**JUNTA CENTRAL ELECTORAL**

# PROPUESTA TECNICA DE AUDITORÍA FORENSE

# AL SISTEMA DE VOTO AUTOMATIZADO


**PKF**

Calle 14 No. 3ª A
Urbanización Fernández
Sto Domingo, Rep. Dom.
Tel:(809) 540-6668
567-2946
Fax:(809) 547-2708
E-mails:
hguzman@guzmantapiapkf.com.do

# TABLA DE CONTENIDO

GUZMAN TAPIA PKF

PKF Accountants & business advisers

**F.L.-01- Formulario de Inscripción**

**Auditoria al software de Votación Automatizada**

| **DATOS DE LA EMPRESA** | | |
|---|---|---|
| Nombre: **Guzman Tapia PKF, SRL** | RNC: **131-02392-4** | RPE: **39854** |
| Dirección: **Calle 14 #3ª, Urbanización Fernandez, Santo Domingo, República Dominicana** | | |
| Correo Electrónico: hguzman@guzmantapiapk.com.do | | Teléfono: **809-540-6668** |
| **DATOS DE LOS REPRESENTANTES** | | |
| **REPRESENTANTE I** | | |
| Nombre: **Hector Enrique Guzman Desangles** | Cédula:**001-0097740-4** | |
| Posición en la empresa: **Socio – Director** | Teléfono: **809-540-6668** | |
| Correo Electrónico: : hguzman@guzmantapiapk.com.do | Móvil: **809-470-2610** | |
| **PERSONA QUE REALIZA LA INSCRIPCIÓN** | | |
| Nombre: **Hector Enrique Guzman Desangles** | Cédula:**001-0097740-4** | |
| Posición en la empresa: **Socio – Director** | Teléfono: **809-540-6668** | |
| Correo Electrónico: : hguzman@guzmantapiapk.com.do | Móvil: **809-470-2610** | |

GUZMAN TAPIA PKF

PKF Accountants & business advisers

**F.L.-02-Presentación de Ofertas**

Fecha: **31 de octubre del 2019**

Señores
**Comité de Compras y Contrataciones**
Junta Central Electoral
Santo Domingo, Distrito Nacional, Rep. Dom.

Nosotros, los suscritos, declaramos que:

Hemos examinado y no tenemos reservas al Pliego de Condiciones para el procedimiento de referencia, incluyendo las adendas realizadas al mismo.

Nuestra oferta se mantendrá vigente por un período de treinta (30) días hábiles, contado a partir de la fecha límite fijada para la presentación de ofertas, de conformidad con el Pliego de Condiciones Específicas. Esta oferta nos obliga y podrá ser aceptada en cualquier momento hasta antes del término de dicho período.

Nuestra empresa, sus afiliadas o subsidiarias, no han sido declaradas inelegibles por la JUNTA CENTRAL ELECTORAL para presentar ofertas.

Si nuestra oferta difiere o no contempla alguna parte de la información requerida y/o suministrada en el Pliego de Condiciones, estamos conscientes de que el riesgo estará a nuestro cargo y de que el resultado será el rechazo de nuestra propuesta. De igual manera, sabemos que después de abierta, esta oferta no podrá ser retirada ni modificada por nosotros, bajo ninguna circunstancia.

Entendemos que esta oferta, en caso de resultar adjudicatarios, constituirá una obligación contractual, hasta la preparación y ejecución del Contrato.

Nombre **Hector Guzman Desangles** en calidad de **Socio Director - Representante** debidamente autorizado para actuar en nombre y representación de **Guzman Tapia PKF, SRL.**

Firma _____
Sello

**Calle 14 No. 3-A, Urb. Fernández Apartado Postal 10-2, Santo Domingo, Rep. Dom**
Email: info@guzmantapiapkf.com.do • Telf.: (809) 540-6668 • (809) 567-2946 • Fax.: (809) 547-2708

# Propuesta Técnica o descripción del servicio ofertado

# INDICE

## 1. QUIENES SOMOS


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 Auditoria, 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.

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


## CERTIFICACIONES RELEVANTES

- Instituto de Contadores Públicos Autorizados de Republica Dominicana (ICPARD)
- 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

## 2. NUESTRA DIRECCIÓN DE AUDITORÍAS DE TI

La Empresa Dominicana 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 ®*
*CSXF®* - *Certified Cybersecurity NEXUS ®*

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).

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

La Firma 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 Auditoria de TI:


RAVICARIBE
SANSOUCI
metro
Puerta del Cielo
HELADOS BON
PKF
SINERCON
VMO
Aguas Cristal
ECOLAB
METALDOM
SCADOM
innova
Astur
Cazar DDB
Plaza Gráfica
j.l.editora
Forbes
AUTOCAMIONES, S.A.
EDOM
REID & COMPAÑIA, S.A.
CAPCANA
Starfish
INDUPALMA
AGRIFEED
ALIANZA ONG
SAN PEDRO BIOENERGY
CIUS HEMINGWAY
cibao
Mercarne
MercaSID
TROPICO
IDDI
SINFONÍA
FUTURO
BID
USAID
Banco Mundial
aecid
PARTICIPACION CIUDADANA
Fundación REDDOM

# 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"

Los líderes 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:
**Ing. Wilson Andia Cuiza, MSc, CISA, CRISC, CSXF, 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), Especialista en Riesgos y Control de Sistemas de Información Certificado (CRISC) y Certified Cybersecurity CSXF. 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.
- 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.

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.

NUESTRO AUDITOR DE TI

Ing. Edgar Pacheco Hernandez, CISA

Profesional universitario egresado en la carrera de Ciencias de la Computación (Bachelor Degree in Computer Science), Cerfificado en Auditoría de Sistemas (CISA) y con más de 20 años de experiencia trabajando en diversas organizaciones (energía, telecomunicaciones, retail y consultoría), apoyando en el mejoramiento de desempeño de negocios en las áreas de auditoría, gestión de proyectos, control interno, gobierno corporativo, riesgos y cumplimiento (GRC). He apoyado a compañías con iniciativas de la Ley Sarbanes-Oxley (SOX-404), proyectos de Auditoría Interna, implementaciones de ERP (SAP y Oracle EBS), proyectos implementación de marcos referenciales COBIT / ITIL, proyectos de aseguramiento de Ingresos, y control interno.

Al equipo, le serán adicionados 5 personas más, cuyos CV serán enviados en breve.

# 5. OBJETIVOS DE LA AUDITORÍA FORENSE REQUERIDAS POR LA JCE

La Junta Central Electoral (JCE) para esta Auditoría Forense, mediante correo electrónico del 28/10/2019 requiere que se realice evalúe los siguientes objetivos y puntos específicos:

1) Secreto del Voto y No trazabilidad
   a) Verificar que no existe una correlación entre el voto y el votante en el comprobante impreso
   b) Comprobar que, en la información registrada en las bases de datos, QRs y comprobantes físicos no hay referencia que permitan, sugieran o induzcan a relacionar el voto y el votante
   c) Comprobar el método utilizado para eliminar la posibilidad de correlacionar el voto y el votante en la base de datos.
2) Integridad de los datos y objetos de la Base de Datos
   a) Confirmar que es auditable
      I) Certificar que lo elegido por el elector es exactamente lo impreso en el comprobante de votación
      II) Certificar que lo impreso es exactamente lo registrado
      III) Certificar que la relación de votación de cada mesa es exactamente la suma de los volantes impresos (consolidación en acta de votación)
      IV) Certificar que la relación de votación transmitida es exactamente la relación de votación recibida
      V) Certificar que la consolidación de los votos transmitidos es exactamente la consolidación de los votos recibidos
   b) Análisis Bases de Datos Unidad Votación Automatizada y Servidores centrales
   c) Análisis del QR
   d) Análisis de transmisión de datos vía modem 3G y QR
   e) Análisis Bases de Datos y del Sistema de Consolidación de resultados de Microsoft Azure
3) Trabajo fuera de línea (no online)
   a) Certificar que durante el proceso de votación el sistema funciona operativamente sin conexión de las redes
4) Análisis programa fuente vs programa Objeto de la Unidad de Votación Automatizada
   a) Certificar que el ejecutable instalado es el mismo en todas las urnas de votación utilizadas
5) Evaluar la Infraestructura Tecnológica que soporta el Sistema de Votación Automatizada, haciendo énfasis en los aspectos de la seguridad

# 6. DESCRIPCIÓN DE LA METODOLOGÍA PARA EJECUTAR EL TRABAJO

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

OBJETIVO 1
Secreto del Voto y No trazabilidad

a) Verificar que no existe una correlación entre el voto y el votante en el comprobante impreso
b) Comprobar que, en la información registrada en las bases de datos, QRs y comprobantes físicos no hay referencia que permitan, sugieran o induzcan a relacionar el voto y el votante.
c) Comprobar el método utilizado para eliminar la posibilidad de correlacionar el voto y el votante en la base de datos.

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:

Para cumplir con este objetivo, realizaremos una lectura del Código Fuente. También extracción de datos de las bases de datos de las mesas y del servidor central, mediante Data Analytics TAAC/CAAT con software de Auditoría IDEA para cumplir los siguientes objetivos específicos:

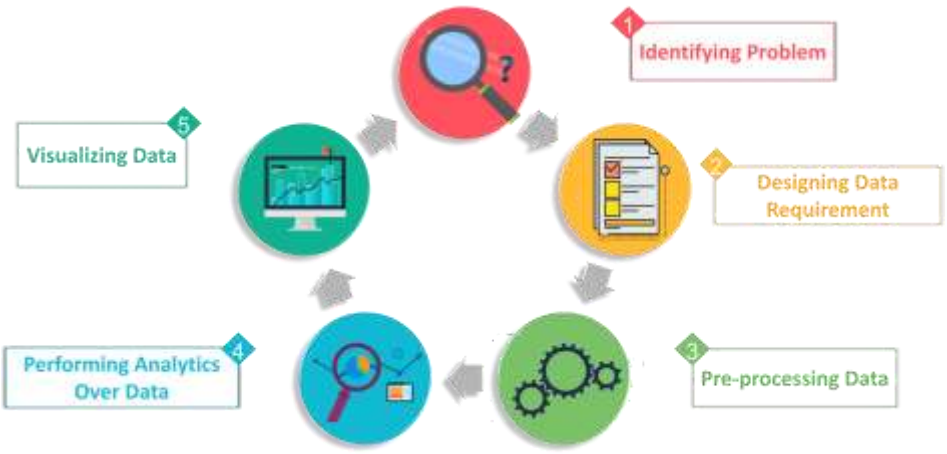
OBJETIVO ESPECÍFICO 1.1
Revisar y evaluar el código fuente del Sistema de Votación Automatizada en cuanto a la Aplicación, Store Procedures, para determinar que no exista correlación alguna entre el voto y el votante o que no se esté guardando este dato en otro lugar y comprobar el método utilizado para eliminar la posibilidad de dicha correlación.

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


OBJETIVO ESPECÍFICO 1.2
Revisar una muestra de comprobantes físicos impresos, verificar que tengan Código QR para decodificar y para comparar con la Base de Datos, tanto en los dispositivos (equipos) de las mesas de votación como del Servidor Central, que obtendremos la data mediante Data Analytics y TAAC/CAAT Software de Auditoría, con la finalidad de verificar que no hay referencia que permitan, sugieran o induzcan a relacionar el voto y el votante.

Decodificaremos la información de los comprobantes impresos y los QR, decodificando para comparar los datos con las bases de datos. Utilizaremos Software de Auditoría y Data Analytics TAAC/CAAT (IDEA) para extraer la data de los votos realizados para analizar y comparar.

Nuestra Firma cuenta con las licencias oficiales respectivas del Software IDEA.




OBJETIVO ESPECÍFICO 1.3
Adicionalmente, evaluaremos la Seguridad de la Información (confidencialidad, integridad, disponibilidad) en sus 3 diferentes estados, es decir:


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.

Con la finalidad de garantizar la Confidencialidad de la Información.

OBJETIVO 2

Integridad de los datos y objetos de la Base de Datos

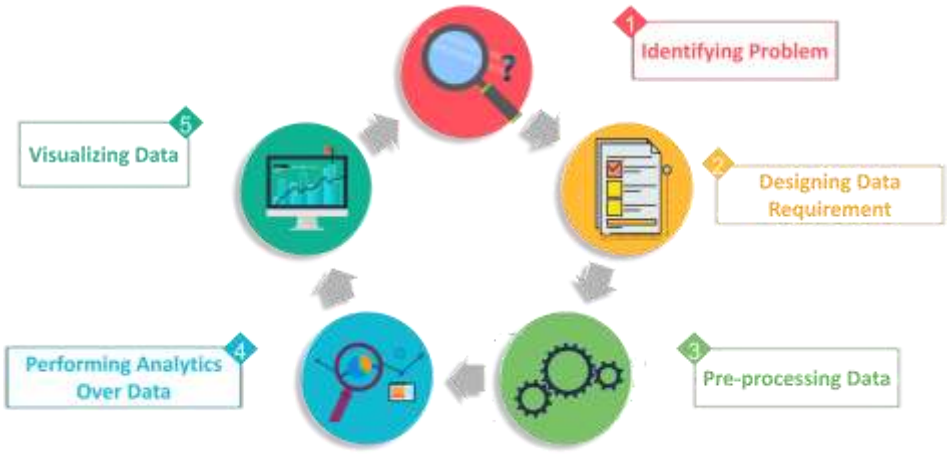
a) Confirmar que es auditable
   I) Certificar que lo elegido por el elector es exactamente lo impreso en el comprobante de votación
   II) Certificar que lo impreso es exactamente lo registrado
   III) Certificar que la relación de votación de cada mesa es exactamente la suma de los volantes impresos (consolidación en acta de votación)
   IV) Certificar que la relación de votación transmitida es exactamente la relación de votación recibida
   V) Certificar que la consolidación de los votos transmitidos es exactamente la consolidación de los votos recibidos
b) Análisis Bases de Datos Unidad Votación Automatizada y Servidores centrales
c) Análisis del QR
d) Análisis de transmisión de datos vía modem 3G y QR
e) Análisis Bases de Datos y del Sistema de Consolidación de resultados de Microsoft Azure

Para cumplir con este objetivo, realizaremos los siguientes objetivos específicos:

OBJETIVO ESPECÍFICO 2.1

- Comparar los comprobantes físicos impresos, de una muestra seleccionada, con la base de datos, verificando la integridad o exactitud, mediante técnicas de extracción, búsquedas y análisis de datos Data (Analytics TAAC/CAAT) con software de Auditoría IDEA.
- Verificación de totales, mediante sumarizaciones automáticas para verificar la integridad de cada base de datos de cada mesa con el acta de votación y esta a su vez con la base de datos del servidor central producto de la transmisión realizada.
- Verificaremos que la data transmitida de las mesas de votación, de una muestra seleccionada, es exacta o integra en la base de datos del Servidor central, es decir la data recibida. Esto con Software de Auditoría IDEA (Analytics TAAC/CAAT).

Nuestra Firma cuenta con las licencias oficiales respectivas del Software IDEA.


OBJETIVO ESPECÍFICO 2.2
Certificar que es Auditable y Comprobable satisfactoriamente

Una vez que realicemos las pruebas descritas en el objetivo anterior 2.1 y verifiquemos que es satisfactorio, emitiremos la Certificación de Auditabilidad y que es Comprobable, caso contrario no emitiremos la certificación.


OBJETIVO ESPECÍFICO 2.3
Analizar las Bases de Datos de Unidad Votación Automatizada (muestras seleccionadas) y Servidores centrales, en cuanto a integridad de objetos e información.

Verificaremos los objetos de la base de datos, usuarios, tablas, store procedures instalados, triggers activados, profiles y de seguridad para comprobar su integridad entre la Base de Datos de la Unidad de Votación con el esquema del Servidor Central.

Verificaremos la Integridad de la data de las unidades de votación automatizadas (muestras seleccionadas), con la base de Datos del Servidor Central, en cuanto a:

OBJETIVO ESPECÍFICO 2.4
Analizar y revisar la generación del código QR y también la decodificación para verificar la integridad de qué datos son los que captura e imprime en los comprobantes físicos que se imprimen.

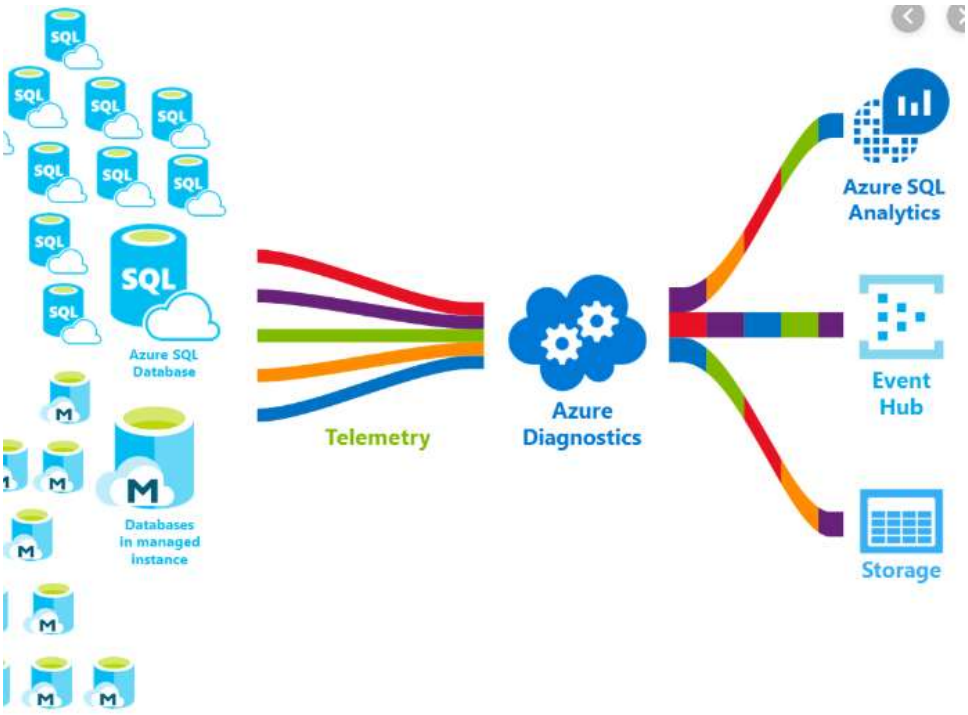
Verificaremos el proceso de generación del código QR que se utilizó y tomaremos una muestra seleccionada de comprobantes físicos impresos para decodificar y verificar la integridad de la información que contiene, comparado con las bases de datos de las mesas de votación y la base de datos del servidor central.

OBJETIVO ESPECÍFICO 2.5
Analizaremos la integridad de la transmisión de la data vía dispositivos modem 3G USB, APN (Access Point Name) y QR con la finalidad del verificar que se transmita la data exacta. Esta prueba se complementa con las pruebas de integridad descritas arriba.

Verificaremos la trama o paquetes que se envían a través de modem 3G para verificar la integridad de la data transmitida. Esta prueba se complementará con la verificación de la integridad de la data transmitida y recibida que se encuentra en las bases de datos de las mesas (de la muestra seleccionada) y del servidor central. Ver objetivo específico arriba.

OBJETIVO ESPECÍFICO 2.6
Analizaremos la integridad y exactitud de la información de los Servidores Centrales con la información de Microsoft Azure, con la finalidad de verificar la confiabilidad de la consolidación de resultados.

- Aplicaremos técnicas de extracción, selección, búsquedas y análisis de datos Data (Analytics TAAC/CAAT) con software de Auditoría IDEA para comparar las bases de datos del servidor central con la base de datos de Microsoft Azure (nube).
- Además, aplicaremos técnicas de agrupación, sumarización de datos para comparar con la consolidación de los resultados de la JCE.



OBJETIVO 3
Trabajo fuera de línea

a) Certificar que durante el proceso de votación el sistema funcionará operativamente sin conexión de las redes.

Según la JCE 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 3.1
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.

OBJETIVO ESPECÍFICO 3.2
Revisar la configuración de los dispositivos modem 3G USB, APN (Access Point Name) con la finalidad del 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 3.3
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 3.4
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:

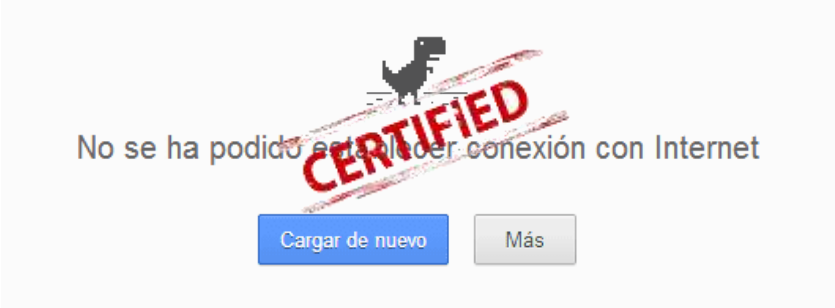
- Cumplimiento de Políticas definidas.
- Usuarios administradores autorizados del IPS
- Roles/Permisos de los usuarios administradores del IPS
- Tipo de tráfico de red que está monitoreando el IPS
- Tipos de actividad maliciosa puede prevenir de forma proactiva el IPS
- Alertas/Notificaciones configuradas 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

OBJETIVO ESPECÍFICO 3.5
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 trafico 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 3.6
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.

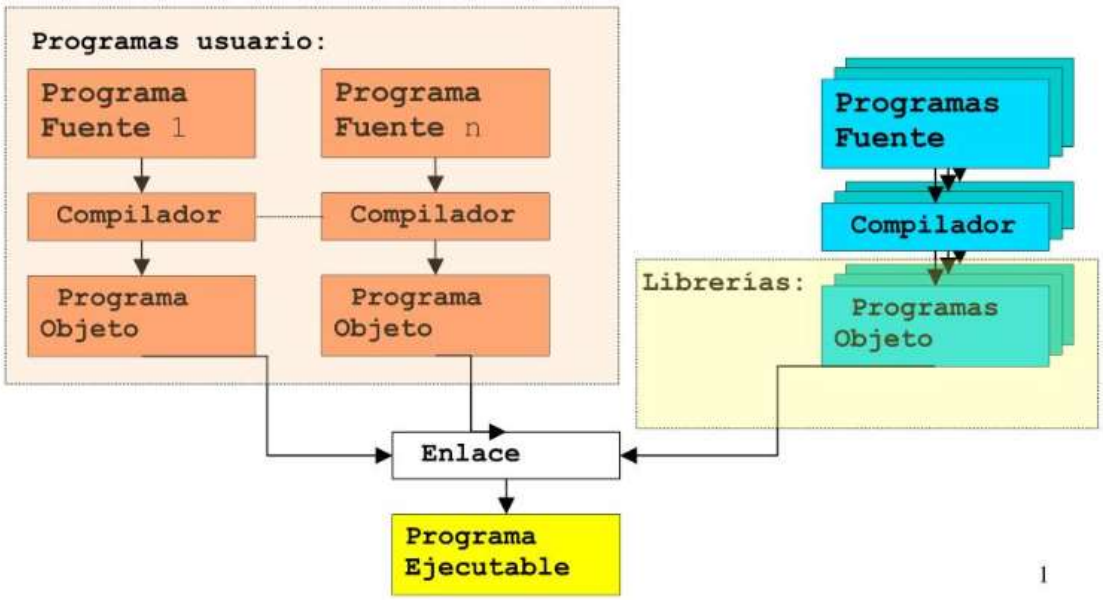


OBJETIVO 4
Análisis programa fuente vs programa Objeto de la Unidad de Votación Automatizada
a) Certificar que el ejecutable instalado es el mismo en todas las urnas de votación utilizadas

OBJETIVO ESPECÍFICO 4.1
Evaluar y revisar la lógica de los programas fuente, procedimientos, funciones y store procedures con la finalidad de identificar posible código malicioso embebido que altere datos o resultados.

A la fecha de la Auditoría Forense, verificaremos el código fuente y la lógica o algoritmos de los programas del Sistema de Votación Automatizado, línea por línea, Procedimientos, Funciones y llamados a Store Procedures, verificando que corresponda al programa Objeto/Ejecutable obtenido y que el mismo esté instalado en los equipos de las mesas de votación de la muestra seleccionada.

También revisaremos la lógica de los programas fuente de los Store Procedures.



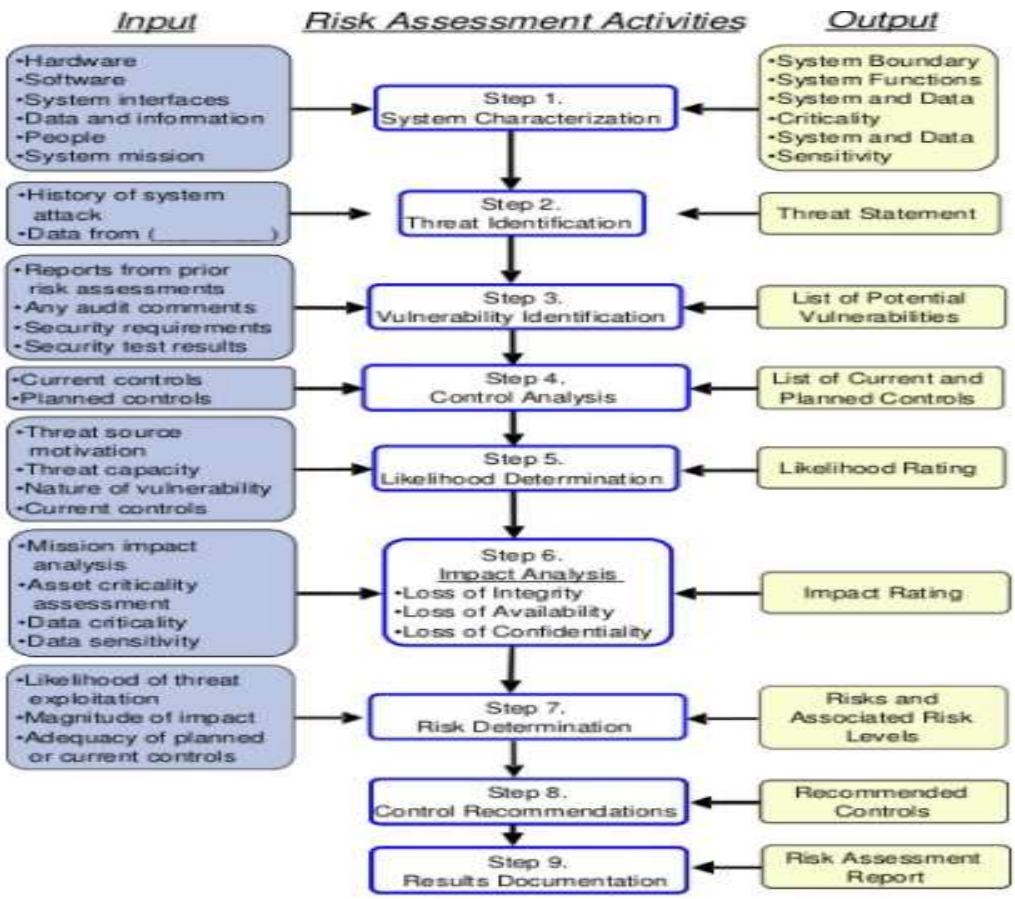

OBJETIVO ESPECÍFICO 4.2
Evaluar el proceso de control de cambios que se tiene en la JCE para realizar cambios a los programas fuente, compilación y pase a producción (Equipos de Votación en mesas y Servidores Centrales).

Revisaremos las políticas, procedimientos de control de cambios a los programas, proceso de compilación, pruebas y pases a los ambientes de producción tanto del programa ejecutable en las mesas de votación (de la muestra seleccionada) y al servidor centrar si fuere el caso.


OBJETIVO 5
Evaluar la Infraestructura Tecnológica que soporta el Sistema de Votación Automatizada, haciendo énfasis en los aspectos de la seguridad.

OBJETIVO ESPECÍFICO 5.1
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).




OBJETIVO ESPECÍFICO 5.2
Evaluar la seguridad de la Infraestructura Tecnológica que soporta el Sistema de Votación Automatizada de la JCE para identificar posibles accesos no autorizados.


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

   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.

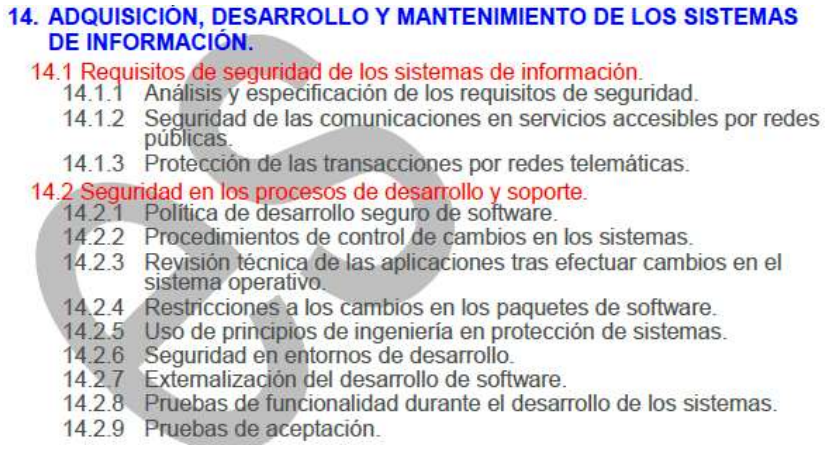
   Con la finalidad de garantizar la Confidencialidad de la Información.

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.
   - Módulo de Seguridad de Administración de Usuarios
   - Roles/Perfiles, Controles de accesos
   - Backdoors
   - Controles de Entrada, Proceso y Salida
   - Verificación y lectura del programa fuente, con la finalidad de verificar que no exista código malisioso.

   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. ADQUISICIÓN, 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 5.3
Evaluar la Seguridad de la Información (confidencialidad, integridad, disponibilidad) en sus 3 diferentes estados, es decir:


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.

# 7. PLAN PARA EJECUTAR EL TRABAJO

| | | 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 | 26 | 27 | 28 | 29 | 30 |
| **REUNIÓN INICIAL**<br>**Tendremos una reunión inicial de coordinación con el Personal de contra parte de la JCE para explicar el proceso de Auditoría y para requerimientos necesarios.** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **OBJETIVO 1**<br>**Secreto del Voto y No trazabilidad**<br>**a) Verificar que no existe una correlación entre el voto y el votante en el comprobante impreso**<br>**b) Comprobar que, en la información registrada en las bases de datos, QRs y comprobantes físicos no hay referencia que permitan, sugieran o induzcan a relacionar el voto y el votante.**<br>**c) Comprobar el método utilizado para eliminar la posibilidad de correlacionar el voto y el votante en la base de datos.** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | **OBJETIVO ESPECÍFICO 1.1** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | **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 entre el voto y el votante o que no se esté guardando este dato en otro lugar y comprobar el método utilizado para eliminar la posibilidad de dicha correlación.** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | **OBJETIVO ESPECÍFICO 1.2** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | **Revisar una muestra de comprobantes físicos impresos, verificar que tengan Código QR para decodificar y para comparar con la Base de Datos, tanto en los dispositivos (equipos) de las mesas de votación como del Servidor Central, que obtendremos la data mediante Data Analytics y TAAC/CAAT Software de Auditoría, con la finalidad de verificar que no hay referencia que permitan, sugieran o induzcan a relacionar el voto y el votante.** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | **OBJETIVO ESPECÍFICO 1.3** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| | **Adicionalmente, evaluaremos la Seguridad de la Información (confidencialidad, integridad, disponibilidad) en sus 3 diferentes estados** | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

| | 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 | 26 | 27 | 28 | 29 | 30 |
| **OBJETIVO 2**<br><br>Integridad de los datos y objetos de la Base de Datos<br>a) Confirmar que es auditable<br>I) Certificar que lo elegido por el elector es exactamente lo impreso en el comprobante de votación<br>II) Certificar que lo impreso es exactamente lo registrado<br>III) Certificar que la relación de votación de cada mesa es exactamente la suma de los volantes impresos (consolidación en acta de votación)<br>IV) Certificar que la relación de votación transmitida es exactamente la relación de votación recibida<br>V) Certificar que la consolidación de los votos transmitidos es exactamente la consolidación de los votos recibidos<br>b) Análisis Bases de Datos Unidad Votación Automatizada y Servidores centrales c) Análisis del QR<br>d) Análisis de transmisión de datos vía modem 3G y QR<br>e) Análisis Bases de Datos y del Sistema de Consolidación de resultados de Microsoft Azure | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| OBJETIVO ESPECÍFICO 2.1<br>• Comparar los comprobantes físicos impresos, de una muestra seleccionada, con la base de datos, verificando la integridad o exactitud, mediante técnicas de extracción, búsquedas y análisis de datos Data (Analytics TAAC/CAAT) con software de Auditoría IDEA.<br>• Verificación de totales, mediante sumarizaciones automáticas para verificar la integridad de cada base de datos de cada mesa con el acta de votación y esta a su vez con la base de datos del servidor central producto de la transmisión realizada.<br>• Verificaremos que la data transmitida de las mesas de votación, de una muestra seleccionada, es exacta o integra en la base de datos del Servidor central, es decir la data recibida. Esto con Software de Auditoría IDEA (Analytics TAAC/CAAT). | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| OBJETIVO ESPECÍFICO 2.2<br>Certificar que es Auditable y Comprobable satisfactoriamente | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| OBJETIVO ESPECÍFICO 2.3<br>Analizar las Bases de Datos de Unidad Votación Automatizada (muestras seleccionadas) y Servidores centrales, en cuanto a integridad de objetos e información. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| OBJETIVO ESPECÍFICO 2.4<br>Analizar y revisar la generación del código QR y también la decodificación para verificar la integridad de qué datos son los que captura e imprime en los comprobantes físicos que se imprimen. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| OBJETIVO ESPECÍFICO 2.5<br>Analizaremos la integridad de la transmisión de la data vía dispositivos modem 3G USB, APN (Access Point Name) y QR con la finalidad del verificar que se transmita la data exacta. Esta prueba se complementa con las pruebas de integridad descritas arriba. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| OBJETIVO ESPECÍFICO 2.6<br>Analizaremos la integridad y exactitud de la información de los Servidores Centrales con la información de Microsoft Azure, con la finalidad de verificar la confiabilidad de la consolidación de resultados. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

| | 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 | 26 | 27 | 28 | 29 | 30 |
| **OBJETIVO 3**<br>Trabajo fuera de línea<br>a) Certificar que durante el proceso de votación el sistema funcionará operativamente sin conexión de las redes. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **OBJETIVO ESPECÍFICO 3.1**<br>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 3.2**<br>Revisar la configuración de los dispositivos modem 3G USB, APN (Access Point Name) con la finalidad del verificar que solo pueda existir conexión a través de estos dispositivos, en los horarios establecidos. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **OBJETIVO ESPECÍFICO 3.3**<br>Revisar la configuración de la Red Privada Virtual (VPN) con la finalidad de identificar usuarios y accesos no autorizados. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| **OBJETIVO ESPECÍFICO 3.4**<br>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 3.5**<br>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 3.6**<br>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. | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

| | 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 26 27 28 29 30 |
| **OBJETIVO 4**<br>Análisis programa fuente vs programa Objeto de la Unidad de Votación Automatizada<br>a) Certificar que el ejecutable instalado es el mismo en todas las urnas de votación utilizadas | |
| **OBJETIVO ESPECÍFICO 4.1**<br>Evaluar y revisar la lógica de los programas fuente, procedimientos, funciones y store procedures con la finalidad de identificar posible código malicioso embebido que altere datos o resultados. | |
| **OBJETIVO ESPECÍFICO 4.2**<br>Evaluar el proceso de control de cambios que se tiene en la JCE para realizar cambios a los programas fuente, compilación y pase a producción (Equipos de Votación en mesas y Servidores Centrales). | |
| **OBJETIVO 5**<br>Evaluar la Infraestructura Tecnológica que soporta el Sistema de Votación Automatizada, haciendo énfasis en los aspectos de la seguridad. | |
| **OBJETIVO ESPECÍFICO 5.1**<br>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**<br>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**<br>Evaluar la Seguridad de la Información (confidencialidad, integridad, disponibilidad) en sus 3 diferentes estados | |
| **1er Informe con Objetivos 2 y 4** | |
| **ENTREGA INFORME**<br>Entrega de Informes Borrador para validación de la JCE y Entrega de Informe Definitivo Autorizado por la JCE | |
| **REUNIÓN CIERRE**<br>Tendremos una reunión final de cierre de la presente Auditoría | |