

**PROPUESTA TÉCNICA
"AUDITORIA TÉCNICA AL SOFTWARE DE VOTACIÓN
AUTOMATIZADA", JCE
FIRMA DE AUDITORÍA: GUZMÁN TAPIA PKF**

Propuesta Técnica o descripción del servicio ofertado

**PROPUESTA TÉCNICA
"AUDITORIA TÉCNICA AL SOFTWARE DE VOTACIÓN
AUTOMATIZADA", JCE
FIRMA DE AUDITORÍA: GUZMÁN TAPIA PKF**

INDICE

- Quienes Somos	14
- Nuestra dirección de Auditorías de TI	16
- Reseña de experiencia en trabajos recientes de auditoría de TI	17
- Información sobre el nivel de Especialización del Personal que acompañará la Firma PKF en el trabajo de "Auditoria Técnica al Software de Votación Automatizada"	19
- Descripción de la Metodología para ejecutar el trabajo	22
- Plan para ejecutar el trabajo	38
- Currículos recientes firmados por el personal profesional propuesto y del Representante Autorizado	43

PROPUESTA TÉCNICA
"AUDITORIA TÉCNICA AL SOFTWARE DE VOTACIÓN
AUTOMATIZADA", JCE
FIRMA DE AUDITORÍA: GUZMÁN TAPIA PKF

1. QUIENES SOMOS

USD \$2.4bn ganancias globales,
400+ oficinas,
Operando en 150 países
Alrededor de 5 regiones

PKF



PKF International Limited es una red de firmas legalmente independientes y no acepta ninguna responsabilidad por las acciones o omisiones de cualquier miembro individual o miembro asociado o firma.

Guzmán Tapia PKF es una firma Dominicana de auditores y consultores, miembro de PKF International Limited, una red de firmas legalmente independientes. Hay 300 firmas miembro y corresponsales exclusivos en 440 ubicaciones en alrededor de 125 países.

Somos una organización profesional local con Posicionamiento Internacional, sabemos cómo interpretar y satisfacer las necesidades de los clientes, dando soluciones personalizadas en cada área de los servicios que prestamos. Tenemos la mejor combinación de experiencia, compromiso, conocimiento y profesionalismo.

Guzmán Tapia PKF es una firma con más de 40 años de experiencia, trabajando en la prestación de servicios y soluciones diversas en materia de Auditoría, Consultoría, Impuestos, entre otros.

Nuestro modelo de trabajo diferenciador está diseñado para *"Aportar valor a los negocios de nuestros clientes"*.

Tenemos amplia experiencia en diferentes industrias y áreas de la economía basada en la experiencia de los socios de la firma y los que compartimos con nuestra red.

Nuestros clientes locales e internacionales avalan la calidad de nuestros servicios.

PROPUESTA TÉCNICA
"AUDITORIA TÉCNICA AL SOFTWARE DE VOTACIÓN
AUTOMATIZADA", JCE
FIRMA DE AUDITORÍA: GUZMÁN TAPIA PKF

Contamos con más de 60 profesionales ubicados en el país y un expertise internacional distribuido en todas las regiones del mundo.

PKF Republica Dominicana está ubicada en Santo Domingo y es una de las top 3 mejores firmas en el país con presencia en Bancos de RD.

SECTORES DE EXPERIENCIA |



Administración Pública	Agricultura, Forestación	Banca Central	Banca Múltiple y de Ahorro y Crédito	Bienes Raíces
Casas de Cambio	Comercio Mayorista y Minorista	Construcción	Generación de Electricidad	Hospitalidad
Hotelería y Turismo	Mercado de Valores	Minería	ONG	Seguros
Servicios Médicos	Transportes y Puertos	Universidades y Colegios		

CERTIFICACIONES RELEVANTES |



- Instituto de Contadores Públicos Autorizados de Republica Dominicana (ICPAD)
- Miembro de la Asociación de Firmas de Contadores Públicos de la RD
- Miembro pleno del Foro de Firmas de la Federación Internacional de Contadores (IFAC)
- Superintendencia de Bancos de la Republica Dominicana (SIB)
- Superintendencia del Mercado de Valores de la Republica Dominicana (SIMV)
- Superintendencia de Seguros de la Republica Dominicana
- Superintendencia de Pensiones de la Republica Dominicana
- Comisión de Bolsa y de Valores de los Estados Unidos (SEC) a través de nuestras oficinas de PKF en Nueva York teniendo la capacidad de emitir informes financieros auditados para las instancias antes mencionadas.
- Registrado como Auditores Independientes del BID (Banco Interamericano de Desarrollo)
- Reconocidos como Auditores por la USAID
- Reconocidos como Auditores por la Inter American Foundation, organización dependiente del Senado de los Estados Unidos

PROPUESTA TÉCNICA
"AUDITORIA TÉCNICA AL SOFTWARE DE VOTACIÓN
AUTOMATIZADA", JCE
FIRMA DE AUDITORÍA: GUZMÁN TAPIA PKF

2. NUESTRA DIRECCIÓN DE AUDITORÍAS DE TI

La Empresa Dominicana Guzmán Tapia PKF miembro de PKF International Limited cuenta en la Dirección de Auditorías de Tecnologías de la Información (TI) con profesionales con más de 20 años de experiencia en TI sumados a nivel local e internacional en Bancos y Empresas prestigiosas de Latinoamérica, contando con personal con Certificaciones Internacionales de ISACA válidas a nivel mundial como:

CISA • - *Certified Information Systems Auditor* •
CRISC™ - *Certified in Risk and Information Systems Control™*
CISM • - *Certified Information Security Manager* •

Y otras certificaciones como:

CISSP - *Certified Security Systems Security Professional*
CEH - *Certified Ethical Hacker*
ISO 27001 LA - *Certificado Profesional Líder en Auditoría de Seguridad ISO 27001.*

El trabajo desarrollado por nuestros Auditores de TI locales e internacionales es basado en metodologías y estándares internacionales como:

- **COBIT** Marco de Gobierno y Control de TI.
- **ISO 27001** Sistema de Gestión de Seguridad de la Información.
- **ISO 27002** Controles de Seguridad de la Información.
- **ISO 22301** de Continuidad de Negocio
- **ISO 27031** de Continuidad de TI (Plan de Recuperación ante Desastres de TI)
- **ISO 27005, NIST, MAGERIT** para análisis de riesgos tecnológicos.
- **ISO 25000** para Evaluar la calidad del Sistema y el producto software.
- **ISO 9126** para la evaluación de la calidad del software
- Mejores prácticas de gestión y administración de hardware y software.
- Aplicación de Software de Auditoría (IDEA y ACL).

PROPUESTA TÉCNICA
"AUDITORIA TÉCNICA AL SOFTWARE DE VOTACIÓN
AUTOMATIZADA", JCE
FIRMA DE AUDITORÍA: GUZMÁN TAPIA PKF

3. RESEÑA DE EXPERIENCIA EN TRABAJOS RECIENTES DE AUDITORÍA DE TI

La Firma Gumán Tapia PKF en los últimos 10 años, ha realizado Auditorías de TI a los siguientes Bancos y Empresas.

BANCO/EMPRESA	AÑOS
• BANCO PROGRESO	2009 hasta 2015
• BANCO SANTA CRUZ	2009 hasta 2016
• BANCO CARIBE	2009 hasta 2016
• BANCO DE DESARROLLO INDUSTRIAL (BDI)	2009 hasta la fecha
• BANCO LÓPEZ DE HARO (BLH)	2009 hasta la fecha
• BANCO ADEMI S.A.	2014 hasta la fecha
• BANCO VIMENCA	2017 hasta la fecha
• BANCO ACTIVO	2017 hasta la fecha
• BANCO CONFISA	2017 hasta la fecha
• BANCO EMPIRE	2009 hasta 2018
• BANCO CAPITAL	2009 hasta 2015
• BANCO FEDERAL	2016 hasta 2018
• Grupo SID (MERCASID)	2010 hasta la fecha
• CORPORACIÓN DE CRÉDITO REIDCO	2010 hasta la fecha
• METALDOM	2010 hasta 2016

Asimismo, desde nuestra creación hemos tenido a los siguientes clientes, y la gran mayoría siguen recibiendo nuestros servicios en Auditorías Financieras en las que incluimos la evaluación o Auditoría de TI:



PROPUESTA TÉCNICA
"AUDITORIA TÉCNICA AL SOFTWARE DE VOTACIÓN
AUTOMATIZADA", JCE
FIRMA DE AUDITORÍA: GUZMÁN TAPIA PKF





Santo Domingo, D. N.
12 de Agosto 2019

A quien corresponda:

El Banco Múltiple BDI, S.A., de la República Dominicana, certifica que la Firma Guzmán Tapia PKF es nuestro Auditor Externo desde el año 1999 a la fecha, quienes además de las Auditorías Financieras, realizan Auditorías de Tecnologías de la Información (TI), haciendo énfasis en la evaluación de Seguridad de la Información, Seguridad Lógica y Física Tecnológica, verificación de procesos de TI, implementación y pruebas del Plan de Continuidad del negocio (BCP), y del Plan de Recuperación ante Desastres Informáticos (DRP), verificando riesgos tecnológicos que podrían afectar la continuidad de las operaciones del Banco y el logro de los objetivos institucionales, además de verificar el cumplimiento de Normas y Estándares Internacionales relacionados a TI.

Es cuanto certifico a petición del interesado.

Yamil A. Mendez Beltré

Director Administrativo y Financiero



Banco Múltiple BDI, S.A.
RNC 1-01-04029-7
Av. Sarasota No.27, La Julia

T 809-535-8586
WWW.bdi.com.do



Santo Domingo, D. N.
12 de Agosto 2019

A quien corresponda:

El BANCO MÚLTIPLE LOPEZ DE HARO, S. A., entidad constituida y existente de conformidad con las leyes de la República Dominicana, provista del R. N. C. No.1-01-14588-9, con su domicilio social principal en la Ave. Sarasota No.20, La Julia, de esta ciudad de Santo Domingo, Distrito Nacional, República Dominicana, certifica que la Firma Guzmán Tapia PKF ha sido nuestro Auditor Externo por más de diez años, quienes además de las Auditorías Financieras, realizan Auditorías de Tecnologías de la Información (TI) haciendo énfasis en la evaluación de Seguridad de la Información, Seguridad Lógica y Física Tecnológica, verificación de procesos de TI, implementación y pruebas del Plan de Continuidad del Negocio (BCP) y del Plan de Recuperación ante Desastres Informáticos (DRP), verificando riesgos tecnológicos que podrían afectar la continuidad de las operaciones del Banco y el logro de los objetivos institucionales, además de verificar el cumplimiento de Normas y Estándares Internacionales relacionados a TI.

Es cuanto certifico a petición del interesado.

A quien corresponda:

Loamy Then Tiburcio
Vicepresidencia de Auditoría Interna





Santo Domingo, D. N.
12 de Agosto 2019

A quien pueda interesar

El Banco Múltiple Ademi, S.A., de la República Dominicana, por este medio certifica que la Firma de Auditores Externos, Guzmán Tapia- PKF es nuestro Auditor Externo desde el año 2012 y hasta la fecha, quienes además de las Auditorías Financieras, realizan Auditorías de Tecnologías de la Información (TI), haciendo énfasis en la evaluación de Seguridad de la Información, Seguridad Lógica, Física y Tecnológica, verificación de procesos de TI, implementación y pruebas del Plan de Continuidad del negocio (BCP), y del Plan de Recuperación ante Desastres Informáticos (DRP), verificando riesgos tecnológicos que podrían afectar la continuidad de las operaciones del Banco y el logro de los objetivos institucionales, además de verificar el cumplimiento de Normas y Estándares Internacionales relacionados a TI.

Esta certificación se emite a petición del interesado.

Cordialmente,



Olga Aponte

Vicepresidente Finanzas, Administración y Planificación



A QUIEN PUEDA INTERESAR

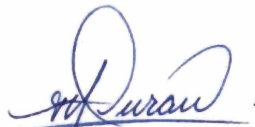
Por medio certificamos que la firma Auditores Externos Guzmán Tapia PKF nos ha estado prestando sus servicios desde el año 2016 hasta la fecha.

En tal sentido, hacemos constar que dicha firma además de las Auditorías Financieras, nos realiza también Auditorías de Tecnologías de la Información (TI), haciendo énfasis en la Evaluación de Seguridad de la Información, Seguridad Lógica y Física Tecnológica, Verificación de Procesos de TI, Implementación y Pruebas del Plan de Continuidad del Negocio (BCP), y del Plan de Recuperación ante Desastres Informáticos (DRP), verificando riesgos tecnológicos que podrían afectar la continuidad de las operaciones de la institución, además verifica el Cumplimiento de Normas y Estándares Internacionales relacionados a TI.

De acuerdo a los resultados del trabajo realizado por la firma **Guzmán Tapia PKF** podemos decir que esta prestigiosa empresa muestra un destacado nivel de profesionalidad y cuenta con un personal bien capacitado y con excelentes valores personales.

La presente certificación se expide a solicitud de la parte interesada, en Santo Domingo, Distrito Nacional, a los quince (15) días del mes de agosto de año dos mil diez y nueve (2019).

Atentamente,



Maricela A. Durán

Vicepresidente de Administración & Finanzas





BANCO CONFISA
De Ahorro y Crédito, S. A.

Santo Domingo de Guzmán, D. N.
12 de agosto de 2019

A QUIÉN PUEDE INTERESAR

Muy amablemente nos permitimos certificar que la Firma Guzmán Tapia PKF es nuestro proveedor habitual de los servicios de auditoría externa del Banco de Ahorro y Crédito Confisa, S. A., desde el año 2017 a la fecha. Quienes además de las Auditorías Financieras, realizan Auditorías de Tecnologías de la Información (TI), haciendo énfasis en la evaluación de Seguridad de la Información, Seguridad Lógica y Física Tecnológica, verificación de procesos de TI, implementación y pruebas del Plan de Continuidad del negocio (BCP), y del Plan de Recuperación ante Desastres Informáticos (DRP), verificando riesgos tecnológicos que podrían afectar la continuidad de las operaciones del Banco y el logro de los objetivos institucionales, además de verificar el cumplimiento de Normas y Estándares Internacionales relacionados a TI.

Se expide la presente certificación en la ciudad de Santo Domingo de Guzmán, D. N., a los doce (12) días del mes de agosto del año 2019.

Sin otro particular por el momento, se despide, atentamente,


Ing. Silvestre Aybar Mota
Vice Presidente



BANCO DE AHORRO Y CRÉDITO CONFISA, S. A.

C/ Francisco Prats Ramírez No. 149, esq. Manuel de Jesús Troncoso, Ens. Plantini • Tel.: 809-227-1066 • Fax: 809-541-6173 • Santo Domingo, D. N.
Suc. Puerto Plata: Ave. Luis Ginebra Km. 1 • Av. Presidente Antonio Guzmán Fernández, Caribbean Plaza No. 15, Suite 3, San Francisco de Macorís.
Tels.: 809-586-3171 y 809-586-4676 • Fax: 809-320-8705 • www.confisa.com.do

RNC 1-01-09009-1



Leasing Confisa
Corporación de Crédito, S. A.

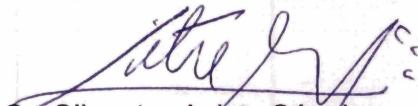
Santo Domingo de Guzmán, D. N.
12 de agosto de 2019

A QUIÉN PUEDE INTERESAR

Muy amablemente nos permitimos certificar que la Firma Guzmán Tapia PKF es nuestro proveedor habitual de los servicios de auditoría externa de la Corporación de Crédito Leasing Confisa, S. A., desde el año 2017 a la fecha. Quienes además de las Auditorías Financieras, realizan Auditorías de Tecnologías de la Información (TI), haciendo énfasis en la evaluación de Seguridad de la Información, Seguridad Lógica y Física Tecnológica, verificación de procesos de TI, implementación y pruebas del Plan de Continuidad del negocio (BCP), y del Plan de Recuperación ante Desastres Informáticos (DRP), verificando riesgos tecnológicos que podrían afectar la continuidad de las operaciones de la Corporación y el logro de los objetivos institucionales, además de verificar el cumplimiento de Normas y Estándares Internacionales relacionados a TI.

Se expide la presente certificación en la ciudad de Santo Domingo de Guzmán, D. N., a los doce (12) días del mes de agosto del año 2019.

Sin otro particular por el momento, se despide, atentamente,


Sr. Silvestre Aybar Sánchez
Presidente



PROPUESTA TÉCNICA
"AUDITORIA TÉCNICA AL SOFTWARE DE VOTACIÓN
AUTOMATIZADA", JCE
FIRMA DE AUDITORÍA: GUZMÁN TAPIA PKF

4. INFORMACIÓN SOBRE EL NIVEL DE ESPECIALIZACIÓN DEL PERSONAL QUE ACOMPAÑARÁ LA FIRMA PKF EN EL TRABAJO DE "AUDITORIA TÉCNICA AL SOFTWARE DE VOTACIÓN AUTOMATIZADA"

Nuestros especialistas en el **ÁREA DE AUDITORÍA DE TI de Guzmán Tapia PKF**, son **INGENIEROS DE SISTEMAS** expertos en Seguridad de la Información, Ciberseguridad, Riesgos Tecnológicos, Desarrollo de Sistemas de Información y cuentan con las Certificaciones Internacionales CISA, CRISC, CISM, CISSP, CSX, CEH e ISO 27001 anteriormente descritos.

NUESTRO DIRECTOR DE AUDITORÍA DE TI:

Wilson Andia Cuiza, MSc, CISA, CRISC, ISO 27001 LA

Tiene en su "ADN" Tecnología y Auditoría, con más de 20 años de experiencia en Auditorías de TI, Seguridad, Riesgos y Control de TI, reconocido en diferentes Bancos como Auditor Externo y por sus conferencias internacionales, así como por las docencias en Certificaciones mundialmente reconocidas y Maestrías de alto impacto.

Wilson cuenta con certificaciones internaciones de ISACA: Certified Information Systems Auditor Auditor de Sistemas de Información Certificado (**CISA**) y Especialista en Riesgos y Control de Sistemas de Información Certificado (**CRISC**). Es certificado Auditor Líder de Seguridad de la Información basado en **ISO 27001** Madrid-España. Ha estudiado Ingeniería de Sistemas con Postgrados en Auditoría y Seguridad de TI y Educación Superior.

Inicialmente fue Analista Programador de Sistemas en diferentes Empresas. Posteriormente trabajó como Consultor Internacional en Auditoría de TI y Seguridad en países de Sud, Centro América y el Caribe en Bancos y Empresas, así como Entidades Fiscalizadoras como Contralorías, Cámaras y Tribunales de Cuentas; Proyectos Financiados por BID, Banco Mundial, PNUD y Unión Europea.

Actualmente es Director de Auditorías y Consultorías de TI de Guzmán Tapia PKF con mayor presencia en República Dominicana en el Sector Bancario, teniendo entre otros clientes a 10 Bancos de prestigio.

Wilson es experto en:

- Auditoría de TI y Seguridad en Bancos Múltiples y de Ahorro y Crédito.
- Auditoría y Seguridad de Core Bancarios: FISERV, FISA, BANCA 2000, SYSDE BANCA, ABANKS.

PROPUESTA TÉCNICA
"AUDITORIA TÉCNICA AL SOFTWARE DE VOTACIÓN
AUTOMATIZADA", JCE
FIRMA DE AUDITORÍA: GUZMÁN TAPIA PKF

- Auditoria a Sistemas MONITOR PLUS, SENTINEL CUMPLIMIENTO/PREVENTION, ULTRAFISGON.
- Auditor de TI en Prevención del Lavado de Activos (PLA/FT).
- Auditoría de cumplimiento PCI-DSS.
- Seguridad, Riesgos y Auditoría de TI basado en metodologías y estándares ISO de TI COBIT, COSO, ISO 27001, 27002, 22301, 27031, 12207, 25000, 9126, 15504.
- Desarrollo e Implementación de Planes de Continuidad (BCP) y de Recuperación ante Desastres Informáticos (DRP).
- Desarrollo e Implementación de Políticas de Seguridad de TI.
- Detección de fraudes o delitos informáticos.
- Análisis Forense Informático usando Software (EnCase y Forensic ToolKit)
- Software de Auditoría (IDEA, ACL, TEAM MATE, MEYCOR COBIT, COBIT ADVISOR)
- Ley Sarbanes Oxley (SOX) relacionado con TI.
- Análisis, Programación e Implementación de Sistemas Informáticos.
- Administración de Bases de Datos ORACLE, SQL SERVER, SYSBASE, DB2.
- Lenguajes de programación ORACLE, .NET. C#, Java.
- Conferencias Internacionales de Seguridad, Auditoría y Riesgos de TI
- Docente de Certificaciones CISA y CRISC en capítulos de ISACA.
- Docente de Maestrías en Auditorías y Seguridad de TI.
- Expositor y capacitador en Auditoría, Riesgos y Seguridad de TI.

NUESTRO AUDITOR SENIOR DE AUDITORÍA DE TI

Ing. Domingo Ormeño, CISA

Domingo, cuenta con 20 años de experiencia en TI Auditorías de TI, Instructor Internacional de CaseWare Working Papers. Ha participado en numerosas auditorías a empresas de la firma, en la cual ha destacado su participación en aspectos relacionados con diagnósticos tecnológicos. Además, de lo anterior posee sólidos conocimientos de sistemas financieros contables, SAP, Softland, y un sin número de desarrollos inhouse.

Ingeniero de Ejecución en Informática, Instituto Profesional IPP, cuenta con un Diploma en Auditoría de Sistemas y TIC's de la Universidad de Chile, Diploma en Gestión de Proyectos del Instituto Profesional IPP, Certified Information Systems Auditor (CISA) del ISACA y Project Management Certificate de The University of Texas at Arlington e Instituto Profesional Providencia y Diplomado en Auditoría Forense de la Universidad de Concepción.

PROPUESTA TÉCNICA
"AUDITORIA TÉCNICA AL SOFTWARE DE VOTACIÓN
AUTOMATIZADA", JCE
FIRMA DE AUDITORÍA: GUZMÁN TAPIA PKF

NUESTRO AUDITOR EN SEGURIDAD Y CIBERSEGURIDAD

Ing. César Millavil, CEH, ISO 27001 LA, ISO 27032

Cesar, cuenta con 8 años en distintas áreas Operativas y más de 7 años en Jefaturas y Gerencias. (15+ años de experiencia profesional)

Áreas de especialización: Ciberseguridad (ISO 27032/COBIT/NIST/OSSTMM/OWASP), Seguridad de la información (ISO 27001), Infraestructura, Tecnologías Microsoft, Tecnologías Linux, Tecnologías de Virtualización, Continuidad Operacional, Tecnologías de Respaldo, plataformas Endpoint de Seguridad (Sophos/Kaspersky), Tecnologías PAM/IDM, SIEM.

Certificaciones: ISO27001 LA, ISO 27032 LM, CEH, Sophos, Thycotic, AlienVault, CISCO, Microsoft, VMWARE, SFIA

En preparación para el examen CISSP.

Rol(es) en el servicio: Controller principal, Responsable de velar por la prestación de los servicios de Auditoría en Seguridad de la información y Ciberseguridad.

PROPUESTA TÉCNICA
"AUDITORIA TÉCNICA AL SOFTWARE DE VOTACIÓN
AUTOMATIZADA", JCE
FIRMA DE AUDITORÍA: GUZMÁN TAPIA PKF

5. DESCRIPCIÓN DE LA METODOLOGÍA PARA EJECUTAR EL TRABAJO

Nuestra propuesta técnica está orientado principalmente a cumplir punto por punto los siguientes objetivos de la Auditoría formulada por la Junta Central Electoral (JCE).

OBJETIVO 1

Certificar que el sistema de votación automatizada implementado por la Junta Central Electoral, garantiza el Secreto del Voto de los Electores.

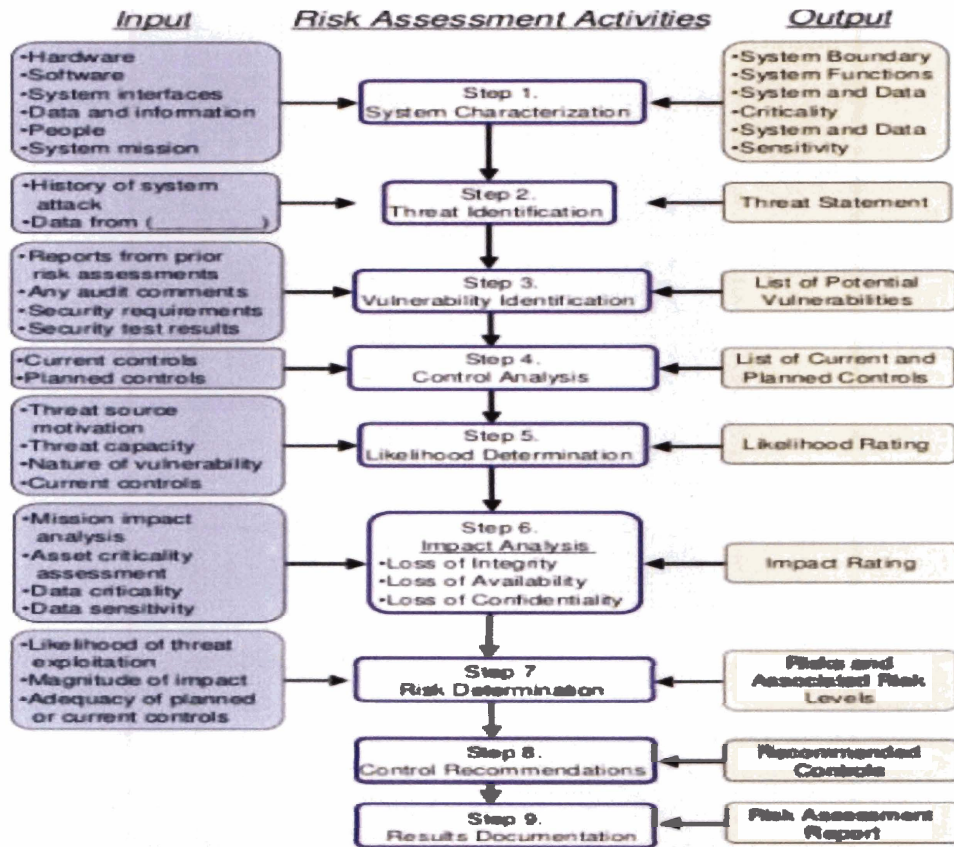
El voto en un Sistema Informático es un dato/información y debe ser secreto, por lo que debe garantizarse la seguridad (confidencialidad, integridad y disponibilidad), en ese sentido, en este punto planteamos los siguientes objetivos específicos:

OBJETIVO ESPECÍFICO 1.1

Identificar y Evaluar los Riesgos Tecnológicos de la Infraestructura Tecnológica del Sistema de Votación Automatizada (Amenazas, Vulnerabilidades, Controles Existentes, Probabilidad de Impacto, Impacto), para recomendar posibles oportunidades de mejora que mitiguen los riesgos).

Identificaremos y evaluaremos los riesgos tecnológicos que podrían existir en el Sistema de Votación Automatizada, aplicando el Estandar para la Evaluación de Riesgos NIST 800-30 del Instituto Nacional de Estándares y Tecnología (NIST por sus siglas en inglés, National Institute of Standards and Technology)..

PROPUESTA TÉCNICA
"AUDITORIA TÉCNICA AL SOFTWARE DE VOTACIÓN
AUTOMATIZADA", JCE
FIRMA DE AUDITORÍA: GUZMÁN TAPIA PKF



OBJETIVO ESPECÍFICO 1.2

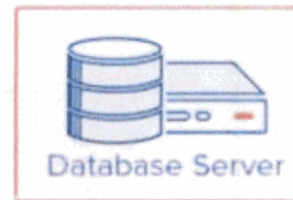
Evaluar la seguridad de la Infraestructura Tecnológica que soporta el Sistema de Votación Automatizada de la JCE para identificar posibles accesos no autorizados.



User



Application Server



Database Server

Es decir, evaluaremos:

- a) La Seguridad del Sistema Operativo Windows (S.O.) y Active Directory tanto de los dispositivos Stand Alone y Servidores de la JCE que reciben información que tienen relación con el Sistema de Votación Automatizada.
 - Accesos y Permisos de usuarios
 - Existencia de usuarios "Administrator", "DomainAdmins"
 - Longitud de contraseñas
 - Expiración de contraseñas
 - Verificación de usuarios que no requieren Password

PROPUESTA TÉCNICA
"AUDITORIA TÉCNICA AL SOFTWARE DE VOTACIÓN
AUTOMATIZADA", JCE
FIRMA DE AUDITORÍA: GUZMÁN TAPIA PKF

Con la finalidad de garantizar la Seguridad a nivel de S.O.

- b) La Seguridad de las Bases de Datos, en cuanto a la configuración de seguridad, usuarios, permisos SYSADMIN, SECURITYADMIN, contraseñas débiles, accesos a Bases de Datos, Tablas y Campos del Sistema de Votación Automatizada.

Con la finalidad de garantizar la Seguridad a nivel de Base de Datos.

- c) La encriptación de la información, para verificar que se garantice la confidencialidad de la información, basándonos en la Norma ISO 27002 (Dominio 10 Cifrado).

10. CIFRADO.

10.1 Controles criptográficos.

10.1.1 Política de uso de los controles criptográficos.

10.1.2 Gestión de claves

Con la finalidad de garantizar la Confidencialidad de la Información.

- d) La gestión y control de accesos, usuarios, roles, perfiles de acceso a la Infraestructura Tecnológica que soporta el Sistema de Votación por ej.: Equipos Stand Alone, Servidores de Aplicación, Sistema Operativo Windows, Servidores de Bases de Datos, DBMS o Base de Datos, Aplicativo o Software de Votación Automatizada, aplicando la Norma ISO 27002 (Dominio 9 Control de Accesos), con la finalidad que solo tengan acceso el personal Autorizado de la JCE.

9. CONTROL DE ACCESOS.

9.1 Requisitos de negocio para el control de accesos

9.1.1 Política de control de accesos

9.1.2 Control de acceso a las redes y servicios asociados

9.2 Gestión de acceso de usuario

9.2.1 Gestión de altas/bajas en el registro de usuarios

9.2.2 Gestión de los derechos de acceso asignados a usuarios

9.2.3 Gestión de los derechos de acceso con privilegios especiales

9.2.4 Gestión de información confidencial de autenticación de usuarios

9.2.5 Revisión de los derechos de acceso de los usuarios.

9.2.6 Retirada o adaptación de los derechos de acceso

9.3 Responsabilidades del usuario

9.3.1 Uso de información confidencial para la autenticación.

9.4 Control de acceso a sistemas y aplicaciones.

9.4.1 Restricción del acceso a la información.

9.4.2 Procedimientos seguros de inicio de sesión.

9.4.3 Gestión de contraseñas de usuario.

9.4.4 Uso de herramientas de administración de sistemas.

9.4.5 Control de acceso al código fuente de los programas.

- e) Verificaremos y evaluaremos la Seguridad en el Desarrollo de la Aplicación/Software desarrollado para la Votación Automatizada.
- o Módulo de Seguridad de Administración de Usuarios
 - o Roles/Perfiles, Controles de accesos
 - o Backdoors
 - o Controles de Entrada, Proceso y Salida
 - o Verificación y lectura del programa fuente, con la finalidad de verificar que no exista código malicioso.

PROPUESTA TÉCNICA "AUDITORIA TÉCNICA AL SOFTWARE DE VOTACIÓN AUTOMATIZADA", JCE FIRMA DE AUDITORÍA: GUZMÁN TAPIA PKF

Aplicando la Norma ISO 27002 (Dominio 14 Seguridad en el Desarrollo y mantenimiento de Sistemas de Información), con la finalidad de garantizar la Seguridad a nivel de Software de Aplicación.

14. ADQUISICION, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.

14.1 Requisitos de seguridad de los sistemas de información.

- 14.1.1 Análisis y especificación de los requisitos de seguridad.
- 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
- 14.1.3 Protección de las transacciones por redes telemáticas.

14.2 Seguridad en los procesos de desarrollo y soporte.

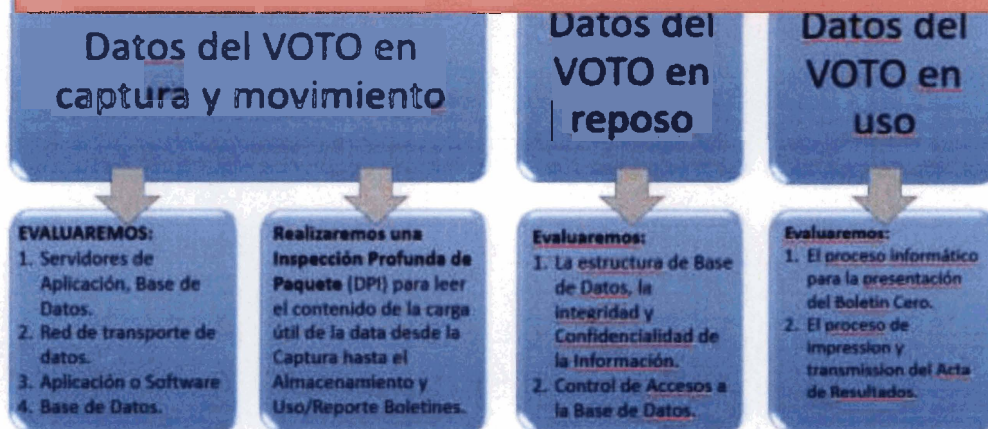
- 14.2.1 Política de desarrollo seguro de software.
- 14.2.2 Procedimientos de control de cambios en los sistemas.
- 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
- 14.2.4 Restricciones a los cambios en los paquetes de software.
- 14.2.5 Uso de principios de ingeniería en protección de sistemas.
- 14.2.6 Seguridad en entornos de desarrollo.
- 14.2.7 Externalización del desarrollo de software.
- 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
- 14.2.9 Pruebas de aceptación.

- f) La oportuna disponibilidad de la información al personal Autorizado de la JCE y únicamente a los dispositivos que determine la JCE (ej. impresoras).

Verificaremos que la información esté disponible de forma oportuna únicamente al personal autorizado de la JCE y hacia los dispositivos autorizados (Impresoras, etc.).

OBJETIVO ESPECÍFICO 1.3

Evaluar la Seguridad de la Información (confidencialidad, integridad, disponibilidad) en sus 3 diferentes estados, es decir:



PROPUESTA TÉCNICA
"AUDITORIA TÉCNICA AL SOFTWARE DE VOTACIÓN
AUTOMATIZADA", JCE
FIRMA DE AUDITORÍA: GUZMÁN TAPIA PKF

Evaluaremos también la encriptación de la información, para verificar que se garantice la confidencialidad de la información, basándonos en la Norma ISO 27002 (Dominio 10 Cifrado).

10. CIFRADO.

10.1 Controles criptográficos.

10.1.1 Política de uso de los controles criptográficos.

10.1.2 Gestión de claves.

OBJETIVO ESPECÍFICO 1.4

Certificar que el Sistema garantiza el Secreto del Voto de los Electores.

certificación del Sistema de Votación Automatizada mencionando que garantiza el secreto del voto de los electores.



PROPUESTA TÉCNICA
"AUDITORIA TÉCNICA AL SOFTWARE DE VOTACIÓN
AUTOMATIZADA", JCE
FIRMA DE AUDITORÍA: GUZMÁN TAPIA PKF

OBJETIVO

Certificar que durante el proceso de votación el sistema funcionará operativamente sin conexión de las redes de internet, y que solo será conectado a una red privada al momento de dar el Boletín Cero y, una vez se proceda a la impresión y transmisión del Acta de Resultado.

Según la JCE mediante carta CCC-330/2019 de respuestas a preguntas realizadas menciona que: "los equipos *funcionan Stand Alone*, conectados entre sí, con conexión punto a punto, siendo todo el tráfico local entre ambos y que únicamente se realiza conexión hacia la sede central al momento de transmitir el boletín cero y el boletín final, mediante la conexión manual de un modem 3G USB, el cual se desconecta automáticamente al concluir la transmisión utilizando SIMCARD personalizados con APN privado exclusivo de la Junta Central Electoral, sin conexión a internet. Estas transmisiones son recibidas en unos equipos balanceadores de carga, los cuales están protegidos por IPS y Firewds en la sede central de la JCE.", evaluaremos los siguientes objetivos específicos:

OBJETIVO ESPECÍFICO 2.1

Identificar los diferentes tipos posibles de conexiones de red que puedan existir en los equipos *Stand Alone*, con la finalidad de identificar que no existan conexiones de red autorizadas.

En esta parte, verificaremos la configuración de los equipos Stand Alone que no tengan ninguna conexión de red que no esté autorizada y que no tenga posibilidad de conexión a internet, revisaremos, por ejemplo:

- Status
- Wi-Fi
- Ethernet
- Dial-Up
- VPN
- Mobile hotspot
- Proxy

Nos basaremos en la Norma ISO 27002 (Dominio 13 Seguridad en las Telecomunicaciones).

13. SEGURIDAD EN LAS TELECOMUNICACIONES.

13.1 Gestión de la seguridad en las redes.

- 13.1.1 Controles de red.
- 13.1.2 Mecanismos de seguridad asociados a servicios en red.
- 13.1.3 Segregación de redes.

13.2 Intercambio de información con partes externas.

- 13.2.1 Políticas y procedimientos de intercambio de información.
- 13.2.2 Acuerdos de intercambio.
- 13.2.3 Mensajería electrónica.
- 13.2.4 Acuerdos de confidencialidad y secreto.

PROPUESTA TÉCNICA
"AUDITORIA TÉCNICA AL SOFTWARE DE VOTACIÓN
AUTOMATIZADA", JCE
FIRMA DE AUDITORÍA: GUZMÁN TAPIA PKF

OBJETIVO ESPECÍFICO 2.2

Revisar la configuración de los dispositivos modem 3G USB, APN (Access Point Name) con la finalidad de verificar que solo pueda existir conexión a través de estos dispositivos, en los horarios establecidos.

Cada dispositivo móvil (por ejemplo, un módem USB), tiene que tener definido el APN a usar para que pueda acceder a una red de datos basada en GPRS o estándares posteriores como 3G y 4G. En este caso. Verificaremos y revisaremos cada dispositivo modem USB autorizado por la JCE que se utilizará.

OBJETIVO ESPECÍFICO 2.3

Revisar la configuración de la Red Privada Virtual (VPN) con la finalidad de identificar usuarios y accesos no autorizados.

Revisaremos en la VPN, por ejemplo:

- Usuarios autorizados
- Roles/permisos de los usuarios autorizados.
- Conexiones autorizadas
- Horarios autorizados

OBJETIVO ESPECÍFICO 2.4

Revisar la configuración de los Dispositivos Sistemas de Prevención de Intrusos (IPS) de oficina central, con la finalidad de verificar su adecuada configuración y que prevenga posibles intrusos y alerte oportunamente.

En los Sistemas de Prevención de Intrusos (IPS) de oficina central, revisaremos:

- Cumplimiento de Políticas definidas.
- Usuarios administradores autorizados del IPS
- Roles/Permisos de los usuarios administradores del IPS
- Tipo de tráfico de red que está monitoreando el IPS
- Tipos de actividad maliciosa puede prevenir de forma proactiva el IPS
- Alertas/Notificaciones configuradas y activadas en los IPS
- Que tipos de LOGs se guardan
- El tipo de IPS: Basados en Red LAN (NIPS), Basados en Red Wireless (WIPS), Análisis de comportamiento de red (NBA), Basados en Host (HIPS)
- Si el IPS está basado en políticas, firmas y anomalías

PROPUESTA TÉCNICA
"AUDITORIA TÉCNICA AL SOFTWARE DE VOTACIÓN
AUTOMATIZADA", JCE
FIRMA DE AUDITORÍA: GUZMÁN TAPIA PKF

OBJETIVO ESPECÍFICO 2.5

Revisar la configuración de los Dispositivos Firewalls de Oficina Central, con la finalidad de verificar su adecuada configuración y que prevenga posibles intrusos y alerte oportunamente.

En los Firewalls de oficina central, revisaremos:

- Cumplimiento de Políticas definidas.
- Usuarios administradores de los Firewalls
- Roles/Permisos de los usuarios administradores de los Firewalls
- Las reglas que permiten bloquear tráfico entrante y saliente
- Las comunicaciones autorizadas desde fuera y desde dentro
- Alertas/Notificaciones configuradas y activadas en los Firewalls
- Que tipos de LOGs guardan los Firewalls.

OBJETIVO ESPECÍFICO 2.6

Certificar que durante el proceso de votación el sistema funcionará operativamente sin conexión de las redes de internet y que solo se conectará a la JCE al momento de emitir boletín cero y transmisión del Acta.

No se ha podido establecer conexión con Internet

Cargar de nuevo

Más

PROPUESTA TÉCNICA
"AUDITORIA TÉCNICA AL SOFTWARE DE VOTACIÓN
AUTOMATIZADA", JCE
FIRMA DE AUDITORÍA: GUZMÁN TAPIA PKF

OBJETIVO 3

Certificar que es auditable y comprobable que la sumatoria de los votos físicos depositados en las urnas de las mesas de votación coincide con el Acta de Resultados.

Para cumplir con este objetivo de Auditoría, debemos realizar pruebas sustantivas de funcionalidad del Software de Votación Automatizada y posteriormente hacer uso de Técnicas de Auditoría Asistidas por Computador (TAAC/CAAT), mediante el Software de Auditoría IDEA, para la extracción y análisis de la data de la Base de Datos (Data Analytics) y hacer de forma automática el conteo (sumarizaciones) de votos y comparar con las actas de resultados, para esto cumpliremos los siguientes objetivos específicos:

OBJETIVO ESPECÍFICO 3.1

Realizar pruebas de funcionalidad del Software de Votación Automatizada con la finalidad de tener resultados de votos realizados, actas de resultados y comparar con el Análisis de Datos (Data Analytics) que realizaremos en el siguiente objetivo.

la configuración de los Dispositivos Sistemas de Prevención de Intrusos (IPS) de oficina central, con la finalidad de verificar su adecuada configuración y que prevenga posibles intrusos y alerte oportunamente.

En un ambiente de pruebas, realizaremos pruebas de caja negra, es decir funcionalidad del Software de Votación Automatizada, simulando el proceso de elecciones en la parte de identificación del elector, momento de la votación, emisión de actas y obtención de resultados finales. Para este punto, conjuntamente con el Personal de la JCE, definiremos una muestra y realizaremos este proceso en conjunto.

Para este objetivo, nos basaremos en el Estándares: ISO 25000 para Evaluar la calidad del Sistema y el producto software, específicamente en los requerimientos: Idoneidad, completitud, disponibilidad, integridad, capacidad de ser probado, como se puede ver a continuación:

ISO 25000 SQuaRE (Software Product Quality Requirements and Evaluation)

PROPUESTA TÉCNICA
"AUDITORIA TÉCNICA AL SOFTWARE DE VOTACIÓN
AUTOMATIZADA", JCE
FIRMA DE AUDITORÍA: GUZMÁN TAPIA PKF



OBJETIVO ESPECÍFICO 3.2

Obtener resultados de las pruebas de votación realizados. Para esto obtendremos la información (votos) directamente de la Base de Datos, mediante Data Analytics y TAAC/CAAT para obtener totales (sumarización) y comparar con las actas de prueba realizadas, con la finalidad de determinar la Auditabilidad y Confiabilidad y asegurar la comprobación.

Utilizaremos Software de Auditoría y Data Analytics (IDEA) para extraer la data de los votos de prueba realizados para analizar, sumarizar y obtener totales, mediante TAAC/CAAT y luego comparar estos datos con las actas de resultados obtenidas en el objetivo específico descrito anteriormente. Nuestra Firma cuenta con las licencias oficiales respectivas del Software IDEA.

PROPUESTA TÉCNICA "AUDITORIA TÉCNICA AL SOFTWARE DE VOTACIÓN AUTOMATIZADA", JCE FIRMA DE AUDITORÍA: GUZMÁN TAPIA PKF

Servicio técnico



Ayuda de CaseWare IDEA
Obtenga ayuda para el uso de CaseWare IDEA.



Noticias
Ver las noticias de CaseWare IDEA.



Contactenos
No dude en contactarnos si necesita ayuda o para enviarnos sugerencias para el desarrollo de un IDEA mejor.



Acerca de IDEA

Versión Cliente: 10.1.2.11 (X86)

Versión servidor: No conectado a IDEA Server

Versión Licencia: ~~XXXXXXXXXXXX~~

Clave de licencia: ~~XXXXXXXXXXXX~~

Utilidades de IDEA



Opciones
Personaliza la visualización y otras configuraciones del programa.



Buscar actualizaciones
Obtener las últimas actualizaciones disponibles para CaseWare IDEA.

Copyright © CaseWare IDEA Inc.

Módulos instalados



PROPUESTA TÉCNICA
"AUDITORIA TÉCNICA AL SOFTWARE DE VOTACIÓN
AUTOMATIZADA", JCE
FIRMA DE AUDITORÍA: GUZMÁN TAPIA PKF

OBJETIVO ESPECÍFICO 3.3
Certificar que es Auditable y Comprobable.

Una vez que realicemos las pruebas descritas en los objetivos anteriores 3.1 y 3.2 emitiremos la Certificación de Auditabilidad y que es Comprobable que la sumatoria de los votos físicos depositados en las urnas de las mesas de votación coincide con el Acta de Resultados



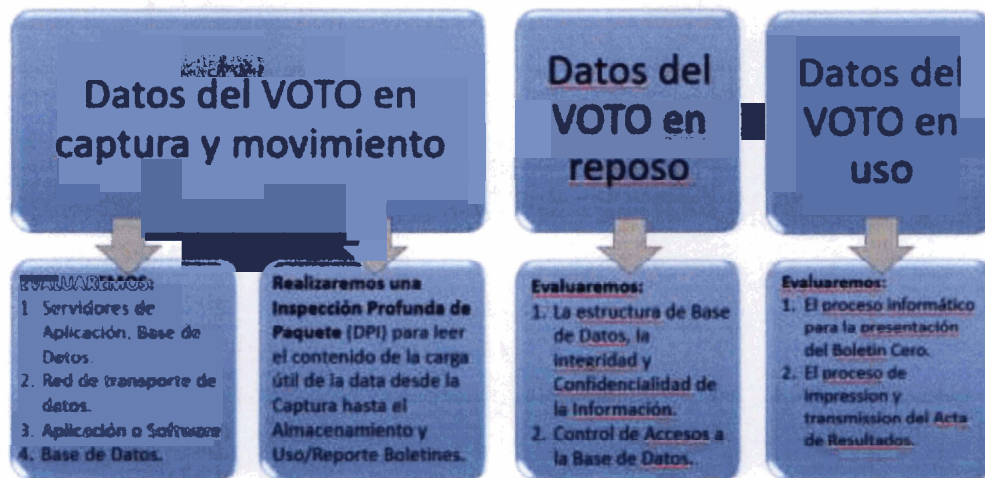
OBJETIVO 4
Certificar que garantiza la integridad en el procesamiento de toda la información

El voto en un Sistema Informático es un dato/información y debe ser íntegro por lo que no debe alterarse o cambiarse durante el proceso de transporte de la data por los medios de conexión Stand Alone y tampoco hacia los diferentes medios de almacenamiento y emisión de resultados. En ese sentido es importante evaluar la integridad, como parte de la Seguridad de la Información.

OBJETIVO ESPECÍFICO 4.1
Evaluar la Seguridad de la Información (integridad de la Data) en sus 3 diferentes estados, es decir:

Verificaremos que la data en sus 3 estados no sea cambiada o alterada por ningún proceso automatizado, así como tampoco manualmente en la base de datos.

PROPUESTA TÉCNICA
"AUDITORIA TÉCNICA AL SOFTWARE DE VOTACIÓN
AUTOMATIZADA", JCE
FIRMA DE AUDITORÍA: GUZMÁN TAPIA PKF



OBJETIVO ESPECÍFICO 4.2

Evaluar la seguridad de la Red, con la finalidad de evitar Sniffers de tráfico de Red.

Revisaremos la seguridad de la Red para verificar los Controles que permitan identificar o evitar Sniffers en la Red que podrían afectar la integridad de la información en modo de transporte de datos por la Red.

Nos basaremos en la Norma ISO 27002 (Dominio 13 Seguridad en las Telecomunicaciones).

13. SEGURIDAD EN LAS TELECOMUNICACIONES.

13.1 Gestión de la seguridad en las redes.

- 13.1.1 Controles de red.
- 13.1.2 Mecanismos de seguridad asociados a servicios en red
- 13.1.3 Segregación de redes.

13.2 Intercambio de información con partes externas.

- 13.2.1 Políticas y procedimientos de intercambio de información.
- 13.2.2 Acuerdos de intercambio.
- 13.2.3 Mensajería electrónica.
- 13.2.4 Acuerdos de confidencialidad y secreto.

PROPUESTA TÉCNICA
"AUDITORIA TÉCNICA AL SOFTWARE DE VOTACIÓN
AUTOMATIZADA", JCE
FIRMA DE AUDITORÍA: GUZMÁN TAPIA PKF

OBJETIVO ESPECÍFICO 4.3

Certificar que garantiza la integridad en el procesamiento de toda la información

Una vez que realicemos las pruebas descritas en los objetivos anteriores 4.1 y 4.2 emitiremos la Certificación que garantiza la integridad en el procesamiento de toda la información.

**INTEGRIDAD EN EL PROCESAMIENTO
DE LA INFORMACIÓN**



OBJETIVO 5

Determinar si es robusto, confiable, seguro y que realiza exclusivamente las operaciones y funciones para las cuales fue diseñado.

Al revisar los objetivos anteriormente planteados y verificar su funcionamiento y la seguridad del Sistema de Votación Automatizado, es posible determinar que el sistema es robusto, confiable y seguro. Al respecto, evaluaremos los siguientes objetivos:

OBJETIVO ESPECÍFICO 5.1 (Aplica mismo Objetivo Específico 1.1, ver arriba)
Identificar y Evaluar los Riesgos Tecnológicos de la Infraestructura Tecnológica del Sistema de Votación Automatizada (Amenazas, Vulnerabilidades, Controles Existentes, Probabilidad de Impacto, Impacto), para recomendar posibles oportunidades de mejora que mitiguen los riesgos).

PROPUESTA TÉCNICA
"AUDITORIA TÉCNICA AL SOFTWARE DE VOTACIÓN
AUTOMATIZADA", JCE
FIRMA DE AUDITORÍA: GUZMÁN TAPIA PKF

OBJETIVO ESPECÍFICO 5.2 (Aplica mismo Objetivo Específico 1.2, ver arriba)
Evaluar la seguridad de la Infraestructura Tecnológica que soporta el Sistema de Votación Automatizada de la JCE para identificar posibles accesos no autorizados.

OBJETIVO ESPECÍFICO 5.3 (Aplica mismo Objetivo Específico 3.1, ver arriba)
Realizar pruebas de funcionalidad del Software de Votación Automatizada con la finalidad de tener resultados de votos realizados, actas de resultados y comparar con el Análisis de Datos (Data Analytics) que realizaremos en el siguiente objetivo.

La configuración de los Dispositivos Sistemas de Prevención de Intrusos (IPS) de oficina central, con la finalidad de verificar su adecuada configuración y que prevenga posibles intrusos y alerte oportunamente.

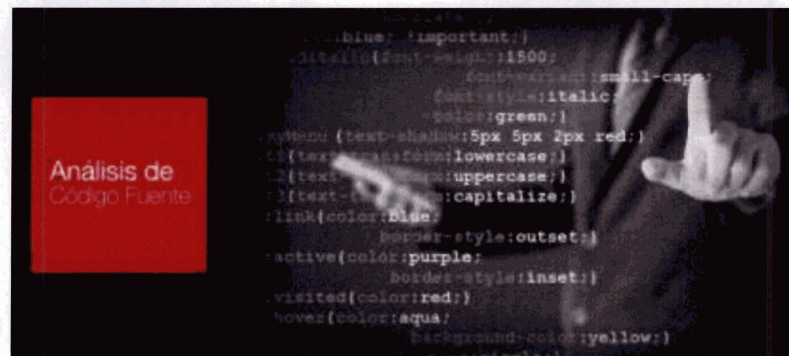
OBJETIVO 6

Certificar que no existe trazabilidad del voto, ni correlación alguna con el elector.

Para cumplir con este objetivo, realizaremos una lectura del Código Fuente, pruebas de funcionalidad y realizaremos pruebas de Data Analytics TAAC/CAAT.

OBJETIVO ESPECÍFICO 6.1
Revisar y evaluar el código fuente del Sistema de votación Automatizada en cuanto a la Aplicación, Store Procedures, para determinar que no exista correlación alguna

Para esto, tenemos la capacidad de entender la lógica de programación debido a que nuestro personal han sido desarrolladores de software en diferentes lenguajes de programación por más de 10 años, como se puede ver en los Curriculums Vitae.



PROPUESTA TÉCNICA
"AUDITORIA TÉCNICA AL SOFTWARE DE VOTACIÓN
AUTOMATIZADA", JCE
FIRMA DE AUDITORÍA: GUZMÁN TAPIA PKF

OBJETIVO ESPECÍFICO 6.2 (Aplica mismo Objetivo Específico 3.2, ver arriba)
Obtener resultados de las pruebas de votación realizados. Para esto obtendremos la información (votos) directamente de la Base de Datos, mediante Data Analytics y TAAC/CAAT para obtener totales (sumariacción) y comparar con las actas de prueba realizadas, con la finalidad de determinar la Auditabilidad y Confiabilidad y asegurar la comprobación.

OBJETIVO ESPECÍFICO 6.3 (Aplica mismo Objetivo Específico 3.1, ver arriba)
Realizar pruebas de funcionalidad del Software de Votación Automatizada con la finalidad de tener resultados de votos realizados, actas de resultados y comparar con el Análisis de Datos (Data Analytics) que realizaremos en el siguiente objetivo.
la configuración de los Dispositivos Sistemas de Prevención de Intrusos (IPS) de oficina central, con la finalidad de verificar su adecuada configuración y que prevenga posibles intrusos y alerte oportunamente.

PROPUESTA TÉCNICA
"AUDITORIA TÉCNICA AL SOFTWARE DE VOTACIÓN AUTOMATIZADA", JCE
FIRMA DE AUDITORÍA: GUZMÁN TAPIA PKF

		NÚMERO DE DÍA DE TRABAJO EN LA JUNTA CENTRAL ELECTORAL (25 días de trabajo)																								
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
OBJETIVO 2																										
Certificar que durante el proceso de votación el sistema funcionará operativamente sin conexión de las redes de internet, y que solo será conectado a una red privada al momento de dar el Boletín Cero y, una vez se proceda a la impresión y transmisión del Acta de Resultado.																										
	OBJETIVO ESPECÍFICO 2.1 Identificar los diferentes tipos posibles de conexiones de red que puedan existir en los equipos Stand Alone, con la finalidad de identificar que no existan conexiones de red autorizadas																									
	OBJETIVO ESPECÍFICO 2.2 Revisar la configuración de los dispositivos modem 3G USB, APN (Access Point Name) con la finalidad de verificar que solo pueda existir conexión a través de estos dispositivos, en los horarios establecidos																									
	OBJETIVO ESPECÍFICO 2.3 Revisar la configuración de la Red Privada Virtual (VPN) con la finalidad de identificar usuarios y accesos no autorizados																									
	OBJETIVO ESPECÍFICO 2.4 Revisar la configuración de los Dispositivos Sistemas de Prevención de Intrusos (IPS) de oficina central, con la finalidad de verificar su adecuada configuración y que prevenga posibles intrusos y alerte oportunamente																									
	OBJETIVO ESPECÍFICO 2.5 Revisar la configuración de los Dispositivos Firewalls de Oficina Central, con la finalidad de verificar su adecuada configuración y que prevenga posibles intrusos y alerte oportunamente																									
	OBJETIVO ESPECÍFICO 2.6 Certificar que durante el proceso de votación el sistema funcionará operativamente sin conexión de las redes de internet y que solo se conectará a la JCE al momento de emitir boletín cero y transmisión del Acta																									

Continúa siguiente página.....

PROPUESTA TÉCNICA
"AUDITORIA TÉCNICA AL SOFTWARE DE VOTACIÓN AUTOMATIZADA", JCE
FIRMA DE AUDITORÍA: GUZMÁN TAPIA PKF

		NÚMERO DE DÍA DE TRABAJO EN LA JUNTA CENTRAL ELECTORAL (25 días de trabajo)																									
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	
OBJETIVO 3																											
Certificar que es auditable y comprobable que la sumatoria de los votos físicos depositados en las urnas de las mesas de votación coincide con el Acta de Resultados.																											
	OBJETIVO ESPECÍFICO 3.1																										
	Realizar <u>pruebas</u> de funcionalidad del Software de Votación Automatizada con la finalidad de tener resultados de votos realizados, actas de resultados y comparar con el Análisis de Datos (Data Analytics) que realizaremos en el siguiente objetivo																										
	OBJETIVO ESPECÍFICO 3.2																										
	Obtener resultados de las <u>pruebas</u> de votación realizados. Para esto obtendremos la información (votos) directamente de la Base de Datos, mediante Data Analytics y TAAC/CAAT para obtener totales (sumarización) y comparar con las actas de prueba realizadas, con la finalidad de determinar la Auditabilidad y Confiabilidad y asegurar la comprobación																										
	OBJETIVO ESPECÍFICO 3.3																										
	Certificar que es Auditable y Comprobable																										
OBJETIVO 4																											
Certificar que garantiza la integridad en el procesamiento de toda la información																											
	OBJETIVO ESPECÍFICO 4.1																										
	Evaluar la Seguridad de la Información (Integridad de la Data) en sus 3 diferentes estados																										
	OBJETIVO ESPECÍFICO 4.2																										
	Evaluar la seguridad de la Red, con la finalidad de evitar Sniffers de tráfico de Red																										
	OBJETIVO ESPECÍFICO 4.3																										
	Certificar que garantiza la integridad en el procesamiento de toda la información																										

Continúa siguiente página.....

PROPUESTA TÉCNICA
"AUDITORIA TÉCNICA AL SOFTWARE DE VOTACIÓN AUTOMATIZADA", JCE
FIRMA DE AUDITORÍA: GUZMÁN TAPIA PKF

	NÚMERO DE DÍA DE TRABAJO EN LA JUNTA CENTRAL ELECTORAL (25 días de trabajo)																								
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
OBJETIVO 5 Determinar si es robusto, confiable, seguro y que realiza exclusivamente las operaciones y funciones para las cuales fue diseñado.																									
OBJETIVO ESPECÍFICO 5.1 (Aplica mismo Objetivo Específico 1.1, ver arriba) Identificar y Evaluar los Riesgos Tecnológicos de la Infraestructura Tecnológica del Sistema de Votación Automatizada (Amenazas, Vulnerabilidades, Controles Existentes, Probabilidad de Impacto, Impacto), para recomendar posibles oportunidades de mejora que mitiguen los riesgos).																									
OBJETIVO ESPECÍFICO 5.2 (Aplica mismo Objetivo Específico 1.2, ver arriba) Evaluar la seguridad de la Infraestructura Tecnológica que soporta el Sistema de Votación Automatizada de la JCE para identificar posibles accesos no autorizados																									
OBJETIVO ESPECÍFICO 5.3 (Aplica mismo Objetivo Específico 3.1, ver arriba) Realizar pruebas de funcionalidad del Software de Votación Automatizada con la finalidad de tener resultados de votos realizados, actas de resultados y comparar con el Análisis de Datos (Data Analytics) que realizaremos en el siguiente objetivo																									

Continúa siguiente página.....

**PROPUESTA TÉCNICA
"AUDITORIA TÉCNICA AL SOFTWARE DE VOTACIÓN AUTOMATIZADA", JCE
FIRMA DE AUDITORÍA: GUZMÁN TAPIA PKF**

	NÚMERO DE DÍA DE TRABAJO EN LA JUNTA CENTRAL ELECTORAL (25 días de trabajo)																									
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	
OBJETIVO 6 Certificar que no existe trazabilidad del voto, ni correlación alguna con el elector.																										
OBJETIVO ESPECÍFICO 6.1 Revisar y evaluar el código fuente del Sistema de Votación Automatizada en cuanto a la Aplicación, Store Procedures, para determinar que no exista correlación alguna																										
OBJETIVO ESPECÍFICO 6.2 (Aplica mismo Objetivo Especifico 3.2, ver arriba) Obtener resultados de las pruebas de votación realizados. Para esto obtendremos la información (votos) directamente de la Base de Datos, mediante Data Analytics y TAAC/CAAT para obtener totales (sumarización) y comparar con las actas de prueba realizadas, con la finalidad de determinar la Auditabilidad y Confiabilidad y asegurar la comprobación.																										
OBJETIVO ESPECÍFICO 6.3 (Aplica mismo Objetivo Especifico 3.1, ver arriba) Realizar pruebas de funcionalidad del Software de Votación Automatizada con la finalidad de tener resultados de votos realizados, actas de resultados y comparar con el Análisis de Datos (Data Analytics) que realizaremos en el siguiente objetivo.																										
ENTREGA INFORME Entrega de Informes Borrador para validación de la JCE y Entrega de Informe Definitivo Autorizado por la JCE																										
REUNIÓN CIERRE Tendremos una reunión final de cierre de la presente Auditoría																										

Fin del PLAN para EJECUTAR EL TRABAJO