PROPUESTA TECNICA

CONSORCIO
PONTEZUELA – TMACHINE – ALHAMBRA EIDOS

Propuesta Técnica

AUDITORIA TÉCNICA AL SOFTWARE DE VOTACIÓN AUTOMATIZADA

CONSORCIO
PONTEZUELA – TMACHINE – ALHAMBRA EIDOS

Contenido

1. Introducción

El pliego de condiciones específicas para la contratación de una empresa para la realización de una auditoría técnica al software desarrollado por la Junta Central Electoral para el proyecto de voto automatizado a implementarse en las Primarias Simultáneas de los Partidos Políticos.

El presente documento tiene como finalidad principal proponer la realización de actividades de auditoría técnica que permitan la efectiva concreción de los objetivos descriptos y la construcción de confianza entre las partes interesadas por medio de una transparencia electoral verificada.

1.1 Objetivos del llamado

La propuesta de trabajo que se describe en este documento, atiende al cumplimiento de los siguientes objetivos:

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.
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.

El presente documento contiene la propuesta técnica para realizar estos requisitos o tareas.

2. Descripción de la firma auditora

2.1 Una breve descripción de la firma auditora

T.MACHINE es una empresa uruguaya dedicada exclusivamente a brindar servicios de control y aseguramiento de calidad de productos y procesos de software. Actualmente cuenta con un staff de 30 profesionales, de los cuales el 90% posee certificaciones internacionales en Testing de Software, Seguridad informática y modelos de mejora de procesos.

Respecto a nuestra oferta de servicios, se agrupan en dos categorías, de acuerdo a su principal objetivo:

- **Testing services**: Este servicio tiene su foco en la productividad y modelos operativos eficientes como factor esencial. El marco de trabajo tiene como objetivo el uso extensivo del conocimiento, herramientas y métricas que ayuden a mejorar el proceso productivo del testing y lograr una alta eficiencia operativa. Esta forma de concebir el trabajo se traduce en la posibilidad de mantener costos adecuados y recursos altamente calificados para atender el mercado nacional e internacional.

  Los roles de nuestros profesionales están definidos en base a los estándares internacionales del ISTQB® (International Software Testing Qualifications Board), y todos los profesionales son certificados en su especialización.

- 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 trabajo, implementar procesos de testing, realizar auditorías especializadas, o acceder a certificaciones internacionales de calidad. El concepto de "studio" busca enfatizar la idea de pocos consultores, con un alto nivel de seniority, y con un alto involucramiento en el proyecto de consultoría.

2.2 Acreditaciones y certificaciones

ISTQB International Software Testing Qualifications Board

2.2.1.1 ISTQB® – International Software Testing Qualifications Board

Desde el año 2012, nuestra empresa está acreditada como Training Provider de ISTQB®, y brinda cursos oficiales de las certificaciones de Foundation Level y Advanced Level. Los Training Providers son las únicas compañías autorizadas para dictar cursos para los exámenes ya que están homologadas para dictar los cursos de certificación.

ScrumAlliance Registered Education Provider

2.2.1.2 Scrum Alliance

TMachine es REP (Registered Education Provider) de Scrum Alliance, y brinda entrenamiento especializado para la implementación de testing en **proyectos** gestionados en modalidad Scrum. Todos los cursos ofrecidos por los **REPs son** verificados por Scrum Alliance, para asegurarse que es consistente con Scrum y con los principios ágiles.

2.2.1.3 Project Management Institute

TMachine es REP (Registered Education Provider) de PMI, y brinda entrenamiento especializado en la integración de los procesos de testing y calidad de software de acuerdo a las prácticas del PMBOK.

2.2.2 Distinciones

Desde abril de **2013**, TMACHINE trabaja aportando la experiencia en proyectos y entrenamiento en técnicas de pruebas a las comunidades de gestión de proyectos. Somos parte de la Scrum Alliance y del PMI (Project Management Institute) y Registered Education Provider de ambos.

En marzo de **2014**, TMACHINE alcanzó el grado de **Silver Partner** del **ISTQB®** (International Software Testing Qualifications Board), debido a la cantidad de certificaciones de su staff. MIW es la única empresa del Cono Sur en tener este nivel.

TMACHINE es miembro del Comité Hispanoamericano de ISTQB®, llamado **HASTQB (Hispanic America Sofware Testing Qualifications Board)**, y ha organizado a la fecha siete instancias de formación en el nivel "Foundations Level", que han certificado más de 30 profesionales de testing en Uruguay.

Asimismo, y debido a las mejoras que se introdujeron en el modelo para optimizar su aplicación al testing de software, en **noviembre de 2015** nos fue otorgado el **premio "Jorge Luis Bória" al mejor artículo del Simposio Brasilero de Ingeniería de Software (WAMPS)**.

En **diciembre de 2016 TMACHINE alcanzó el grado de Golden Partner del International Software Testing Qualifications Board**, debido a que es una de las tres únicas empresas en América Latina en cuyo staff permanente hay personal con certificaciones ISTQB® de Nivel avanzado y más del 80% de Testers Certificados por este organismo.

2.3 Certificado como Auditor

Las certificaciones son de los profesionales presentados.

2.4 Referencias

Ver Anexo de RECOMENDACIONES y CVs.

agesic
agencia de gobierno electrónico y sociedad de la información

2.4.1 AGESIC – Agencia para el Gobierno Electrónico y Sociedad de la Información - Uruguay

PRUEBAS DE PERFORMANCE SOBRE LA APLICACIÓN PARA EL RUTEO Y LA TRAZABILIDAD DE EXPEDIENTES ELECTRÓNICOS (ARTEE)

2.4.1.1 Características del proyecto de pruebas

Complejidad: Mediana / Alta

El proyecto involucraba objetivos de negocio clave para AGESIC.

Metodología: Testing de performance.

Testing técnico sobre webservices y de integración de con PGE utilizando emuladores

La aplicación para ruteo y trazabilidad de expedientes electrónicos implementa el ruteo de expedientes y trazas entre los diferentes organismos asociados a la plataforma. Por ejemplo, si un expediente de un organismo debe ser autorizado por el Tribunal de Cuentas, ese expediente y todas sus actuaciones, "viajan" a través de la plataforma siguiendo el protocolo de comunicación definido.

Las pruebas de performance sobre la plataforma de ARTEE fueron ejecutadas para evaluar su comportamiento en las condiciones de carga esperadas para el proyecto piloto con tres organismos en producción, y en situaciones de stress emuladas a partir de las proyecciones de crecimiento para los próximos cinco años.

La ejecución de estas pruebas permitió:

- Identificar "cuellos de botella" y sus causas principales.
- Optimizar y realizar el "tunning" de la configuración de la plataforma (hardware y software) para lograr una performance aceptable para la primera "ola" de implementación.
- Evaluar la confiabilidad de la aplicación en escenarios de picos de demanda.

agesic
agencia de gobierno electrónico y sociedad de la información

2.4.2 AGESIC – Agencia para el Gobierno Electrónico y Sociedad de la Información - Uruguay

PRUEBAS FUNCIONALES PARA PROYECTOS EN EL MARCO DE LA LICITACIÓN PARA LA IMPLEMENTACIÓN DE TRÁMITES DIGITALES

Año 2014 hasta la fecha

Complejidad: Mediana / Alta

El proyecto involucraba objetivos de negocio clave para AGESIC.

2.4.2.1 Proyectos involucrados

- Agenda Electrónica – Activos de Trámites – 2015
- Trazabilidad de Trámites – Activos de Trámites – 2015
- E-Notificaciones – 2014
- Evaluación de estado de situación de GRP (ACCE) – 2016
- Desarrollo de pautas para el testing de aplicaciones móviles de gobierno electrónico – (finalizado)
- Desarrollo de pautas de Control y Gestión de Calidad de soluciones de gobierno electrónico (en curso)

agesic
agencia de gobierno electrónico y sociedad de la información

2.4.3 AGESIC – Agencia para el Gobierno Electrónico y Sociedad de la Información - Uruguay

AUDITORÍA DE GESTIÓN DE LA CONFIGURACIÓN SOBRE EL SISTEMA DE EXPEDIENTES ELECTRÓNICOS DEL GOBIERNO

Año 2015 / 4 meses

Complejidad: Mediana / Alta

El proyecto involucraba objetivos de negocio clave para AGESIC.

Porte: Mediano

1 Test Manager, 1 Analista de Testing, 2 Tester Profesionales.
Aproximadamente 1.500 horas hombre.

Se creó un marco de trabajo para el control de la configuración de componentes de software y hardware donde actualmente están alojadas las soluciones de expediente electrónico. Este

marco de control tuvo como principal objetivo evaluar el impacto de los cambios, correcciones y mejoras sobre las soluciones en producción. También formó parte de los objetivos de este proyecto proponer a los proveedores de servicios de desarrollo y hosting de la solución de expediente electrónico, una metodología de trabajo controlada y definida que formalice los aspectos de control de la configuración.

Las definiciones, productos de trabajo y procesos que se generaron durante la ejecución de este servicio están alineadas a los siguientes estándares de referencia de la industria:

- CMMI for Development y CMMI for Services para las definiciones pertinentes al control de la configuración de las actividades inherentes al desarrollo y mantenimiento correctivo-evolutivo.
- ITIL para las definiciones pertinentes a las actividades de gestión de la configuración durante la gestión de cambios y la gestión de incidentes.
- COBIT para enmarcar la definición de los objetivos de control que se establezcan como parte de la evaluación de los procesos de trabajo.

agesic
agencia de gobierno electrónico y sociedad de la información

2.4.4 AGESIC – Agencia para el Gobierno Electrónico y Sociedad de la Información - Uruguay

AUDITORÍA SOBRE ESTADO DE SITUACIÓN DEL SISTEMA DE COMBRAS DEL ESTADO URUGUAYO

Año 2016 / 2 meses

Complejidad: Mediana

El proyecto involucraba objetivos de negocio clave para AGESIC.

El objetivo de este proyecto fue observar y analizar el grado de conformidad de la solución GRP, en el contexto del servicio de mantenimiento correctivo-evolutivo brindado por el proveedor. Esta actividad surge ante la necesidad de conocer el estado actual de la solución, debido a varios inconvenientes que los usuarios finales detectaron en el producto, algunos de los cuales datan desde la implementación original.

Debido a la importancia del sistema de compras en el presupuesto nacional, se realizaron varias actividades de análisis de actividades de usuarios, auditorías de seguridad e integridad de la información, y se definió un plan de acción basado en las recomendaciones elaboradas.

INEFOP

2.4.5 INEFOP – Instituto Nacional de Empleo y Formación - Uruguay

SERVICIOS DE SEGURIDAD Y HACKING ÉTICO

Año 2018 / 19

Consultores: Ing. Mateo Martínez / Mauricio Campiglia

- Consultoría de implementación ISO 27001
- Hacking Ético
- Implementación de Honeypots
- Business Impact Analysis (BIA)
- Implementación de metodología de gestión de riesgos
- Plan de concientización en seguridad de la información
- Plan de Continuidad de Negocio (BCP)
- Plan de Recuperación ante Desastres (DRP)
- Auditoria de Sistemas

2.4.6 VN Studio - Uruguay

SERVICIOS DE SEGURIDAD Y HACKING ÉTICO

Año 2014 a 2019

Consultores: Ing. Mateo Martínez / Mauricio Campiglia / Jorge Parra

- Hacking Ético
- Implementación de Honeypots
- Business Impact Analysis (BIA)
- Implementación de metodología de gestión de riesgos
- Auditoria de Sistemas

2.4.7 Security Advisor - Chile

SERVICIOS DE SEGURIDAD Y HACKING ÉTICO

Año 2017

Consultores: Ing. Mateo Martínez / Mauricio Campiglia

- Creación de CSIRT / Consultoría en Seguridad

2.4.8 Security Advisor / Transbank - Chile

SERVICIOS DE SEGURIDAD Y HACKING ÉTICO

Año 2017

Consultores: Ing. Mateo Martínez / Mauricio Campiglia

- Creación de CSIRT / Consultoría en Seguridad

2.4.9 Fondo Nacional de Garantías - Uruguay

SERVICIOS DE SEGURIDAD Y HACKING ÉTICO

Año 2017

Consultores: Ing. Mateo Martínez / Mauricio Campiglia

- Creación de CSIRT / Consultoría en Seguridad

2.4.10 AB InBev - Uruguay

SERVICIOS DE SEGURIDAD Y HACKING ÉTICO

Año 2017

Consultores: Ing. Mateo Martínez / Mauricio Campiglia

- Creación de CSIRT / Consultoría en Seguridad
- Plan Estratégico de Ciberseguridad

2.4.11 ONE S.A. - Paraguay

SERVICIOS DE SEGURIDAD Y HACKING ÉTICO

Año 2017

Consultores: Ing. Mateo Martínez / Mauricio Campiglia

- Creación de CSIRT / Consultoría en Seguridad
- Plan Estratégico de Ciberseguridad

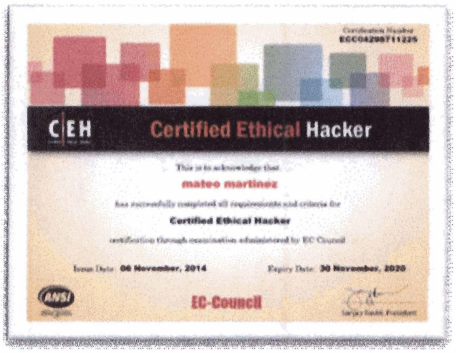
3. Información sobre el nivel de especialización del personal que acompañará la firma.

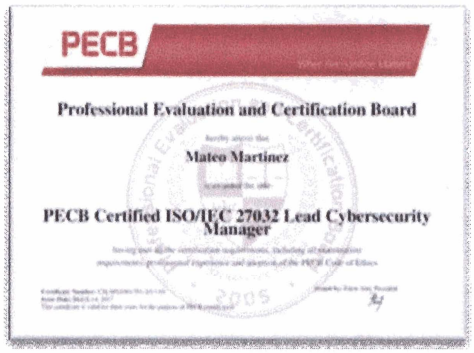
Los profesionales propuestos son Ingenieros en Informática, con certificaciones internacionales en seguridad informática y auditoria.

Asimismo, cuentan con experiencia probada en proyectos nacionales e internacionales con gobierno e instituciones privadas.

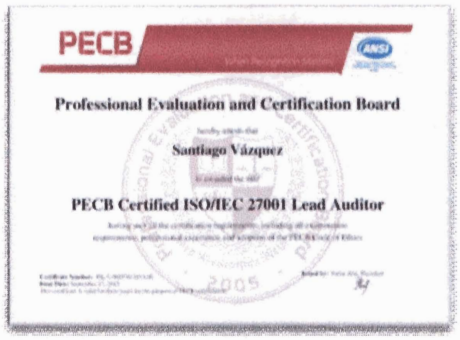
En el Anexo RECOMENDACIONES se encuentran las recomendaciones de algunos clientes.

Aquí un resumen de las certificaciones:






Information Systems Audit and Control Association
Ethel Kornecki
CISA
Certified Information Systems Auditor
GRANTED THIS DAY, 1 October 2001


PECB
Professional Evaluation and Certification Board
Santiago Vázquez
PECB Certified ISO/IEC 27001 Lead Auditor


PECB
Professional Evaluation and Certification Board
Santiago Vázquez
PECB Certified ISO/IEC 27001 Lead Implementer


PECB
Professional Evaluation and Certification Board
Santiago Vázquez
PECB Certified ISO 22301 Lead Auditor


CISM
Certified Information Security Manager
Sr. Alvaro Andres Melo
Certified Information Security Manager
ISACA

4. Metodología y plan de trabajo

Una auditoría para un sistema de información busca determinar si éste es robusto, confiable, seguro y realiza exclusivamente las operaciones y funciones para las cuales fue diseñado, de acuerdo al análisis y diseño, garantizando la integridad en el procesamiento de toda la información.

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

4.1 Referencias de estándares internacionales revisados para esta propuesta

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), y 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 Carter22.

Lista de estándares consultados:

- UNDP, Electoral Results Management Systems
- Organización de los Estados Americanos, Tecnologías Aplicadas Al Ciclo Electoral (OEA, 2014).
- The Carter Center. The Carter Center Handbook on Observing Electronic Voting. (Atlanta: The Carter Center, 2012)

4.2 Metodología

La metodología de trabajo está basada en las recomendaciones en común que tienen los estándares anteriormente descriptos, y tiene como fin último sugerir mejoras al sistema electoral y construir confianza en todas las partes interesadas, a partir de los resultados de la auditoría realizada.

Estos puntos de acuerdo que determinan las bases de las actividades propuestas, se listan a continuación:

- Acceso a la información del sistema y al código fuente;
- Conformidad con el marco legal regulatorio;
- Trazabilidad de cambios, correcciones, producto de software e implementación final;
- Integridad de la información;
- Validación de la tercerización;

- Certificación y auditoría 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 firme 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 el voto con el votante.

La Auditoría sobre 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 al voto.

4.2.1 PREPARACIÓN Y ANÁLISIS: Actividades para verificar y auditar el acceso a la información del sistema y al código fuente

Todos los estándares analizados comparten la necesidad de que los sistemas respondan a un principio de transparencia para con todos los actores interesados. Todos los ejercicios de transparencia tienen como objetivo garantizar los derechos de la ciudadanía tanto en la parte manual del proceso como en la digital para generar confianza en el sistema electoral.

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

Esto incluye validar la disponibilidad y contenido de toda la documentación generada durante las fases del ciclo de vida donde ser realizaron las siguientes tareas:

análisis de necesidades de la organización electoral y el proceso de voto automático,
especificación de requisitos de producto (funcionales y no funcionales),
diseño del producto,
arquitectura del sistema,
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 auditoría.

Se debe auditar que el código que puede ser potencialmente entregado a los actores interesados sea el mismo al utilizado durante el proceso electoral.

El plan de proyecto debe considerar el hito de la entrega del software en su ambiente entendido de uso con el tiempo suficiente para garantizar un análisis exhaustivo previo a las elecciones.

Es recomendable que en el plan de proyecto de voto automático se incluyan protocolos de observación electoral tanto para las actividades manuales como para las electrónicas.

Sobre el proceso de desarrollo

Los estándares resaltan que en el proceso de desarrollo no debería haber cambios al sistema a menos que sean aceptados por los actores, se haga la correspondiente auditoría y se actualice el sistema en todos los dispositivos. Durante la auditoría se verificará la aplicación de estos procedimientos y su registro adecuado.

Cada vez que se arreglen errores, el fabricante debe ofrecer pruebas de corrección del sistema, que serán objeto de revisión de la auditoría.

Se deben verificar lo 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 deberán estar disponibles para su revisión.

Finalmente, verificarán y auditarán los logs del aplicativo, que debe ser capaz de identificar quién ingresó, cuándo lo hizo y qué ingresó al sistema.

4.2.2 EJECUCIÓN DE PRUEBAS - Actividades para verificar la integridad de la información y la seguridad del sistema

Las actividades de esta fase buscarán validar que el proceso de construcción y mantenimiento del sistema posean procedimientos apropiados para mantener la integridad de la información en casos de emergencia o posibles intentos de fraude. Igualmente, en este punto se pueden identificar cuatro buenas prácticas internacionales que serán las bases del proceso de auditoría:

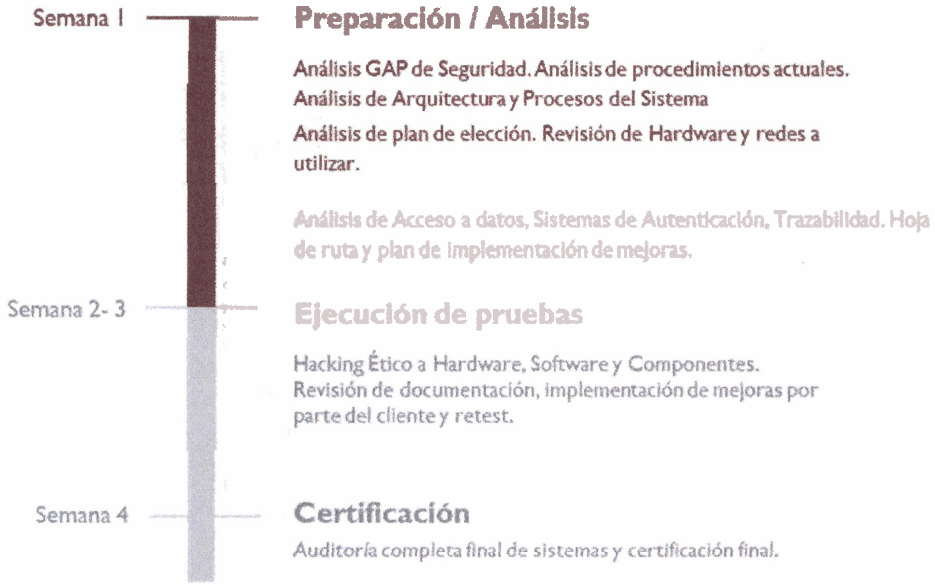
1 – Resguardo de la información por un tercero: Se validará la posibilidad de hacer una copia de replicación debidamente resguardada por un tercero imparcial con toda la información ingresada en el sistema para que, en caso de emergencia, sea posible recuperar integralmente los datos que se han ingresado.

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

4.2.3 Planificación de la Auditoría



4.2.3.1 Dedicación de recursos

4.2.3.1.1 Alhambra

La estimación de recursos y su dedicación por parte de Alhambra es la siguiente:

ROL	TAREAS	ESTIMACIÓN DE ESFUERZO
Auditor Senior – Líder de implementación / Project Manager	Onboarding al proyecto. Setup de equipos. Plan inicial de trabajo. Kick-off. Elaboración del informe de recomendaciones y Plan de acción para la implementación de mejoras y correcciones necesarias para la certificación. Análisis de mejoras realizadas. Auditoría de procesos.	120 hs
Especialista en Seguridad Informática	Preparación y recopilación de material de referencia. Verificación y auditoría sobre las correcciones recomendadas.	40 hs
Auditor Senior certificado ISACA	Auditoría de código para validar logs y posibles puntos de hacking. Auditoría sobre procesos de identificación de máquinas y funcionarios, y capacidades del sistema y los procesos definidos para control de versiones y la implementación de "double blid	160 hs

	entry". Auditoría sobre la garantía de integridad de la información, copias de seguridad, flujo de la información de votos y traslado de información digital. Certificación y presentación final.	

4.2.3.1.2 Gobierno

La dedicación por parte del cliente es la siguiente:

ROL	TAREAS
Líder de proyecto	Onboarding al proyecto. Setup de equipos. Plan inicial de trabajo. Kick-off.
JCE	Recopilación y presentación de material de referencia. Presentación del contexto de información del proceso de compra y adjudicación. Presentación de versiones y formas de acceso al código fuente. Análisis del proceso de validación y homologación con usuarios de JCE. Presentación de la de conformidad con marco legal regulatorio.
Equipo de desarrollo / Arquitectos / Especialistas en seguridad / Líder de proyecto	Disponibilidad para los hallazgos de la auditoría de código para validar logs y posibles puntos de hacking. Hacking Ético a Hardware, Software y Componentes. Disponibilidad para la auditoría sobre procesos de identificación de máquinas y funcionarios, y capacidades del sistema y los procesos definidos para control de versiones y la implementación de "double blid entry". Disponibilidad para la auditoría sobre la garantía de integridad de la información, copias de seguridad, flujo de la información de votos y traslado de información digital.
Especialista en Seguridad Informática / Arquitecto / Equipo de desarrollo	Disponibilidad para corregir los hallazgos de las actividades de Hacking ético sobre el software, auditoría de código y prácticas de ciberseguridad. Disponibilidad para corregir los hallazgos de las actividades de auditorías de código para validar buenas prácticas de seguridad.
Todo el equipo	Participación en la presentación del informe de recomendaciones y Plan de acción para la implementación de mejoras y correcciones necesarias para la certificación.
Todo el equipo	Verificación y auditoría sobre las correcciones recomendadas. Análisis de mejoras realizadas. Auditoría de procesos.
Todo el equipo	Certificación y presentación final.

5. Personal propuesto

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

NOMBRE	ROL	ACTIVIDADES
MATEO MARTÍNEZ	LÍDER DE IMPLEMENTACIÓN	Onboarding al proyecto. Preparación y recopilación de material de referencia. Setup de equipos. Plan inicial de trabajo. Kick-off. Elaboración del informe de recomendaciones y Plan de acción para la implementación de mejoras y correcciones necesarias para la certificación. Seguimiento y control. Verificación y auditoría sobre las correcciones recomendadas. Análisis de mejoras realizadas. Auditoría de procesos. Certificación.
MAURICIO CAMPLIGLIA SANTIAGO VÁZQUEZ ÁLVARO MELO	ESPECIALISTA EN SEGURIDAD INFORMÁTICA	Auditoría de código para validar logs y posibles puntos de hacking. Hacking Ético a Hardware, Software y Componentes. Actividades de Hacking ético sobre el software, auditoría de código y prácticas de ciberseguridad
ETHEL KORNECKI	ESPECIALISTA EN AUDITORÍA Y SEGURIDAD	(4.2.1) 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 de JCE. Auditoría sobre la garantía de integridad de la información, copias de seguridad, flujo de la información de votos y traslado de información digital. Elaboración del informe de recomendaciones y Plan de acción para la implementación de mejoras y correcciones necesarias para la certificación. Verificación y auditoría sobre las correcciones recomendadas. Análisis de mejoras realizadas. Auditoría de procesos.

5.1 CV

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.