Instituto Nacional Electoral

Anexo 4

Concentrado de recomendaciones COTAPREP Federal

Reuniones con los 32 Organismos Públicos Locales

Abril 2024

UTSI | Unidad Técnica de Servicios de Informática

Concentrado de recomendaciones COTAPREP Federal
Reuniones con los Organismos Públicos Locales

Particulares

- Verificar que, como parte de los alcances de la auditoría, se incluyan los componentes asociados al uso de la tecnología de inteligencia artificial que se implementará para la lectura de la información de las actas.

- Verificar que el *software* libre que se utilice para el desarrollo del sistema informático del PREP cuente con soporte, actualizaciones regulares y un esquema sólido de trabajo; del mismo modo, procurar utilizar la versión más actualizada de dicho software para garantizar su seguridad y compatibilidad con las necesidades del sistema. Verificar que el software libre esté dentro del alcance de la evaluación de auditoría para asegurar su idoneidad y cumplimiento con los estándares requeridos.

- Para los casos en los que se implementará alguna herramienta de captura automatizada, se considera importante que, durante las pruebas y simulacros, se realice una medición de los tiempos a fin de evaluar el rendimiento y eficiencia de los procesos.

- En caso de utilizar los dispositivos móviles personales de las y los CAEL, verificar los controles de seguridad, conectividad y funcionalidad para asegurar la operatividad del PREP durante la fase de toma fotográfica del Acta PREP y de captura, así también como evitar la fuga o difusión de información sensible.

- Para futuras implementaciones, valorar la inclusión de la doble captura como parte del Proceso Técnico Operativo.

- Es importante establecer controles de seguridad que permitan identificar, en las distintas etapas de la implementación y operación del PREP, que el sistema informático en su conjunto es el mismo que fue auditado.

- Hacer pruebas y ver la posibilidad que cuando se contrate el servicio de MDM, éste detecte si algún dispositivo está *rooteado*.[1]

- Se considera importante llevar a cabo las acciones necesarias a fin de asegurar que los CATD estén instalados y habilitados previo al inicio de los simulacros.

[1] Operación que se debe realizar para obtener permisos de un dispositivo móvil con la finalidad de hacer cambios profundos dentro del sistema operativo.

- Para futuros Procesos Electorales la contratación de una solución MDM para automatizar el control de los dispositivos utilizados en el proyecto.

Generales

- Establecer un plan de destrucción de la información almacenada, incluidas bases de datos y repositorios, con el fin de proteger la propiedad y la privacidad de los datos ciudadanos y evitar que terceros accedan a información sensible.

- Establecer un esquema sólido de comunicación entre el COTAPREP Local, ente auditor y el tercero con la finalidad de mejorar los trabajos que se hacen en el diseño, implementación y operación del PREP.

- Analizar las cargas que estarán recibiendo el personal capturista en los CATD, con la finalidad de que, en caso de ser necesario y viable económicamente, contratar un número mayor de personal, a fin de disminuir la carga de captura y hacer más eficiente el proceso.

- En el proceso de captura de actas, contemplar medidas para evitar que el personal operativo pueda vincular la cantidad de votos con las fuerzas contendientes, entre otras, evitar la presentación de los emblemas, ello para mitigar posibles casos de mal uso.

- Evaluar la ubicación y accesibilidad de los Centros de Acopio de Transmisión de Datos y Centros de Captura y Verificación para garantizar una logística eficiente durante el proceso electoral.

- Realizar pruebas de toma fotográfica de las actas en diferentes condiciones, incluyendo la variabilidad de la iluminación en horarios nocturnos, para evaluar la efectividad de los sistemas y procesos bajo diferentes circunstancias.

- Verificar si como parte del esquema de arquitectura de infraestructura de almacenamiento, comunicaciones y energía eléctrica se están considerando elementos redundantes y diversificación de proveedores para reducir los riesgos y propiciar la continuidad de las operaciones en caso de que se presenten incidentes.

- Analizar si dentro del esquema de monitoreo, se están contemplando herramientas de *software* que fortalezcan la seguridad perimetral del sistema informático y la detección de tráfico inusual durante el desarrollo de las actividades para reducir el riesgo de lentitud o intermitencias en la disponibilidad del sistema.

- Verificar si como parte del esquema de pruebas se está incluyendo ejecutar, al menos, un simulacro de falla total de la infraestructura de almacenamiento, comunicaciones y energía eléctrica principal para medir el nivel de respuesta de los elementos de respaldo.

- Corroborar que como parte de las medidas en materia de seguridad que se están implementando para garantizar la integridad del sistema, se considere la autenticación en dispositivos y el cambio de credenciales al concluir la configuración de la infraestructura.

- Fortalecer los controles de seguridad en los dispositivos para la captura del acta mediante el aplicativo de PREP Casilla, a fin de garantizar la integridad y protección de la información.

- Realizar simulaciones de desastres para evaluar la eficacia del plan de recuperación de desastres, incluyendo cambios de infraestructura de servidores y la medición de tiempo de recuperación.

- Involucrar al personal operativo en los simulacros de incidentes para obtener una experiencia práctica y mejorar la preparación ante posibles contingencias.

- Realizar cálculos precisos de carga para determinar la capacidad necesaria de la planta de energía en los sitios relevantes del proyecto.

- Establecer mecanismos de monitoreo constante para detectar el posible mal uso de credenciales legítimas, considerando escenarios de riesgo donde los usuarios autorizados realizan actividades no autorizadas.

- Mantener una estrecha comunicación y coordinación entre el OPL y el ente auditor y, en su caso, el tercero que auxilie en la implementación y operación del PREP. En la misma tesitura, se reiteró la importancia de cumplir en tiempo y forma las actividades relacionadas con la auditoría por parte del ente auditor.

- Proporcionar al ente auditor un ambiente de pruebas idéntico al ambiente de producción a fin de llevar a cabo los trabajos correspondientes.

- Analizar, en conjunto con el COTAPREP, la estrategia para las pruebas de ataque volumétrico tomando en cuenta las tecnologías de nube que permite escalamiento de la disponibilidad.

- Proporcionar al ente auditor toda la información que requiera para la correcta ejecución de sus actividades.

- Revisar y dar seguimiento a los tiempos para el desarrollo de la auditoría considerando como buena práctica que el ente lleve a cabo una ronda de trabajo que le permita verificar la atención de los hallazgos.

- Para el caso de las instituciones académicas designadas como ente auditor en más de un OPL, se considera importante evaluar la disponibilidad de recursos humanos y técnicos para garantizar la cobertura y efectividad de las pruebas de penetración simultáneas. Se recomienda identificar posibles recursos adicionales o establecer prioridades para garantizar una cobertura efectiva.

- Tener un monitoreo permanente del desarrollo de los trabajos del PREP durante su operación a fin de mejorar la oportunidad de respuesta ante posibles incidencias.

- Vigilar y fortalecer la cadena de custodia con la finalidad de robustecer las medidas de seguridad en el traslado de las Actas.

- Analizar la factibilidad técnica y económica de fortalecer el área de informática con personal especializado en temas de seguridad.