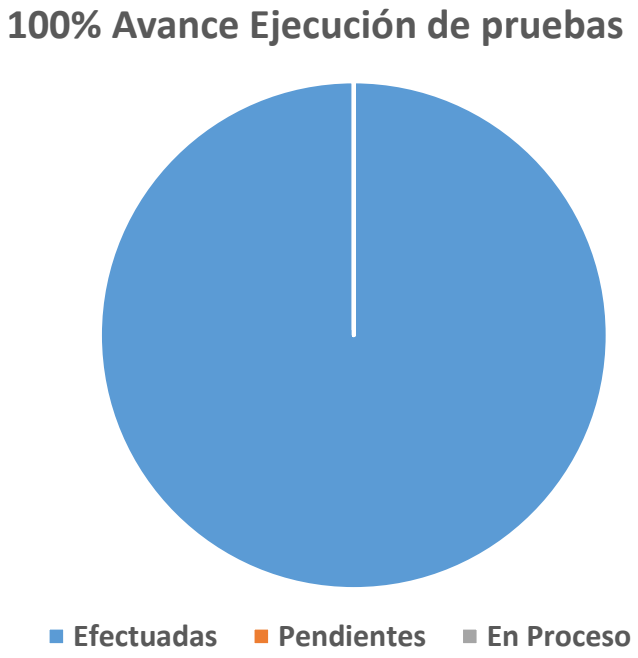
Tecnológico de Monterrey

Reporte Auditoría Seguridad IEPC

Resumen Ejecutivo Auditoría Seguridad 2024 – Reporte al 22 de agosto de 2024

Resumen Actividades (22/Agosto)

Pruebas	Avance	Por ejecutarse
Pruebas Vulnerabilidad	• Pruebas ejecutadas	
Pruebas Pentest	• Pruebas de penetración no necesarias	
Revisión Configuraciones	• Pruebas ejecutadas	
Pruebas Integridad y BD	• Revisión y validación de proceso	• Cierre de código y generación de hash ante notario el día de la jornada.



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.	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.	No aplica
	SPV06 – EL sitio de publicación deberá tener un certificado y tener habilitado protocolo de cifrado.	No aplica

Pruebas Pentest

Las pruebas de penetración solo se realizan si se encuentra vulnerabilidades altas o críticas explotables y no subsanables.

Revisión de Configuraciones 1/4

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.	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.	No aplica
	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.	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.	No aplica
	SPI13 – Control de acceso al sitio donde está la infraestructura del PREP.	No aplica
	SPI14 – Verificar si hay control de acceso a teléfonos móviles.	No aplica

Revisión de Configuraciones 2/4

Prueba	Criterio Aceptación	Revisado
Red Backend Sitio Publicación	**PRS01 –** El OPL debe tener un manual de capacitación para el personal de captura.	No aplica
	PRS02 – Debe haber un centro telefónico para consultas o dudas en los distintos procesos o módulos del PREP.	No aplica
	PRS03 – Debe existir un proceso de resolución de inconsistencias al momento de captura de acta.	No aplica
	PRS04 – Contratos de soporte externo en caso de eventualidades sobre las plataformas operativas que se utilizan en el PREP (para sistemas desarrollados por terceros).	No aplica
	PRS05 – Tener los contratos con los proveedores de telecomunicaciones (primario y secundario) con los mapas de escalación de ellos para reportar eventos.	No aplica
	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.	No aplica

Revisión de Configuraciones 3/4

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.	No aplica
	SPI10 – La infraestructura de los ambientes de desarrollo debe estar segregada de la infraestructura de ambientes operativos.	No aplica
	SPI11 – El sistema debe tener recursos dedicados por lo que no debe compartir recursos con otros sistemas o plataformas ajenos al PREP en evaluación.	No aplica
	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 4/4

Prueba	Criterio Aceptación	Revisado
Red CCV	**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).	No aplica
	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).	No aplica
	PRS07 – Tener la documentación del sistema PREP del OPL actualizado y en resguardo por los encargados del área de tecnología del OPL.	No aplica

Pruebas de Integridad y BD

Prueba	Prueba	Revisado
Integridad y BD	Proceso de inicialización de base de datos	Aceptado
	Proceso de generación de hash	Aceptado

- Las pruebas de revisión de firma digital y reinicio de base de datos se han llevado a cabo en simulacros.