SERVICIO DE AUDITORÍA ESPECIALIZADA PARA LA SOLUCIÓN TECNOLÓGICA DEL VOTO DIGITAL- EG 2026.

1. ÁREA SOLICITANTE

Gerencia de Informática y Tecnología Electoral (GITE).

2. ANTECEDENTES

- Resolución Jefatural N° 000051-2025-JN/ONPE (07ABR2025), que aprueba el "Plan Operativo Electoral – Elección del Presidente de la República, Vicepresidentes, Senadores y Diputados del Congreso de la República y Representantes Peruanos ante el Parlamento Andino 2026, Versión 00".
- Objetivo Estratégico Institucional OEI 1. Fortalecer la organización de procesos electorales transparentes y eficientes para la obtención de la fiel y libre expresión de la voluntad ciudadana.
- Actividad del Programa 5005023. Resultados electorales procesados, computados y gestionados.

3. DESCRIPCIÓN GENERAL DEL REQUERIMIENTO

Contratar a una persona natural o jurídica que brinde el SERVICIO DE AUDITORÍA ESPECIALIZADA PARA LA SOLUCIÓN TECNOLÓGICA DEL VOTO DIGITAL - EG 2026. Esta auditoría informática especializada se llevará a cabo sobre la Solución Tecnológica del Voto Digital que será utilizada en las Elecciones Generales 2026, conforme a lo solicitado por la Gerencia de Informática y Tecnología Electoral (GITE) de la ONPE.

4. FINALIDAD PÚBLICA

El presente servicio de auditoría técnica y de seguridad electoral es requerido como parte de la actividad 5005023. Resultados electorales procesados, computados y gestionados, del OEI 1. Fortalecer la organización de procesos electorales transparentes y eficientes para la obtención de la fiel y libre expresión de la voluntad ciudadana, con la finalidad de contribuir a que la Solución Tecnológica del Voto Digital esté alineada dentro del marco legal vigente y en cumplimiento de la Ley Nº 32270 y su Reglamento, normativa que establece la obligatoriedad de auditar dicha solución antes y después de cada proceso electoral, así como los principios y estándares técnicos de seguridad, integridad y procesamiento de la información. De esta manera, se busca preservar la confiabilidad, la integridad y la seguridad de los sistemas informáticos electorales y de los resultados que se generen, cumpliendo así la transparencia en los resultados de las Elecciones Generales 2026.

5. OBJETIVOS DE LA CONTRATACIÓN

Objetivo General:

La Oficina Nacional de Procesos Electorales (ONPE), a solicitud de la Gerencia de Informática y Tecnología Electoral (GITE), requiere contratar un servicio especializado de auditoría para la Solución Tecnológica del Voto Digital, a fin de evaluar su funcionamiento para las Elecciones Generales 2026. El objetivo de esta auditoria es verificar el ciclo de desarrollo definido por la entidad, la arquitectura tecnológica utilizada, la funcionalidad, la seguridad, los flujos de información, el código fuente y la documentación asociada, para determinar la conformidad de la Solución Tecnológica del Voto Digital, con la normativa legal vigente, aplicando las mejores prácticas y estándares tecnológicos.

6. FUENTE DE FINANCIAMIENTO

Recursos Ordinarios RO

7. DESCRIPCION DEL SERVICIO

ITEM	Cantidad	Unidad de Medida	Descripción del Servicio
01	01	Servicio	SERVICIO DE AUDITORÍA ESPECIALIZADA PARA LA SOLUCIÓN TECNOLÓGICA DEL VOTO DIGITAL- EG 2026

7.A. ALCANCE DEL SERVICIO

El servicio tiene como alcance realizar una auditoría técnica y de seguridad electoral a la SOLUCIÓN TECNOLÓGICA DEL VOTO DIGITAL (STVD), conforme a lo dispuesto en la Ley Nº 32270 y su Reglamento, así como dentro del marco legal vigente y aplicando las mejores prácticas y estándares tecnológicos.

La auditoría comprenderá el ciclo de desarrollo definido por la entidad y los componentes propios de la solución tecnológica de voto digital. Las características del STVD se encuentran descritas en el **ANEXO A** del presente documento.

7.B. FASES DE LAS AUDITORÍA

7.B.1. PLANIFICACIÓN DE LA AUDITORÍA

Elaborar el plan y cronograma de auditoría, que debe incluir las actividades a realizar, los responsables, la duración, las fechas e hitos de cada actividad planificada, así como reuniones de coordinación periódicas. El plan debe detallar en que consiste cada actividad a desarrollar.

El plan y cronograma de auditoría debe incluir, entre sus actividades e hitos, dos reportes preliminares de avance documentado, que contenga evidencias concretas. Estos reportes deben detallar los hallazgos (si corresponden), su criticidad, impacto y cualquier otra información relevante que facilite su análisis. Además, el Reporte 1 debe estar disponible a los sesenta y nueve (69) días calendario contados a partir del día siguiente de la firma del acta de inicio del servicio y el Reporte 2 a los ciento cuarenta y cuatro (144) días calendario contados a partir del día siguiente de la firma del acta de inicio del servicio, previa notificación de la orden de servicio y/o la firma del contrato (ver línea de tiempo de la auditoria).

El plan de auditoria debe contener como mínimo las siguientes actividades (cronograma de auditoria):

7.B.1.1. EVALUACIÓN DE FUNCIONALIDADES

a) Analizar el ciclo de desarrollo de software, establecido por la entidad, para determinar su alineamiento a las buenas prácticas reconocidas internacionalmente y relacionadas con los métodos utilizados.
b) Analizar y evaluar el desempeño y tiempo de respuesta respecto a las etapas de instalación, sufragio y escrutinio de la STVD y determinar si existen procesos que ralentizan su funcionamiento, indicar las causas.
c) Evaluar la recopilación, distribución y utilización de datos y de los resultados.
d) Validar que la información mostrada en los reportes de los diversos módulos, sea congruente a lo procesado y almacenado en la base de datos.
e) Verificar la integridad y consistencia de los datos durante las etapas de instalación, sufragio y escrutinio de la STVD.
f) Validar la confidencialidad de la información durante las etapas de instalación, sufragio y escrutinio de la STVD.
g) Verificar que los datos se interpretan, registren y retroalimenten correctamente.
h) Revisar los controles de estándares aplicables a la STVD, así como los métodos, guía y normas internacionales de seguridad, tales como los estándares ISO/IEC 27001 (Anexo A de dicha norma), ISO/IEC 27002, ISO/TS 54001:2019, OWASP, NIST Cybersecurity

Framework. Además, utilizar los marcos de referencia y metodologías ISSAF, Seguridad SANS y CAPEC.

7.B.1.2 ANÁLISIS DE AMENAZAS Y VULNERABILIDADES (SEGURIDAD)

a) Determinar si existen posibles defectos o deficiencias en la Solución Tecnológica del Voto Digital.
b) Ejecutar el análisis de vulnerabilidades.
c) Realizar el análisis de penetración para la parte web de la solución, evaluadas de acuerdo con la Guía de Evaluación de OWASP, entre otras, ver listado de pruebas de seguridad que forman parte del **ANEXO C**.
d) Realizar el diagnóstico respecto a la penetración de aplicaciones de la parte de escritorio de la solución, las mismas que deberán ser evaluadas de acuerdo con el OWASP Desktop App Security en su última versión, entre otras; Ver listado de pruebas de seguridad que forma parte de **ANEXO C**.
e) Evaluar la integridad, disponibilidad, confidencialidad del ambiente de la infraestructura tecnológica y de la información.
f) Realizar pruebas de caja blanca y caja negra, para identificar vulnerabilidades en la lógica de la STVD.
g) Realizar la explotación de vulnerabilidades a fin de Identificar los riesgos, que contenga como mínimo la siguiente Información:
   - Descripción de la Actividad.
   - Amenaza.
   - Vulnerabilidad.
   - Descripción del Riesgo.
   - Probabilidad de Ocurrencia.
   - Impacto.
   - Nivel de riesgo.
   - Actividades, configuración o actualizaciones que lo mitigan.
h) Evaluar la infraestructura tecnológica que soporta la Solución Tecnológica del Voto Digital en búsqueda de vulnerabilidades que afecten la seguridad de la información.

7.B.1.3. EVALUACIÓN DEL CÓDIGO FUENTE Y DOCUMENTACIÓN

a) Analizar desde una perspectiva de desarrollador la consistencia y legibilidad del código fuente, con el fin de evaluar su calidad, mantenibilidad e identificar posibles áreas de mejora.
b) Verificar si tiene puntos vulnerables o funciones que pudieran ser aprovechadas para efectuar ataques.

c) Evaluar la arquitectura del software, para identificar posibles áreas de mejora incluyendo la modularidad planteada, los componentes y su reutilización.
d) Realizar la revisión del código fuente de la STVE mediante una herramienta de análisis estático de código fuente, que permita lo siguiente:
   - Determinar la condición general del proyecto analizado: Apto o con Fallas.
   - Mostrar un resumen de los bugs encontrados en el código fuente del voto digital, agrupado por lenguaje de programación.
   - Mostrar la cantidad de errores de código(bugs), debe mostrar el hallazgo en forma detallada y, en resumen. Además, debe de indicar la severidad: Bloqueante, Crítico, Mayor, Menor o Informativo.
   - Mostrar la cantidad de código sucio (malas prácticas que dificultan que el código pueda mantenerse), debe mostrar el hallazgo en forma detallada y, en resumen. Además, debe de indicar la severidad: Bloqueante, Crítico, Mayor, Menor o Informativo.
   - Detallar las vulnerabilidades en puntos de acceso de seguridad (Security Hotspots).
   - Mostrar la cantidad de vulnerabilidades (errores que afectan la seguridad) en el código fuente, de existir algún hallazgo se debe mostrar en forma detallada y, en resumen. Además, debe de indicar la severidad: Bloqueante, Crítico, Mayor, Menor o Informativo.
   - Mostrar el porcentaje de cobertura del análisis al código fuente del voto digital.
   - Mostrar la cantidad de código duplicado y bloques de código duplicado, debe mostrar el hallazgo en forma detallada y en porcentaje.
   - Analizar la complejidad del código fuente.
   - Mostrar el porcentaje de código comentado en el código fuente del voto digital.
   - Indicar métrica de deuda técnica, de acuerdo con los errores encontrados.
e) Para la revisión de la documentación se debe considerar como mínimo lo siguiente:
   - Especificaciones de Requisitos de Software (ERS)
   - Reglas de Negocio (RN)
   - Manual de Usuario (MU)
   - Manual Técnico (MT)

7.B.2. EJECUCIÓN DE LA AUDITORIA

Considerando que el periodo de la auditoría abarca 219 días calendario, su ejecución técnica se llevará a cabo en cinco etapas:

7.B.2.1. ETAPA 1 - PRIMERA PARTE DE EJECUCIÓN TÉCNICA DE AUDITORIA

Se deben desarrollar las actividades contempladas en el plan de auditoría y cronograma de auditoría. Esta primera parte de la ejecución técnica de la auditoría se centra en la evaluación integral de la STVD, y para ello se deberán de considerar las siguientes disposiciones:

Para la ejecución de las actividades, el contratista deberá contar con los recursos tecnológicos, como: software, hardware debidamente licenciados para la realización del servicio, así mismo, contar con las herramientas o recursos para el desenvolvimiento de las tareas que ejecutará su personal clave en la prestación del servicio, como, por ejemplo, equipos laptop, acceso a servicio de Internet, herramientas (extensiones eléctricas, cables de interconexión, equipamiento externo, software de vulnerabilidades, software de análisis de configuraciones, equipos de mediciones de redes, entre otros necesarios para la adecuada prestación del servicio). Los recursos pueden ser licenciados y de software libre debidamente demostrado.

7.B.2.2. ETAPA 2 - LEVANTAMIENTO Y REVALIDACIÓN DE OBSERVACIONES

Realizar las actividades contempladas en el plan de auditoría y cronograma de auditoría. La Etapa 2 de levantamiento y revalidación de observaciones, se desarrolla a partir de la primera parte de ejecución técnica de auditoría (Etapa 1). Para ello se deberán de considerar las siguientes disposiciones mínimas:

- Reporte preliminar 1 de avance, correspondiente a la Etapa 1, tal como lo indique el Plan y cronograma de auditoría.
- De existir hallazgos, explicar el contexto y las implicaciones de cada uno de ellos, permitiendo las aclaraciones o información adicional por parte del auditado.
- Revalidar los hallazgos, verificando la efectividad de las acciones implementadas, recopilando nuevas evidencias que demuestren la corrección completa de lo observado, para ello, el auditado alcanzara las evidencias para el levantamiento de las observaciones, así como la definición de las acciones correctivas, responsables y establecer plazos adecuados para la implementación de las acciones.
- Realizar el seguimiento de las acciones correctivas, monitoreando el progreso de las acciones acordadas, proporcionar la orientación debida si surgen obstáculos y documentar los avances y cambios realizados.

7.B.2.3. ETAPA 3 - SEGUNDA PARTE DE EJECUCIÓN TECNICA DE AUDITORIA

Se deben desarrollar las actividades contempladas en el plan de auditoría y cronograma de auditoría. Esta segunda parte de la ejecución técnica de la auditoría se centra en la validación final del estado de la STVD previo a su despliegue en las Elecciones Generales 2026, para ello se deberán de considerar las mismas disposiciones indicadas en el numeral 7.B.2.1 - ETAPA 1.

7.B.2.4. ETAPA 4 - LEVANTAMIENTO Y REVALIDACIÓN DE OBSERVACIONES

Realizar las actividades contempladas en el plan de auditoría y cronograma de auditoría. La Etapa 4 de levantamiento y revalidación de observaciones, se desarrolla a partir de la segunda

parte de ejecución técnica de auditoría (Etapa 3) correspondiente a la validación final de la STVD. Para ello se deberán de considerar las siguientes disposiciones mínimas:

- Reporte preliminar 2 de avance, correspondiente a la Etapa 3, tal como lo indique el Plan y cronograma de auditoría.
- Las demás disposiciones indicadas en el numeral 7.B.2.2 Etapa 2.

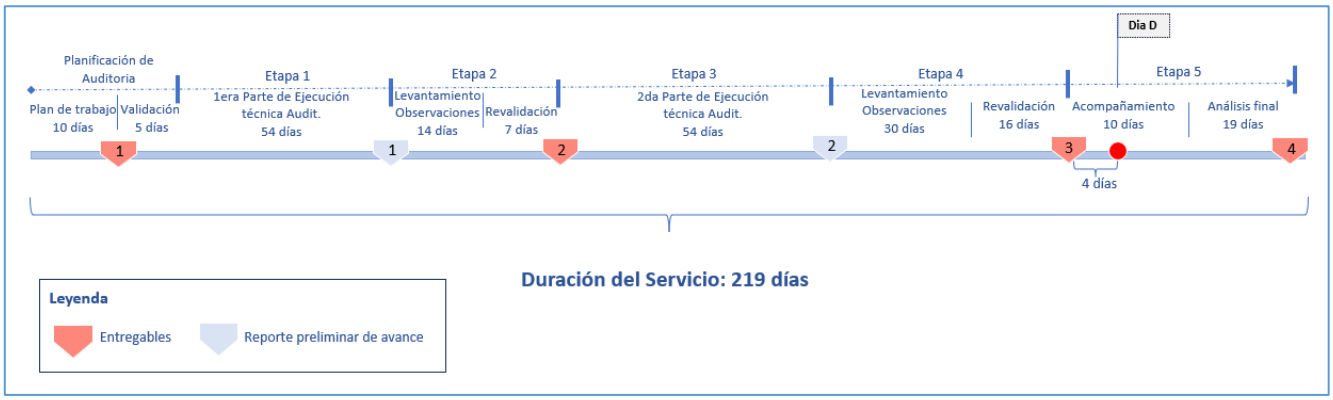
7.B.2.5. ETAPA 5 - ACOMPAÑAMIENTO Y ANÁLISIS FINAL

Realizar las actividades contempladas en el plan de auditoría y cronograma de auditoría, estimándose para esta etapa se contemple lo siguientes:

- Contar con los recursos necesarios, incluyendo los tecnológicos, que le permitan desarrollar las actividades acompañamiento complementario durante la ejecución del proceso electoral,
- Es importante que se gestione o coordine los permisos necesarios, con la debida anticipación, de preferencia 7 días calendarios antes de la actividad.

7.C. LINEA DE TIEMPO DE LA AUDITORIA

En el siguiente grafico se detalla cada una de las partes para la ejecución del Servicio de Auditoria Informática para la STVD:



Asimismo, el contratista del Servicio se encuentra obligado a tener en cuenta, la normativa descrita en el **ANEXO D**, sin perjuicio de otra normativa de alcance general o institucional que sea aplicable para la ejecución del presente servicio.

PLAN DE TRABAJO

a) **Planificación**

El contratista deberá elaborar un plan de trabajo en cumplimiento del servicio donde establecerá, de manera clara, los tiempos de ejecución de cada una de las fases, la metodología y los entregables asociados al análisis a realizar, así como el mecanismo de comunicación e intercambio de información entre el Contratista y la ONPE, y el esquema que se utilizará para dar seguimiento a los recursos materiales y técnicos necesarios para llevar a cabo este servicio.

El plan de trabajo del servicio debe ser entregado a la entidad dentro de los diez (10) días calendario, contabilizados a partir del día siguiente de la firma del acta de inicio, previa notificación de la orden de servicio y/o firma de contrato; este documento será validado por la ONPE en un máximo de cinco (5) días a partir de su recepción a efecto de que considere los aspectos que a continuación se detallan y de no existir observaciones será aceptada con acta correspondiente firmada por ambas partes.

- Objetivo y actividades para la ejecución del servicio, incluyendo su calendarización, responsables, los entregables, revisiones adicionales, entre otros.
- Alcance conforme a lo solicitado por la ONPE, indicando los detalles que se deberán contemplar para la ejecución del presente servicio.
- Identificación del equipo de trabajo y recursos necesarios para el desarrollo del servicio, así como los canales de comunicación con la ONPE.
- Diseño y las pruebas que llevará a cabo, de acuerdo con los procesos y componentes de la Solución Tecnológica del Voto Digital que serán revisados, así como el análisis de los resultados derivados de las pruebas.
- Procedimientos para la revisión de la solución tecnológica del voto digital, así como los recursos y requerimientos, considerando al menos las fases de análisis, planeación, ejecución y finalización del servicio (debe incluir el flujo y procedimiento de remediación).
- Riesgos del proyecto (debe incluir la matriz de riesgos).

b) **Ejecución**

La ejecución del servicio se llevará a cabo de acuerdo con lo establecido en el Plan de Trabajo del Servicio y a las líneas de acción descritas en el numeral 7, considerando buenas prácticas y/o estándares en tecnología.

El contratista debe emitir los entregables según lo descrito en el numeral 14 Entregables.

El horario de disponibilidad para el desarrollo del servicio, por parte del Contratista deberá ser de lunes a viernes de 8:30 am a 5:00 pm, salvo. que por motivos del servicio mismo se requiera trabajar fuera de ese horario, lo que deberá ser coordinado con la Entidad en sesiones programadas.

c) **Gestión del cambio**

- El equipo de trabajo de la ONPE, por motivos internos o externos a la ejecución del servicio, coordinará con el Contratista cualquier cambio a producirse dentro del plan de trabajo del servicio presentado y aprobado por el proveedor.
- De considerarse fundamentada la necesidad del cambio de actividad y/o entrega especificada en el plan de trabajo del servicio, se registrará en un acta el detalle del cambio a ser realizado, el motivo por el cual se realiza el cambio y los acuerdos tomados conjuntamente con el proveedor, esta acta será firmada conjuntamente, por los responsables de los equipos de trabajo conformados para el servicio del proveedor y de la ONPE.
- Los cambios que sean considerados necesarios y se realicen durante el servicio no generaran o irrogaran costo adicional a ser asumido por la ONPE.

d) **Finalización del servicio**

Para la finalización del servicio deben emitir los entregables del servicio, descritos en el numeral 14 Entregables.

8. MODALIDAD DE PAGO

El presente procedimiento se rige por la modalidad de pago a suma alzada.

9. REQUISITOS QUE DEBERÁ CUMPLIR EL POSTOR

El servicio deberá ser prestado por una persona natural o jurídica, el cual debe cumplir con lo siguiente:

A. Personal mínimo requerido

- Auditor líder

  El Contratista debe garantizar como mínimo a Un (01) auditor líder, con la responsabilidad de coordinar las actividades del servicio entre el personal de la ONPE y personal del contratista asignado al servicio.

- Auditores Especialistas

  El Contratista debe garantizar como mínimo a tres (03) auditores especialistas, quienes realizarán las evaluaciones y el asesoramiento requeridos en el servicio.

- Experto en Ciberseguridad

  El Contratista debe garantizar como mínimo a un (01) Experto en Ciberseguridad, quien verificará la robustez de los mecanismos de cifrado, autenticación y confidencialidad de los componentes de todo el sistema electoral.

El detalle de los perfiles y experiencias se encuentran en el numeral, *"REQUISITOS DE CALIFICACIÓN"*

B. Antecedentes Electorales del personal propuesto del Postor

El personal propuesto para brindar el servicio en todo el periodo solicitado deberá cumplir con lo siguiente:

- Que el personal requerido no debe pertenecer o haber pertenecido en los últimos cuatro (4) años, a una organización política.
- Que el personal requerido no desempeña cargos directivos, con carácter nacional, en las organizaciones políticas, ni haberlos desempeñado en los últimos cuatro (4) años anteriores a la postulación;
- Que el personal requerido no ha sido candidato a cargos de elección popular, en los últimos cuatro (4) años.
- El personal requerido no debe tener algún tipo de relación laboral, ni contractual con la ONPE o con alguna institución de la administración pública, que pueda derivar en un conflicto de intereses.

10. REQUISITOS QUE DEBERÁ CUMPLIR LA ENTIDAD

- Disponer un documento (Compromiso de no divulgación) que contenga cláusulas de confidencialidad de toda información entregada al contratista y generada en el marco del servicio.
- Todas las actividades que sean realizadas durante la ejecución del servicio, serán efectuadas de manera presencial o no presencial, suscribiéndose los acuerdos de confidencialidad correspondientes y en caso de requerir se estará habilitándose un ambiente en el local principal Jr. Washington 1894, Cercado de Lima, en el horario de lunes a viernes de 8:30 am a 5:00 pm, donde se tendrá habilitado, por el tiempo que dure el servicio, la infraestructura

tecnológica donde se va a simular todo el proceso electoral, con los resguardos de seguridad de información y equipamiento tecnológico que puedan ser considerados en el **ANEXO B** del presente documento. Como parte de la transferencia de información al contratista, se brindará la siguiente información: especificaciones de requerimientos, diagramas, diseños, manuales de usuario y sistema, políticas, procedimientos, etc.; también la ONPE dispondrá de sesiones programadas de acuerdo la necesidad del servicio, con los especialistas designados para absolver consultas sobre la Solución Tecnológica del Voto Digital, las cuales serán llevada a cabo según la necesidad para la ejecución del servicio.

- La ONPE proporcionará los siguientes recursos o facilidades para la ejecución del servicio:

A. Equipo de trabajo

La ONPE formará un equipo de trabajo que actúe como contraparte del contratista a efectos de coordinar la prestación del servicio, entregar documentación pertinente y absolver consultas; estas se harán a través de sesiones programadas de acuerdo a la necesidad del servicio, este equipo estará disponible cuando el contratista lo requiera.

B. Documentación

Los siguientes documentos serán entregados al Contratista luego de la presentación del plan de trabajo del servicio.

- Especificaciones de requerimientos funcionales y no funcionales del STVD.
- Reglas de Negocio del STVD.
- Manuales de usuario, Manuales Técnicos y Manuales de Instalación (según sea el caso).

Toda la documentación necesaria para el cumplimiento del servicio será proporcionada al contratista por parte de la ONPE, según corresponda por parte del equipo de trabajo formado para la interacción de la ONPE con el Contratista, en sesiones programadas.

11. OBLIGACIONES DEL CONTRATISTA

- El contratista es el único responsable ante la ONPE de cumplir con la contratación, no pudiendo transferir esa responsabilidad a otras entidades ni terceros en general.
- El representante legal del contratista debe suscribir y entregar a la firma del acta de inicio del servicio el 'Compromiso de no divulgación' provisto por ONPE, en dicho documento el contratista asume la responsabilidad en el caso de filtración de información.

12. PLAZO DE EJECUCIÓN DEL SERVICIO

El plazo de ejecución es de doscientos diecinueve (219) días calendario, el mismo que se computa a partir del día siguiente de la firma del acta de inicio del servicio, previa notificación de la orden de servicio y/o la firma del contrato.

13. LUGAR DE LA PRESTACIÓN DEL SERVICIO

El servicio se llevará a cabo bajo la modalidad mixta (presencial y no presencial), conforme al detalle siguiente:

- Presencial: Las actividades se desarrollarán en las instalaciones de la sede central de la ONPE, sita en Jirón Washington N° 1894, Cercado de Lima, en el horario comprendido entre las 08:30 a.m. y las 5:00 p.m.
- No presencial: Las actividades se efectuarán de manera remota, utilizando mecanismos seguros que garanticen la confidencialidad y la integridad de la información.

Estas actividades pueden ser realizadas de manera presencial o no presencial a excepción de las realizadas desde simulacro oficial hasta la entrega de resultados de la STVD.

14. ENTREGABLES

Para verificar el cumplimiento de la ejecución del servicio, el contratista deberá entregar informes de ejecución del servicio, conformado por cuatro (4) entregables dichos informes deberán ser presentados en medio físico y/o digital, mediante la mesa de partes virtual y/o presencial en medios ópticos o impresos

Se entregarán en total cuatro (4) informes de acuerdo con el siguiente detalle:

N°	Entregables	Plazo de Entrega
1	Entregable 1: Planificación de auditoría	Deberá presentar el entregable hasta los diez (10) días calendario, contabilizados a partir del día siguiente de la firma del acta de inicio del servicio, previa notificación de la orden de servicio y/o la firma del contrato.
2	Entregable 2: Informe con el Pre-dictamen 1 de la primera parte de la auditoria.	Deberá presentar el entregable hasta los noventa (90) días calendario, contabilizados a partir del día siguiente de la firma del acta de inicio del servicio, previa notificación de la orden de servicio y/o la firma del contrato.

N°	Entregables	Plazo de Entrega
3	Entregable 3: Informe con el Pre-dictamen 2 de la segunda parte de la auditoria	Deberá presentar el entregable hasta los ciento noventa (190) días calendario, contabilizados a partir del día siguiente de la firma del acta de inicio del servicio, previa notificación de la orden de servicio y/o la firma del contrato.
4	Entregable 4: Informe Final y Dictamen del resultado de la auditoria.	Deberá presentar el entregable a los doscientos diecinueve (219) días calendario, contabilizados a partir del día siguiente de la firma del acta de inicio del servicio, previa notificación de la orden de servicio y/o la firma del contrato.

El contenido de los entregables se describe a continuación:

✓ **ENTREGABLE 1: PLANIFICACIÓN DE AUDITORÍA**

a. Plan de trabajo del servicio.

- Que refleje de manera clara las diferentes actividades, tareas, recursos, entregables del proyecto hitos y fechas de la entrega de esos documentos, así como las reuniones de trabajo; además debe corresponderse con las necesidades de este tipo de proyectos, considerar también lo indicado en el numeral 7.a Alcance del Servicio. El plan de trabajo del servicio incluye el plan de auditoría.

b. Plan de auditoría.

- Detallando como mínimo las actividades, responsables, duraciones y fechas de cada actividad planificada, según lo descrito en el numeral 7.B.
- Es importante describir cada actividad a desarrollar por parte del contratista.
- El plan de auditoria debe indicar los objetivos de la auditoría, documentos y criterios de referencia.
- Se debe definir los métodos de levantamiento de información a utilizar, (por ejemplo, análisis de documentación, observación, entrevistas, inducciones, cuestionarios, etc.) Además, incluir un cronograma para el desarrollo de las actividades e identificar los actores por cada actividad a realizar.
- Incluir el cronograma de ejecución, prioridad, descripción, las acciones a realizar y los resultados esperados. Además, se deberá indicar la estrategia a seguir en la ejecución de las pruebas y determinar los casos de prueba detallados tomando como apoyo

documentos base (FM40-GITE/TI: Especificación de requerimiento de software y FM39-GITE/TI: Reglas del negocio)
- Incluir pruebas de integración modular entre los diferentes módulos de la STVD.
- Es necesario que el plan y cronograma de auditoría, dentro de las actividades e hitos, contemple un reporte preliminar de avance documentado, con evidencias concretas, que identifique el detalle de los hallazgos (de corresponder), criticidad, impacto, y otra información relevante que permita el análisis del mismo, este reporte debe estar disponible dentro de los 90 días calendarios contabilizados a partir del día siguiente de la firma del acta de inicio del servicio, previa notificación de la orden de servicio y/o la firma del contrato.

✓ **ENTREGABLE 2: INFORME CON EL PRE-DICTAMEN 1 DE LA PRIMERA PARTE DE LA AUDITORIA**

El Pre - dictamen 1 de la primera parte la Auditoria se desarrolla en base a la Etapa 1 y la Etapa 2, correspondiente a la revisión de la STVD. Está compuesto por:

a. Pre - dictamen 1 de la primera parte de la auditoria. - El documento debe incluir como mínimo:

- Marco normativo utilizado en el análisis y servicio.
- Fases del análisis.
- Componentes tecnológicos analizados.
- Descripción de los resultados de las evaluaciones funcionales al STVD.
- Descripción de los resultados del análisis de las amenazas y vulnerabilidades de STVD.

b. Informe ejecutivo con los resultados del pre - dictamen 1 de la primera parte de la auditoria.- El documento debe detallar un resumen de los aspectos más relevantes realizados, conteniendo como mínimo:

- Introducción, metodología, alcance, resumen de las pruebas
- Evaluación de las funcionalidades de la STVD.
- Análisis de amenazas y vulnerabilidades
- Evaluación del código fuente y documentación.
- Hallazgos de corresponder
- Conclusiones y recomendaciones las cuales deberá incluir la viabilidad de utilizar la STVD en las EG2026.
- Matriz de los hallazgos evidenciados en la auditoria (de corresponder), detallando como mínimo la criticidad, impacto, y otra información relevante que permita el análisis del mismo, estos deben estar bien identificados y documentados.

✓ **ENTREGABLE 3: INFORME CON EL PRE-DICTAMEN 2 DE LA SEGUNDA PARTE DE LA AUDITORIA**

El Pre-dictamen 2 de la segunda parte de la Auditoría se desarrolla en base a la Etapa 3 y la Etapa 4, correspondiente a la revisión final de la Solución Tecnológica del Voto Digital (STVD). Está compuesto por:

a. Pre - dictamen 2 de la segunda parte de la auditoria. - El documento debe incluir como mínimo:

- Marco normativo utilizado en el análisis y servicio.
- Fases del análisis.
- Componentes tecnológicos analizados.
- Descripción de los resultados de las evaluaciones funcionales a la STVD.
- Descripción de los resultados del análisis de las amenazas y vulnerabilidades de la STVD.

b. Informe ejecutivo con los resultados del pre - dictamen 2 de la segunda parte de la auditoria.- El documento debe detallar un resumen de los aspectos más relevantes realizados, conteniendo como mínimo:

- Introducción, metodología, alcance, resumen de las pruebas
- Evaluación de las funcionalidades de la STVD.
- Análisis de amenazas y vulnerabilidades.
- Evaluación del código fuente y documentación.
- Hallazgos de corresponder.
- Conclusiones y recomendaciones.
- Matriz de los hallazgos evidenciados en la auditoria (de corresponder), detallando como mínimo la criticidad, impacto, y otra información relevante que permita el análisis del mismo, estos deben estar bien identificados y documentados.

✓ **ENTREGABLE 4: INFORME FINAL Y DICTAMEN DEL RESULTADO DE LA AUDITORIA**

a. Dictamen de Auditoria. - El documento debe incluir como mínimo:

- Marco normativo utilizado en el análisis y servicio.
- Fases del análisis.
- Componentes tecnológicos analizados.
- Descripción de los resultados de la evaluación de las funcionalidades de la STVD.

- Descripción de los resultados del análisis de las amenazas y vulnerabilidades de la STVD.
- Descripción de los resultados de la evaluación del Código fuente y documentación.

b. Informe ejecutivo de los resultados de la Auditoria. - El documento debe detallar un resumen de los aspectos más relevantes de los resultados, conteniendo como mínimo:

- Introducción, metodología, alcance, resumen de las pruebas.
- Resumen de la evaluación de funcionalidades (7.B.1.1).
- Resumen del Análisis de amenazas y vulnerabilidades (7.B.1.2).
- Resumen de la evaluación del código fuente y documentación (7.B.1.3).
- Resumen de las acciones.
- Conclusiones y recomendaciones.

c. Informe Final de la auditoría. - El documento debe contener como mínimo

- Informe de evaluación de funcionalidades, detallando las acciones realizadas según lo descrito en el numeral 7.B.1.1.
- Informe de amenazas y vulnerabilidades, detallando las acciones realizadas según lo descrito en el numeral 7.B.1.2.
- Informe de evaluación del código fuente, detallando las acciones realizadas según lo descrito en el numeral 7.B.1.3.
- Cada informe debe tener como mimo una matriz con los resultados de las pruebas realizadas.
- Matriz de los hallazgos evidenciados en la auditoria (de corresponder), detallando como mínimo la criticidad, impacto, las acciones correctivas realizadas y otra información relevante que permita el análisis del mismo, estos deben estar bien identificados y documentados.

15. CONFORMIDAD DEL SERVICIO

Será otorgada por la Gerencia de Informática y Tecnología Electoral (GITE), previo informe de conformidad emitido por la Sub Gerencia de Gobierno Digital e Innovación (SGGDI), a través de la verificación del cumplimiento de las condiciones establecidas en los términos de referencia en el plazo máximo de diez (10) días calendario de producida la recepción (de la prestación parcial o total efectuada, de ser el caso). En caso de observaciones, se procederá de acuerdo a lo indicado en el artículo 144 del Reglamento de la Ley 32069, Ley General de Contrataciones Públicas.

16. FORMA DE PAGO

El pago se realizará en cuatro (4) pagos parciales, uno por cada entregable, previa conformidad emitida por la Gerencia de Informática y Tecnología Electoral (GITE), en moneda nacional y a la presentación del comprobante de pago por parte del contratista.

Para el pago, el contratista debe haber cumplido con remitir los entregables correspondientes en cada periodo de acuerdo con lo señalado en la sección ENTREGABLES.

Pagos	*% Total de Servicio*	N° Entregable
1er. Pago	10%	Entregable 1
2do. Pago	30%	Entregable 2
3er. Pago	30%	Entregable 3
4to. Pago	30%	Entregable 4

Cuadro – Forma de pago.

El pago se efectuará mediante el respectivo abono en la cuenta bancaria individual del postor ganador, dentro de los diez (10) días hábiles siguientes de otorgada la conformidad, sea a través del Banco de la Nación o de cualquier otra institución bancaria del Sistema Financiero Nacional, para cuyo efecto EL CONTRATISTA comunicará su CODIGO DE CUENTA INTERBANCARIO (CCI), y se debe de contar además con:

- Conformidad por parte del área usuaria.
- Comprobante de pago.

Dicha documentación será entregada mediante la mesa de partes virtual externa de la institución a través de la página web de la ONPE (www.onpe.gob.pe) o en la oficina de trámite documentario de la Sede Central de la ONPE, situado en Jr. Washington 1894, Cercado de Lima, en el horario de lunes a viernes de 8:30 a 16:30 horas.

17. RESPONSABILIDAD DEL CONTRATISTA

El Contratista es responsable por la calidad ofrecida y por los vicios ocultos de los servicios ofertados por un plazo de un (01) año contado a partir de la conformidad otorgada por la Entidad.

18. PENALIDADES APLICABLES

18.1. Penalidades por Mora

En caso de retraso injustificado del contratista en la ejecución de las prestaciones objeto del contrato, la entidad contratante le aplica automáticamente una penalidad por mora por cada día.

18.2. Otras penalidades

Otras penalidades			
N°	**Supuestos de aplicación de penalidad**	**Forma de cálculo**	**Procedimiento**
1	Penalidad por demora o retraso en la presentación de entregables establecidos en el Numeral 14.	**Monto total de la penalidad = 10% x (valor de la UIT) x T** Donde: **UIT:** Unidad Impositiva Tributaria **T:** Total de días calendario acumulados en la demora o retraso de la presentación de entregables (*). (*) La fracción será considerada como un (1) día.	El tiempo de demora se contabiliza desde la finalización del plazo definido para los documentos establecidos en el numeral "ENTREGABLES" hasta que el Contratista presente los entregables en la mesa de partes presencial de la Sede Central de la ONPE o mediante la mesa de partes virtual externa de la institución a través de la página web de la ONPE (https://www.web.onpe.gob.pe/mpve/#/) en caso de tratarse de documentos.

La suma de la aplicación de las penalidades por mora y otras penalidades no debe exceder el 10% del monto vigente del contrato o, de ser el caso, del ítem correspondiente

19. ANTICORRUPCIÓN Y ANTISOBORNO

EL CONTRATISTA declara y garantiza no haber ofrecido, negociado, prometido o efectuado ningún pago o entrega de cualquier beneficio o incentivo ilegal, de manera directa o indirecta, a cualquier servidor de la entidad contratante.

Asimismo, EL CONTRATISTA se obliga a mantener una conducta proba e íntegra durante la vigencia del contrato, y después de culminado el mismo en caso existan controversias pendientes de resolver, lo que supone actuar con probidad, sin cometer actos ilícitos, directa o indirectamente.

Aunado a ello, EL CONTRATISTA se obliga a abstenerse de ofrecer, negociar, prometer o dar regalos, cortesías, invitaciones, donativos o cualquier beneficio o incentivo ilegal, directa o indirectamente, a funcionarios públicos, servidores públicos, locadores de servicios o proveedores de servicios del área usuaria, de la dependencia encargada de la contratación, y/o cualquier servidor de la entidad contratante, con la finalidad de obtener alguna ventaja indebida o beneficio ilícito. En esa línea, se obliga a adoptar las medidas técnicas, organizativas y/o de personal necesarias para asegurar que no se practiquen los actos previamente señalados.

Adicionalmente, EL CONTRATISTA se compromete a denunciar oportunamente ante las autoridades competentes los actos de corrupción o de inconducta funcional de los cuales tuviera conocimiento durante la ejecución del contrato con LA ENTIDAD CONTRATANTE.

Tratándose de una persona jurídica, lo anterior se extiende a sus accionistas, participacionistas, integrantes de los órganos de administración, apoderados, representantes legales, funcionarios, asesores o cualquier persona vinculada a la persona jurídica que representa; comprometiéndose a informarles sobre los alcances de las obligaciones asumidas en virtud del presente contrato.

Finalmente, el incumplimiento de las obligaciones establecidas en esta cláusula, durante la ejecución contractual, otorga a LA ENTIDAD CONTRATANTE el derecho de resolver total o parcialmente el contrato. Cuando lo anterior se produzca por parte de un proveedor adjudicatario de los catálogos electrónicos de acuerdo marco, el incumplimiento de la presente cláusula conllevará que sea excluido de los Catálogos Electrónicos de Acuerdo Marco. En ningún caso, dichas medidas impiden el inicio de las acciones civiles, penales y administrativas a que hubiera lugar.

20. INTEGRIDAD

En caso de falsedad de cualquiera de las declaraciones efectuadas por el Contratista, la ONPE podrá declarar la nulidad del presente contrato/orden de servicio por infracción del principio de presunción de veracidad, de conformidad a lo establecido en la Ley 32069, Ley General de Contrataciones Públicas y su Reglamento.

21. CONFIDENCIALIDAD DE LA INFORMACIÓN

El CONTRATISTA deberá mantener estricta confidencialidad sobre la información a que tendrá acceso durante la ejecución del servicio, no podrá disponer de la misma para fines distintos al desarrollo del servicio. El proveedor y su personal, deben comprometerse a mantener las reservas del caso y no transmitir los datos e información de ONPE a ninguna persona (natural o jurídica) que no sea debidamente autorizada por la ONPE.

22. REQUISITOS DE CALIFICACIÓN

22.1. Requisitos de Calificación Obligatoria

A.	EXPERIENCIA DEL POSTOR EN LA ESPECIALIDAD
	Requisitos: El postor debe acreditar un monto facturado acumulado equivalente a S/

	3,500,000.00 (Tres millones quinientos mil con 00/100 soles), por la contratación de servicios iguales o similares al objeto de la convocatoria de los cuales uno debe ser una auditoría que incluya un sistema de votación por internet en un proceso electoral organizado por la autoridad electoral competente de un país, de los cuales deben haber sido realizados durante los quince (15) años anteriores a la fecha de la presentación de ofertas que se computa desde la fecha de la conformidad o emisión del comprobante de pago, según corresponda. Se considera servicios similares a los siguientes: • Servicios de auditoría de sistemas de votación digital por internet, en un proceso electoral organizado por la autoridad electoral competente de un país. • Servicios de auditoría de sistemas de votación electrónica por internet, en un proceso electoral organizado por la autoridad electoral competente de un país. • Servicios de auditoría sistemas o aplicaciones de votación por internet, en un proceso electoral organizado por la autoridad electoral competente de un país. • Servicios de auditoría de sistemas de votación no presencial, en un proceso electoral organizado por la autoridad electoral competente de un país. • Servicios de auditoría de soluciones de votación en línea, en un proceso electoral organizado por la autoridad electoral competente de un país. • Realización de auditorías de seguridad de la información • Servicios de Auditoría en Sistemas de Información • Servicios de gestión de proyectos de TI. • Servicio de Ethical Hacking. • Servicio de Análisis de Vulnerabilidades • Servicio de Pruebas de Penetración. • Servicio de Pentesting • Servicio de gestión de riesgos. • Realización auditorías a infraestructura tecnológica. • Realización de auditorías de ciberseguridad. • Realización de consultorías de definición de un modelo de seguridad de la información y ciberseguridad. • Servicios de implementación de un sistema de gestión de seguridad de la información (SGSI), que incluya auditoria de seguridad de la información, gestión de riesgos e implementación de controles de seguridad.

Acreditación:

La experiencia del postor en la especialidad se acreditará con copia simple de (i) contratos u órdenes de servicios, y su respectiva conformidad o constancia de prestación; o (ii) comprobantes de pago cuya cancelación se acredite documental y fehacientemente, con constancia de depósito, nota de abono, reporte de estado de cuenta, cualquier otro documento emitido por entidad del sistema financiero que acredite el abono o mediante cancelación en el mismo comprobante de pago, correspondientes a un máximo de veinte (20) contrataciones. En caso el postor sustente su experiencia en la especialidad mediante contrataciones realizadas con privados, para acreditarla debe presentar de forma obligatoria lo indicado en el numeral (ii) del presente párrafo; no es posible que acredite su experiencia únicamente con la presentación de contratos u órdenes de compra con conformidad o constancia de prestación.

En caso los postores presenten varios comprobantes de pago para acreditar una sola contratación, se debe acreditar que corresponden a dicha contratación; de lo contrario, se asumirá que los comprobantes acreditan contrataciones independientes, en cuyo caso solo se considerará, para la evaluación, las veinte (20) primeras contrataciones indicadas en el **Anexo Nº 11** referido a la Experiencia del Postor en la Especialidad.

En el caso de servicios de ejecución periódica o continuada, solo se considera como experiencia la parte del contrato que haya sido ejecutada durante los quince (15) años anteriores a la fecha de presentación de ofertas, debiendo adjuntarse copia de las conformidades correspondientes a tal parte o los respectivos comprobantes de pago cancelados.

Si el titular de la experiencia no es el postor, consignar si dicha experiencia corresponde a la matriz en caso de que el postor sea sucursal, o fue transmitida por reorganización societaria, debiendo acompañar la documentación sustentatoria correspondiente.

Si el postor acredita experiencia de otra persona jurídica como consecuencia de una reorganización societaria, debe presentar adicionalmente el **Anexo N° 14.**

Las personas jurídicas resultantes de un proceso de reorganización societaria no pueden acreditar como experiencia del postor en la especialidad que le hubiesen transmitido como parte de dicha reorganización las personas jurídicas sancionadas con inhabilitación vigente o definitiva.

Cuando en los contratos, órdenes de servicios o comprobantes de pago el monto

	facturado se encuentre expresado en moneda extranjera, debe indicarse el tipo de cambio venta publicado por la Superintendencia de Banca, Seguros y AFP correspondiente a la fecha de suscripción del contrato, de emisión de la orden de servicio o de cancelación del comprobante de pago, según corresponda. Sin perjuicio de lo anterior, los postores deben llenar y presentar el **Anexo Nº 11** referido a la Experiencia del Postor en la Especialidad.
B.	**CAPACIDAD TÉCNICA Y PROFESIONAL**
B.1	**EXPERIENCIA DEL PERSONAL CLAVE**
	Auditor Líder Requisitos: • El personal clave: Auditor Líder debe acreditar cinco (5) años de experiencia laboral como mínimo, como auditor de TI en instituciones privadas y/o gubernamentales. La experiencia profesional será validada desde la obtención del título profesional. Acreditación: • La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto. • Los documentos que acreditan la experiencia deben incluir los nombres y apellidos del personal clave, el cargo desempeñado, el plazo de la prestación indicando el día, mes y año de inicio y culminación, el nombre de la entidad u organización que emite el documento, la fecha de emisión y nombres y apellidos de quien suscribe el documento. • En caso los documentos para acreditar la experiencia establezcan el plazo de la experiencia adquirida por el personal clave en meses sin especificar los días se debe considerar el mes completo. • Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas. • De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado.

Auditores Especialistas:

Requisitos:

- El personal clave: Cada Auditor Especialista debe acreditar tres (3) años de experiencia laboral como mínimo, como auditor o analista de TI en instituciones privadas y/o gubernamentales, dentro de los cuales se requiere una experiencia profesional mínima de dos (02) años en auditorías de seguridad y/o revisión de la seguridad del código fuente de aplicaciones y/o pruebas de seguridad y/o auditoría de aplicación y/o auditoría de sistemas y/o Ethical Hacking, análisis de vulnerabilidades y/o pruebas de penetración o servicios de auditoría de seguridad y/o seguridad de procesos de información y/o revisión de la seguridad de aplicaciones y/o pruebas de seguridad y/o auditoría de aplicación de TI.

La experiencia profesional será validada desde la obtención del título profesional.

Acreditación:

- La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto.
- Los documentos que acreditan la experiencia deben incluir los nombres y apellidos del personal clave, el cargo desempeñado, el plazo de la prestación indicando el día, mes y año de inicio y culminación, el nombre de la entidad u organización que emite el documento, la fecha de emisión y nombres y apellidos de quien suscribe el documento.
- En caso los documentos para acreditar la experiencia establezcan el plazo de la experiencia adquirida por el personal clave en meses sin especificar los días se debe considerar el mes completo.
- Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas.
- De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado.

Experto en Ciberseguridad:

	Requisitos: • El personal clave: Experto en Ciberseguridad, debe acreditar cinco (5) años de experiencia laboral como mínimo, en auditoría de sistemas de seguridad o auditoría de sistemas en arquitecturas criptográficas. La experiencia profesional será validada desde la obtención del título profesional. Acreditación: • La experiencia del personal clave se acreditará con cualquiera de los siguientes documentos: (i) copia simple de contratos y su respectiva conformidad o (ii) constancias o (iii) certificados o (iv) cualquier otra documentación que, de manera fehaciente demuestre la experiencia del personal propuesto. • Los documentos que acreditan la experiencia deben incluir los nombres y apellidos del personal clave, el cargo desempeñado, el plazo de la prestación indicando el día, mes y año de inicio y culminación, el nombre de la entidad u organización que emite el documento, la fecha de emisión y nombres y apellidos de quien suscribe el documento. • En caso los documentos para acreditar la experiencia establezcan el plazo de la experiencia adquirida por el personal clave en meses sin especificar los días se debe considerar el mes completo. • Se considerará aquella experiencia que no tenga una antigüedad mayor a veinticinco (25) años anteriores a la fecha de la presentación de ofertas. De presentarse experiencia ejecutada paralelamente (traslape), para el cómputo del tiempo de dicha experiencia sólo se considerará una vez el periodo traslapado.
B.2	**CALIFICACIONES DEL PERSONAL CLAVE**
B.2.1	**FORMACIÓN ACADÉMICA**
	Auditor Líder Requisitos: • Un (01) profesional Titulado y Colegiado, de corresponder (colegiatura vigente durante el servicio), en una de las siguientes especialidades: ingeniería de sistemas o ingeniería informática o ingeniería en computación e informática o ingeniería electrónica o ingeniería en telecomunicaciones o ingeniería industrial o ingeniería de seguridad y auditoria informática o

administración con mención en negocios y tecnología o licenciado en computación o en ciencias de la computación.

Acreditación:

- El grado o título profesional requerido será verificado por los evaluadores en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: *https://enlinea.sunedu.gob.pe/*
- El postor debe señalar los nombres y apellidos, DNI y profesión del personal clave, así como el nombre de la universidad o institución educativa que expidió el grado o título profesional requerido.
- En caso el grado o título profesional requerido no se encuentre inscrito en los referidos registros, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.
- En caso se acredite estudios en el extranjero del personal clave, debe presentarse adicionalmente copia simple del documento de la revalidación o del reconocimiento ante SUNEDU, del grado académico o título profesional otorgados en el extranjero, según corresponda.
- La colegiatura será verificada por los evaluadores mediante consulta en la página web del colegio profesional correspondiente.

Auditores Especialistas:

Requisitos:

- Tres (03) profesionales Titulados en una de las siguientes especialidades: ingeniería de sistemas o ingeniería informática o ingeniería de software o ingeniería de seguridad informática o ingeniería de seguridad y auditoria informática o computación e informática o ingeniería electrónica o industrial o administración con mención en negocios y tecnología o licenciado en computación o en ciencias de la computación.

Acreditación:

- El grado o título profesional requerido será verificado por los evaluadores en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link:

https://enlinea.sunedu.gob.pe/.

- El postor debe señalar los nombres y apellidos, DNI y profesión del personal clave, así como el nombre de la universidad o institución educativa que expidió el grado o título profesional requerido.
- En caso el grado o título profesional requerido no se encuentre inscrito en los referidos registros, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.
- En caso se acredite estudios en el extranjero del personal clave, debe presentarse adicionalmente copia simple del documento de la revalidación o del reconocimiento ante SUNEDU, del grado académico o título profesional otorgados en el extranjero, según corresponda.

Experto en Ciberseguridad:

Requisitos:

- Un (01) profesional Titulado y Colegiado, de corresponder (colegiatura vigente durante el servicio), en una de las siguientes especialidades: ingeniería de sistemas o ingeniería informática o ingeniería en computación e informática o ingeniería de seguridad o matemáticas.
- Con Maestría en Ciencias en Ingeniería Electrónica o en Ciberseguridad o en Ingeniería de Seguridad Informática o disciplinas afines directamente relacionadas con la seguridad informática o criptografía.

Acreditación:

- El grado o título profesional requerido será verificado por los evaluadores en el Registro Nacional de Grados Académicos y Títulos Profesionales en el portal web de la Superintendencia Nacional de Educación Superior Universitaria - SUNEDU a través del siguiente link: *https://enlinea.sunedu.gob.pe/*
- El postor debe señalar los nombres y apellidos, DNI y profesión del personal clave, así como el nombre de la universidad o institución educativa que expidió el grado o título profesional requerido.
- En caso el grado o título profesional requerido no se encuentre inscrito en los referidos registros, el postor debe presentar la copia del diploma respectivo a fin de acreditar la formación académica requerida.
- En caso se acredite estudios en el extranjero del personal clave, debe presentarse adicionalmente copia simple del documento de la revalidación o

	del reconocimiento ante SUNEDU, del grado académico o título profesional otorgados en el extranjero, según corresponda. • La Maestría se acreditará con Certificado de estudios completos y/o Diploma y/o Titulo. La colegiatura será verificada por los evaluadores mediante consulta en la página web del colegio profesional correspondiente.
C.	**PARTICIPACIÓN DE CONSORCIO**
	<u>Requisitos:</u> • El porcentaje mínimo de participación en la ejecución del contrato, para el integrante del consorcio que acredite mayor experiencia, es de 70%. <u>Acreditación</u>: Se acredita con la promesa de consorcio.

Visado digitalmente por
FERNANDO ZAPATA MIRANDA
Subgerente de Gobierno Digital e Innovación
SUBGERENCIA DE GOBIERNO DIGITAL E INNOVACIÓN

Visado digitalmente por
ROBERTO CARLOS MONTENEGRO VEGA
Gerente de la Gerencia de Informática y Tecnología Electoral
GERENCIA DE INFORMÁTICA Y TECNOLOGÍA ELECTORAL

ANEXO A

ENTENDIMIENTO DE LA SOLUCION TECNOLÓGICA ELECTORALES

SOLUCIÓN TECNOLÓGICA DEL VOTO DIGITAL (STVD)

1.1. DESCRIPCIÓN TÉCNICA DEL PRODUCTO

El voto digital cumple con las siguientes características técnicas:

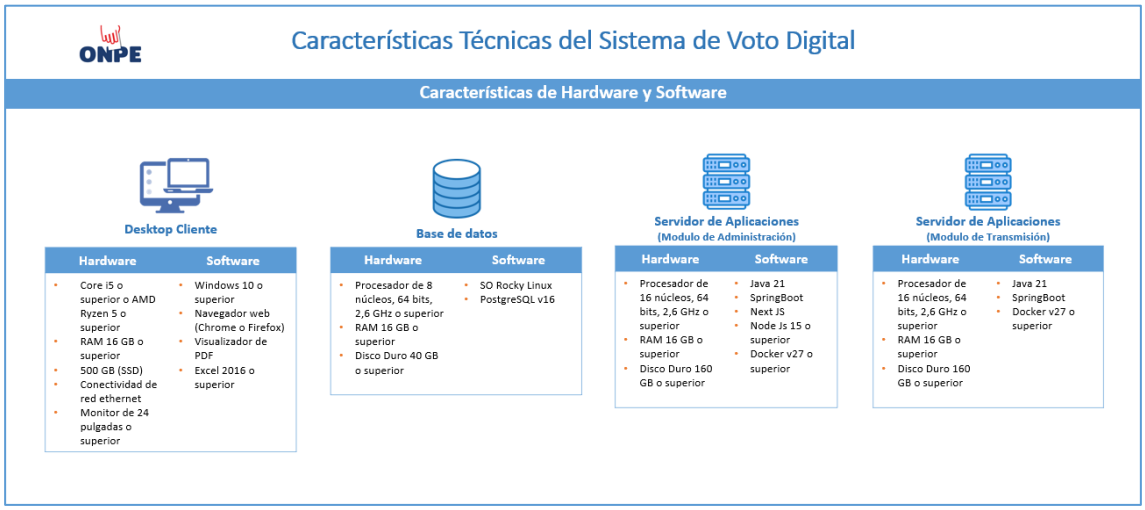


Ilustración 1. Características de Hardware y Software del Sistema de Voto Digital.

1.2. ALCANCE DEL SISTEMA INFORMÁTICO ELECTORAL

La Solución Tecnológica del Voto Digital es una solución diseñada para garantizar la participación electoral de manera segura, eficiente y transparente en cualquier tipo de proceso electoral. Su alcance abarca la implementación en diversas instituciones y niveles de gobierno, incluyendo elecciones nacionales, regionales y locales, así como procesos internos de organizaciones privadas y públicas.

El sistema está diseñado para permitir la votación desde cualquier ubicación, facilitando la inclusión de ciudadanos residentes en el extranjero y de poblaciones con dificultades de acceso a centros de votación físicos. Además, asegura la integridad del proceso mediante el uso de tecnologías avanzadas de autenticación, cifrado de datos y auditoría en tiempo real.

1.3. DESCRIPCIÓN Y FUNCIONALIDADES GENERALES

La Solución Tecnológica del Voto Digital está diseñada bajo una arquitectura orientada a microservicios, lo que permite una segmentación eficiente de la aplicación en servicios pequeños, independientes y especializados. Estos microservicios interactúan entre sí mediante protocolos ligeros como HTTP/REST, gRPC o mensajería basada en eventos, garantizando una comunicación ágil y eficiente.

Cada microservicio tiene una responsabilidad específica dentro del sistema electoral, lo que facilita su desarrollo, implementación y escalabilidad de forma independiente. Este modularidad permite actualizaciones sin afectar el sistema completo, mejorando la capacidad de respuesta ante cambios normativos o nuevas necesidades funcionales.

El Sistema de Voto Digital, es una herramienta informática que permite a los usuarios:

- Emitir su voto de manera segura, sin importar su ubicación geográfica.
- Garantizar la autenticidad del votante, utilizando mecanismos de identificación robustos, como autenticación biométrica o verificación de identidad digital.
- Proteger la integridad del proceso, asegurando que cada voto sea único e inalterable mediante tecnología blockchain o cifrado avanzado.
- Automatizar el escrutinio y la publicación de resultados, reduciendo tiempos de procesamiento y minimizando errores humanos.
- Facilitar la accesibilidad, garantizando que personas con discapacidad puedan ejercer su derecho al voto a través de interfaces adaptadas.
- Proporcionar un entorno auditable, permitiendo la verificación del proceso por parte de entidades de control y observadores electorales.

El Sistema de Voto Digital, cuenta con los siguientes módulos y funcionalidades:

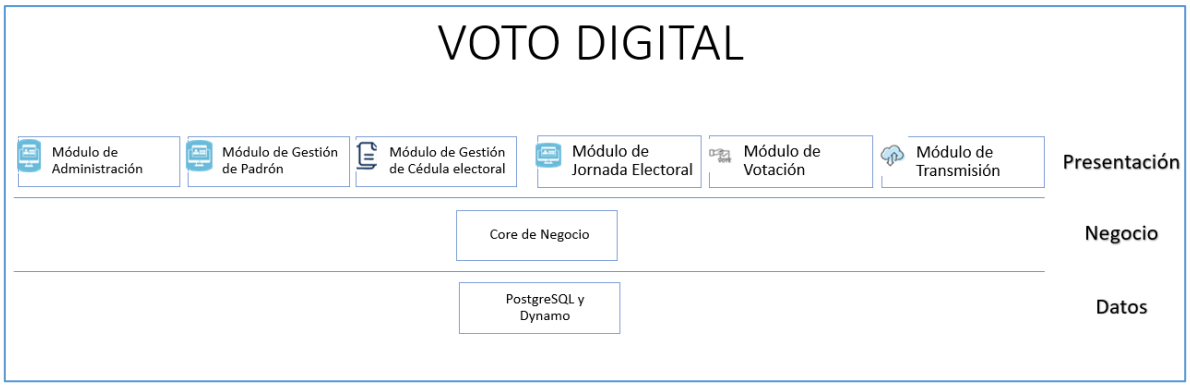


Ilustración 2 - Modelo Vista Controlador del Sistema de Voto Digital

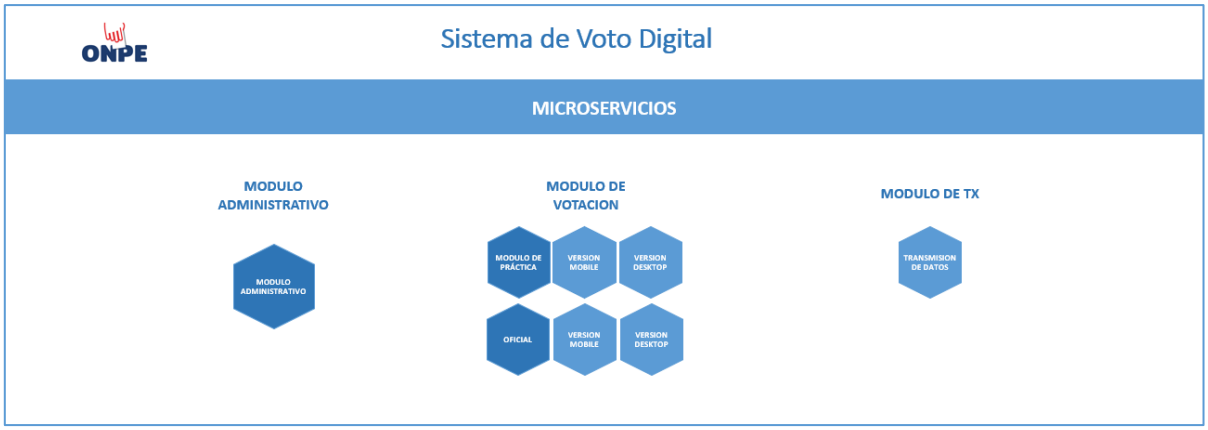


Ilustración 3 -

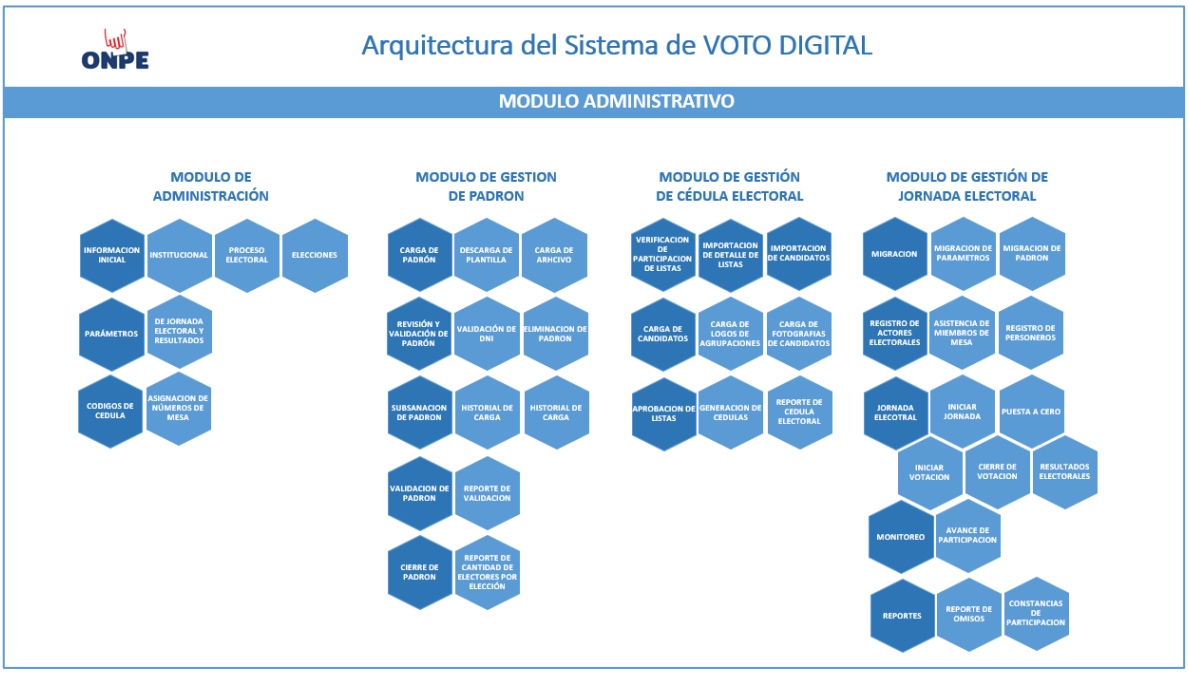


Ilustración 4 - Diagrama de módulos y funcionalidades Sistema de Voto Digital

ANEXO B

CARACTERÍSTICAS Y RESTRICCIONES DEL AMBIENTE DISPONIBLE PARA LA EJECUCIÓN DEL SERVICIO

Descripción del uso del Ambiente

La ONPE, de ser necesario, habilitará un ambiente que se encontrará disponible en el horario de 8:30 a.m. a 5:00 p.m., el cual dispondrá de mesas de trabajo, equipos informáticos (PC o laptop) con restricciones de acceso a red e internet y al uso de componentes externos y/o memorias extraíbles, además de una impresora y hojas a solicitud; adicionalmente la ONPE habilitará la arquitectura tecnológica de simulación de los procesos electorales implementando la Solución Tecnológica del Voto Digital en los cuales el contratista podrá ejecutar todas las actividades para la auditoria en servicios informáticos como parte del servicio; asimismo será en este ambiente donde se ejecutarán las sesiones programadas con los especialistas designados por la ONPE en la transferencia de la información que pueda ser requerida.

Utilización del Ambiente

El ambiente estará restringido para su utilización exclusiva por parte del personal que el contratista presente para su ejecución del servicio, el mismo que deberá encontrarse autorizado por la Gerencia de Informática y Tecnología Electoral, todos los integrantes del personal deberán ser identificados con su DNI o carnet de extranjería según sea el caso, nombres y apellidos, y actividades a ejecutar, quienes deberán firmar el documento de “Compromiso de no divulgación para servicios contratados”, en resguardo de la propiedad, transferencia, eliminación o disociación de la información que pueda ser entregada por la ONPE.

Para el acceso al ambiente se dispondrá de un registro de ingreso y salida, al cual no podrá ingresarse con equipos móviles, cámaras o unidades de almacenamiento de información extraíbles como lo son USB, memorias o discos duros.

El contratista podrá realizar la instalación de software en los equipos para la ejecución del servicio, contemplando que dicho software deberá encontrarse debidamente licenciado, siendo la ONPE a través de la GITE quien verificará el licenciamiento del software.

El ambiente dispuesto para este servicio estará a cargo de un profesional responsable por parte de la ONPE con quién deberá coordinarse su acceso y utilización, así como el cumplimiento de las restricciones expresadas.

ANEXO C

LISTADO DE CONTROLES Y ESTANDARES PARA EVALUACIÓN DEL SOFTWARE

a) Anexo A del ISO/IEC 27001:2022 E ISO/IEC 27002-2022 (Estándar para Sistemas de Gestión de Seguridad de la Información)

CEI 27002 control identificador	Nombre de control	Descripción
5.1	Políticas de seguridad de la información.	La política de seguridad de la información y las políticas específicas de temas serán definidas, aprobadas por la gerencia, publicadas, comunicadas y reconocidas por el personal relevante y las partes interesadas relevantes, y revisadas a intervalos planificados y si se producen cambios significativos.
5.2	Funciones y responsabilidades de seguridad de la información	Las funciones y responsabilidades de seguridad de la información se definirán y asignarán de acuerdo con las necesidades de la organización.
5.3	Segregación de funciones	Se separarán las tareas y áreas de responsabilidad en conflicto.
5.4	responsabilidades de gestión	La gerencia debe exigir a todo el personal que aplique la seguridad de la información de acuerdo con la política de seguridad de la información establecida, las políticas y los procedimientos específicos del tema de la organización.
5.5	Contacto con autoridades	La organización deberá establecer y mantener contacto con las autoridades pertinentes.
5.6	Contacto con grupos de interés especial	La organización deberá establecer y mantener contacto con grupos de interés especial u otros foros especializados en seguridad y asociaciones profesionales.
5.7	Inteligencia de amenazas	La información relacionada con las amenazas a la seguridad de la información se recopilará y analizará para generar información sobre amenazas.
5.8	Seguridad de la información en la gestión de proyectos.	La seguridad de la información se integrará en la gestión de proyectos.
5.9	Inventario de información y otros activos asociados	Se debe desarrollar y mantener un inventario de información y otros activos asociados, incluidos los propietarios.
5.10	Uso aceptable de la información y otros activos asociados	Se identificarán, documentarán e implementarán reglas para el uso aceptable y procedimientos para el manejo de la información y otros activos asociados.

CEI 27002 control identificador	Nombre de control	Descripción
5.11	Devolución de activos	El personal y otras partes interesadas, según corresponda, devolverán todos los activos de la organización que estén en su poder al cambiar o terminar su empleo, contrato o acuerdo.
5.12	Clasificación de la información	La información se clasificará de acuerdo con las necesidades de seguridad de la información de la organización en función de la confidencialidad, la integridad, la disponibilidad y los requisitos pertinentes de las partes interesadas.
5.13	Etiquetado de información	Se debe desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado de la información de acuerdo con el esquema de clasificación de la información adoptado por la organización.
5.14	Transferencia de información	Deben existir reglas, procedimientos o acuerdos de transferencia de información para todos los tipos de instalaciones de transferencia dentro de la organización y entre la organización y otras partes.
5.15	Control de acceso	Las reglas para controlar el acceso físico y lógico a la información y otros activos asociados se establecerán e implementarán en función de los requisitos de seguridad de la información y del negocio.
5.16	Gestión de identidad	Se gestionará el ciclo de vida completo de las identidades.
5.17	Información de autenticación	La asignación y gestión de la información de autenticación se controlará mediante un proceso de gestión, incluido el asesoramiento al personal sobre el manejo adecuado de la información de autenticación.
5.18	Derechos de acceso	Los derechos de acceso a la información y otros activos asociados deben proporcionarse, revisarse, modificarse y eliminarse de acuerdo con la política y las reglas de control de acceso específicas del tema de la organización.
5.19	Seguridad de la información en las relaciones con los proveedores	Se deben definir e implementar procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con el uso de los productos o servicios del proveedor.
5.20	Abordar la seguridad de la información en los acuerdos con los proveedores	Los requisitos de seguridad de la información pertinentes se establecerán y acordarán con cada proveedor en función del tipo de relación con el proveedor.
5.21	Gestión de la seguridad de la información en la cadena de suministro de tecnologías de la información y la comunicación (TIC)	Se deben definir e implementar procesos y procedimientos para gestionar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de TIC.
5.22	Seguimiento, revisión y gestión de cambios de servicios de proveedores	La organización debe monitorear, revisar, evaluar y gestionar periódicamente los cambios en las prácticas de seguridad de la información del proveedor y la prestación de servicios.
5.23	Seguridad de la información para el uso de servicios en la nube	Los procesos de adquisición, uso, gestión y salida de los servicios en la nube se deben establecer de acuerdo con los requisitos de seguridad de la información de la organización.
5.24	Planificación y preparación de la gestión de incidentes de seguridad de la información	La organización debe planificar y prepararse para la gestión de incidentes de seguridad de la información definiendo, estableciendo y comunicando procesos, roles y responsabilidades de gestión de incidentes de seguridad de la información.

CEI 27002 control identificador	Nombre de control	Descripción
5.25	Evaluación y decisión sobre eventos de seguridad de la información	La organización debe evaluar los eventos de seguridad de la información y decidir si se clasificarán como incidentes de seguridad de la información.
5.26	Respuesta a incidentes de seguridad de la información	Se debe responder a los incidentes de seguridad de la información de acuerdo con los procedimientos documentados.
5.27	Aprender de los incidentes de seguridad de la información	El conocimiento obtenido de los incidentes de seguridad de la información se utilizará para fortalecer y mejorar los controles de seguridad de la información.
5.28	Recolección de evidencia	La organización debe establecer e implementar procedimientos para la identificación, recolección, adquisición y preservación de evidencia relacionada con eventos de seguridad de la información.
5.29	Seguridad de la información durante la interrupción	La organización debe planificar cómo mantener la seguridad de la información en un nivel adecuado durante la interrupción.
5.30	Preparación de las TIC para la continuidad del negocio	La preparación de las TIC debe planificarse, implementarse, mantenerse y probarse en función de los objetivos de continuidad del negocio y los requisitos de continuidad de las TIC
5.31	Requisitos legales, estatutarios, reglamentarios y contractuales	Los requisitos legales, estatutarios, reglamentarios y contractuales relevantes para la seguridad de la información y el enfoque de la organización para cumplir con estos requisitos deben identificarse, documentarse y mantenerse actualizados.
5.32	Derechos de propiedad intelectual	La organización debe implementar procedimientos apropiados para proteger los derechos de propiedad intelectual.
5.33	Protección de registros	Los registros deben protegerse contra pérdida, destrucción, falsificación, acceso no autorizado y publicación no autorizada.
5.34	Privacidad y protección de la información de identificación personal (PII)	La organización deberá identificar y cumplir los requisitos relacionados con la preservación de la privacidad y la protección de la PII de acuerdo con las leyes y reglamentos aplicables y los requisitos contractuales.
5.35	Revisión independiente de la seguridad de la información.	El enfoque de la organización para gestionar la seguridad de la información y su implementación, incluidas las personas, los procesos y las tecnologías, se revisará de forma independiente a intervalos planificados o cuando se produzcan cambios significativos.
5.36	Cumplimiento de políticas, normas y estándares de seguridad de la información	El cumplimiento de la política de seguridad de la información de la organización, las políticas, las reglas y los estándares específicos de cada tema se revisará periódicamente.
5.37	Procedimientos operativos documentados	Los procedimientos operativos para las instalaciones de procesamiento de información deben documentarse y ponerse a disposición del personal que los necesite.

6 - Controles de personas

CEI 27002 control identificador	nombre de control	Descripción
6.1	Poner en pantalla	Los controles de verificación de antecedentes de todos los candidatos para convertirse en personal se llevarán a cabo antes de unirse a la organización y de manera continua, teniendo en cuenta las leyes, los reglamentos y la ética aplicables, y serán proporcionales a los requisitos comerciales, la clasificación de la información a la que se accederá y los riesgos percibidos.
6.2	Términos y condiciones de empleo	Los acuerdos contractuales de trabajo deben establecer las responsabilidades del personal y de la organización en materia de seguridad de la información.
6.3	Concientización, educación y capacitación en seguridad de la información	El personal de la organización y las partes interesadas relevantes deben recibir la conciencia, educación y capacitación adecuadas en seguridad de la información y actualizaciones periódicas de la política de seguridad de la información de la organización, las políticas y los procedimientos específicos del tema, según sea relevante para su función laboral.
6.4	Proceso Disciplinario	Se formalizará y comunicará un proceso disciplinario para tomar acciones contra el personal y otras partes interesadas relevantes que hayan cometido una violación a la política de seguridad de la información.
6.5	Responsabilidades después de la terminación o cambio de empleo	Las responsabilidades y deberes de seguridad de la información que sigan siendo válidos después de la terminación o el cambio de empleo se definirán, aplicarán y comunicarán al personal pertinente y otras partes interesadas.
6.6	Acuerdos de confidencialidad o no divulgación	Los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información deben ser identificados, documentados, revisados regularmente y firmados por el personal y otras partes interesadas relevantes.
6.7	Trabajo remoto	Se implementarán medidas de seguridad cuando el personal trabaje de forma remota para proteger la información a la que se acceda, procese o almacene fuera de las instalaciones de la organización.
6.8	Informes de eventos de seguridad de la información	La organización debe proporcionar un mecanismo para que el personal informe eventos de seguridad de la información observados o sospechados a través de los canales apropiados de manera oportuna.

7 - Controles físicos

CEI 27002 control identificador	nombre de control	Descripción
7.1	Perímetros físicos de seguridad	Los perímetros de seguridad se definirán y utilizarán para proteger las áreas que contienen información y otros activos asociados.
7.2	Entrada física	Las áreas seguras deben estar protegidas por controles de entrada y puntos de acceso apropiados.
7.3	Asegurar oficinas, salas e instalaciones	Se diseñará e implementará la seguridad física de las oficinas, salas e instalaciones.
7.4	Monitoreo de seguridad física	Los locales deberán ser monitoreados continuamente para el acceso físico no autorizado.
7.5	Protección contra amenazas físicas y ambientales.	Se debe diseñar e implementar la protección contra amenazas físicas y ambientales, tales como desastres naturales y otras amenazas físicas intencionales o no intencionales a la infraestructura.
7.6	Trabajar en áreas seguras	Se diseñarán e implementarán medidas de seguridad para trabajar en áreas seguras.
7.7	Escritorio despejado y pantalla despejada	Se deben definir y hacer cumplir adecuadamente las reglas de escritorio limpio para documentos y medios de almacenamiento extraíbles y las reglas de pantalla limpia para las instalaciones de procesamiento de información.
7.8	Emplazamiento y protección de equipos	El equipo se colocará de forma segura y protegida.
7.9	Seguridad de los activos fuera de las instalaciones	Se protegerán los activos fuera del sitio.
7.10	Medios de almacenamiento	Los medios de almacenamiento deben gestionarse a lo largo de su ciclo de vida de adquisición, uso, transporte y eliminación de acuerdo con el esquema de clasificación y los requisitos de manipulación de la organización.
7.11	Utilidades de apoyo	Las instalaciones de procesamiento de información deben estar protegidas contra cortes de energía y otras interrupciones causadas por fallas en los servicios públicos de apoyo.
7.12	seguridad del cableado	Los cables que transportan energía, datos o servicios de información de apoyo deben estar protegidos contra intercepciones, interferencias o daños.
7.13	Mantenimiento de equipo	El equipo se mantendrá correctamente para garantizar la disponibilidad, integridad y confidencialidad de la información.

CEI 27002 control identificador	nombre de control	Descripción
7.14	Eliminación segura o reutilización de equipos	Los elementos del equipo que contengan medios de almacenamiento se verificarán para garantizar que todos los datos confidenciales y el software con licencia se hayan eliminado o sobrescrito de forma segura antes de su eliminación o reutilización.

8 - Controles tecnológicos

CEI 27002 control identificador	nombre de control	Descripción
8.1	Dispositivos de punto final de usuario	Se protegerá la información almacenada, procesada o accesible a través de los dispositivos finales del usuario.
8.2	Derechos de acceso privilegiado	La asignación y uso de los derechos de acceso privilegiado se restringirá y gestionará.
8.3	Restricción de acceso a la información	El acceso a la información y otros activos asociados se restringirá de acuerdo con la política específica del tema establecida sobre el control de acceso.
8.4	Acceso al código fuente	El acceso de lectura y escritura al código fuente, las herramientas de desarrollo y las bibliotecas de software se gestionará adecuadamente.
8.5	Autenticación segura	Las tecnologías y procedimientos de autenticación segura se implementarán en función de las restricciones de acceso a la información y la política específica del tema sobre el control de acceso.
8.6	Gestión de capacidad	El uso de los recursos se controlará y ajustará de acuerdo con los requisitos de capacidad actuales y previstos.
8.7	Protección contra malware	La protección contra el malware se implementará y respaldará mediante la conciencia adecuada del usuario.
8.8	Gestión de vulnerabilidades técnicas	Se debe obtener información sobre las vulnerabilidades técnicas de los sistemas de información en uso, se debe evaluar la exposición de la organización a tales vulnerabilidades y se deben tomar las medidas apropiadas.
8.9	Gestión de la configuración	Las configuraciones, incluidas las configuraciones de seguridad, de hardware, software, servicios y redes deben establecerse, documentarse, implementarse, monitorearse y revisarse.

CEI 27002 control identificador	nombre de control	Descripción
8.10	Eliminación de información	La información almacenada en los sistemas de información, dispositivos o en cualquier otro medio de almacenamiento será eliminada cuando ya no sea necesaria.
8.11	Enmascaramiento de datos	El enmascaramiento de datos se debe utilizar de acuerdo con la política específica del tema de la organización sobre el control de acceso y otras políticas relacionadas con el tema específico, y los requisitos comerciales, teniendo en cuenta la legislación aplicable.
8.12	Prevención de fuga de datos	Las medidas de prevención de fuga de datos se aplicarán a los sistemas, redes y cualquier otro dispositivo que procese, almacene o transmita información sensible.
8.13	Copia de seguridad de la información	Las copias de seguridad de la información, el software y los sistemas se mantendrán y probarán periódicamente de acuerdo con la política de copia de seguridad específica del tema acordada.
8.14	Redundancia de las instalaciones de procesamiento de información	Las instalaciones de procesamiento de información se implementarán con suficiente redundancia para cumplir con los requisitos de disponibilidad.
8.15	Inicio sesión	Se producirán, almacenarán, protegerán y analizarán registros que registren actividades, excepciones, fallas y otros eventos relevantes.
8.16	Actividades de seguimiento	Las redes, los sistemas y las aplicaciones deberán ser monitoreados por comportamiento anómalo y se tomarán las acciones apropiadas para evaluar posibles incidentes de seguridad de la información.
8.17	Sincronización de reloj	Los relojes de los sistemas de procesamiento de información utilizados por la organización deben estar sincronizados con las fuentes de tiempo aprobadas.
8.18	Uso de programas de utilidad privilegiados	El uso de programas de utilidad que puedan anular los controles del sistema y de la aplicación debe estar restringido y estrictamente controlado.
8.19	Instalación de software en sistemas operativos	Se implementarán procedimientos y medidas para gestionar de forma segura la instalación de software en los sistemas operativos.
8.20	Seguridad en redes	Las redes y los dispositivos de red se asegurarán, administrarán y controlarán para proteger la información en los sistemas y aplicaciones.

CEI 27002 control identificador	nombre de control	Descripción
8.21	Seguridad de los servicios de red.	Se identificarán, implementarán y controlarán los mecanismos de seguridad, los niveles de servicio y los requisitos de servicio de los servicios de red.
8.22	Segregación de redes	Los grupos de servicios de información, usuarios y sistemas de información deben estar segregados en las redes de la organización.
8.23	Filtrado web	El acceso a sitios web externos se gestionará para reducir la exposición a contenido malicioso.
8.24	Uso de criptografía	Se deben definir e implementar reglas para el uso efectivo de la criptografía, incluida la gestión de claves criptográficas.
8.25	Ciclo de vida de desarrollo seguro	Se establecerán y aplicarán reglas para el desarrollo seguro de software y sistemas.
8.26	Requisitos de seguridad de la aplicación	Los requisitos de seguridad de la información deben identificarse, especificarse y aprobarse al desarrollar o adquirir aplicaciones.
8.27	Principios de arquitectura e ingeniería de sistemas seguros	Se deben establecer, documentar, mantener y aplicar principios para la ingeniería de sistemas seguros en cualquier actividad de desarrollo de sistemas de información.
8.28	Codificación segura	Los principios de codificación segura se aplicarán al desarrollo de software.
8.29	Pruebas de seguridad en desarrollo y aceptación.	Los procesos de pruebas de seguridad se definirán e implementarán en el ciclo de vida del desarrollo.
8.30	Desarrollo subcontratado	La organización debe dirigir, monitorear y revisar las actividades relacionadas con el desarrollo de sistemas subcontratados.
8.31	Separación de los entornos de desarrollo, prueba y producción	Los entornos de desarrollo, prueba y producción deben estar separados y protegidos.
8.32	Gestión del cambio	Los cambios en las instalaciones de procesamiento de información y los sistemas de información estarán sujetos a procedimientos de gestión de cambios.
8.33	Información de prueba	La información de las pruebas se seleccionará, protegerá y gestionará adecuadamente.
8.34	Protección de los sistemas de información durante las pruebas de auditoría	Las pruebas de auditoría y otras actividades de aseguramiento que involucren la evaluación de los sistemas operativos deben planificarse y acordarse entre el evaluador y la gerencia correspondiente.

b) OWASP (Estándar de Verificación de Seguridad en Aplicaciones)

- **Listado de pruebas a realizar para aplicaciones web**

Nro. Control	CODIGO OWASP	PRUEBA POR REALIZAR	Objetivos
Obtención de Información			
1	WSTG-INFO-01	Realizar el descubrimiento y reconocimiento de divulgación de información basados en motores de búsqueda	- Identificar información sensible de diseño y configuración de la aplicación, sistema u organización que esté expuesta directamente (en el sitio web de la organización) o indirectamente (a través de servicios de terceros).
2	WSTG-INFO-02	Identificar el software de Web	- Determinar la versión y el tipo de un servidor web, en ejecución, para permitir un mayor descubrimiento de cualquier vulnerabilidad.
3	WSTG-INFO-03	Revisar archivos con metadata en búsqueda de divulgación de información	- Identificar rutas y funcionalidades ocultas u ofuscadas mediante el análisis de archivos de metadatos. - Extraer y mapear otra información que pueda conducir a una mejor comprensión de los sistemas en cuestión.
4	WSTG-INFO-04	Enumerar las aplicaciones en el servidor web	- Enumerar las aplicaciones que existen dentro del ámbito en un servidor web.
5	WSTG-INFO-05	Revisar los comentarios y metadata de las páginas web buscando divulgación de información	- Revisar los comentarios y metadatos de las páginas web para detectar cualquier fuga de información. - Recopilar archivos JavaScript y revisar el código JS para comprender mejor la aplicación y encontrar cualquier fuga de información. - Identificar si existen archivos de mapeo de origen (source map files) u otros archivos de depuración front-end.
6	WSTG-INFO-06	Identificar los puntos de entrada de las aplicaciones	- Identificar posibles puntos de entrada e inyección a través de solicitudes y análisis de respuesta.
7	WSTG-INFO-07	Mapear las rutas de ejecución a través de las aplicaciones	- Mapear la aplicación de destino y comprender los principales flujos de trabajo.
8	WSTG-INFO-08	Identificar el Framework usado por las aplicaciones	- Identificar los componentes utilizados por las aplicaciones web.
9	WSTG-INFO-09	Identificar la aplicación	- Identificar los componentes utilizados por las aplicaciones web.
10	WSTG-INFO-10	Mapear la arquitectura de las aplicaciones	- Generar un mapa de la aplicación basado en la investigación conducido.

Nro. Control	CODIGO OWASP	PRUEBA POR REALIZAR	Objetivos
Evaluación de la Gestión de Configuración y Despliegue			
11	WSTG-CONF-01	Evaluar la configuración de la red/infraestructura	- Revise las configuraciones de las aplicaciones establecidas en la red y valide que no sean vulnerables. - Validar que los marcos y sistemas utilizados sean seguros y no susceptibles a vulnerabilidades conocidas debido a software no mantenido o configuraciones y credenciales predeterminadas
12	WSTG-CONF-02	Evaluar la configuración de la plataforma de las aplicaciones	- Asegurarse de que se hayan eliminado las configuraciones predeterminadas y los archivos conocidos. - Validar que no queda código de depuración ni extensiones en los entornos de producción. - Revise los mecanismos de registro establecidos para la aplicación.
13	WSTG-CONF-03	Evaluar el manejo de las extensiones de nombres de archivos en búsqueda de información sensible	- Realizar un escaneo de directorios en busca de extensiones de archivo sensibles o que puedan contener datos sin procesar (por ejemplo, scripts, datos sin procesar, credenciales, etc.) - Validar que no existan bypass de marco del sistema en las reglas establecidas
14	WSTG-CONF-04	Buscar información sensible en archivos de copia de seguridad y no referenciados	- Encontrar y analizar archivos no referenciados que puedan contener información sensible. información.
15	WSTG-CONF-05	Enumerar las interfaces de administración de infraestructura y de las aplicaciones	- Identificar las interfaces y funcionalidades ocultas del administrador.
16	WSTG-CONF-06	Evaluar los métodos HTTP	- Enumera los métodos HTTP soportados - Prueba de anulación del control de acceso. - Prueba de vulnerabilidades XST. - Pruebe las técnicas de anulación de métodos HTTP.
17	WSTG-CONF-07	Evaluar la seguridad estricta en el transporte vía HTTP	- Revise el encabezado HSTS y su validez.
18	WSTG-CONF-08	Evaluar el cumplimiento de las políticas de "dominio s cruzados" para las aplicaciones tipo RIA (aplicaciones de Internet enriquecidas)	- Revisar y validar los archivos de políticas.

Nro. Control	CODIGO OWASP	PRUEBA POR REALIZAR	Objetivos
Evaluación de la Gestión de Configuración y Despliegue			
19	WSTG-CONF-09	Permiso de archivos de prueba	- Revisar e identificar cualquier permiso de archivo no autorizado.
20	WSTG-CONF-10	Prueba de toma de control de subdominios	- Enumerar todos los dominios posibles (anteriores y actuales). - Identificar dominios olvidados o mal configurados.
21	WSTG-CONF-11	Prueba de almacenamiento en la nube	- Evalúe que la configuración de control de acceso para el almacenamiento servicios esté debidamente implantado.

Nro. Control	CODIGO OWASP	PRUEBA POR REALIZAR	Objetivos
Evaluación de la Gestión de la identidad			
22	WSTG-IDNT-01	Evaluar las definiciones de roles	- Identificar y documentar los roles utilizados por la aplicación. - Intentar cambiar, modificar o acceder a otro rol. - Revise la granularidad de los roles y las necesidades detrás de los permisos otorgados.
23	WSTG-IDNT-02	Evaluar los procesos de registro de usuarios	- Compruebe que los requisitos de identidad para el registro de usuarios son los siguientes alineados con los requisitos empresariales y de seguridad. - Validar el proceso de registro.
24	WSTG-IDNT-03	Evaluar el proceso de provisionamiento de las cuentas de usuario	- Verificar qué cuentas pueden aprovisionar otras cuentas y de qué tipo.
25	WSTG-IDNT-04	Evaluar la enumeración de cuentas de usuario y las "cuentas adivinables"	- Revisar los procesos relativos a la identificación de usuarios (*ej. registro, inicio de sesión, etc.). - Enumerar a los usuarios cuando sea posible mediante el análisis de las respuestas.
26	WSTG-IDNT-05	Evaluar las políticas débiles o no forzadas para nombres de usuarios	- Determinar si una estructura de nombres de cuenta coherente hace que la aplicación vulnerable a la enumeración de cuentas. - Determine si los mensajes de error de la aplicación permiten la enumeración de cuentas.

Nro. Control	CODIGO OWASP	PRUEBA POR REALIZAR	Objetivos
Evaluación de la Gestión de la Autenticación			
27	WSTG-ATHN-01	Evaluación de credenciales transportadas sobre un canal no encriptado	- Evaluar si algún caso de uso del sitio web o la aplicación hace que el servidor o el cliente intercambien credenciales sin cifrado.
28	WSTG-ATHN-02	Evaluar las credenciales default	- Enumerar las aplicaciones para las credenciales predeterminadas y validar si aún existen. - Revisar y evaluar las nuevas cuentas de usuario y si se crean con algún valor predeterminado o patrones identificables
29	WSTG-ATHN-03	Evaluar los mecanismos débiles de bloqueo de cuentas	- Evaluar la capacidad del mecanismo de bloqueo de cuentas para mitigar los intentos de adivinanza de contraseñas por fuerza bruta. - Evaluar la resistencia del mecanismo de desbloqueo ante el desbloqueo no autorizado de cuentas.
30	WSTG-ATHN-04	Evaluar la evasión del esquema de autenticación	- Asegúrese de que la autenticación se aplica en todos los servicios que lo requieren.
31	WSTG-ATHN-05	Evaluar la funcionalidad de recordar contraseña	- Validar que la sesión generada se gestione de forma segura y no ponga en peligro las credenciales del usuario.
32	WSTG-ATHN-06	Evaluar las debilidades del caché del browser	- Revise si la aplicación almacena información sensible en el lado del cliente. - Revisar si se puede acceder sin autorización
33	WSTG-ATHN-07	Evaluar las políticas de contraseña débiles	- Determinar la resistencia de la aplicación contra los intentos de adivinanza de contraseñas por fuerza bruta utilizando diccionarios de contraseñas disponibles, evaluando la longitud, complejidad, reutilización y requisitos de antigüedad de las contraseñas.
34	WSTG-ATHN-08	Evaluar los mecanismos débiles de recuperación de acceso mediante pregunta/respuesta	- Evaluar la complejidad y cuán directas son las preguntas. - Evaluar las posibles respuestas de los usuarios y las capacidades de fuerza bruta
35	WSTG-ATHN-09	Evaluar funcionalidades débiles de cambio de contraseña o reinicialización	- Determinar la resistencia de la aplicación a la subversión del proceso de cambio de cuenta que permita a alguien cambiar la contraseña de una cuenta.

Nro. Control	CODIGO OWASP	PRUEBA POR REALIZAR	Objetivos
Evaluación de la Gestión de la Autenticación			
			- Determinar la resistencia de la funcionalidad de restablecimiento de contraseñas contra adivinación o evasión.
36	WSTG-ATHN-10	Evaluar autenticaciones débiles mediante canales alternos	- Identificar canales de autenticación alternativos. - Evalúe las medidas de seguridad utilizadas y si existe algún bypass en los canales alternativos.

Nro. Control	CODIGO OWASP	PRUEBA POR REALIZAR	Objetivos
Evaluación de Autorización			
37	WSTG-ATHZ-01	Evaluar el recorrido de directorios/inclusión de archivos	- Identificar los puntos de inyección relacionados con el recorrido. - Evalúe las técnicas de derivación e identifique el alcance del cruce de rutas.
38	WSTG-ATHZ-02	Evaluar la evasión del esquema de autorización	- Evaluar si es posible el acceso horizontal o vertical.
39	WSTG-ATHZ-03	Evaluar el escalamiento de privilegios	- Identificar puntos de inyección relacionados con la manipulación de privilegios. - Realizar pruebas de fuzzing o intentar de otro modo eludir las medidas de seguridad.
40	WSTG-ATHZ-04	Evaluar las referencias inseguras a objetos de forma directa	- Identificar puntos donde pueden ocurrir referencias a objetos. - Evaluar las medidas de control de acceso y si son vulnerables a IDOR (Insecure Direct Object References).

Nro. Control	CODIGO OWASP	PRUEBA POR REALIZAR	Objetivos
Evaluar el Manejo de Sesiones			
41	WSTG-SESS-01	Evaluar la evasión del esquema de manejo de sesiones	- Recopilar tokens de sesión, para el mismo usuario y para diferentes usuarios cuando sea posible. - Analizar y asegurarse de que exista suficiente aleatoriedad para detener los ataques de falsificación de sesiones. - Modificar cookies que no estén firmadas y contengan información que pueda manipularse
42	WSTG-SESS-02	Evaluar los atributos de las cookies	- Asegúrese de que se ha establecido la configuración de seguridad adecuada para las cookies.

Nro. Control	CODIGO OWASP	PRUEBA POR REALIZAR	Objetivos
Evaluar el Manejo de Sesiones			
43	WSTG-SESS-03	Evaluar la "fijación" de sesiones	- Analizar el mecanismo de autenticación y su flujo. - Forzar las cookies y evaluar el impacto.
44	WSTG-SESS-04	Evaluar variables de sesión expuestas	- Asegurarse de que se implemente una encriptación adecuada. - Revisar la configuración de caché. - Evaluar la seguridad del canal y de los métodos.
45	WSTG-SESS-05	Evaluar la ocurrencia de falsificación de requerimientos cruzados (Cross Site Request Forgery)	- Determinar si es posible iniciar solicitudes en nombre de un usuario que no sean iniciadas por el propio usuario.
46	WSTG-SESS-06	Evaluar la funcionalidad de termino de sesión (logout)	- Evaluar la interfaz de usuario de cierre de sesión. - Analizar el tiempo de espera de la sesión y verificar si la sesión se cierra correctamente después del cierre de sesión.
47	WSTG-SESS-07	Evaluar el tiempo máximo de inactividad por sesión	- Validar que exista un tiempo de espera de sesión estricto.
48	WSTG-SESS-08	Evaluar el uso inapropiado de variables de sesión (Session puzzling).	- Identificar todas las variables de sesión. - Romper el flujo lógico de generación de sesiones.
49	WSTG-SESS-09	Pruebas de secuestro de sesión	- Identificar cookies de sesión vulnerables. - Secuestrar cookies vulnerables y evaluar el nivel de riesgo.

Nro. Control	CODIGO OWASP	PRUEBA POR REALIZAR	Objetivos
Evaluar la Validación de Datos			
50	WSTG-INPV-01	Evaluar Cross Site Scripting Reflejado	- Identificar las variables que se reflejan en las respuestas. - Evaluar la entrada que aceptan y la codificación que se aplica al devolverla (si corresponde).
51	WSTG-INPV-02	Evaluar Cross Site Scripting Almacenado	- Identificar la entrada almacenada que se refleja en el lado del cliente. - Evaluar la entrada que aceptan y la codificación que se aplica al devolverla (si corresponde)
52	WSTG-INPV-03	Evaluar la manipulación de verbos HTTP	- Enumerar los métodos HTTP admitidos. - Prueba de omisión del control de acceso. - Pruebe las vulnerabilidades de XST.

Nro. Control	CODIGO OWASP	PRUEBA POR REALIZAR	Objetivos
Evaluar la Validación de Datos			
			- Pruebe las técnicas de anulación del método HTTP.
53	WSTG-INPV-04	Evaluar la "contaminación" de parámetros HTTP	- Identificar el backend y el método de análisis utilizado. - Evaluar los puntos de inyección e intentar eludir los filtros de entrada utilizando HPP (HTTP Parameter Pollution).
54	WSTG-INPV-05	Evaluar inyecciones de SQL	- Identificar los puntos de inyección SQL. - Evaluar la gravedad de la inyección y el nivel de acceso que se puede lograr a través de ella
55	WSTG-INPV-06	Evaluar inyecciones de LDAP	- Identificar los puntos de inyección LDAP. - Evaluar la gravedad de la inyección.
56	WSTG-INPV-07	Evaluar inyecciones de XML	- Identificar los puntos de inyección XML. - Evaluar los tipos de exploits que se pueden obtener y su gravedad.
57	WSTG-INPV-08	Evaluar inyecciones de SSI	- Identificar los puntos de inyección SSI. - Evaluar la gravedad de la inyección.
58	WSTG-INPV-09	Evaluar inyecciones de XPath	- Identificar los puntos de inyección XPATH
59	WSTG-INPV-10	Evaluar inyecciones IMAP/SMTP	- Identificar los puntos de inyección IMAP/SMTP. - Comprender el flujo de datos y la estructura de despliegue del sistema. - Evaluar los impactos de la inyección
60	WSTG-INPV-11	Evaluar inyecciones de código	- Identificar los puntos de inyección donde se puede inyectar código en la aplicación. - Evaluar la gravedad de la inyección.
61	WSTG-INPV-12	Evaluar inyecciones de comandos	- Identificar y evaluar los puntos de inyección de comandos.
62	WSTG-INPV-13	Pruebas de inyección de cadenas de formato	- Evaluar si la inyección de especificadores de conversión de cadenas de formato en campos controlados por el usuario causa un comportamiento no deseado en la aplicación.
63	WSTG-INPV-14	Evaluar vulnerabilidades incubadas	- Identificar inyecciones que son almacenadas y requieren un paso de recuperación para la inyección almacenada. - Comprender cómo podría ocurrir un paso de recuperación. - Configurar escuchas o activar el paso de recuperación si es posible.

Nro. Control	CODIGO OWASP	PRUEBA POR REALIZAR	Objetivos
Evaluar la Validación de Datos			
64	WSTG-INPV-15	Pruebas de contrabando de división HTTP	- Evaluar si la aplicación es vulnerable a la división, identificando qué posibles ataques se pueden lograr. - Evaluar si la cadena de comunicación es vulnerable al contrabando, identificando qué posibles ataques se pueden lograr.
65	WSTG-INPV-16	Pruebas de solicitudes entrantes HTTP	- Monitorear todas las solicitudes HTTP entrantes y salientes al servidor web para inspeccionar cualquier solicitud sospechosa. - Monitorear el tráfico HTTP sin cambios en el proxy del navegador del usuario final o en la aplicación del lado del cliente
66	WSTG-INPV-17	Pruebas de inyección de encabezado de host	- Evaluar si el encabezado Host se analiza dinámicamente en la aplicación. - Eludir los controles de seguridad que dependen del encabezado.
67	WSTG-INPV-18	Pruebas de inyección de plantillas en el servidor	- Detectar puntos de vulnerabilidad de inyección de plantillas. - Identificar el motor de plantillas. - Construir el exploit.
68	WSTG-INPV-19	Pruebas de falsificación de peticiones del lado del servidor	- Identificar los puntos de inyección SSRF. - Probar si los puntos de inyección son explotables. - Evaluar la gravedad de la vulnerabilidad

Nro. Control	CODIGO OWASP	PRUEBA POR REALIZAR	Objetivos
Error Handling			
69	OTG-ERR-001	Análisis de códigos de error	- Identificar la salida de error existente. - Analiza los diferentes resultados devueltos.
70	OTG-ERR-002	Análisis de trazados de pila	- Determinar si es posible inferir la lógica de procesos y otras interioridades de la aplicación, producto de una mala gestión de la pila de mensajes de excepciones que pueden desencadenarse bajo ciertas operaciones.

Nro. Control	CODIGO OWASP	PRUEBA POR REALIZAR	Objetivos
Criptografía			

71	WSTG-CRYP-01	Evaluar cifrados débiles de SSL/TSL, protección protecciones insuficientes en el transporte	- Validar la configuración del servicio. - Revise la fuerza criptográfica y la validez del certificado digital. - Asegúrese de que la seguridad TLS no se puede eludir y de que está correctamente implementada en toda la aplicación.
72	WSTG-CRYP-02	Evaluar ataques del tipo "Padding Oracle"	- Identificar los mensajes cifrados que se basan en el relleno. - Intentar romper el relleno de los mensajes cifrados y analizar los mensajes de error devueltos para su posterior análisis.
73	WSTG-CRYP-03	Evaluar información sensible enviada por canales no encriptados.	- Identificar la información sensible transmitida a través de los distintos canales. - Evaluar la privacidad y seguridad de los canales utilizados.
74	WSTG-CRYP-04	Pruebas de cifrado débil	- Proporcionar una directriz para la identificación de cifrado débil o usos e implementaciones de hashing.

Nro. Control	CODIGO OWASP	PRUEBA POR REALIZAR	Objetivos
Evaluación de la Lógica de Negocio			
75	WSTG-BUSL-01	Evaluar la validación de datos de la lógica negocio	- Identificar los puntos de inyección de datos. - Validar que todas las comprobaciones se realizan en el back- end y no pueden eludirse. - Intentar romper el formato de los datos esperados y analizar cómo lo gestiona la aplicación.
76	WSTG-BUSL-02	Evaluar la posibilidad de falsificar peticiones	- Revise la documentación del proyecto en busca de funcionalidades adivinables, predecibles u ocultas de los campos. - Insertar datos lógicamente válidos para eludir la actividad normal flujo de trabajo lógico.
77	WSTG-BUSL-03	Evaluar los controles de integridad	- Revise la documentación del proyecto para conocer los componentes del sistema que mueven, almacenan o manejan datos. - Determine qué tipo de datos son lógicamente aceptables por el componente y contra qué tipos debe protegerse el sistema. - Determine quién debe estar autorizado a modificar o leer esos datos en cada componente.

Nro. Control	CODIGO OWASP	PRUEBA POR REALIZAR	Objetivos
Evaluación de la Lógica de Negocio			
			- Intento de insertar, actualizar o eliminar valores de datos utilizados por cada componente que no deberían estar permitidos por la lógica empresarial.
78	WSTG-BUSL-04	Evaluar el tiempo de procesamiento	- Revise la documentación del proyecto en busca de funcionalidades del sistema que puedan verse afectadas por el tiempo. - Desarrollar y ejecutar casos de uso indebido.
79	WSTG-BUSL-05	Evaluar la cantidad de veces que una función puede ser usada sin límites	- Identificar las funciones que deben establecer límites a las veces que pueden ser llamadas. - Evaluar si hay un límite lógico establecido en las funciones y si es debidamente validada.
80	WSTG-BUSL-06	Evaluar las desviaciones en flujos de trabajo	- Revise la documentación del proyecto en busca de métodos para omitir o realizar los pasos del proceso de aplicación en un orden distinto al flujo lógico empresarial previsto. - Desarrollar un caso de uso indebido y tratar de eludir cada flujo lógico identificado.
81	WSTG-BUSL-07	Evaluar las defensas ante malos usos de las aplicaciones	- Generar notas de todas las pruebas realizadas con el sistema. - Revisar qué pruebas tenían una funcionalidad diferente en función de la entrada agresiva. - Comprender las defensas existentes y verificar si son suficientes para proteger el sistema contra las técnicas de evasión.
82	WSTG-BUSL-08	Evaluar la carga de archivos de tipos no esperados	- Revise la documentación del proyecto para conocer los tipos de archivo que rechaza el sistema. - Compruebe que los tipos de archivo no deseados se rechazan y se gestionan de forma segura. - Compruebe que las cargas de archivos por lotes son seguras y no permiten ninguna saltarse las medidas de seguridad establecidas.
83	WSTG-BUSL-09	Evaluar la carga de archivos con contenido malicioso	- Identifique la funcionalidad de carga de archivos. - Revise la documentación del proyecto para identificar qué tipos de archivos se consideran aceptables y qué tipos se considerarían peligrosos o maliciosos. - Determina cómo se procesan los archivos cargados.

Nro. Control	CODIGO OWASP	PRUEBA POR REALIZAR	Objetivos
Evaluación de la Lógica de Negocio			
			- Obtener o crear un conjunto de archivos maliciosos para las pruebas. - Intenta subir los archivos maliciosos a la aplicación y determina si es aceptada y procesada.

Nro. Control	CODIGO OWASP	PRUEBA POR REALIZAR	Objetivos
Evaluación del Lado Cliente			
84	WSTG-CLNT-01	Evaluar Cross Site Scripting basados en DOM (Document Object Model)	- Identificar los sumideros de DOM. - Construye cargas útiles que correspondan a cada tipo de sumidero.
85	WSTG-CLNT-02	Evaluar la ejecución de JavaScript	- Identificar sumideros y posibles puntos de inyección de JavaScript.
86	WSTG-CLNT-03	Evaluar inyecciones de HTML	- Identificar los puntos de inyección HTML y evaluar la gravedad del contenido inyectado.
87	WSTG-CLNT-04	Evaluar redirecciones de URL en el Lado Cliente	- Identificar puntos de inyección que manejen URLs o rutas. - Evalúe las ubicaciones a las que podría redirigirse el sistema.
88	WSTG-CLNT-05	Evaluar inyecciones de CSS	- Identificar los puntos de inyección de CSS. - Evaluar el impacto de la inyección.
89	WSTG-CLNT-06	Evaluar la manipulación de recursos del Lado Cliente	- Identificar sumideros con validación de entrada débil. - Evaluar el impacto de la manipulación de los recursos.
90	WSTG-CLNT-07	Evaluar "Cross Origin Resource Sharing"	- Identificar los puntos finales que implementan CORS. - Asegúrese de que la configuración CORS es segura o inocua.
91	WSTG-CLNT-08	Evaluar "Cross Site Flashing"	- Descompilar y analizar el código de la aplicación. - Evaluar las entradas de los sumideros y los usos de métodos inseguros.
92	WSTG-CLNT-09	Evaluar "Clickjacking"	- Comprender las medidas de seguridad existentes. - Evalúe lo estrictas que son las medidas de seguridad y si se pueden eludir.
93	WSTG-CLNT-10	Evaluar WebSockets	- Identificar el uso de WebSockets. - Evalúe su aplicación utilizando las mismas pruebas en canales HTTP normales.

Nro. Control	CODIGO OWASP	PRUEBA POR REALIZAR	Objetivos
Evaluación del Lado Cliente			
94	WSTG-CLNT-11	Evaluar "Web Messaging" (Cross Document Messaging)	- Evaluar la seguridad del origen del mensaje. - Validar que está utilizando métodos seguros y validar su entrada.
95	WSTG-CLNT-12	Evaluar almacenamiento local	- Determine si el sitio web almacena datos confidenciales en el almacenamiento del lado del cliente. - El manejo de código de los objetos de almacenamiento debe ser examinado para posibilidades de ataques de inyección, como la utilización de entradas no validadas o bibliotecas vulnerables.
96	WSTG-CLNT-13	Pruebas de inclusión de scripts en sitios cruzados	- Localizar datos sensibles en todo el sistema. - Evaluar la fuga de datos sensibles mediante diversas técnicas.

Nro. Control	CODIGO OWASP	PRUEBA POR REALIZAR	Objetivos
API Testing			
97	WSTG-APIT-01	Testing GraphQL	- Evaluar que se despliega una configuración segura y lista para la producción. - Validar todos los campos de entrada contra ataques genéricos. - Asegúrese de que se aplican los controles de acceso adecuados.

- Pruebas para aplicaciones de desktop

Nro. Control	CODIGO OWASP	PRUEBA POR REALIZAR	Objetivos
1	DA1	Inyecciones	- Evaluar las Inyecciones SQL; LDAP, XML inyección de comandos del sistema operativo, etc. ocurren cuando se pasa una entrada que no es de confianza al intérprete como parte de una consulta/comando.

Nro. Control	CODIGO OWASP	PRUEBA POR REALIZAR	Objetivos
2	DA2	Autenticación interrumpida y gestión de sesiones	- Evaluar la autenticación rota y gestión de sesiones Autenticación de cuenta de SO, Escritorio, Aplicación y gestión de sesión, autenticación para importación/exportación con unidad externa, autenticación para unidades compartidas de red u otros dispositivos periféricos.
3	DA3	Exposición de datos confidenciales	- Exposición de datos confidenciales, datos en la memoria después del cierre de sesión de la aplicación, registros con información confidencial, secretos codificados en archivos, etc.
4	DA4	Uso inadecuado de la criptografía	- Evaluar el uso incorrecto de criptografía debido a algoritmos criptográficos obsoletos o claves débiles, uso inadecuado de funciones criptográficas, reutilización de parámetros criptográficos en todas las instalaciones, uso inadecuado de criptografía para verificación de integridad
5	DA5	Autorización indebida	- Autorización Indebida, estas incluyen permisos débiles de archivos/carpetas por rol de usuario, falta del principio del enfoque de privilegios mínimos, roles de usuario inadecuados, registro no autorizado o acceso a variables de entorno
6	DA6	Configuración incorrecta de seguridad	- Evaluar la configuración incorrecta de seguridad las fallas incluyen políticas de grupo / registro / reglas de firewall mal configuradas, etc., tipo de archivo faltante / verificación de contenido para aplicaciones de procesamiento de archivos, canalizaciones con nombre mal configuradas, servicios de soporte mal configurados utilizados por la aplicación, servicios de terceros mal configurados (SQL, AD, etc.).

Nro. Control	CODIGO OWASP	PRUEBA POR REALIZAR	Objetivos
7	DA7	Comunicación insegura	- Evaluar la Comunicación Insegura Cuando cualquier aplicación necesita comunicarse con los servicios remotos, como servidores SQL remotos, servicios web, transferencia de archivos, envío de comandos o cualquier otro proceso que se ejecuta en el servidor remoto, pero utiliza protocolos de comunicación de texto sin formato para consumir servicios, dichas vulnerabilidades se incluyen en Comunicación insegura. Los problemas de comunicación insegura incluyen el uso de protocolos de comunicación de texto sin formato como FTP, TELNET, HTTP, MQTT, WS, etc. o el uso de protocolos/conjuntos de cifrado TLS/DTLS débiles, conexiones de base de datos de texto sin formato, uso de certificados auto firmados para comunicación de canal seguro, etc.
8	DA8	Mala calidad del código	- Evaluar la mala calidad de código tal como el uso de software obsoleto o uso de componentes/servicios obsoletos de Windows/proveedores externos
9	DA9	Uso de componentes con vulnerabilidades conocidas	- Evaluar el uso de componentes con vulnerabilidades conocidas Uso de software obsoleto o uso de componentes o servicios obsoletos de Windows o de proveedores externos
10	DA10	Registro y monitoreo insuficientes	- Evaluar los registros y supervisión insuficiente o inadecuado, control periódico inexistente para detectar abusos

c) NORMA NIST Cyber Security Framework (Instituto Nacional de Estándares y Tecnología)

FUNCIÓN 1: GOVERN (GV) - GOBERNANZA		
GV.OC - Contexto Organizacional		
ID	Subcategoría	Descripción
GV.OC-01	Misión Organizacional	La misión organizacional se entiende para priorizar la gestión de riesgos de ciberseguridad
GV.OC-02	Expectativas de Partes Interesadas	Se determinan las partes interesadas internas y externas y sus expectativas sobre la gestión de riesgos
GV.OC-03	Requisitos Legales y Regulatorios	Se entienden y gestionan los requisitos legales, regulatorios y contractuales
GV.OC-04	Objetivos Críticos	Se determinan y comunican objetivos, capacidades y servicios críticos
GV.OC-05	Dependencias Organizacionales	Se determinan y comunican resultados, capacidades y servicios críticos de los que depende la organización
GV.RM - Estrategia de Gestión de Riesgos		
ID	Subcategoría	Descripción
GV.RM-01	Objetivos de Gestión de Riesgos	Se establecen objetivos de gestión de riesgos de ciberseguridad acordados por las partes interesadas
GV.RM-02	Estrategia de Cadena de Suministro	Se establece estrategia de gestión de riesgos de cadena de suministro de ciberseguridad
GV.RM-03	Apetito y Tolerancia al Riesgo	Se determinan y comunican declaraciones de apetito y tolerancia al riesgo
GV.RM-04	Integración Empresarial	La gestión de riesgos de ciberseguridad se considera parte de la gestión de riesgos empresariales
GV.RM-05	Marco de Gestión de Riesgos	Se establece, comunica y mantiene un marco de gestión de riesgos de ciberseguridad
GV.RM-06	Planificación de Riesgos	Los planes de gestión de riesgos de ciberseguridad incluyen roles, responsabilidades y autoridades
GV.RM-07	Riesgos Positivos	Se consideran riesgos positivos en las discusiones de riesgos de ciberseguridad organizacionales
GV.RR - Roles, Responsabilidades y Autoridades		
ID	Subcategoría	Descripción
GV.RR-01	Liderazgo Organizacional	El liderazgo organizacional es responsable de los resultados de ciberseguridad
GV.RR-02	Roles y Responsabilidades	Se asignan y comunican roles y responsabilidades de ciberseguridad
GV.RR-03	Recursos Adecuados	Se proporcionan recursos adecuados para respaldar los roles de ciberseguridad
GV.RR-04	Prácticas de Recursos Humanos	La ciberseguridad se incluye en las prácticas de recursos humanos
GV.PO - Política		
ID	Subcategoría	Descripción
GV.PO-01	Política Organizacional	Se establece una política organizacional de ciberseguridad
GV.PO-02	Comunicación de Política	Se comunica la política a las partes interesadas organizacionales

GV.OV - Supervisión		
ID	Subcategoría	Descripción
GV.OV-01	Estrategia de Supervisión	Se evalúa estratégicamente la estrategia de gestión de riesgos de ciberseguridad
GV.OV-02	Supervisión de Resultados	Los resultados de la estrategia de gestión de riesgos de ciberseguridad se revisan para informar mejoras
GV.OV-03	Rendimiento General	Se evalúa el rendimiento general del programa de ciberseguridad
GV.SC - Gestión de Riesgos de Cadena de Suministro		
ID	Subcategoría	Descripción
GV.SC-01	Política de Cadena de Suministro	Se establece una política de cadena de suministro de ciberseguridad
GV.SC-02	Identificación de Proveedores	Se identifican proveedores de tecnología y su lugar en la cadena de suministro
GV.SC-03	Contratos con Terceros	Los contratos con proveedores incluyen disposiciones para abordar riesgos de ciberseguridad
GV.SC-04	Planificación de Proveedores	La planificación incluye proveedores y otros terceros
GV.SC-05	Respuesta a Cambios en el Riesgo	Los planes de respuesta abordan cambios en el riesgo de los proveedores
GV.SC-06	Evaluación de Proveedores	La planificación incluye la evaluación de la criticidad y sensibilidad de lo que los proveedores brindan
GV.SC-07	Evaluación de Riesgos de Proveedores	Los riesgos de los proveedores se evalúan antes de la adquisición
GV.SC-08	Evaluación de Controles de Proveedores	Se evalúan los controles relevantes de proveedores que son críticos
GV.SC-09	Monitoreo de Proveedores	Se monitorean las prácticas de seguridad de los proveedores durante el ciclo de vida
GV.SC-10	Gestión de Incidentes de Proveedores	Los planes incluyen a los proveedores en la gestión de incidentes
FUNCIÓN 2: IDENTIFY (ID) - IDENTIFICAR		
ID.AM - Gestión de Activos		
ID	Subcategoría	Descripción
ID.AM-01	Inventario de Activos Físicos	Se inventarían los activos físicos dentro de la organización
ID.AM-02	Inventario de Activos de Software	Se inventarían los activos de software dentro de la organización
ID.AM-03	Comunicación y Flujos de Datos	Se mapean los flujos de comunicación y datos organizacionales
ID.AM-04	Servicios Externos	Se catalogan los servicios externos
ID.AM-05	Clasificación de Recursos	Los recursos se clasifican según su criticidad para los objetivos organizacionales
ID.AM-06	Roles de Ciberseguridad	Se establecen roles de ciberseguridad y responsabilidades para todo el personal
ID.AM-07	Inventario de Datos	Se mantienen inventarios de datos y metadatos correspondientes
ID.AM-08	Sistemas que Almacenan Datos	Se identifican los sistemas que almacenan, procesan o transmiten datos

ID.RA - Evaluación de Riesgos		
ID	**Subcategoría**	**Descripción**
ID.RA-01	Identificación de Vulnerabilidades	Se identifican y documentan las vulnerabilidades de los activos
ID.RA-02	Inteligencia de Amenazas	Se recibe y analiza inteligencia de amenazas de múltiples fuentes
ID.RA-03	Amenazas Internas y Externas	Se identifican las amenazas internas y externas a la organización
ID.RA-04	Impactos Potenciales	Se identifican los impactos potenciales y la probabilidad de que ocurran
ID.RA-05	Amenazas, Vulnerabilidades e Impactos	Se usan amenazas, vulnerabilidades e impactos para determinar el riesgo
ID.RA-06	Identificación y Priorización de Riesgos	Se identifican y priorizan los riesgos de respuesta
ID.RA-07	Monitoreo de Cambios en Riesgos	Se monitorean los cambios en los riesgos con el tiempo
ID.RA-08	Evaluación de Eficacia de Respuesta	Se evalúa la eficacia de la respuesta al riesgo
ID.RA-09	Autenticidad e Integridad del Hardware	Se evalúa la autenticidad e integridad del hardware y software
ID.RA-10	Criticidad de Proveedores	Se evalúa la criticidad de los proveedores de software, hardware y servicios
FUNCIÓN 3: PROTECT (PR) - PROTEGER		
PR.AA - Control de Acceso e Identidad		
ID	**Subcategoría**	**Descripción**
PR.AA-01	Gestión de Identidades y Credenciales	Se gestionan identidades y credenciales para usuarios autorizados
PR.AA-02	Control de Acceso Físico	Se gestiona el acceso físico a activos
PR.AA-03	Acceso Remoto	Se gestiona el acceso remoto
PR.AA-04	Permisos de Acceso	Se gestionan los permisos de acceso mediante principios de menor privilegio
PR.AA-05	Integridad de Red	Se protege la integridad de la red
PR.AA-06	Autenticación de Identidades	Las identidades se autentican de manera acorde al riesgo de la transacción
PR.AT - Concienciación y Entrenamiento		
ID	**Subcategoría**	**Descripción**
PR.AT-01	Concienciación del Personal	Todo el personal está informado y entrenado
PR.AT-02	Usuarios Privilegiados	Los usuarios privilegiados comprenden roles y responsabilidades
PR.DS - Seguridad de Datos		
ID	**Subcategoría**	**Descripción**
PR.DS-01	Protección de Datos en Reposo	Se protegen los datos en reposo
PR.DS-02	Protección de Datos en Tránsito	Se protegen los datos en tránsito
PR.DS-03	Gestión de Activos durante Ciclo de Vida	Se gestionan los activos durante remoción, transferencias y disposición
PR.DS-04	Capacidad Adecuada	Se mantiene capacidad adecuada para garantizar disponibilidad

PR.DS-05	Protección contra Fuga de Datos	Se implementan protecciones contra fuga de datos
PR.DS-06	Verificación de Integridad	Se verifica la integridad de software, firmware e información
PR.DS-07	Entorno de Desarrollo y Pruebas	Los entornos de desarrollo y pruebas se separan del entorno de producción
PR.DS-08	Verificación de Integridad de Hardware y Software	Se verifica la integridad del hardware y software durante desarrollo
PR.IR - Procesos y Procedimientos de Protección de Información		
ID	**Subcategoría**	**Descripción**
PR.IR-01	Políticas de Protección	Se mantiene una política de protección de información
PR.IR-02	Gestión de Configuración	Se implementa gestión de configuración de sistemas organizacionales
PR.MA - Mantenimiento		
ID	**Subcategoría**	**Descripción**
PR.MA-01	Mantenimiento de Activos Organizacionales	Se realiza mantenimiento de activos organizacionales
PR.MA-02	Mantenimiento Remoto	El mantenimiento remoto se autoriza, monitorea y registra
PR.PT - Tecnología de Protección		
ID	**Subcategoría**	**Descripción**
PR.PT-01	Configuración de Sistemas de Auditoría	Se auditan las configuraciones de sistemas organizacionales
PR.PT-02	Eliminación de Componentes Removibles	Los medios removibles se protegen y su uso se restringe
PR.PT-03	Control de Acceso a Configuraciones	El acceso a configuraciones de sistemas se controla
PR.PT-04	Comunicaciones y Control de Redes	Las redes de comunicaciones se gestionan y controlan
PR.PT-05	Mecanismos de Control de Tecnología	Se implementan mecanismos para lograr resistencia a los requisitos
FUNCIÓN 4: DETECT (DE) - DETECTAR		
DE.AE - Anomalías y Eventos		
ID	**Subcategoría**	**Descripción**
DE.AE-01	Establecimiento de Líneas Base	Se establecen y gestionan líneas base de actividades de red y datos esperados
DE.AE-02	Análisis de Eventos Potencialmente Adversos	Los eventos potencialmente adversos se analizan
DE.AE-03	Correlación de Información	La información de eventos se correlaciona desde múltiples fuentes
DE.AE-04	Determinación de Impacto	Se determina el impacto de los eventos
DE.AE-05	Establecimiento de Umbrales de Alerta	Se establecen umbrales de alerta de incidentes
DE.AE-06	Inteligencia de Amenazas	La inteligencia de amenazas se integra en el análisis
DE.AE-07	Análisis de Amenazas	Las amenazas se analizan usando inteligencia relevante
DE.AE-08	Objetivos de Atacantes	Se analizan los objetivos de los adversarios

DE.CM - Monitoreo Continuo de Seguridad		
ID	Subcategoría	Descripción
DE.CM-01	Monitoreo de Redes	Las redes se monitorean para detectar eventos potencialmente adversos
DE.CM-02	Monitoreo del Entorno Físico	El entorno físico se monitorea para detectar eventos potencialmente adversos
DE.CM-03	Monitoreo de Personal	Las actividades del personal se monitorean para detectar eventos potencialmente adversos
DE.CM-04	Detección de Código Malicioso	Se detecta actividad de código malicioso
DE.CM-05	Monitoreo de Conexiones Externas	Se monitorean las conexiones de servicios externos no confiables
DE.CM-06	Monitoreo de Acceso Externo	Se monitorea el acceso externo a servicios
DE.CM-07	Monitoreo para Divulgación No Autorizada	Se monitorea para la divulgación no autorizada de información organizacional
DE.CM-08	Escaneo de Vulnerabilidades	Se realizan escaneos de vulnerabilidades
DE.CM-09	Monitoreo de Activos No Autorizados	Se monitorean activos de hardware, software, conexiones y dispositivos no autorizados
FUNCIÓN 5: RESPOND (RS) - RESPONDER		
RS.MA - Gestión de Respuesta		
ID	Subcategoría	Descripción
RS.MA-01	Ejecución de Planes de Respuesta	Se ejecutan los planes de respuesta a incidentes durante o después de un evento
RS.MA-02	Coordinación con Partes Interesadas	Se coordina la respuesta a incidentes con partes interesadas
RS.MA-03	Información Adicional	Se obtiene información adicional sobre incidentes
RS.MA-04	Clasificación de Incidentes	Los incidentes se clasifican y priorizan
RS.MA-05	Criterios para Escalamiento	Se establecen y siguen criterios para escalamiento e iniciación de recuperación
RS.AN - Análisis		
ID	Subcategoría	Descripción
RS.AN-01	Investigación de Incidentes	Se investigan los incidentes
RS.AN-02	Comprensión del Impacto	Se comprende el impacto del incidente
RS.AN-03	Análisis Forense	Se realiza análisis forense
RS.AN-04	Categorización de Incidentes	Los incidentes se categorizan de manera consistente
RS.AN-05	Procesos y Procedimientos	Se siguen procesos y procedimientos para el análisis de incidentes
RS.MI - Mitigación		
ID	Subcategoría	Descripción
RS.MI-01	Contención de Incidentes	Los incidentes se contienen
RS.MI-02	Mitigación de Incidentes	Los incidentes se mitigan
RS.MI-03	Mitigación de Vulnerabilidades	Las vulnerabilidades recién identificadas se mitigan o documentan como riesgos aceptados

FUNCIÓN 6: RECOVER (RC) - RECUPERAR		
RC.RP - Planificación de Recuperación		
ID	**Subcategoría**	**Descripción**
RC.RP-01	Ejecución del Plan de Recuperación	Se ejecuta el plan de recuperación durante o después de un evento de ciberseguridad
RC.RP-02	Selección de Estrategias de Recuperación	Las estrategias de recuperación se implementan para restaurar sistemas y activos
RC.RP-03	Alcance de Esfuerzos de Recuperación	El alcance de los esfuerzos de recuperación se comunica a las partes interesadas
RC.RP-04	Validación de Sistemas Restaurados	Los sistemas restaurados se verifican
RC.RP-05	Coordinación de Recuperación	Los procesos de recuperación se coordinan con partes internas y externas
RC.RP-06	Comunicación de Estado de Recuperación	El estado de recuperación se comunica a las partes interesadas
RC.CO - Comunicaciones		
ID	**Subcategoría**	**Descripción**
RC.CO-01	Gestión de Relaciones Públicas	Se gestiona la reputación pública después de un evento de ciberseguridad
RC.CO-02	Comunicación con Stakeholders	Los hallazgos de recuperación se comunican a las partes interesadas designadas
RC.CO-03	Comunicación de Actividades de Recuperación	Las actividades de recuperación se comunican a partes interesadas internas
RC.CO-04	Coordinación con Partes Externas	Se coordina con partes externas para las actividades de recuperación

d) ISO/TS 54001:2019 (Estándar para Sistemas de Gestión de Calidad - Requisitos específicos para la aplicación de la Norma ISO 9001:2015 a organizaciones electorales en todos los niveles de gobierno)

SECCIÓN
6. Riesgos
6.1 Acciones para abordar riesgos y oportunidades
6.2 Objetivos de la calidad y planificación para lograrlos
6.3 Planificación de los cambios
7. Apoyo
7.1.3 Infraestructura
7.1.4 Ambiente para la operación de los procesos

8. Operación
8.1 Planificación y control operacional
8.2 Requisitos para los productos y servicios
8.2.1 Comunicación con el cliente
8.2.2 Determinación de los requisitos para los productos y servicios
8.2.3 Revisión de los requisitos para los productos y servicios
8.2.4 Cambios en los requisitos para los productos y servicios
8.3 Diseño y desarrollo de los productos y servicios
8.3.1 Generalidades
8.3.2 Planificación del diseño y desarrollo
8.3.3 Entradas para el diseño y desarrollo
8.3.4 Controles del diseño y desarrollo
8.3.5 Salidas del diseño y desarrollo
8.3.6 Cambios del diseño y desarrollo
8.4 Control de los procesos, productos y servicios suministrados externamente
8.4.1 Generalidades
8.4.2 Tipo y alcance del control
8.4.3 Información para los proveedores externos
8.5 Producción y provisión del servicio
8.5.1 Control de la producción y de la provisión del servicio
8.5.2 Identificación y trazabilidad
8.5.3 Propiedad perteneciente a los clientes o proveedores externos
8.5.4 Preservación
8.5.5 Actividades posteriores a la entrega
8.5.6 Control de los cambios
8.6 Liberación de los productos y servicios
8.7 Control de las salidas no conformes

LISTADO DE MARCOS DE TRABAJO Y ESTANDARES DE REFERENCIA PARA LA EVALUACIÓN

a) LISTADO CAPEC - POR DOMINIOS DE ATAQUE

SECCIÓN	DETALLE
1	Software
1.1	Exploitation of Trusted Identifiers
1.2	Exploiting Trust in Client
1.3	Forced Deadlock
1.4	Leveraging Race Conditions
1.5	Fuzzing
1.6	Manipulating State
1.7	Adversary in the Middle (AiTM)
1.8	Brute Force
1.9	Interface Manipulation
1.10	Authentication Abuse
1.11	Authentication Bypass
1.12	Excavation
1.13	Interception
1.14	Privilege Abuse
1.15	Buffer Manipulation
1.16	Shared Resource Manipulation
1.17	Flooding
1.18	Pointer Manipulation
1.19	Excessive Allocation
1.20	Resource Leak Exposure
1.21	Parameter Injection
1.22	Content Spoofing
1.23	Identity Spoofing
1.24	Input Data Manipulation
1.25	Resource Location Spoofing
1.26	Infrastructure Manipulation
1.27	File Manipulation
1.28	Footprinting
1.29	Action Spoofing

SECCIÓN	DETALLE
1.30	Code Inclusion
1.31	Configuration/Environment Manipulation
1.32	Software Integrity Attack
1.33	Reverse Engineering
1.34	Functionality Misuse
1.35	Fingerprinting
1.36	Sustained Client Engagement
1.37	Privilege Escalation
1.38	Resource Injection
1.39	Code Injection
1.40	Command Injection
1.41	Protocol Manipulation
1.42	Information Elicitation
1.43	Modification During Manufacture
1.44	Malicious Logic Insertion
1.45	Contaminate Resource
1.46	Local Execution of Code
1.47	Functionality Bypass
1.48	Use of Known Domain Credentials
1.49	Object Injection
1.50	Traffic Injection
1.51	Obstruction
2	Hardware
2.1	Leveraging Race Conditions
2.2	Manipulating State
2.3	Interface Manipulation
2.4	Authentication Abuse
2.5	Excavation
2.6	Privilege Abuse
2.7	Shared Resource Manipulation
2.8	Content Spoofing
2.9	Resource Location Spoofing
2.10	Infrastructure Manipulation
2.11	Configuration/Environment Manipulation

SECCIÓN	DETALLE
2.12	Reverse Engineering
2.13	Protocol Analysis
2.14	Functionality Misuse
2.15	Privilege Escalation
2.16	Modification During Manufacture
2.17	Manipulation During Distribution
2.18	Hardware Integrity Attack
2.19	Malicious Logic Insertion
2.20	Contaminate Resource
2.21	Use of Known Domain Credentials
2.22	Obstruction
2.23	Hardware Fault Injection
3	Communications
3.1	Exploiting Trust in Client
3.2	Adversary in the Middle (AiTM)
3.3	Interception
3.4	Flooding
3.5	Excessive Allocation
3.6	Content Spoofing
3.7	Identity Spoofing
3.8	Resource Location Spoofing
3.9	Infrastructure Manipulation
3.10	Footprinting
3.11	Protocol Analysis
3.12	Communication Channel Manipulation
3.13	Resource Injection
3.14	Protocol Manipulation
3.15	Traffic Injection
3.16	Obstruction
3.17	Hardware Fault Injection
4	Supply Chain
4.1	Excavation
4.2	Configuration/Environment Manipulation
4.3	Software Integrity Attack

SECCIÓN	DETALLE
4.4	Modification During Manufacture
4.5	Manipulation During Distribution
4.6	Hardware Integrity Attack
4.7	Malicious Logic Insertion
5	Social Engineering
5.1	Parameter Injection
5.2	Identity Spoofing
5.3	Resource Location Spoofing
5.4	Action Spoofing
5.5	Software Integrity Attack
5.6	Information Elicitation
5.7	Manipulate Human Behavior
5.8	Obstruction
6	Physical Security
6.1	Excavation
6.2	Interception
6.3	Reverse Engineering
6.4	Bypassing Physical Security
6.5	Hardware Integrity Attack
6.6	Physical Theft
6.7	Obstruction

b) VULNERABILIDADES DE SEGURIDAD DE SANS (Sistema de Administración, Auditoria, red y seguridad, Network en Aplicaciones de Software)

SECCIÓN	DETALLE
1	Error de búfer de memoria
2	Scripting entre sitios
3	Error de entrada no validado
4	Error de exposición de información sensible
5	Error de lectura y escritura fuera de límites
6	Inyección SQL
7	Memoria previamente liberada
8	Error de desbordamiento de enteros

SECCIÓN	DETALLE
9	Falsificación de solicitudes entre sitios
11	Inyección de comandos del sistema operativo
12	Error de autenticación incorrecto
13	Des referenciación de un puntero NULL
14	Asignación de permisos incorrecta
15	Carga de archivos sin restricciones
16	Exposición de información a través de entidades XML
17	Inyección de código
18	Clave de acceso codificada
19	Consumo incontrolado de recursos

c) ISSAF (Marco de Evaluación de Seguridad de Sistemas de Información)

FASE I: PLANIFICACIÓN Y PREPARACIÓN		
Actividad	**Descripción**	**Controles/Verificaciones**
Acuerdo de Evaluación	Firmar acuerdo formal antes de cualquier prueba	• Protección legal mutua • Especificación de alcance • Definición de métodos
Identificación de Contactos	Establecer personas de contacto de ambas organizaciones	• Contactos técnicos. • Contactos legales. • Escalamiento de privilegios
Reunión Inicial	Confirmar alcance, enfoque y metodología	• Casos de prueba específicos • Caminos de escalada • Fechas y horarios
Definición de Alcance	Establecer límites y objetivos de la evaluación	• Sistemas incluidos/excluidos • Horarios permitidos • Restricciones específicas
FASE II: EVALUACIÓN (9 PASOS EN CAPAS)		
Capa 1: Recopilación de Información		
Control	Descripción	Métodos
Información Técnica	Recopilar datos técnicos del objetivo	• Consultas DNS/WHOIS • Escaneo de puertos • Fingerprinting
Información No Técnica	Obtener información pública y social	• Motores de búsqueda • Redes sociales

		• Sitios web corporativos
Ingeniería Social	Recopilar información mediante técnicas sociales	• Phishing • Pretexting • Baiting
Capa 2: Mapeo de Red		
Control	**Descripción**	**Objetivos**
Identificación de Sistemas	Mapear todos los sistemas y recursos de la red objetivo	• Topología de red • Sistemas activos • Servicios ejecutándose
Enumeración de Servicios	Identificar servicios y versiones específicas	• Versiones de software • Configuraciones • Puntos de entrada
Análisis de Arquitectura	Comprender la estructura de la red	• Segmentación • Puntos críticos • Rutas de acceso
Capa 3: Identificación de Vulnerabilidades		
Control	**Descripción**	**Métodos de Detección**
Vulnerabilidades Conocidas	Detectar vulnerabilidades documentadas	• Scanners automáticos • Bases de datos CVE • Análisis manual
Configuraciones Inseguras	Identificar malas configuraciones	• Passwords por defecto • Servicios innecesarios • Permisos excesivos
Análisis de Aplicaciones	Evaluar seguridad de aplicaciones web	• Inyección SQL • XSS • CSRF
Capa 4: Penetración		
Control	**Descripción**	**Técnicas de Explotación**
Explotación de Vulnerabilidades	Ganar acceso no autorizado	• Exploit públicos • Exploits custom • Bypass de controles
Bypass de Medidas de Seguridad	Evadir controles de seguridad	• Evasión de firewalls • Bypass AV • Técnicas stealth
Capa 5: Acceso y Escalada de Privilegios		
Control	**Descripción**	**Objetivos**
Escalada Horizontal	Obtener acceso a más sistemas	• Acceso inicial • Validación de vulnerabilidades
Escalada Vertical	Obtener privilegios administrativos	• Acceso más amplio posible

Capa 6: Enumeración Adicional		
Control	**Descripción**	**Información Objetivo**
Enumeración de Procesos	Analizar procesos y servicios activos	• Servicios ejecutándose • Procesos de usuario • Conexiones de red
Análisis de Datos	Buscar información sensible	• Archivos confidenciales • Credenciales • Configuraciones
Capa 7: Compromiso de Usuarios/Sitios Remotos		
Control	**Descripción**	**Objetivos**
Explotación de Relaciones de Confianza	Comprometer relaciones entre sistemas	• Acceso a redes remotas
Lateral Movement	Moverse lateralmente en la red	• Remote execution • Credential reuse • Network shares
Capa 8: Mantenimiento de Acceso		
Control	**Descripción**	**Técnicas de Persistencia**
Backdoors	Establecer acceso persistente	• Registry modifications • Service installation • Scheduled tasks
Canales de Comando y Control	Establecer comunicación encubierta	• DNS tunneling • HTTP/HTTPS channels • Encrypted channels
Capa 9: Limpieza de Rastros		
Control	**Descripción**	**Técnicas de Evasión**
Log Cleaning	Limpiar evidencias en logs	• Event log clearing • Log file modification • Timestamp manipulation
Artifact Removal	Eliminar artefactos de la intrusión	• File deletion • Registry cleanup • Process hiding
FASE III: REPORTE, LIMPIEZA Y DESTRUCCIÓN DE ARTEFACTOS		
Actividad	**Descripción**	• Componentes
Reporte Verbal	Comunicación inmediata de issues críticos	• Vulnerabilidades críticas • Compromisos activos • Actividades ilegales
Reporte Escrito	Documentación formal completa	• Resumen ejecutivo • Hallazgos técnicos • Recomendaciones • Evidencias

Limpieza de Sistemas	Remover todos los artefactos creados	• Archivos temporales • Backdoors instalados • Modificaciones realizadas
Destrucción Segura	Eliminar datos de prueba de forma segura	• Encriptación de datos • Sanitización • Destrucción física si es necesario

ANEXO D

NORMATIVA PARA LA PRESTACIÓN DEL SERVICIO

El contratista del Servicio se encuentra obligado a cumplir la normativa listada a continuación y sus modificatorias, sin perjuicio de otra normativa de alcance general o institucional que sea aplicable para la prestación del presente servicio.

1. Ley N° 26859 de fecha 25SET1997, Ley Orgánica de Elecciones.
2. Ley N° 26487 de fecha 02JUN1995, Ley Orgánica de la ONPE.
3. Ley N°28094 de fecha 01NOV2003, Ley de Organizaciones Políticas.
4. Ley Nº 32270 de fecha 24.03.2025, Ley que modifica la Ley 26859, Ley Orgánica de Elecciones, a fin de incorporar el Voto Digital.
5. Decreto de Urgencia N° 006-2020 de fecha 08ENE2020, que crea el Sistema Nacional de Transformación Digital.
6. Decreto de Urgencia N° 157-2020-PCM de fecha 24SEP2021, que aprobó el Reglamento del Decreto Supremo N° 006-2020.
7. Decreto de Urgencia N° 007-2020 de fecha 08ENE2020, que crea el Marco de Confianza Digital y dispone medidas para su fortalecimiento.
8. Decreto Legislativo N° 1412 de fecha 12SEP2020, que aprobó la Ley de Gobierno Digital.
9. Decreto Supremo N° 029-2021-PCM de fecha 18FEB2021 que aprobó el Reglamento de la Ley de Gobierno Digital.
10. Ley N° 27269 de fecha 26MAY2000, Ley de Firmas y Certificados Digitales.
11. Decreto Supremo N° 052-2018-PCM de fecha 18JUL2008 que aprobó el Reglamento de la Ley de Firmas y Certificados Digitales.
12. Decreto Legislativo N° 681 de fecha 11OCT1991, que aprueba normas que regulan el uso de tecnologías avanzadas en materia de archivo de documentos e información tanto respecto a la elaborada en forma convencional cuanto la producida por procedimientos informáticos en computadoras.
13. Ley N° 29733 de fecha 21JUN2011, Ley de Protección de Datos Personales.
14. Decreto Supremo N° 003-2013-JUS de fecha 21MAR2013, que aprobó el Reglamento de la Ley de Protección de Datos Personales.
15. Reglamento de Organización y Funciones, aprobado mediante la Resolución Jefatural N°000125-2024 JN/ONPE de fecha 27JUN2024, a través del cual se aprueba el Texto Integrado del Reglamento de Organización y Funciones de la Oficina Nacional de Procesos Electorales, que constan de dos (02) títulos, ocho (08) capítulos, ciento diecisiete (117) artículos y un (01), Anexo que contiene el Organigrama de la ONPE, en el cual se compilan las Resoluciones Jefaturales n.° 000902-2021-JN/ONPE, n.° 001732-2021-JN/ONPE, n.° 000710-2022-JN/ONPE,

n.° 001541-2022-JN/ONPE, n.° 002307-2022-JN/ONPE, 003405-2022-JN/ONPE, n.° 000598-2023-JN/ONPE, n.° 000072-2024-JN/ONPE, y en donde se establece las funciones de la GITE.

16. Resolución Jefatural N° 162-2020-JN/ONPE de fecha 21JUL2021 que aprobó el Plan Estratégico Institucional 2020-2025 de la ONPE.
17. Ley N° 32069, Ley General de Contrataciones Públicas, publicada el 24JUN2024 que entra en vigencia el 22ABR2025
18. Reglamento de la Ley N° 32069, Ley General de Contrataciones Públicas, aprobado mediante el Decreto Supremo Nº 009-2025-EF, que entra en vigencia el 22ABR2025
19. Otra normativa de carácter general y/o institucional aplicable para la prestación del presente servicio. (Políticas, Directivas, Manuales, etc.)