nombre único. Ejemplo: Colegio Don Bosco.

b) El encargado del sitio de votación (“Election Judge” en VVSG) tiene una contraseña, la cual funcionará solo en ese sitio de votación. El encargado puede ser una persona delegada o asignada por el organismo regulador de las elecciones.
c) Un delegado del organismo regulador de las elecciones (“Central Election Official” en VVSG) tiene otra contraseña.
d) El sistema se autentificará con el servidor utilizando el nombre del sitio, ambas contraseñas y la fecha y hora. Solo cuando el servidor acepte los datos permitirá al cliente ejecutar sesiones de votación; eso es, solo así mostrará la pantalla para que el elector ingrese a votar.
e) Para mejorar la seguridad se puede también autentificar datos específicos del cliente como direcciones IP preestablecidas.

Este método tiene las siguientes características:

- Se puede votar solo en sitios autorizados.
- La persona encargada del sitio de votación no puede iniciar por su propia decisión sesiones de votación.
- Los delegados del organismo regulador de las elecciones no pueden iniciar por su propia decisión sesiones de votación.
- No se pueden iniciar sesiones de votación fuera de la fecha y hora permitida para las elecciones.
- Personas ajenas al control de elecciones no pueden iniciar sesiones de votación.

- Se puede registrar el sitio donde el elector votó.
- El elector no puede votar desde su computador personal
- Se requiere un esfuerzo de logística para asignar personas encargadas de los sitios de votación, los delegados del organismo regulador de elecciones, para distribuir seguramente las contraseñas, para asignar direcciones IP fijas.
- Se necesita capacitación para las personas asignadas a las tareas antes descritas.
- Se necesita comprar, alquilar o de alguna manera contratar computadores personales para los sitios de votación.
- Se necesita conseguir un lugar con acceso a Internet para que funcione como sitio de votación.

Anexo 3: Mensajes del sistema

Ubicación	***Código***	***Mensaje***
vt_inicio.jsp	E001	El parametro de estado del sistema tiene un valor incorrecto
vt_inicio.jsp	E002	No se pudo conectar a la base de datos para obtener el estado del sistema
Vt_inicio.java	I001	Intento de ingreso del usuario '%usuario%'
Vt_inicio.java	I002	El usuario '%usuario%' ha realizado el intento numero '%intentos%' de ingreso con la contrasena incorrecta
Vt_inicio.java	I003	El usuario '%usuario%' ha iniciado una sesion en el sistema
Vt_inicio.java	A001	No existe el usuario '%usuario%'
Vt_inicio.java	A002	El usuario '%usuario%' ha exedido el numero de intentos de ingreso
Vt_inicio.java	E003	No se pudo conectar a la base de datos para validar el usuario
Vt_inicio.java	E004	No se pudo iniciar la sesion para el usuario '%usuario%'
VotanteBean.java	E005	No se pudo conectar a la base de datos para obtener el estado del sistema en VotanteBean.java
Vt_principal.java	A003	No se pudo terminar la sesion de base de datos para el usuario '%usuario%'
Vt_principal.java	A004	No se pudo acceder al bean Votante de la sesion actual
Vt_principal.java	I004	El usuario '%usuario%' ha terminado la sesion
Vt_principal.java	I005	El usuario '%usuario%' ha comenzado a votar
Vt_principal.java	I006	El usuario '%usuario%' intento votar despues de ya tener su voto registrado
Vt_presi.java	A005	No se pudo acceder al bean Votante de la sesion actual
Vt_dipu.java	A006	No se pudo acceder al bean Votante de la sesion actual
Vt_dipu_pro.java	A007	No se pudo acceder al bean Votante de la sesion actual
vt_conf.jsp	A008	No se pudo acceder al bean Votante de la sesion actual
Vt_conf.java	I007	El elector '%usuario%' ha intentado votar pero el sistema esta finalizado
Vt_conf.java	I008	El elector '%usuario%' ha intentado votar pero el sistema esta suspendido
Vt_conf.java	I009	El elector '%usuario%' ha votado exitosamente
Vt_conf.java	A009	No se pudo acceder al bean Votante de la sesion actual
Vt_conf.java	E006	El intento de voto del elector '%usuario%' ha fallado

Ubicación	***Código***	***Mensaje***
Vt_conf.java	A012	El elector '%usuario%' ha intentado ingresar un voto pero ya tiene registrado su voto en el sistema
Vt_conf.java	E008	El sistema no puede conectarse al puerto %puerto% para enviar datos
Vt_conf.java	A013	La direccion IP %ip% puede no ser valida
Vt_conf.java	E009	La direccion IP especificada para enviar los datos %ip% no es valida
Vt_conf.java	I020	Enviando el voto [%codigo%,%idcandidato%] a la direccion %ip%:%puerto%
Vt_conf.java	E010	No se pudo enviar el voto [%codigo%,%idcandidato%] a la direccion %ip%:%puerto%
Vt_conf.java	I021	Enviando el contador de votos [%contador%] a la direccion %ip%:%puerto%
Vt_conf.java	E011	No se pudo enviar el contador de votos [%contador%] a la direccion %ip%:%puerto%
Vt_conf.java	E012	No se pudo obtener el objeto Elector del bean
Vt_conf.java	E013	No se pudo crear el codigo de confirmacion para el elector %usuario%
vt_final.jsp	A010	No se pudo acceder al bean Votante de la sesion actual
vt_final.jsp	E014	No se puede obtener el codigo de confirmacion del elector %usuario%
Vt_final.java	A011	No se pudo acceder al bean Votante de la sesion actual
Vt_final.java	I005	El usuario '%usuario%' ha terminado la sesion
ad_test.jsp	E007	No se pudo conectar a la base de datos
ad_test.jsp	I010	Fecha y hora de la comprobacion del sistema: %fechaHora%
ad_test.jsp	I011	Estado del sistema: %estado%
ad_test.jsp	I012	Numero total de electores: %electores%
ad_test.jsp	I013	Numero total de candidatos: %candidatos%
ad_test.jsp	I014	Electores habilitados para votar: %electores%
ad_test.jsp	I015	Electores que no disponen de una contrasena: %electores%
ad_test.jsp	I016	Electores que han sido inhabilitados por sobrepasar el numero de intentos de ingreso: %electores%
ad_test.jsp	I017	Numero maximo de intentos de ingreso permitidos: %intentos%
ad_test.jsp	I018	Electores que ya han votado: %electores%
ad_test.jsp	I019	Electores que no han votado: %electores%

Tabla 14: Mensajes del sistema

Bibliografía

Technical Guidelines Development Committee (TGDC). “Voluntary Voting System Guidelines Recommendations to the Election Assistance Commission”. 31 Ago 2007.

Stefan Popoveniuc. “A technical analysis of the VVSG 2007”. The PunchScan Project. George Washington University.

Andrew S. Tanenbaum. “Modern Operating Systems”. Second edition. Prentice-Hall, 2001.

Elaine Barker, William Barker, William Burr, William Polk, Miles Smid. “Recommendation for Key Management”. National Institute of Standards and Technology (NIST). Mar 2007.

EL UNIVERSO (2006). “El proceso electoral costará $ 11,5 millones más”. 15 May 2006.
<http://archivo.eluniverso.com/2006/05/15/0001/8/AB23E67498814589A57667258EB59031.aspx >

EL UNIVERSO (2006). “TSE trabajará con técnicos ecuatorianos para desarrollar urnas electrónicas”. 10 Jul 2006.
<http://www.eluniverso.com/2006/07/10/0001/8/67614F29F5034750AE3D47CE2B600EDB.aspx>

National Institute of Standards and Technology (2003). "NIST and the Help America Vote Act of 2002". National Institute of Standards and Technology. 30 Jul 2003
<http://www.nist.gov/public_affairs/factsheet/voting_symposium.htm>

Technical Guidelines Development Committee. “Voluntary Voting System Guidelines Recommendations to the Election Assistance Commission”. 31 Ago 2007.

Wikipedia contributors. “Trusted Platform Module.”. 17 Sep 2008. Wikipedia, The Free Encyclopedia. 18 Sep 2008. <http://en.wikipedia.org/w/index.php?title=Trusted_Platform_Module&oldid=239003681>

Wikipedia. “FIPS 140-2”. 20 Nov 2007. Wikimedia Foundation, Inc. 2 May 2008. <http://en.wikipedia.org/w/index.php?title=FIPS_140-2&oldid=172738027>

Oracle. "Oracle 10g Application Server (9.0.4) FIPS Certification". Oracle Corporation. 2 May 2008 <http://www.oracle.com/technology/deploy/security/as_security/sslfipsfaq_r1.html>

ISO. “ISO – FAQs – Date and time format”. International Organization for Standarization. 7 May 2008. <http://www.iso.org/iso/date_and_time_format>

die.net. ”syslog(2) – Linux man page” . Man Pages. Die.net. 11 May 2008 <http://linux.die.net/man/2/syslog>