Santo Domingo, D. N.,
10 de septiembre de 2019.

JCE
RECIBIDO
COMITÉ DE COMPRAS Y CONTRATACIONES
11 SEP 2019
HORA 2:33 Pm
FIRMA

Señores:
Dr. Luis Ramón Cordero
Presidente

Lic. Leonardo García
Coordinador

Comisión de Compras y Licitaciones,
Sus Despachos.-

Distinguidos señores:

Cortésmente, después de manifestarles saludos cordiales, atendiendo a su comunicación No. CCC-350/2019, de fecha 2 de septiembre de 2019, donde se nos solicita realizar la evaluación de las propuestas presentadas por los oferentes concursantes en la licitación Ref.: JCE-CCC-PU-02-03-20195, referente a la Auditoria técnica para el Software desarrollado para la implementación del voto automatizado, detallamos a continuación el resultado de la referida evaluación.

El objetivo principal de la licitación es realizar una auditoría técnica donde se puedan certificar diferentes aspectos que abarcan el desarrollo del Software de Votación Automatizado, tales como:

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

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.

Ave. 27 de Febrero, Esq. Gregorio Luperón
Santo Domingo, República Dominicana, Tél.: 809-539-5419
www.jce.gob.do

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.

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

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

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

La documentación que se les requirió presentar a los oferentes en su propuesta técnica fueron las siguientes:

1. Credenciales Profesionales que autentiquen su condición como Auditores Externos certificados.

2. Propuesta Técnica o descripción del servicio ofertado, la cual debe incluir lo siguiente:
   a. Una breve descripción de la firma auditora.

   b. Reseña de su experiencia en trabajos recientes de carácter similar, donde se incluyan certificaciones sobre el grado de satisfacción alcanzado por el cliente (contratante), la duración del trabajo y el monto del contrato.

   c. Información sobre el nivel de especialización del personal que acompañará la firma.

   d. Una descripción de la metodología y el plan para ejecutar el trabajo.

   e. La lista del personal propuesto, por especialidad, con indicación de las actividades que les serán asignadas y el tiempo que participarán en ellas.

Ave. 27 de Febrero, Esq. Gregorio Luperón
Santo Domingo, República Dominicana, Tél.: 809-539-5419
www.jce.gob.do

f. Currículos recientes firmados por el personal profesional propuesto y por el representante autorizado que presenta la propuesta. La información básica deberá incluir el número de años de trabajo en la firma y el nivel de responsabilidad asumida en las labores desempeñadas.

Los criterios de evaluación utilizados se basan en que el oferente demuestre que tiene capacidad y experiencia en el tipo de trabajo a realizar y en las condiciones establecidas para garantizar la calidad del servicio y su correspondencia con los requerimientos.

En ocasión de conocer las propuestas técnicas presentadas por los dos (2) oferentes; Guzman Tapia PKF y Consorcio Pontezuela-Bidaga-Alhambra Eidos, luego de la revisión de la documentación técnica suministrada por ambos, podemos resumir lo siguiente:

1) Evaluación Propuesta oferente: Guzman Tapia PKF

B1-Certificaciones que autentiquen su condición como auditores Externos Certificados. [CUMPLE]

- Institutos de Contadores Públicos Autorizados de RD (ICAPRD).
- Superintendencia de Bancos (SIB) .

Personal con Certificaciones:

- CISA: Certified Information System Auditor.
- CRISC: Certified in Risk and Information System Control.
- CISM: Certified Information Security manager.
- CISSP: Certified Security System Security Professional.
- CEH: Certified Ethical Hacker.
- ISO 27001 LA: Certificado Profesional Líder en Auditoria de Seguridad ISO 27001.

Uso de estándares Internacionales como:

- COBIT: Marco de Gobierno y Control TI.
- ISO 27001: Sistema de Gestión de Seguridad de Información.
- ISO 27002: Controles de Seguridad de la Información.

Ave. 27 de Febrero, Esq. Gregorio Luperón
Santo Domingo, República Dominicana, Tél.: 809-539-5419
www.jce.gob.do

- ISO 22301: Continuidad de Negocio.
- ISO 27031: Continuidad de TI, Plan de Recuperación ante Desastres de TI.
- ISO 27005, NIST, MAGERIT: Análisis de Riesgos Tecnológicos.
- ISO 25000: Evaluar Calidad del Sistema y Producto de Software.
- ISO 9126: Evaluación de la calidad del Software.
- Software de Auditoria IDEA y ACL

2- Propuesta Técnica o descripción del servicio ofertado, la cual debe incluir lo siguiente:

2-i-Una breve descripción de la firma auditora. [CUMPLE]

Firma miembro de PKF International Limited, con más de 40 años de experiencia en Auditoria, Consultoría e Impuestos, entre otros. Experiencia en diferentes industrias y áreas de la economía basada en la amplia experiencia de los socios de la firma y lo que comparten con su red de socios.

2-ii-Reseña de su experiencia en trabajos recientes de carácter similar, donde se incluyan certificaciones sobre el grado de satisfacción alcanzado por el cliente (contratante), la duración del trabajo y el monto del contrato. [CUMPLE]

- **Banco BDI**: Auditor Externo desde 1999 en Auditorias Financieras y además realizan Auditorias tecnológicas 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). Verificar el cumplimiento de Normas y Estándares Internacionales relacionados a TI. [Timbrada, Sellada]

- **Banco Múltiple Lopez de Haro:** Auditor Externo por más de 10 años en Auditorias Financieras y además realizan Auditorias tecnológicas 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). Verificar el cumplimiento de Normas y Estándares Internacionales relacionados a TI.[Timbrada, Sellada]

- **Banco Ademi:** Auditor Externo desde el año 2012 en Auditorias Financieras y además realizan Auditorias tecnológicas en la evaluación de seguridad de la

Ave. 27 de Febrero, Esq. Gregorio Luperón
Santo Domingo, República Dominicana, Tél.: 809-539-5419
www.jce.gob.do

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). Verificar el cumplimiento de Normas y Estándares Internacionales relacionados a TI.[Timbrada, Sellada]

Banco Vimenca: Prestado servicios desde el año 2016, en Auditorias Financieras y además realizan Auditorias tecnológicas 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). Verificar el cumplimiento de Normas y Estándares Internacionales relacionados a TI. Se Destacan por un alto nivel de profesionalidad y cuentan con personal capacitado. [Timbrada, Sellada]

Banco Vimenca: Proveedor de Servicios de Auditoria Financiera desde el año 2017, y Auditorias tecnológicas 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). Verificar el cumplimiento de Normas y Estándares Internacionales relacionados a TI.[Timbrada, Sellada]

- **Leasing Confisa:** Proveedor de Servicios de Auditoría Externa desde el año 2017, y Auditorias tecnológicas 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). Verificar el cumplimiento de Normas y Estándares Internacionales relacionados a TI.[Timbrada, Sellada]

2-iii-Información sobre el nivel de especialización del personal que acompañará la firma. [CUMPLE]

- MSc, CISA, CRISC, CISM, CISSP, CEH, ISO 27001, ISO 27032, ISACA,COBIT, NIST, OSSTMM, OWASP
- Auditorias de TI, Seguridad, Riesgos y Control TI, Auditoria Forense.

Ave. 27 de Febrero, Esq. Gregorio Luperón
Santo Domingo, República Dominicana, Tél.: 809-539-5419
www.jce.gob.do

- Auditoria de Seguridad Core Bancarios.
- Auditoria a Sistemas Monitor Plus y Sentinel, UltraFisgon.
- Auditoria de Cumplimiento PCI-DSS.
- Gestión de Proyectos.

2-iv-Una descripción de la metodología y el plan para ejecutar el trabajo. [CUMPLE]

Tiempo de entrega de informe final: 25 días

- **OBJETIVO 1 [Duración 12 días]**
  - Certificar que el sistema de votación automatizada implementado por la Junta Central Electoral garantiza el Secreto del Voto de los Electores.
  - 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. Usando el metodo de evaluacion estandar ***NIST-800-30***

- **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.
  - 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.
  - 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.
  - La encriptación de la información, para verificar que se garantice la confidencialidad de la información, basándonos en la Norma ISO 27002 (Dominio 10 Cifrado).
  - La gestión y control de accesos, usuarios, roles, perfiles de acceso a la Infraestructura Tecnológica que soporta el Sistema de Votación por ej.:

Ave. 27 de Febrero, Esq. Gregorio Luperón
Santo Domingo, República Dominicana, Tél.: 809-539-5419
www.jce.gob.do

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.

- Verificaremos y evaluaremos la Seguridad en el Desarrollo de la Aplicación/Software desarrollado para la Votación Automatizada.
- 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.
- 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:
  - Datos del VOTO en captura y movimiento, Datos del VOTO en reposo y Datos del VOTO en uso.
  - 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).

- **OBJETIVO ESPECÍFICO 1.4**
  - Certificar que el sistema garantiza el secreto del voto de los electores.

OBJETIVO 2 [Duración 11 días]

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.

Ave. 27 de Febrero, Esq. Gregorio Luperón
Santo Domingo, República Dominicana, Tél.: 809-539-5419
www.jce.gob.do

- **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: Wifi, Ethernet, Dial-up, VPN, Mobile Hotspot, Proxy. Nos basaremos en la Norma ISO 27002 (Dominio 13 Seguridad en las Telecomunicaciones).

OBJETIVO ESPECÍFICO 2.2

- 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 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.

Ave. 27 de Febrero, Esq. Gregorio Luperón
Santo Domingo, República Dominicana, Tél.: 809-539-5419
www.jce.gob.do

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 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.

Ave. 27 de Febrero, Esq. Gregorio Luperón
Santo Domingo, República Dominicana, Tél.: 809-539-5419
www.jce.gob.do

OBJETIVO 3 [Duración 8 días]

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

- **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)

Ave. 27 de Febrero, Esq. Gregorio Luperón
Santo Domingo, República Dominicana, Tél.: 809-539-5419
www.jce.gob.do

- **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.

- **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 [Duración 8 días]

- 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.

Ave. 27 de Febrero, Esq. Gregorio Luperón
Santo Domingo, República Dominicana, Tél.: 809-539-5419
www.jce.gob.do

- **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.

- **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).

- **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.

- **OBJETIVO 5 [Duración 7 días]**
  - 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,

Ave. 27 de Febrero, Esq. Gregorio Luperón
Santo Domingo, República Dominicana, Tél.: 809-539-5419
www.jce.gob.do

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.
  - 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 [Duración 14 días]**
  - 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.

Ave. 27 de Febrero, Esq. Gregorio Luperón
Santo Domingo, República Dominicana, Tél.: 809-539-5419
www.jce.gob.do

- **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 (sumariazción) 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.

- **FIN DE AUDITORIA**
  Entrega de informe borrador para validación por parte de la JCE y entrega de informe definitivo autorizado por JCE.
  Reunión de cierre para cierre de la Auditoria.

2-v-La lista del personal propuesto, por especialidad, con indicación de las actividades que les serán asignadas y el tiempo que participarán en ellas. [CUMPLE PARCIALMENTE] No Indican detalle de las actividades a realizar.

Hector Enrique Guzmán Desangles -> Representante de la firma.
Wilson Andia Cuiza-> Director Auditoria
Domingo Ormeño -> Auditor Senior
Cesar Millavil -> Auditor de Seguridad y CiberSeguridad

Ave. 27 de Febrero, Esq. Gregorio Luperón
Santo Domingo, República Dominicana, Tél.: 809-539-5419
www.jce.gob.do

2-vi-Currículos recientes firmados por el personal profesional propuesto y por el representante autorizado que presenta la propuesta La información básica deberá incluir el número de años de trabajo en la firma y el nivel de responsabilidad asumida en las labores desempeñadas. [CUMPLE PARCIALMENTE]

Hector Enrique Guzmán Desangles

- Firmado: **No**
- Número de años en la firma: **38 años**
- Nivel de Responsabilidad: **Representante de la firma.**
- Evaluación de Riesgo.
- Analisis y Mitigacion de Riesgo
- MBA, ACL, MIA-PKF, ISQC1-PKF, NIIFS

Wilson Andia Cuiza

- Firmado: **Si**
- Número de años en la firma: **9 años**
- Nivel de Responsabilidad: **Director Auditoria**
- MSc, CISA, CRISC, ISO 27001 LA, ISACA
- 20 años experiencia en Auditorias de TI, Seguridad, Riesgos y Control TI.
- Auditoria de Seguridad Core Bancarios
- Auditoria a Sistemas Monitor Plus y Sentinel, UltraFisgon
- Auditoria de Cumplimiento PCI-DSS

Domingo Ormeño

- Firmado: **Si**
- Número de años en la firma: **No especifica.**
- Nivel de Responsabilidad: **Auditor Senior**
- CISA
- 20 años de experiencia en Auditorias de TI.
- Diploma en Auditoria de Sistemas y TIC
- Diploma de Gestión de Proyectos
- Diploma de Project Management
- Diploma en Auditoria Forense

Ave. 27 de Febrero, Esq. Gregorio Luperón
Santo Domingo, República Dominicana, Tél.: 809-539-5419
www.jce.gob.do

Cesar Millavil

- Firmado: **Si**
- Número de años en la firma: **No especifica.**
- Nivel de Responsabilidad: **Auditor de Seguridad y CiberSeguridad**
- CEH, ISO 270001 LA, ISO 27032
- Cuenta con 8 años de experiencia en áreas operativas y más de 7 años en jefaturas y gerencias, para un total de 15 años de experiencia profesional.
- Ciberseguridad: ISO 27001 LA, ISO 27032 LM, COBIT, NIST, OSSTMM, OWASP

Ave. 27 de Febrero, Esq. Gregorio Luperón
Santo Domingo, República Dominicana, Tél.: 809-539-5419
www.jce.gob.do

2) Evaluación Propuesta oferente: Consorcio Pontezuela - Bidaga - Alhambra EIDOS

B1-Certificaciones que autentiquen su condición como auditores Externos Certificados. [CUMPLE]

- **Personal con Certificaciones:**
  - Certificación TRACE, sobre anti soborno.
  - CISA: Certified Information System Auditor.
  - CISSP: Certified Security System Security Professional.
  - CISM: Certified Information Security manager.
  - CEH: Certified Ethical Hacker.
  - ISO 27001: Certificado Profesional Lider en Implementador de Seguridad ISO 27001
  - ISO 27032: Certificado Profesional Lider en CiberSeguridad ISO 27032
  - ISO 22301: Certificado Profesional Lider en Auditoria ISO 22301
  - Payment Card Industry Professional (PCI-P)

- **Personal con Certificaciones mencionadas:**
  - CISM: Certified Information Security manager.
  - COBIT 4 Foundation 4.
  - ITIL.

- **Personal Miembro:**
  - Institute of Internal Auditors (IIA).
  - International Association of Engineers (IAE).
  - Association of Computing Machinery (ACM).

2-Propuesta Técnica o descripción del servicio ofertado, la cual debe incluir lo siguiente:

Ave. 27 de Febrero, Esq. Gregorio Luperón
Santo Domingo, República Dominicana, Tél.: 809-539-5419
www.jce.gob.do

2-i-Una breve descripción de la firma auditora. [CUMPLE]

Pontezuela Tech es una empresa dedicada a los servicios en tecnología de la información fundada en el año 2013. Cuenta con 22 colaboradores especializados en diferentes áreas y unas 5 divisiones de servicios:

- Proyectos Business Intelligence /Analíticos.
- Desarrollo de Software.
- Auditorias y Consultorías de Buenas Prácticas TIC.
  SPN Software.
- Capacitación.

La firma ha desarrollado importantes proyectos tanto en el sector público como en el sector privado a organizaciones nacionales e internacionales.

Tmachine: es una empresa uruguya dedicada exclusivamente a brindar servicios de control y aseguramiento de calidad de productos y procesos de software. Los servicios que ofertan se agrupan en dos categorías:

- Testing Services: Este servicio tiene su foco en la productividad y modelos operativos eficientes, con el uso extensivo del conocimiento, herramientas y métricas que ayuden a mejorar el proceso productivo del testing y lograr una alta eficiencia operativa.

  Consulting Studio: El foco es brindar servicios de consultoría personalizados a clientes de la industria del software, que buscan mejorar la calidad de sus procesos de testing, realizar auditorías especializadas, o acceder a certificaciones internacionales de calidad.

2-ii-Reseña de su experiencia en trabajos recientes de carácter similar, donde se incluyan certificaciones sobre el grado de satisfacción alcanzado por el cliente (contratante), la duración del trabajo y el monto del contrato. [CUMPLE PARCIALMENTE] Las cartas de certificación se refieren a la compañía Krav Maga Hacking, SRL y no a ninguna de las integrantes del consorcio, aunque los ejecutores participaran en este proyecto.

Ave. 27 de Febrero, Esq. Gregorio Luperón
Santo Domingo, República Dominicana, Tél.: 809-539-5419
www.jce.gob.do

- Instituto Nacional de Empleo y Formación Profesional (INEFOP: 2018,2019) [Timbrada, No Sellada]
- --> Krav Maga Hacking, SRL --> Mateo Martínez & Mauricio Campiglia.
    - Consultoría de Implementación ISO 27001.
    - Hacking Ético.
    - Implementación de Honeypots.
    - Business Impact Analysis.
    - Implementación de metodologías de gestión de riesgos.
    - Plan de Concientización en seguridad de información.
    - Plan de Continuidad de Negocios (BCP).
    - Plan de Recuperación de Desastres (DRP).
    - Auditoria de Sistemas.
- MG2 Training & Consulting Group (2018,2019) [Timbrada, No Sellada]
- --> Krav Maga Hacking, SRL --> Mateo Martínez & Mauricio Campiglia.
    - Hacking Ético.
    - Gestión de Riesgos.
    - Entrenamiento Ciberseguridad.
    - Implementación de marco Gobierno y Control.
    - Auditoria de Sistemas.
    - Continuidad de Negocios.

- VN Studios Consultoría y Desarrollo IT (2014- 2019) [Timbrada, No Sellada]
- --> Krav Maga Hacking, SRL --> Mateo Martínez & Mauricio Campiglia & Jorge Parra.
    - Hacking Ético.
    - Consultoría en Ciberseguridad.
    - Implementación de Honeypots & Honeynets.
    - BIA y Plan de continuidad de Negocios (BCP).
    - Implementación ISO 27001.
    - Gestión de Riesgos.
    - Auditorias de Sistemas.

- Interfisa Banco (2017,2018) [Timbrada, No Sellada]
- --> Krav Maga Hacking, SRL --> Mateo Martínez & Mauricio Campiglia.
    - Hacking Ético.

Ave. 27 de Febrero, Esq. Gregorio Luperón
Santo Domingo, República Dominicana, Tél.: 809-539-5419
www.jce.gob.do

- Crian Software (2017,2018) [No Timbrada, No Sellada]
- --> Krav Maga Hacking, SRL --> Mateo Martínez & Mauricio Campiglia.
  - Hacking Ético.
    Consultoría en Ciberseguridad.

- Tecn010gika (2017,2018) [Timbrada, Sellada]
- --> Krav Maga Hacking, SRL --> Mateo Martínez & Mauricio Campiglia.
  - Hacking Ético.
  - Consultoría en Ciberseguridad.

- Orange Attitude (2017,2018) [No Timbrada, No Sellada]
- --> Krav Maga Hacking, SRL --> Mateo Martínez & Mauricio Campiglia.
  - Hacking Ético.
  - Consultoría en Ciberseguridad.

- AB InBev (2017,2018) [No Timbrada, No Sellada]
- --> Krav Maga Hacking, SRL --> Mateo Martínez & Mauricio Campiglia.
  - Hacking Ético.
  - Consultoría en Ciberseguridad.
  - Plan Estratégico de Ciberseguridad.

- PC Micro SAS y Fondo Nacional de Garantias (2017) [Timbrada, No Sellada]
- --> Krav Maga Hacking, SRL --> Mateo Martínez & Mauricio Campiglia.
  - Hacking Ético.
- Security Advisor Chile para Combanc (2017) [No Timbrada, No Sellada]
- --> Krav Maga Hacking, SRL --> Mateo martinez & Mauricio Campiglia.
  - Creación de CSIRT.
  - Consultoría en Seguridad.

2-iii-Información sobre el nivel de especialización del personal que acompañará la firma. [CUMPLE]

CISA, PCI-P, CISM, CISSP, CEH, ISO 27001, ISO 27032, ISO 22301, COBIT, OWASP, CIA

- Seguridad Informática.
- Seguridad de Desarrollo de Software.

Ave. 27 de Febrero, Esq. Gregorio Luperón
Santo Domingo, República Dominicana, Tél.: 809-539-5419
www.jce.gob.do

- Especialidad en Centros de Respuesta.
- Auditoria de Cumplimiento PCI-P
- Analista Forense, Pentester.
- MBA

2-iv-Una descripción de la metodología y el plan para ejecutar el trabajo. [CUMPLE]

Tiempo de entrega de informe: 30 días

Una auditoria para un sistema de información, busca determinar si este es robusto, confiable, seguro y realiza exclusivamente las operaciones y funciones para las cuales fue diseñado, garantizando la integridad en el procesamiento de toda información.

La auditoría está basada en las recomendaciones derivadas de los estándares internacionales en auditorias y transparencia de sistemas electrónicos en elecciones, analiza otras experiencias que pueden servir de referencia, presenta una propuestas de pruebas para la realización de auditorías de diferente profundidad para el software de escrutinio, plantea posibles escenarios y finalmente introduce una propuesta de auditoria de revisión intermedia para ser implementada en el ejercicio electoral de Primarias Simultaneas de los partidos Políticos en octubre 2019.

Se analizaron estándares construidos por organizaciones intergubernamentales, como el Consejo Europeo, la Organización para la Seguridad y la Cooperación en Europa (OSCE) y el programa de las Naciones Unidas para el Desarrollo (UNDP), además de estándares construidos por organizaciones sin ánimo de lucro a nivel internacional para incentivar sistemas que sean más participativos transparentes y seguros. Entre estas organizaciones están el instituto Internacional para la Democracia y Asistencia Electoral (IDEA), la Fundación Internacional para los Sistemas Electorales (IFES), y el Centro Carter 22.

Lista de estándares consultados:

- UNDP, Electoral Results Management Systems.
- Organización de los Estados Americanos, Tecnologías Aplicadas al Ciclo Electoral (OEA 2014)
- The Carter Center Handbook on Observing Electronic Voting.

Ave. 27 de Febrero, Esq. Gregorio Luperón
Santo Domingo, República Dominicana, Tél.: 809-539-5419
www.jce.gob.do

La Metodología de trabajo está basada en las recomendaciones los estándares antes descritos, que determinan las bases para las actividades propuestas, las cuales se listan a continuación:

Acceso a la información del sistema y código fuente.

- Conformidad con el marco legal regulatorio.
- Trazabilidad de cambios, correcciones, productos de software e implementación final.
  Integridad de la Información.
  Validación de la tercerización.
- Certificación y auditoria de un organismo independiente.

La auditoría para verificar el acceso a la información y la integridad del código fuente se realizará en una primera fase preparatoria, junto a la planificación de las actividades posteriores. El objetivo será verificar el software de la máquina de votación, a través de la observación y revisión de la aplicación, del código fuente y la firma electrónica de la aplicación.

Se buscará comprobar que no exista alteración alguna en la ejecución del software que pueda favorecer alguna respuesta en particular; demostrar la inviolabilidad del derecho al voto, mediante la certificación de que la máquina de votación no guarda ningún tipo de secuencia interna para determinar la trazabilidad entre voto con el votante.

La auditoría a la infraestructura tecnológica tiene como objetivo evaluar la seguridad del sistema de comunicaciones contra ataques e intrusiones externas y contra eventualidades, así como la seguridad del secreto del voto.

Actividades para verificar y auditar el acceso a la información del sistema y código fuente:

1. Verificar que todos los actores involucrados tengan acceso a la documentación completa de cotización, compra y funcionamiento interno del software electoral, incluyendo validar la disponibilidad y contenido de

Ave. 27 de Febrero, Esq. Gregorio Luperón
Santo Domingo, República Dominicana, Tél.: 809-539-5419
www.jce.gob.do

toda documentación generada durante las fases del ciclo de vida donde se realizaron las siguientes tareas:

a. Análisis de necesidades de la organización electoral y el proceso de voto automático.
b. Especificación de requisitos de productos (Funcionales y no funcionales).
c. Diseño del producto.
d. Arquitectura del sistema.
e. Transferencia a operaciones.

2. Validar que el código fuente cuenta con los mecanismos de acceso para que los actores como los partidos, entes de control y de observación electoral puedan revisar una copia del código fuente para auditoria. Se debe auditar que el código que puede ser potencialmente entregado a los actores interesados sea el mismo al utilizado en el proceso electoral. Se debe entregar el software en su ambiente entendido con el suficiente tiempo para garantizar un análisis exhaustivo previo a las elecciones. Es necesario que se incluyan protocolos de observación electoral tanto para las actividades manuales como para las electrónicas.
3. Verificar los Logs de acceso al software y a todos los productos de trabajo realizadas por parte tanto de los funcionarios de la JCE, de los fabricantes y de cualquier otro actor involucrado. Todas las minutas de resoluciones deben estar disponibles para revisión.

4. Verificar los Los del aplicativo, que debe ser capaz de identificar quien ingreso, cuando y que ingreso al sistema.

Actividades para verificar la integridad de la información y la seguridad del sistema:

1. Resguardo de la información por un tercero: Se validará la posibilidad de hacer una copia de replicación debidamente resguardada por un tercero imparcial con toda la información ingresada al sistema para que en caso de emergencia sea posible recuperar integralmente los datos que se han ingresado.

2. Validar la capacidad de cumplir con la recomendación de las organizaciones internacionales para crear un Trigger o un software capaz de identificar

Ave. 27 de Febrero, Esq. Gregorio Luperón
Santo Domingo, República Dominicana, Tél.: 809-539-5419
www.jce.gob.do

inconsistencias en los datos ingresados a través de los mecanismos para mantener datos para cotejar.

3. Analizar el flujo de la información para encontrar vulnerabilidades en los puntos en que se mueve los datos de un punto a otro.

4. Luego de analizar los puntos de contingencia y vulnerabilidades se revisarán los protocolos de seguridad definidos para mover la información por medios magnéticos que aseguren la confiabilidad e integridad de la información electoral.

Planificación de la Auditoria

Semana 1 -- Preparación / Análisis
- Análisis GAP de Seguridad.
- Análisis de procedimientos actuales.
- Análisis de Arquitectura y Procesos del Sistema.
- Análisis de Plan de Elección.
- Revisión de Hardware y redes a utilizar.
- Análisis de Acceso a datos.
- Sistema de Autenticación.
- Trazabilidad.
- Hoja de ruta y plan de implementación de mejoras.

- Semana 2 & 3 -- Ejecución de Pruebas
  - Hacking Ético a hardware, Software y componentes.
  - Revisión de documentación
  - Implementación de mejoras por parte del cliente.
  - Retest.

Semana 4 -- Certificación
- Auditoria completa final de sistemas.
- Certificación Final.

Ave. 27 de Febrero, Esq. Gregorio Luperón
Santo Domingo, República Dominicana, Tél.: 809-539-5419
www.jce.gob.do

2-v-La lista del personal propuesto, por especialidad, con indicación de las actividades que les serán asignadas y el tiempo que participarán en ellas. [CUMPLE]

- Ariel González -> Gerente del Proyecto
- Mateo Martínez --> Líder de Implementación. (120hs)
  - On boarding al proyecto.
  - Preparación y recopilación de material referencia.
  - Setup de equipos.
  - Plan Inicial de trabajo.
  - Kick-off.

Mauricio Campiglia--> Especialista en Seguridad Informática. (40 hs)

- Santiago Vázquez--> Especialista en Seguridad Informática. (40 hs)
- Alvaro Melo --> Especialista en Seguridad Informática. (40 hs)
  - Auditoria de Código para validar Logs y posibles puntos de hacking.
  - Hacking Ético a Hadware, Software y Componentes.
  - Auditoria de código y prácticas de Ciberseguridad.

Ethel Kornecki --> Especialista en Auditoria y Seguridad. (160hs)

- Análisis del contexto de información del proceso de compra y adjudicación.
- Verificación de versiones y acceso al código fuente.
- Análisis del proceso de validación y homologación con usuarios JCE.
- Auditoria sobre la garantía de integridad de la información, copias de seguridad, flujo de la información de votos y traslado de información digital.
- Elaboración de informe de recomendaciones y Plan de acción para la implementación de mejoras y correcciones necesarias para la certificación.
- Verificación y auditoria sobre las correcciones recomendadas.
- Análisis de mejoras realizadas
- Auditorias de procesos

Ave. 27 de Febrero, Esq. Gregorio Luperón
Santo Domingo, República Dominicana, Tél.: 809-539-5419
www.jce.gob.do

2-vi-Currículos recientes firmados por el personal profesional propuesto y por el representante autorizado que presenta la propuesta La información básica deberá incluir el número de años de trabajo en la firma y el nivel de responsabilidad asumida en las labores desempeñadas. [CUMPLE PARCIALMENTE]

Mauricio Campiglia

- Firmado: **Si**
- Numero de años en la firma: **No especifica**
- Nivel de Responsabilidad: **Especialista en Seguridad Informática**.
- Especialista de productos de seguridad de reconocidas marcas.
- Consultor y arquitecto de soluciones de seguridad informática multiplataforma.
- CISA, PCI-P
- Analista Forense
- Ethical Hacker & PenTester
- 18 años experiencia en Soluciones de Seguridad.

Mateo Martínez

- Firmado: **Si**
- Numero de años en la firma: **No especifica**
- Nivel de Responsabilidad: **Líder de Implementación**.
- CEH, CISSP
- ISO 27001, ISO 27032
- ITIL, OWASP
- Ethical Hacker
- Master en Seguridad Informática.
- Especializado en Centros de Respuesta.
- Seguridad en el Desarrollo de Software.
- 18 años experiencia en Seguridad de la Información, Consultor, Auditor, pentester.

Ave. 27 de Febrero, Esq. Gregorio Luperón
Santo Domingo, República Dominicana, Tél.: 809-539-5419
www.jce.gob.do

Ethel Kornecki

- Firmado: **Si**
- Numero de años en la firma: **No especifica**
- Nivel de Responsabilidad: **Especialista en Auditoria y Seguridad.**
- CISA, CISM, COBIT 4, CIA
- Analista programador.
- Auditoria Interna.
- 36 años experiencia como responsable del área de IT de empresas industriales.

Ave. 27 de Febrero, Esq. Gregorio Luperón
Santo Domingo, República Dominicana, Tél.: 809-539-5419
www.jce.gob.do

Nivel de Cumplimiento de los Oferentes

REQUERIMIENTOS TERMINOS DE REFERENCIA: JCE-CCC-PU-02-03-2019	GUZMAN TAPIA PKF	PONTEZUELA - BIDAGA - ALHAMBRA EIDOS
A. Documentación a Presentar		
1. Credenciales Profesionales que autentiquen su condición como Auditores Externos certificados.	CUMPLE	CUMPLE
2. Propuesta Técnica o descripción del servicio ofertado, la cual debe incluir lo siguiente:		
i. Una breve descripción de la firma auditora.	CUMPLE	CUMPLE
ii. Reseña de su experiencia en trabajos recientes de carácter similar, donde se incluyan certificaciones sobre el grado de satisfacción alcanzado por el cliente (contratante), la duración del trabajo y el monto del contrato.	CUMPLE	CUMPLE PARCIALMENTE
iii. Información sobre el nivel de especialización del personal que acompañará la firma.	CUMPLE	CUMPLE
iv. Una descripción de la metodología y el plan para ejecutar el trabajo.	CUMPLE	CUMPLE
v. La lista del personal propuesto, por especialidad, con indicación de las actividades que les serán asignadas y el tiempo que participarán en ellas.	CUMPLE PARCIALMENTE	CUMPLE
vi. Currículos recientes firmados por el personal profesional propuesto y por el representante autorizado que presenta la propuesta. La información básica deberá incluir el número de años de trabajo en la firma y el nivel de responsabilidad asumida en las labores desempeñadas.	CUMPLE PARCIALMENTE	CUMPLE PARCIALMENTE
B. Criterios de Evaluación		
1. Que el oferente demuestre que tiene capacidad y experiencia en el tipo de trabajo a realizar y en las condiciones establecidas para garantizar la calidad del servicio y su correspondencia con los requerimientos.	CUMPLE	CUMPLE

Ave. 27 de Febrero, Esq. Gregorio Luperón
Santo Domingo, República Dominicana, Tél.: 809-539-5419
www.jce.gob.do

Notas de Referencia de renglones con Cumplimiento Parcial:

GUZMAN TAPIA PKF

2-v. La lista del personal propuesto, por especialidad, con indicación de las actividades que les serán asignadas y el tiempo que participarán en ellas.

Se requiere que se detallen las actividades que les serán asignadas a los participantes en el proyecto, y este requerimiento no fue detallado en la propuesta.

2-vi. Currículos recientes firmados por el personal profesional propuesto y por el representante autorizado que presenta la propuesta. La información básica deberá incluir el número de años de trabajo en la firma y el nivel de responsabilidad asumida en las labores desempeñadas.

Se requiere que se especifique el número de años trabajando en la firma, y los señores Domingo Ormeño y Cesar Millavil no especificaron este requerimiento.

PONTEZUELA - BIDAGA - ALHAMBRA EIDOS

2-ii. Reseña de su experiencia en trabajos recientes de carácter similar, donde se incluyan certificaciones sobre el grado de satisfacción alcanzado por el cliente (contratante), la duración del trabajo y el monto del contrato.

Las cartas de referencia, certificando y expresando el grado de satisfacción alcanzado por el cliente, por desempeñar labores similares a la solicitada, no están certificando a ninguna de las compañías que conforman el consorcio, sino a la compañía Krav Maga Hacking, SRL con los señores Mateo Martínez y Mauricio Campiglia, como ejecutores de los trabajos, los cuales forman parte de la propuesta para este proyecto.

Ave. 27 de Febrero, Esq. Gregorio Luperón
Santo Domingo, República Dominicana, Tél.: 809-539-5419
www.jce.gob.do

En ese mismo sentido, pudimos evidenciar que algunas de las cartas de referencia no estaban confeccionadas con papel timbrado, ni con el sello de la compañía. pero si firmadas.

2-vi. Currículos recientes firmados por el personal profesional propuesto y por el representante autorizado que presenta la propuesta. La información básica deberá incluir el número de años de trabajo en la firma y el nivel de responsabilidad asumida en las labores desempeñadas.

Se requiere que se especifique el número de años trabajando en la firma, y los señores mauricio Campiglia, Mateo Martínez, Ethel Kornecki no especificaron el requerimiento.

A modo de conclusión

Al completar la evaluación de los documentos de las propuestas técnicas presentadas por los dos (2) oferentes, es oportuno reiterar que este informe es el resultado del análisis de los datos contenidos, exclusivamente, en los documentos presentados por los participantes en la licitación, en los cuales se establecen las acreditaciones, certificaciones y competencias de estos.

En el aspecto técnico general ambas propuestas cumplen, en vista de que el personal que participará en la misma cuenta con la experiencia, acreditaciones y certificaciones para realizar trabajos de esta naturaleza. Las observaciones de cumplimiento parciales de ambos oferentes no son tan relevantes y más bien son de carácter subsanables, y no afectan la ejecución del proyecto, dado que los datos omitidos no afectan la ejecución técnica del proyecto.

Ave. 27 de Febrero, Esq. Gregorio Luperón
Santo Domingo, República Dominicana, Tél.: 809-539-5419
www.jce.gob.do

Un aspecto muy importante para el éxito de la auditoria, es el factor tiempo, a la fecha: 10 de septiembre de 2019, quedan solamente 26 días para la celebración de las Elecciones Primarias de los Partidos Políticos, del 6 de octubre de 2019, y los dos oferentes en sus planes de trabajo, proponen un tiempo de entrega de informes finales de 25 y 30 días respectivamente para la conclusión de la auditoria, sin considerar cualquier imprevisto que se pueda presentar durante el desarrollo de la misma, es decir, que no habría margen para cualquier corrección o mejora que sea necesario realizar al sistema. Es muy importante destacar, que las actividades para la logística, preparación de equipos, clonado, personalización y distribución de los kit's de votación automatizada, requieren por lo menos 15 días de antelación a la fecha de las elecciones, por lo que vemos casi imposible el poder realizar la auditoria con esos márgenes de tiempo especificados sin impactar y poner en riesgo el proceso.

En vista de lo antes citado, somos de opinión salvo su mejor parecer, que vemos factible postergar la realización de la auditoria para las elecciones primarias y planificar la misma con miras al software de votación automatizada que será utilizado en los comicios electorales del año 2020, dado que luego de concluir las elecciones primarias, se contará con el tiempo suficiente para realizar una auditoría de calidad, acorde a las normas para auditorias de este tipo, desarrollando las actividades de los planes de trabajo, permitiendo realizar las correcciones o mejoras de lugar al software de votación Automatizada, garantizando la seguridad, no trazabilidad, confiabilidad y cumplimiento con los estándares para aplicativos de esta naturaleza .

Ave. 27 de Febrero, Esq. Gregorio Luperón
Santo Domingo, República Dominicana, Tél.: 809-539-5419
www.jce.gob.do

Por ello será oportuno acoger una propuesta en la que se incluya o incorpore profesionales de instituciones con reputada solvencia técnica, que en un tiempo breve puedan brindar una opinión que nos permita establecer que nuestro software cumple con los estándares requeridos y con las exigencias de los Partidos Políticos para las elecciones Primarias Simultáneas del 6 de octubre de 2019.

Agradeciendo su atención a la presente,

Muy atentamente,

Lic. Miguel Angel Garcia
Director de Informática

Lic. Mario Núñez Valdez
Director de Elecciones

Ave. 27 de Febrero, Esq. Gregorio Luperón
Santo Domingo, República Dominicana, Tél.: 809-539-5419
www.jce.gob.do