Resumen Auditoría del PREP 2021
OPLE Veracruz

Resumen del proceso de auditoría del Programa Preliminar de Resultados Electorales 2021 para el Organismo Público Local Electoral.

05 Junio 2021

Líneas de revisión auditoría

La auditoría fue planteada en 6 distintas líneas de revisión y al día 05 de junio se tiene el siguiente estado:

#	Línea Revisión	Estado	Observaciones
1	Pruebas Caja Negra	Terminado	Todas las funcionalidades del sistema PREP, en sus distintas fases (digitalización, captura y publicación), fueron exitosas cumpliendo con los requerimientos de seguridad así como los de funcionalidad
2	Validación Sistema Informático e Integridad PREP y BD	En Proceso	Se revisaron los procesos de reinicio de la Base de datos así como el de la generación de llave de integridad, falta la entrega de los hashes del sistema informático para resguardo y la ejecución del proceso al inicio de la jornada electoral el 06 de junio.
3	Entregables PenTest	Terminado	Para las vulnerabilidades presentadas no hay explotaciones definidas
4	Análisis Vulnerabilidades Infraestructura PREP	Terminado	Las vulnerabilidades encontradas son de nivel bajo o medio sin exploits conocidos.
5	Pruebas DOS a PREP	Terminado	Pruebas volumétricas realizadas, sin impacto. En todos los casos, no hay afectación en tiempos de respuesta del servidor de publicación. En todas las pruebas, los tiempos de respuesta no exceden 200ms El DNS no es propenso a ataques de amplificación.
6	Informe Jornada PREP	Pendiente	

Pruebas Caja Negra

Las pruebas se clasifican basado en el Open Web Application Security Protect Mobile (OWASP-Mobile). Esta metodología representa un consenso a nivel desarrolladores sobre los riesgos más críticos para las aplicaciones.

#	Clasificación	Descripción
M1	Uso impropio de la plataforma	Mal uso de una característica de la plataforma o falla de controles de seguridad de esta.
M2	Almacenamiento inseguro de datos	Están combinadas dos categorías que se habían liberado en la versión previa y cubre almacenamiento inseguro de datos y fuga no-intencional de estos.
M3	Comunicación insegura	Esta clasificación cubre una mala negociación entre dos puntos por cuestiones de versiones de SSL, negociación débil, comunicaciones en texto sin cifrado en activos sensibles.
M4	Autenticación insegura	Esta categoría tiene que ver con un mal proceso de autenticación en la sesión ya sea por falla al identificar el usuario, falla al mantener la identidad del usuario al ser requerida o debilidad en la gestión de la sesión.
M5	Criptografía insuficiente	Esta clasificación tiene que ver con la aplicación de criptografía de un modo insuficiente.
M6	Autorización insegura	Esta categoría captura cualquier tipo de falla en la autorización
M7	Calidad en el Código cliente	Esta categoría tiene que ver con los problemas de implementación a nivel código en el cliente móvil.
M8	Modificación de Código	Esta categoría cubre lo que viene a ser actualizaciones, parches y modificaciones locales de código y modificaciones dinámicas de memoria.
M9	Ingeniería en reversa	Esta categoría incluye análisis del código binario para determinar su código origen, librerías, algoritmos y otros activos.
M10	Funcionalidades extrañas	Funciones escondidas de desarrollo como backdoors, controles de seguridad que no fueron inicialmente programados para ser liberados en un ambiente de producción.

Pruebas Caja Negra - Digitalización

Controles Especificados	Resultado
SPD01 – Control de acceso a la aplicación Móvil de digitalización mediante usuario/contraseña.	Aceptado
SPD02 – Bloqueo aplicación móvil por usuario contraseña errónea después de varios intentos	Aceptado
SPD03 – Usuario bloqueado deberá cambiarse mediante mesa de servicio	Aceptado
SPD04 – Dispositivos móviles con aplicación controlada e inventariada	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

Tecnológico de Monterrey

OPLE Veracruz
ORGANISMO PÚBLICO LOCAL ELECTORAL

Pruebas Caja Negra - Captura

Controles Especificados	Resultado
SPC01 – Control de acceso a la estación de captura mediante usuario/contraseña.	Aceptado
SPC02 – Bloqueo de usuario 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	Aceptado
SPC07 - Las estaciones de captura solo deben tener acceso hacia las aplicaciones del PREP de la jornada 2021	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

Pruebas Caja Negra – Captura Datos en Cumplimiento INE

Controles Especificados	Resultado
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 INE para cálculos adecuados	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

Pruebas Caja Negra – Datos Publicación

Controles Especificados	Resultado
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 deberán publicar en el sitio oficial, de donde se distribuirán a los sitios replicantes de información oficial deben contener los siguientes valores	Aceptado
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

Pruebas Caja Negra – Datos Publicación

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	Aceptado
PPR11 – Requerimientos de portal MÓVIL para publicación – Interfaz Principal	Aceptado
PPR12 – Requerimientos de portal MÓVIL para publicación – Encabezado	Aceptado
PPR13 – Requerimientos de portal MÓVIL para publicación – Menú Desplegable	Aceptado
PPR14 – Requerimientos de portal MÓVIL para publicación – Menú Desplegable > Mi Casilla	Aceptado

Pruebas Caja Negra – Datos Publicación

Controles Especificados	Resultado
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	Aceptado

Pruebas Caja Negra – Casos de Uso

Se llevan a cabo dos pruebas de funcionalidad antes del inicio de los simulacros, la primera el día 16 de abril, la segunda el 01 de mayo del presente año.

Diputaciones

Controles Especificados	Casos de Uso (Escenarios PREP)	Criterio de Aceptación	Resultado
PFD – 01	PÁNUCO – Sección 2815	CATD Móvil, código QR no colocado, inconsistencia: Todos ilegibles.	Aceptado.
PFD – 02	COSOLEACAQUE – Sección 4557	CAE – QR correcto, Algún campo ilegible.	Aceptado.
PFD – 03	PAPANTLA – Sección 2901	CAE - -QR correcto, Excede Lista Nominal.	Aceptado.
PFD – 04	XALAPA – Sección 1854	Escáner, QR correcto, Sin inconsistencias.	Aceptado.
PFD – 05	VERACRUZ – Sección 4482	Escáner, QR correcto, Todos sin dato.	Aceptado.
PFD – 06	MEDELLÍN DE BRAVO – Sección 2994	Escáner, QR erróneo, Algún campo sin dato.	Aceptado.
PFD - 07	HUATUSCO – Sección 1601	Escáner, QR correcto, Fuera de catálogo.	Aceptado

Tecnológico de Monterrey

OPLE Veracruz
ORGANISMO PÚBLICO LOCAL ELECTORAL

Pruebas Caja Negra – Casos de Uso

En la segunda prueba de funcionalidad se verifica el comportamiento esperado de las casos de uso, tanto de ayuntamientos como de diputaciones.

Ayuntamientos

Controles Especificados	Casos de Uso (Escenarios PREP)	Criterio de Aceptación	Resultado
PFD – 08	CÓRDOBA – Sección 989	CAE – QR correcto, Datos todos ilegibles.	Aceptado.
PFD – 09	ORIZABA – Sección 2708	CAE - QR correcto, Algún campo ilegible.	Aceptado.
PFD – 10	NOGALES – Sección 2621	CATD Móvil - QR correcto, excede Lista Nominal.	Aceptado.
PFD – 11	COSAMALOAPAN – Sección 1094	Escáner - QR correcto, Todos sin dato.	Aceptado.
PFD – 12	SAN ANDRÉS TUXTLA – Sección 3361	Escáner - QR correcto, Algún campo sin dato.	Aceptado.
PFD – 13	TATAHUICAPAN – Sección 2382	Escáner - QR correcto, Fuera del catálogo.	Aceptado.
PFD - 14	MINATITLÁN – Sección 2441	CATD Móvil - QR correcto, sin inconsistencias.	Aceptado.

Validación Sistema Informático e Integridad PREP y BD

Transferencia del archivo

Después de haber transmitido/compartido el archivo, se debe realizar una comprobación. Para hacer esto, se ejecuta el siguiente comando para poder validar la integridad del archivo.

```
# sha256sum -c (archivo hash compartido).sha256
```

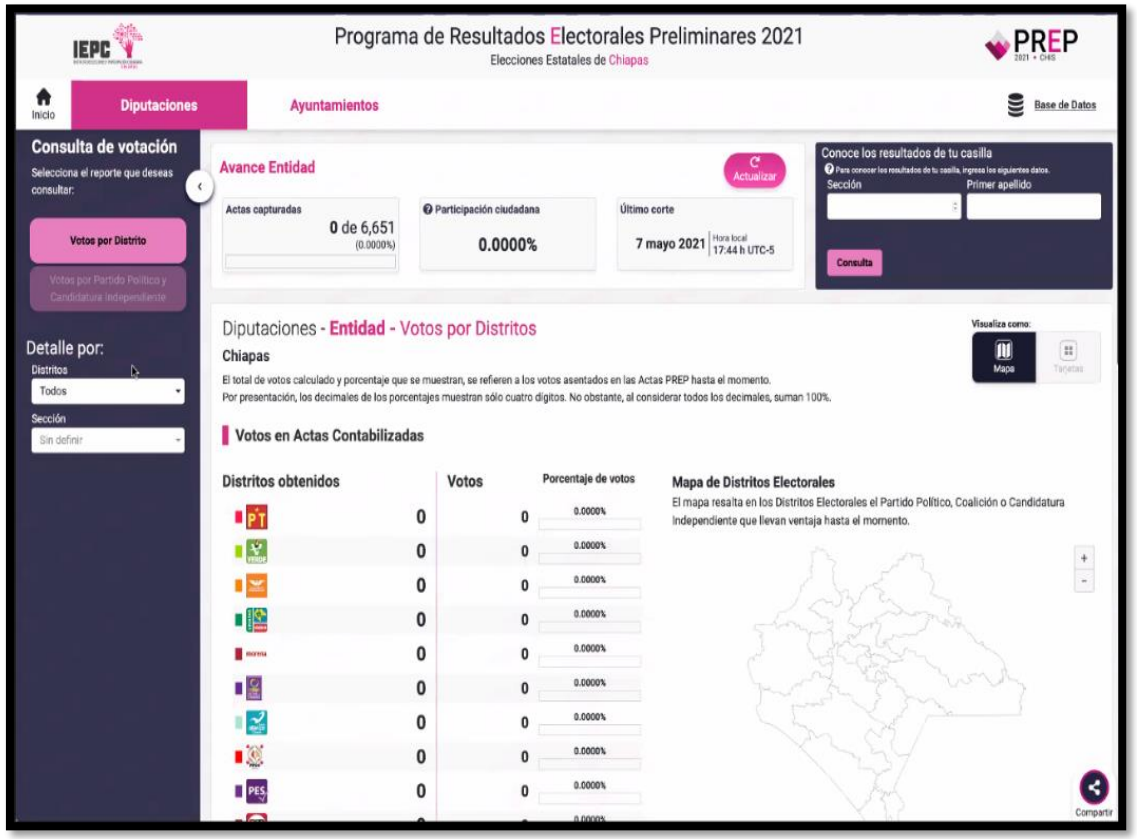
Se muestra el siguiente mensaje cuando el archivo pasa la prueba de integridad:

en el directorio hash se compartió un sha generado antes del envío del archivo

El siguiente mensaje se muestra cuando el archivo no pasa la prueba de integridad.

Esta firma permitirá tener un string de dígitos el cual es la representación numérica de los archivos que están dentro del directorio.

Proceso Hash del sistema informático



Validación de proceso de inicialización de la Base de datos

Tecnológico de Monterrey

OPLE Veracruz
ORGANISMO PÚBLICO LOCAL ELECTORAL

Criterios utilizados para la auditoría

Los criterios de aceptación de cada prueba están documentados en la tabla para lo cual la prueba debe cumplir con ellos. Cada prueba puede tener uno de tres tipos de resultados que pueden ser los descritos en la tabla siguiente:

Resultado Prueba	Descripción de Criterio	Acciones
Aceptado	La prueba cumplió satisfactoriamente con los criterios de aceptación	Prueba es aceptada y se da por cerrado el inciso de esta prueba. De ser necesario ejecutar el plan de nuevo en otra iteración, esta prueba no se volverá a ejecutar.
Rechazado	La prueba no cumplió con los criterios de aceptación	Prueba no es aceptada, se documenta el resultado y recomendaciones. Esta prueba se volverá a ejecutar en la siguiente iteración para revisar la implementación de las recomendaciones dadas en el resultado de las pruebas.
Aceptado con Observaciones	La prueba cumplió con una parte de los criterios o cumplió totalmente con observaciones.	Prueba es aceptada, pero con recomendaciones. Esto significa que las recomendaciones son solo eso, no sería obligatoria su implementación y solo queda como sugerencia o recomendación.

Análisis Vulnerabilidades Infraestructura PREP

Prueba	Resultado
SPI01 – Validar que la configuración de los equipos de red siga mejores prácticas y no haya inconsistencias en ésta	Aceptado
SPI02 – Los equipos de comunicaciones sólo podrán ser accesibles desde la red interna y con protocolo seguro (SSH)	Aceptado
SPI03 – Equipos de ruteo y conmutadores 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 con observaciones
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 con observaciones
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

Tecnológico de Monterrey

OPLE Veracruz
ORGANISMO PÚBLICO LOCAL ELECTORAL

Análisis Vulnerabilidades Infraestructura PREP

Prueba	Resultado
SPV01 – Escaneo de los activos dentro de la red o segmento del PREP. Los activos deben estar justificados 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 éstos	Aceptado
SPV06 – EL sitio de publicación deberá tener un certificado y tener habilitado protocolo de cifrado	Aceptado
PRS01 – La 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 con observaciones
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 de la OPL actualizado y en resguardo por los encargados del área de tecnología de la OPL	Aceptado

Tecnológico de Monterrey

OPLE Veracruz
ORGANISMO PÚBLICO LOCAL ELECTORAL

Pruebas DOS a PREP

Los criterios que se usaron para la ejecución y presentar el resumen se describen en la siguiente tabla:

Definición	Descripción	Acciones
Aceptado	La prueba cumplió satisfactoriamente con los criterios de aceptación	Prueba es aceptada y se da por cerrado el inciso de esta prueba. De ser necesario ejecutar el plan de nuevo en otra iteración, esta prueba no se volverá a ejecutar.
Rechazado	La prueba no cumplió con los criterios de aceptación	Prueba no es aceptada, se documenta el resultado y recomendaciones. Esta prueba se volverá a ejecutar en la siguiente iteración para revisar la implementación de las recomendaciones dadas en el resultado de las pruebas.
Aceptado con Observaciones	La cumplió con una parte de los criterios o cumplió totalmente con observaciones.	Prueba es aceptada, pero con recomendaciones. Esto significa que las recomendaciones son solo eso, no serían obligatoria su implementación y solo queda como sugerencia o recomendación.
No Ejecutada	Prueba no fue ejecutada en el ciclo por cuestiones de tiempo o por decisión mutua	La prueba se volverá a ejecutar en otro ensayo o bien si no se ejecuta, se agregará la justificación del por que de esto.
Sustituida	Prueba inicialmente diseñada pero que se intercambio por otra acción debido a cierta condición de la prueba inicial	La prueba que inicialmente se planeo no fue ejecutada dado que alguna condición de esta se debía modificar, cambiar o modificar al momento de su ejecución

Pruebas DOS a PREP

El objetivo de estas pruebas es para validar la resiliencia y funcionamiento de la plataforma informática bajo un ataque de tráfico en varios escenarios que afecten el funcionamiento de ésta.

Resultados Preliminares Escaneo Vulnerabilidades de Activos Instituto Electoral de Veracruz 2021	
Prueba	Resultado
SPN01 – La infraestructura debe soportar un ataque volumétrico TCP	Aceptado
SPN02 – La infraestructura deberá soportar un ataque volumétrico por UDP-DNS	Aceptado
SPN03 – La infraestructura deberá poder soportar un ataque volumétrico por ICMP	Aceptado
SPN04 – La infraestructura deberá poder manejar un ataque en la capa de aplicación	Aceptado

Pruebas DOS a PREP

Controles compensatorios validados

Resultados Preliminares Escaneo Vulnerabilidades de Activos Instituto Electoral de Veracruz 2021	
Prueba	**Resultado**
SPN05 – Validación de las cuotas de servicio configuradas en las suscripciones de servicios de nube	Aceptado
SPN06 – Existencia de un plan o procedimiento a seguir en caso de evento de ataque de DOS	Aceptado
SPN07- Existencia de contratos de servicio de protección de exceso de tráfico o para blindar contra ataques DOS	Aceptado
SPN08 – Existencia de un plan de comunicación hacia la comunidad en caso de eventos de DOS	Aceptado

Tecnológico de Monterrey

OPLE Veracruz
ORGANISMO PÚBLICO LOCAL ELECTORAL

Observaciones durante simulacros

Se toma una muestra representativa de los CATD y PREP casilla del Estado de Veracruz durante los simulacros.

- **Simulacro 01 – CCV Xalapa, Distrito Xalapa 10, Distrito Xalapa 11, Distrito Coatepec, Municio 181 Tlalnelhuayocan, Municipio 194 Xico, Municipio 27 Banderilla.**
  - En esta ocasión se observó un poco de desorganización y dudas con respecto a los procesos a seguir, se presentan varios detalles con la aplicación PREP casilla. Se entrega documentación de lo observado.

- **Simulacro 02 – Distrito Córdoba, Distrito Orizaba, Municipio 70 Fortín, Municipio 14 Amatlán de los Reyes, Municiío 196 Yanga.**
  - Se percibe una mejor organización de lo coordinadores de los CATD, la aplicación PREP casilla incluye el escaneo con QR, aún se presentan algunos detalles con este aplicativo. Se llevan a cabo pruebas exitosas de desconexión de internet y falla eléctrica.

- **Simulacro 03 - Distrito Veracruz, Distrito Boca del Río, Municipio 12 Alvarado.**
  - Los CATDs se observan inmersos en el proceso, los coordinadores son figura importante en la organización, se presentan menos fallas humanas durante el simulacro debido al conocimiento y práctica de los procesos involucrados. La comunicación directa con CCV Xalapa agiliza la atención de incidentes. Se llevan a cabo pruebas exitosas de desconexión de internet y falla eléctrica.

Conclusiones

Como resultado de las pruebas realizadas hasta el día de hoy, se concluye que los servidores e infraestructura pertenecientes al sistema PREP del estado de Veracruz cuentan con nivel de riesgo bajo debido a la configuración robusta de la tecnología implicada y los controles de protección aplicados.

El sistema cumple con los requerimientos funcionales solicitados por el INE y se encuentra en condiciones adecuadas para su correcta operación durante la jornada electoral de este 06 de junio del presente año.

M.C. Jessica Izquierdo
Ente Auditor PREP VER
05 de junio, 2021

Tecnológico de Monterrey

OPLE Veracruz
ORGANISMO PÚBLICO LOCAL ELECTORAL