TECNOLÓGICO DE MONTERREY®

Reporte Auditoría Seguridad PREP 2024

Resumen Ejecutivo Auditoría Seguridad para el Instituto Electoral de Coahuila

31 de Mayo 2024

Tecnológico de Monterrey

Funcionalidad Caja Negra 1/3

Prueba	Criterio Aceptación	Revisado
Pruebas Aplicación Mòvil	**SPD01** – Control de acceso a la aplicación móvil de digitalización mediante usuario/contraseña.	**Aceptado**
	SPD02 – Bloqueo aplicación móvil por usuario con contraseña errónea.	**Aceptado**
	SPD03 – Usuario bloqueado deberá cambiarse mediante mesa de servicio.	**Aceptado**
	SPD04 – Dispositivos móviles con aplicación controlada.	**Aceptado**
	SPD05 – Distribución de aplicación controlada.	**Aceptado**
	SPD06 – Identificación con factor adicional para teléfonos móviles en el uso de la aplicación y firma de la plataforma.	**Aceptado**
	SPD07 – Alta de actas por parte del equipo móvil registrado.	**Aceptado**
	SPD08 – Alta de acta equivocada (no pertenece a la casilla).	**Aceptado**
	SPD09 – Transmisión de acta digitalizada al sitio o BD de actas.	**Aceptado**
	SPD10 – Transmisión cifrada del acta hacia el repositorio o BD del PREP (sea móvil o escáner).	**Aceptado**
	SPD11 – Transmisión cifrada del acta digitalizada hacia el repositorio o BD del PREP (escáner).	**Aceptado**
	SPD12 – Confirmación de integridad del acta digitalizada y guardada en la BD del PREP.	**Aceptado**

Funcionalidad Caja Negra 2/3

Prueba	Criterio Aceptación	Revisado
Pruebas Estación de Captura	**SPC01** – Control de acceso a la estación de captura mediante usuario/contraseña.	**Aceptado**
	SPC02 – Bloqueo de usuario con contraseña errónea.	**Aceptado**
	SPC03 – Sistema operativo de la estación de captura debe ser vigente (no estar descontinuado por el fabricante).	**Aceptado**
	SPC04 – Las estaciones de captura deberán estar conectadas a la red mediante cable y no de forma inalámbrica.	**Aceptado**
	SPC05 – Usuarios de estación de captura con privilegios mínimos de administración.	**Aceptado**
	SPC06 – Sistema Operativo de la plataforma de captura deberá tener negado el acceso a Internet y el acceso remoto.	**Aceptado**
	SPC07 - Las estaciones de captura solo deben tener acceso hacia las aplicaciones del sistema de elecciones.	**Aceptado**
	SPC08 – Sistema Operativo de la plataforma de captura no deberá permitir acceder a medios externos de almacenamiento de datos (USB, CD, CD-ROM).	**Aceptado**
	SPC09 – Portal de captura al que acceden las estaciones de captura, deberá ser un portal en SSL y con certificado válido.	**Aceptado**
	SPC10 - Estaciones de captura de voto deben bloquearse.	**Aceptado**
Pruebas Captura Datos	**PCD01** – Validar proceso de cotejo de acta digitalizada contra los campos de captura del acta.	**Aceptado**
	PCD02 – El sistema PREP Local deberá considerar para la captura los siguientes datos requeridos por parte del OPL para cálculos adecuado.	**Aceptado**
	PCD03 – Datos a calcular por la plataforma PREP en la que se debe validar que los siguientes valores se den como resultado del cálculo en cada nivel de agregación que aplique (acta, sección, distrito electoral, entidad federativa y nacional).	**Aceptado**

Tecnológico de Monterrey

Funcionalidad Caja Negra 3/3

Prueba	Criterio Aceptación	Revisado
Pruebas PREP Digitalización	**PPR01 –** Resultados de porcentajes, los decimales deberán calcularse a cuatro posiciones (diezmilésimas) y no deberán truncarse ni redondearse.	**Aceptado**
	PPR02 – El portal debe tener la liga para poder bajar los datos en formato .CSV para cargarlos en hojas de cálculo.	**Aceptado**
	PPR03 – Datos a Publicar se deberán publicar en el sitio oficial, de donde se distribuirán a los sitios replicantes de información oficial. Deben contener los valores.	**Pendiente**
	PPR04 – Requerimientos de portal WEB para publicación – Interfaz Principal.	**Aceptado**
	PPR05 – Requerimientos de portal WEB para publicación – Encabezado.	**Aceptado**
	PPR06 – Requerimientos de portal WEB para publicación – Menú Colapsable.	**Aceptado**
	PPR07 – Requerimientos de portal WEB para publicación – Avance entidad.	**Aceptado**
	PPR08 – Requerimientos de portal WEB para publicación – Resultados Tu Casilla.	**Aceptado**
	PPR09 – Requerimientos de portal WEB para publicación – Estadística de Entidad.	**Aceptado**
	PPR10 – Requerimientos de portal WEB para publicación – Pie de Página (*footer*).	**Aceptado**
	PPR14 – Requerimientos de portal MÓVIL para publicación – Mi Sección	**Aceptado**
	PPR15 – Requerimientos de portal MÓVIL para publicación – Avance Entidad.	**Aceptado**
	PPR16 – Requerimientos de portal MÓVIL para publicación – Consulta de Votación.	**Aceptado**
	PPR17 – Requerimientos de portal MÓVIL para publicación – Estadística Entidad.	**Aceptado**
	PPR18 – Requerimientos de portal MÓVIL para publicación – Pie de página (*footer*).	**Aceptado**
	PPR19 – Requerimiento de actas de Voto anticipado. Dependiendo del estado, podrá haber Voto Anticipado por postración o prisión preventiva.	**Aceptado**
	PPR20 – Requerimiento de actas de voto por urna electrónica (si aplica)	**Aceptado**

Pruebas Pentest

Prueba	Prueba	Revisado
Pentest	No se encontró vulnerabilidades altas o críticas para ejecutar un ejercicio de pentest	**Aceptado**

Tecnológico de Monterrey

Análisis de Vulnerabilidades 1/2

Prueba	Criterio Aceptación	Revisado
Red de backend de sitio de publicación	**SPV01** – Escaneo de los activos dentro de la red o segmento del PREP. Los activos deben estar justificado en cuanto a su uso.	**Aceptado**
	SPV02 – Escaneo de los puertos o servicios habilitados en los activos de la red o segmento del PREP debe estar justificado en cuanto a su uso.	**Aceptado**
	SPV03 – El escaneo de servicios hecho a la infraestructura no debe no debe tener existencia de vulnerabilidades altas (7.0 – 8.9) o Críticas (9.0 – 10) basados en la clasificación estándar CVSS.	**Aceptado**
	SPV04 – El escaneo de servicios hechos a la infraestructura no debe tener explotaciones (exploits) desarrollados contra la infraestructura.	**Aceptado**
	SPV05 – Listar mediante un escaneo de los servidores WEB las vulnerabilidades que pueda haber en estos.	**Pendiente**
	SPV06 – EL sitio de publicación deberá tener un certificado y tener habilitado protocolo de cifrado.	**Aceptado**
Red de CATD	**SPV01** – Escaneo de los activos dentro de la red o segmento del PREP. Los activos deben estar justificado en cuanto a su uso.	**Aceptado**
	SPV02 – Escaneo de los puertos o servicios habilitados en los activos de la red o segmento del PREP debe estar justificado en cuanto a su uso.	**Aceptado**
	SPV03 – El escaneo de servicios hecho a la infraestructura no debe no debe tener existencia de vulnerabilidades altas (7.0 – 8.9) o Críticas (9.0 – 10) basados en la clasificación estándar CVSS.	**Aceptado**
	SPV04 – El escaneo de servicios hechos a la infraestructura no debe tener explotaciones (exploits) desarrollados contra la infraestructura.	**Aceptado**
	SPV05 – Listar mediante un escaneo de los servidores WEB las vulnerabilidades que pueda haber en estos.	**Aceptado**
	SPV06 – EL sitio de publicación deberá tener un certificado y tener habilitado protocolo de cifrado.	**Aceptado**

Análisis de Vulnerabilidades 2/2

Prueba	Prueba	Revisado
Red CCV	**SPV01** – Escaneo de los activos dentro de la red o segmento del PREP. Los activos deben estar justificado en cuanto a su uso.	**Aceptado**
	SPV02 – Escaneo de los puertos o servicios habilitados en los activos de la red o segmento del PREP debe estar justificado en cuanto a su uso.	**Aceptado**
	SPV03 – El escaneo de servicios hecho a la infraestructura no debe no debe tener existencia de vulnerabilidades altas (7.0 – 8.9) o Críticas (9.0 – 10) basados en la clasificación estándar CVSS.	**Aceptado**
	SPV04 – El escaneo de servicios hechos a la infraestructura no debe tener explotaciones (exploits) desarrollados contra la infraestructura.	**Aceptado**
	SPV05 – Listar mediante un escaneo de los servidores WEB las vulnerabilidades que pueda haber en estos.	**Aceptado**
	SPV06 – EL sitio de publicación deberá tener un certificado y tener habilitado protocolo de cifrado.	**Aceptado**

Revisión de Configuraciones 1/6

Prueba	Criterio Aceptación	Revisado
Red Backend Sitio Publicación	**SPI01 –** Validar la configuración de los equipos de red siga mejores prácticas y no haya inconsistencias en esta.	**No Aplica**
	SPI02 – Los equipos de comunicaciones solo podrán ser accesibles desde la red interna y con protocolo seguro (SSH).	**No Aplica**
	SPI03 – Equipos de ruteo y switches deberán tener versiones de sistemas operativos actualizados y bajo soporte.	**No Aplica**
	SPI04 – Equipos de comunicaciones y redes deberán estar con soporte y/o sustitución en caso de falla.	**No Aplica**
	SPI05 – El sistema PREP deberá contar con esquema de redundancia de comunicaciones.	**No Aplica**
	SPI06 – El sistema PREP deberá contar con redundancia eléctrica en caso de caída o fallas en la red eléctrica durante la jornada electoral.	**No Aplica**
	SPI07 – Los activos involucrados en el PREP deberán de tener habilitado la función de bitácora (logging) para guardar eventos.	**Aceptado**
	SPI08 – Los sistemas involucrados del PREP deberán tener un centro de control y comando que permita el monitoreo de sus sistemas.	**Aceptado**
	SPI09 – En los centros de captura no debe haber redes inalámbricas que conecten la infraestructura de captura o del OPL**.**	**No aplica**
	SPI10 – La infraestructura de los ambientes de desarrollo debe estar segregada de la infraestructura de ambientes operativos.	**Aceptado**
	SPI11 – El sistema debe tener recursos dedicados por lo que no debe compartir recursos con otros sistemas o plataformas ajenos al PREP en evaluación.	**Aceptado**
	SPI12 – Controles de acceso físico a los centros de captura.	**Aceptado**
	SPI13 – Control de acceso al sitio donde está la infraestructura del PREP.	**Aceptado**
	SPI14 – Verificar si hay control de acceso a teléfonos móviles.	**Aceptado**

Revisión de Configuraciones 2/6

Prueba	Criterio Aceptación	Revisado
Red Backend Sitio Publicación	**SPV01** – Escaneo de los activos dentro de la red o segmento del PREP. Los activos deben estar justificado en cuanto a su uso.	**Aceptado**
	SPV02 – Escaneo de los puertos o servicios habilitados en los activos de la red o segmento del PREP debe estar justificado en cuanto a su uso.	**Aceptado**
	SPV03 – El escaneo de servicios hecho a la infraestructura no debe no debe tener existencia de vulnerabilidades altas (7.0 – 8.9) o Críticas (9.0 – 10) basados en la clasificación estándar CVSS.	**Aceptado**
	SPV04 – El escaneo de servicios hechos a la infraestructura no debe tener explotaciones (exploits) desarrollados contra la infraestructura.	**Aceptado**
	SPV05 – Listar mediante un escaneo de los servidores WEB las vulnerabilidades que pueda haber en estos.	**Aceptado**
	SPV06 – EL sitio de publicación deberá tener un certificado y tener habilitado protocolo de cifrado.	**Aceptado**
	PRS01 – El OPL debe tener un manual de capacitación para el personal de captura.	**Aceptado**
	PRS02 – Debe haber un centro telefónico para consultas o dudas en los distintos procesos o módulos del PREP.	**Aceptado**
	PRS03 – Debe existir un proceso de resolución de inconsistencias al momento de captura de acta.	**Aceptado**
	PRS04 – Contratos de soporte externo en caso de eventualidades sobre las plataformas operativas que se utilizan en el PREP (para sistemas desarrollados por terceros).	**Aceptado**
	PRS05 – Tener los contratos con los proveedores de telecomunicaciones (primario y secundario) con los mapas de escalación de ellos para reportar eventos.	**Aceptado**
	PRS06 – Tener los contratos con los proveedores de nube, así como los procedimientos de reporte en caso de eventos hacia ellos. (si se está utilizando nube como repositorio operativo del PREP).	**Aceptado**
	PRS07 – Tener la documentación del sistema PREP del OPL actualizado y en resguardo por los encargados del área de tecnología del OPL.	**Aceptado**

Tecnológico de Monterrey

Revisión de Configuraciones 3/6

Prueba	Criterio Aceptación	Revisado
Red CATD	**SPI01 –** Validar la configuración de los equipos de red siga mejores prácticas y no haya inconsistencias en esta.	**Aceptado**
	SPI02 – Los equipos de comunicaciones solo podrán ser accesibles desde la red interna y con protocolo seguro (SSH).	**Aceptado**
	SPI03 – Equipos de ruteo y switches deberán tener versiones de sistemas operativos actualizados y bajo soporte.	**Aceptado**
	SPI04 – Equipos de comunicaciones y redes deberán estar con soporte y/o sustitución en caso de falla.	**Aceptado**
	SPI05 – El sistema PREP deberá contar con esquema de redundancia de comunicaciones.	**Aceptado**
	SPI06 – El sistema PREP deberá contar con redundancia eléctrica en caso de caída o fallas en la red eléctrica durante la jornada electoral.	**Aceptado**
	SPI07 – Los activos involucrados en el PREP deberán de tener habilitado la función de bitácora (logging) para guardar eventos.	**Aceptado**
	SPI08 – Los sistemas involucrados del PREP deberán tener un centro de control y comando que permita el monitoreo de sus sistemas.	**Aceptado**
	SPI09 – En los centros de captura no debe haber redes inalámbricas que conecten la infraestructura de captura o del OPL**.**	**Aceptado**
	SPI10 – La infraestructura de los ambientes de desarrollo debe estar segregada de la infraestructura de ambientes operativos.	**Pendiente**
	SPI11 – El sistema debe tener recursos dedicados por lo que no debe compartir recursos con otros sistemas o plataformas ajenos al PREP en evaluación.	**Aceptado**
	SPI12 – Controles de acceso físico a los centros de captura.	**Aceptado**
	SPI13 – Control de acceso al sitio donde está la infraestructura del PREP.	**Aceptado**
	SPI14 – Verificar si hay control de acceso a teléfonos móviles.	**Aceptado**

Revisión de Configuraciones 4/6

Prueba	Criterio Aceptación	Revisado
Red CATD	**SPV01** – Escaneo de los activos dentro de la red o segmento del PREP. Los activos deben estar justificado en cuanto a su uso.	**Aceptado**
	SPV02 – Escaneo de los puertos o servicios habilitados en los activos de la red o segmento del PREP debe estar justificado en cuanto a su uso.	**Aceptado**
	SPV03 – El escaneo de servicios hecho a la infraestructura no debe no debe tener existencia de vulnerabilidades altas (7.0 – 8.9) o Críticas (9.0 – 10) basados en la clasificación estándar CVSS.	**Aceptado**
	SPV04 – El escaneo de servicios hechos a la infraestructura no debe tener explotaciones (exploits) desarrollados contra la infraestructura.	**Aceptado**
	SPV05 – Listar mediante un escaneo de los servidores WEB las vulnerabilidades que pueda haber en estos.	**Aceptado**
	SPV06 – EL sitio de publicación deberá tener un certificado y tener habilitado protocolo de cifrado.	**Aceptado**
	PRS01 – El OPL debe tener un manual de capacitación para el personal de captura.	**Aceptado**
	PRS02 – Debe haber un centro telefónico para consultas o dudas en los distintos procesos o módulos del PREP.	**Aceptado**
	PRS03 – Debe existir un proceso de resolución de inconsistencias al momento de captura de acta.	**Aceptado**
	PRS04 – Contratos de soporte externo en caso de eventualidades sobre las plataformas operativas que se utilizan en el PREP (para sistemas desarrollados por terceros).	**Aceptado**
	PRS05 – Tener los contratos con los proveedores de telecomunicaciones (primario y secundario) con los mapas de escalación de ellos para reportar eventos.	**Aceptado**
	PRS06 – Tener los contratos con los proveedores de nube, así como los procedimientos de reporte en caso de eventos hacia ellos. (si se está utilizando nube como repositorio operativo del PREP).	**Aceptado**
	PRS07 – Tener la documentación del sistema PREP del OPL actualizado y en resguardo por los encargados del área de tecnología del OPL.	**Aceptado**

Revisión de Configuraciones 5/6

Prueba	Criterio Aceptación	Revisado
Red CCV	**SPI01 –** Validar la configuración de los equipos de red siga mejores prácticas y no haya inconsistencias en esta.	**Aceptado**
	SPI02 – Los equipos de comunicaciones solo podrán ser accesibles desde la red interna y con protocolo seguro (SSH).	**Aceptado**
	SPI03 – Equipos de ruteo y switches deberán tener versiones de sistemas operativos actualizados y bajo soporte.	**Aceptado**
	SPI04 – Equipos de comunicaciones y redes deberán estar con soporte y/o sustitución en caso de falla.	**Aceptado**
	SPI05 – El sistema PREP deberá contar con esquema de redundancia de comunicaciones.	**Aceptado**
	SPI06 – El sistema PREP deberá contar con redundancia eléctrica en caso de caída o fallas en la red eléctrica durante la jornada electoral.	**Aceptado**
	SPI07 – Los activos involucrados en el PREP deberán de tener habilitado la función de bitácora (logging) para guardar eventos.	**Aceptado**
	SPI08 – Los sistemas involucrados del PREP deberán tener un centro de control y comando que permita el monitoreo de sus sistemas.	**Aceptado**
	SPI09 – En los centros de captura no debe haber redes inalámbricas que conecten la infraestructura de captura o del OPL**.**	**Aceptado**
	SPI10 – La infraestructura de los ambientes de desarrollo debe estar segregada de la infraestructura de ambientes operativos.	**Aceptado**
	SPI11 – El sistema debe tener recursos dedicados por lo que no debe compartir recursos con otros sistemas o plataformas ajenos al PREP en evaluación.	**Aceptado**
	SPI12 – Controles de acceso físico a los centros de captura.	**Aceptado**
	SPI13 – Control de acceso al sitio donde está la infraestructura del PREP.	**Aceptado**
	SPI14 – Verificar si hay control de acceso a teléfonos móviles.	**Aceptado**

Revisión de Configuraciones 6/6

Prueba	Criterio Aceptación	Revisado
Red CCV	**SPV01** – Escaneo de los activos dentro de la red o segmento del PREP. Los activos deben estar justificado en cuanto a su uso.	**Aceptado**
	SPV02 – Escaneo de los puertos o servicios habilitados en los activos de la red o segmento del PREP debe estar justificado en cuanto a su uso.	**Aceptado**
	SPV03 – El escaneo de servicios hecho a la infraestructura no debe no debe tener existencia de vulnerabilidades altas (7.0 – 8.9) o Críticas (9.0 – 10) basados en la clasificación estándar CVSS.	**Aceptado**
	SPV04 – El escaneo de servicios hechos a la infraestructura no debe tener explotaciones (exploits) desarrollados contra la infraestructura.	**Aceptado**
	SPV05 – Listar mediante un escaneo de los servidores WEB las vulnerabilidades que pueda haber en estos.	**Aceptado**
	SPV06 – EL sitio de publicación deberá tener un certificado y tener habilitado protocolo de cifrado.	**Aceptado**
	PRS01 – El OPL debe tener un manual de capacitación para el personal de captura.	**Aceptado**
	PRS02 – Debe haber un centro telefónico para consultas o dudas en los distintos procesos o módulos del PREP.	**Aceptado**
	PRS03 – Debe existir un proceso de resolución de inconsistencias al momento de captura de acta.	**Aceptado**
	PRS04 – Contratos de soporte externo en caso de eventualidades sobre las plataformas operativas que se utilizan en el PREP (para sistemas desarrollados por terceros).	**Aceptado**
	PRS05 – Tener los contratos con los proveedores de telecomunicaciones (primario y secundario) con los mapas de escalación de ellos para reportar eventos.	**Aceptado**
	PRS06 – Tener los contratos con los proveedores de nube, así como los procedimientos de reporte en caso de eventos hacia ellos. (si se está utilizando nube como repositorio operativo del PREP).	**Aceptado**
	PRS07 – Tener la documentación del sistema PREP del OPL actualizado y en resguardo por los encargados del área de tecnología del OPL.	**Aceptado**

Tecnológico de Monterrey

Pruebas de Negación de Servicio (DDOS)

Prueba	Prueba	Revisado
Pruebas Negación de Servicio SitioPREP	**SPN01 –** La infraestructura debe soportar un ataque volumétrico HTTP/HTTPS	**Aceptado**
	SPN02 – La infraestructura deberá soportar un ataque volumétrico por UDP-DNS Amplification.	**Aceptado**
	SPN03 – LA infraestructura deberá poder soportar un ataque volumétrico por SynFlood	**Aceptado**
	SPN04 – Pruebas de ICMP Flood	**Aceptado**
	SPN05 – Validación de las cuotas de servicio configuradas en las subscripciones de servicios de nube (si aplica)	**Aceptado**
	SPN06 – Revisar con la OPL la existencia de un plan o procedimiento a seguir en caso de evento de ataque de DOS	**Aceptado**
	SPN07- Validar la existencia de contratos de servicio de protección de exceso de tráfico o para blindar contra ataques DOS	**Aceptado**
	SPN08 – Validar la existencia de un plan de comunicación hacia la comunidad en caso de eventos de DOS	**Aceptado**

Tecnológico de Monterrey

Pruebas de Integridad y BD

Prueba	Prueba	Revisado
Integridad y BD	Revisión de proceso de firma digital de código mediante un hash SHA256	**Aceptado**
	Revisión y aseguramiento del reinicio de base de daos para el PREP	**Aceptado**

Tecnológico de Monterrey