



TECNOLÓGICO
DE MONTERREY®

Instituto Electoral Coahuila

Resumen Ejecutivo Auditoría PREP – Elecciones 2018

Resultados, hallazgos y recomendaciones de la auditoría al sistema del Programa Preliminar de Resultados Electorales del Instituto Electoral de Coahuila

29 Junio 2018

Agenda

Pruebas de Caja Negra

- En Aplicación Móvil
- En Escáner CATD
- Datos de Captura para Calculo y Publicación

Pruebas de Ataque de Negación de Servicio (DOS)

Pruebas de Análisis de Vulnerabilidades

- De La Arquitectura de Red
- De La Validación Estaciones de Captura
- De los Controles operacionales PREP
- De los Controles Comunicaciones Seguras
- Del Escaneo y la Revisión configuraciones

Glosario

Pruebas Caja Negra: En Aplicación Móvil

Prueba	Criterio Para Aceptación	Resultado 10/Junio	Resultado 17/Junio	Resultado 24/Junio	Comentarios/Acciones
7.1 Condiciones iniciales de pruebas APP Móvil	Verificar funcionamiento correcto dispositivo, comunicación establecida, app instalada.	ACEPTADO	ACEPTADO	ACEPTADO	Se confirmaron las condiciones iniciales establecidas.
7.2 Acceso a la aplicación	Entrar exitosamente a la aplicación con usuario/clave asignado.	ACEPTADO	ACEPTADO	ACEPTADO	Se confirmo la entrada a la aplicación usando el Usuario/Pass único asociado a dispositivo
7.3 Registro correcto de Actas	Registrar actas proporcionadas exitosamente.	RECHAZADO	ACEPTADO	ACEPTADO	Se encontró problemas con el registro de actas en el primer simulacro pero después de realizar actualización de software se corrigió el problema detectado, confirmando la captura exitosa en el segundo simulacro.
7.4 Registro incorrecto de Actas	Tener pantalla para revisar el acta sin permitir el acceso a capturar acta.	ACEPTADO	ACEPTADO	ACEPTADO	La aplicación permite revisar el código del acta para validar que corresponda al dispositivo antes de realizar la captura.
7.5 Tomar la Foto desde el Teléfono	Confirmar tener la foto escaneada en una resolución "legible".	ACEPTADO	ACEPTADO	ACEPTADO	Se confirmo que la resolución obtenida con la app es de 4160x1320 pixeles..
7.6 Transmisión del App al Sitio central					
7.6.1 Comunicaciones entre el APP y el sitio central	Confirmar que en las pruebas de alcance se tenga un 90% de efectividad (ICMP).	RECHAZADO	ACEPTADO	ACEPTADO	Se encontró en el primer simulacro problemas debido a la falla de la app móvil razón por la que no se logró el criterio de aceptación de este punto pero al realizar la actualización de software se corrigió en el 2º simulacro.
7.6.2 Corte de Comunicaciones entre el APP y el sitio central	Confirmar que el acta queda en sección de Seguimiento marcada como pendiente.	ACEPTADO	ACEPTADO	ACEPTADO	Se verificó que en la sección de "Pendientes" en la app se puede realizar el seguimiento de actas en casos de falla de comunicación.
7.7 Seguimiento de actas	Validar que se le puede dar seguimiento al acta en caso de corte de comunicaciones.	ACEPTADO	ACEPTADO	ACEPTADO	Se validó que el funcionamiento del apartado de seguimiento de actas fue correcto.
7.8 Validación de conexión segura entre el APP y el sitio central	Verificar que la Autenticación e identificación entre el APP y sitios central sea única.	ACEPTADO	ACEPTADO	ACEPTADO	Se validó la confidencialidad de la sesión mediante SSL, autenticación de múltiples factores: usuario, contraseña, dispositivo, IMEI

Pruebas Caja Negra: En Aplicación Móvil

Prueba	Criterio Para Aceptación	Resultado 10/Junio	Resultado 17/Junio	Resultado 24/Junio	Comentarios/Acciones
7.9 Validación de passwords	Revisar la estructura de los passwords que por recomendación deben ser 8 caracteres, con mezcla de letras (mayúsculas, minúsculas, números y caracteres especiales)	ACEPTADO	ACEPTADO	ACEPTADO	Se confirmó la utilización de script para generar passwords con los requerimientos de aceptación.
7.10 Validación en sitio central de recepción del acta (Recepción del acta)	Validar que haya un recibo tipo Timestamp de recepción del acta debe ser la misma que se recibió del teléfono.	ACEPTADO	ACEPTADO	ACEPTADO	Se confirma que se tienen registros de Timestamps de llegada y movimiento de archivos entre contenedores.

Hallazgos y Recomendaciones	
Clasificación	Descripción Hallazgo o Recomendación
M1 – Improper Platform Usage	
M2 – Insecure Data Storage	
M3 – Insecure Communication	
M4 – Insecure Authentication	
M5 – Insufficient Cryptography	
M6 – Insecure Authorization	
M7 – Client Code Quality	Se recomienda homogeneizar versiones para apps móviles
M8 – Code Tampering	
M9 – Reverse Engineering	
M10 – Extraneous Functionality	

Pruebas Caja Negra: En Escáner CATD

Prueba	Criterio Para Aceptación	Resultado 10/Junio	Resultado 17/Junio	Resultado 24/Junio	Comentarios/Acciones
8 Casos de prueba CATD con Multifuncional					
8.1 Condiciones iniciales de pruebas Multifuncional	Confirmar condiciones iniciales de prueba: Perfil cargado, conexión VPN establecida	ACEPTADO	ACEPTADO	ACEPTADO	Se validó las condiciones iniciales de prueba: Los escáners tienen un perfil de uso cargado para conectividad VPN.
8.2 Enlace del Multifuncional hacia sitio central	Confirmar que las pruebas de alcance se tenga un 90% de efectividad (ICMP)	RECHAZADO	ACEPTADO con observaciones	ACEPTADO con observaciones	Simulacro 1: En CATD Saltillo el enlace no permitió una conectividad eficiente (luego se amplió enlace a 100MB). Simulacro 2: Ráfagas de datos (comportamiento no habitual en elecciones) ocasionó que el enlace presentara retardos. Se ejecutaron escenarios falla de enlace y servidor principales. Simulacro 3: Escenario de falla sitio central y alterno.
8.3 Validación de conexión segura entre el Multifuncional y sitio central	Confirmar que la comunicación se da con conexiones seguras validadas en firewall o router	ACEPTADO	ACEPTADO	ACEPTADO	Se confirmo que los escáners transmiten mediante una conexión de VPN.
8.4 Validación de passwords	Validar que los passwords deben ser 8 caracteres, con mezcla de letras (mayúsculas, minúsculas, números y caracteres especiales)	SUSTITUIDA	SUSTITUIDA	SUSTITUIDA	Se encontró que el uso de los escáners está restringido de forma física a las personas que tienen acceso al edificio resguardado. La comunicación viaja segura a través de la VPN.
8.5 Escanear el acta	Validar que el archivo escaneado quede en formato PDF o gráfico en el multifuncional con nombre único para ser enviado al centro de procesamiento.	ACEPTADO	ACEPTADO	ACEPTADO	Se validó que la imagen escaneada es identificada de forma única.

Pruebas Caja Negra: En Escáner CATD

Prueba	Criterio Para Aceptación	Resultado 10/Junio	Resultado 17/Junio	Resultado 24/Junio	Comentarios/Acciones
8.6 Comunicación para envío desde el CATD					
8.6.1 Envío del acta desde el escáner	Validar que el archivo de acta deberá residir, después del envío en la BD del centro de procesamiento.	ACEPTADO	ACEPTADO	ACEPTADO	Se confirmó que no hay almacenamiento local en sitio, se recibe el archivo directo en base de datos interna PREP.
8.6.2 Interrupción en el envío del acta desde el APP	Confirmar que el acta no queda en el centro de procesamiento y se conserva en el multifuncional para su envío posterior.	ACEPTADO	ACEPTADO	ACEPTADO	Se confirma que al enviarla se manda un error de transmisión y se vuelve hacer intento de envío.
8.6.3 Validación en sitio central de recepción del acta (Recepción del acta)	Validar que el acta se recibe posterior a caída de enlace del archivo encolado (no enviado) en el multifuncional .	NO EJECUTADA	ACEPTADO	ACEPTADO	Se verificó el reenvío con la simulación de falla de enlace, server y sitio.
8.7 Validación en sitio central de recepción de acta (caso de doble envío del acta)	Validar que el timestamp de recepción del acta debe ser la misma que se recibió del teléfono.	NO EJECUTADA	ACEPTADO	ACEPTADO	Se validó que se tienen registros de Timestamps de llegada y movimiento de archivos entre contenedores.
8.8 Obtención del acta por equipo de capturistas del PREP (acta única)	La imagen del acta puede ser obtenida por el personal en el centro de captura con una resolución adecuada.	ACEPTADO	ACEPTADO	ACEPTADO con observaciones	En simulacro 3 se presenta detalle con recepción de imágenes de escáners después de 3 hrs se soluciona y se percibe mejora en desempeño de aplicación.
8.9 Obtención del acta por equipo de capturistas del PREP (acta repetida)	Confirmar que existe un proceso en caso de acta repetida.	ACEPTADO	ACEPTADO	ACEPTADO	Se confirma que para actas repetidas se toma la 1er acta recibida asociada al código de barra.

Pruebas Caja Negra: En Datos de Captura para Calculo y Publicación

Prueba	Criterio Para Aceptación	Resultado 10/Junio	Resultado 17/Junio	Resultado 24/Junio	Comentarios/Acciones
9 Datos de captura para cálculo y Publicación					
9.1 Condiciones Iniciales de Captura	Validar que la base de datos inicia en limpio.	ACEPTADO	ACEPTADO	ACEPTADO	Se confirma el cumplimiento con el proceso de limpiar Base de Datos en los 3 simulacros.
9.2 Captura de valores requeridos del Acta en la Base de datos del SIPRE	Confirmar que los valores mínimos requeridos deben estar para su captura en la interfase del PREP.	ACEPTADO	ACEPTADO	ACEPTADO	Se confirma que se cumple con los valores requeridos a publicar.
9.3 Datos a Calcular	Validar que se tienen los datos mínimos a calcular en la interfase del PREP deben reflejarse.	ACEPTADO	ACEPTADO	ACEPTADO	Se validó que se cumple con los cálculos necesarios y con el número de decimales solicitados para la precisión de la información.
9.4 Datos a Publicar	Confirmar que se presenten los datos a publicar que se mencionan en el documento de plan de pruebas como entregables mínimo.	ACEPTADO	ACEPTADO con observaciones	ACEPTADO	Se confirmó que se publican todos los datos listados como requerimientos, sólo en simulacro 2 se observan algunos detalles con la publicación de datos de la BD por municipio. Corregido en el 3er simulacro.
9.5 Corrección de actas duplicadas	Documentar proceso mediante el cuál se validan las actas duplicadas.	ACEPTADO	ACEPTADO	ACEPTADO	La primer imagen correspondiente al identificador del acta se toma como válida. Si no es legible, entonces se solicita re-digitalización, de lo contrario, no es posible acceder a otra imagen de la misma acta.

Pruebas de Ataques de Negación de Servicio (DOS)

Prueba	Criterio Para Aceptación	Resultado 10/Junio	Resultado 17/Junio	Resultado 24/Junio	Comentarios/Acciones
7.1 Ataque volumétrico por TCP – SYN FLOOD	Verificar que no haya afectación al tráfico legítimo pudiendo detener el tráfico de ataque que se origina..	SUSTITUIDA	SUSTITUIDA	SUSTITUIDA	La prueba se considera ACEPTADA debido a no tener permiso de ejecución de este tipo de ataques sobre infraestructura de terceros (CLOUDFLARE) . Se confirma que los controles existentes en la nube de CLOUDFLARE disminuyen el riesgo de este tipo de ataques.
7.2 Ataque volumétrico por UDP - DNS AMPLIFICATION	Verificar que no haya afectación al tráfico legítimo pudiendo detener el tráfico de ataque que se origina..	SUSTITUIDA	SUSTITUIDA	SUSTITUIDA	La prueba se considera ACEPTADA debido a no tener permiso de ejecución de este tipo de ataques sobre infraestructura de terceros (CLOUDFLARE) . Se confirma que los controles existentes en la nube de CLOUDFLARE disminuyen el riesgo de este tipo de ataques.
7.3 Ataque volumétrico por ICMP – ICMP FLOOD	Verificar que no haya afectación al tráfico legítimo pudiendo detener el tráfico de ataque que se origina..	SUSTITUIDA	SUSTITUIDA	SUSTITUIDA	La prueba se considera ACEPTADA debido a no tener permiso de ejecución de este tipo de ataques sobre infraestructura de terceros (CLOUDFLARE) . Se confirma que los controles existentes en la nube de CLOUDFLARE disminuyen el riesgo de este tipo de ataques.
7.4 Ataque en a capa de aplicación – SLOWRIS ATTACK	Asegurar que las sesiones arrancadas simulando baja velocidad, deberán cerrarse por falta de respuesta en tiempos adecuados para no sobrecargar el servidor de WEB.	SUSTITUIDA	SUSTITUIDA	SUSTITUIDA	La prueba se considera ACEPTADA debido a no tener permiso de ejecución de este tipo de ataques sobre infraestructura de terceros (CLOUDFLARE) . Se confirma que los controles existentes en la nube de CLOUDFLARE disminuyen el riesgo de este tipo de ataques.

- Estas pruebas fueron sustituidas por la revisión de las políticas y filtros implementados en el proveedor CLOUDFLARE ya que por ser infraestructura de un tercero (CLOUDFLARE) se requiere la autorización de este para realizar este tipo de pruebas.
- Estas pruebas se sustituyeron por la validación de los filtros y la arquitectura mediante la cual protege el contenido de los clientes.
- En base a esta situación se acordó **mutuamente ente el ente auditor y el IEC a no hacer este tipo de ataques** por no contar con permiso del proveedor CLOUDFLARE para estas pruebas

Análisis de Vulnerabilidades: De la Arquitectura de Red

Prueba	Criterio Para Aceptación	Resultado 10/Junio	Resultado 17/Junio	Resultado 24/Junio	Comentarios/Acciones
4.1.1 Diseño jerárquico de la red	Validar diagrama muestra estructura y modelo de red.	NO EJECUTADA	NO EJECUTADA	ACEPTADO	Se pudo validar que se cuenta con un modelo jerárquico comprimido ya que por la cantidad de dispositivos es suficiente.
4.1.2 Redundancia en conexión	Verificar que haya conexión alterna de salida del centro captura.	NO EJECUTADA	NO EJECUTADA	ACEPTADO	Se verificó que sí se cuenta con enlace principal de Alestra y enlace secundario de Espectro.
4.1.3 Direccionamiento adecuado y eficiente	Confirmar que el direccionamiento este segmentado por funciones, alcances y responsabilidades.	NO EJECUTADA	NO EJECUTADA	ACEPTADO	Se confirmó que se cuenta con segmentación de red, permitiendo separación de servicios y usuarios.
4.1.4 Acceso controlado a redes en sitios de captura	Validar que el acceso a los closets de telecom debe estar controlado y asegurado.	NO EJECUTADA	NO EJECUTADA	ACEPTADO	Se pudo validar que el acceso al site principal y secundario se encuentra restringido.
4.2 Validación de versiones sin vulnerabilidades críticas	Verificar que las versiones de los switches y routers no deben presentar vulnerabilidades críticas ni altas.	NO EJECUTADA	NO EJECUTADA	ACEPTADO	Se verificó que las versiones actuales se consideran estables y sin vulnerabilidades críticas.
4.3 Soporte manual a infraestructura	Confirmar que se cuenta con contratos de soporte, así como soporte en sitio y vía telefónica para soporte.	NO EJECUTADA	NO EJECUTADA	ACEPTADO con observaciones	Se confirmó que hay uno de los firewalls en uso que no cuenta con contrato vigente, sin embargo, se tiene un dispositivo como respaldo con la misma configuración que sí cuenta con este requisito.

Análisis de Vulnerabilidades: De la Estaciones de captura

Prueba	Criterio Para Aceptación	Resultado 10/Junio	Resultado 17/Junio	Resultado 24/Junio	Comentarios/Acciones
4.4.1 Acceso con privilegios mínimos	Validar que se cuenta con acceso del usuario solo a lo que requiere.	NO EJECUTADA	NO EJECUTADA	ACEPTADO	Se pudo validar que sólo usuario asignado puede hacer uso de estación de trabajo. No tiene usuario admin, no tiene permiso de instalación y no tiene acceso a internet.
4.4.2 Servicios habilitados en estaciones de captura	Validar la lista de servicios abiertos en estaciones captura.	NO EJECUTADA	NO EJECUTADA	ACEPTADO	Se pudo validar que debido a que las máquinas sólo tienen acceso a red local del PREP no es factible usar otros servicios compartidos, sólo locales.
4.4.3 Vulnerabilidades en las estaciones de captura	Validar que no haya lista de vulnerabilidades de nivel crítico y alto en las estaciones de captura.	NO EJECUTADA	NO EJECUTADA	ACEPTADO	Se pudo validar que no se encuentran vulnerabilidades críticas en estaciones.
4.4.4 Acceso de las estaciones de captura	Confirmar que las estaciones de captura solo tienen la aplicación para captura de elecciones.	NO EJECUTADA	NO EJECUTADA	ACEPTADO	Se confirmó que las estaciones de captura sólo tienen acceso a red local del PREP y se encuentra asociada al usuario que le dará el uso durante el evento del 1ro de julio.
4.4.5 Acceso a la infraestructura de comunicaciones	Confirmar que hay bloqueo de puertos TELNET, WEB, si no es así, debe haber lista de acceso. Acceso solo vía SSH.	NO EJECUTADA	NO EJECUTADA	ACEPTADO	Se confirmó que los puertos están cerrados y sólo existe conexión a la red local, no cuentan con salida a internet.
4.4.6 Puertos dedicados	Confirmar que se tiene habilitado Port Blocking.	NO EJECUTADA	NO EJECUTADA	ACEPTADO con observaciones	Se confirmó que el switch utilizado para interconexión de las máquinas no permite esta característica pero está restringido de forma física el uso de la computadora al usuario asignado.

Análisis de Vulnerabilidades: De los Controles de Seguridad de Operación

PruebaResultado	Criterio Para Aceptación	Resultado 10/Junio	Resultado 17/Junio	Resultado 24/Junio	Comentarios/Acciones
4.5.1 Seguridad en Operaciones: Administración de la Capacidad	Validar la existencia de control de aplicaciones y/o enlace desborde para consumo ancho banda.	NO EJECUTADA	NO EJECUTADA	ACEPTADO	Se validó que se cuentan con dos enlaces en site principal, otro en site alterno, más el servicio contratado en la nube.
4.5.2 Seguridad en Operaciones: Protección contra malware	Confirmar la existencia de controles para evitar la introducción de malware en la red.	NO EJECUTADA	NO EJECUTADA	ACEPTADO con observaciones	Se confirmó que no existe una aplicación específica contra malware pero las máquinas se encuentran totalmente aisladas, sin acceso a internet y sin privilegios de instalación, de esta forma se previene este tipo de ataques.
4.5.3 Seguridad en Operaciones: Bitácora de eventos	Validar la existencia de bitácoren de eventos del ambiente de red LAN y WAN.	NO EJECUTADA	NO EJECUTADA	ACEPTADO	Se validó que se utiliza un software de monitoreo que permite tener datos de la salud de equipos (errores, warnings, uso de disco, RAM, CPU, uso de red) salud de base de datos y WEB servers.
4.5.4 Seguridad en Operaciones: Restricciones para instalación de SW	Validar la existencia de controles para evitar instalación de SW no permitido en estaciones de trabajo.	NO EJECUTADA	NO EJECUTADA	ACEPTADO	Se validó que en los teléfonos se encuentra restringida la instalación de apps externas, además la cuenta asociada a la playstore es del IEC.

Análisis de Vulnerabilidades: De los Controles de Comunicaciones Seguras

Prueba	Criterio Para Aceptación	Resultado 10/Junio	Resultado 17/Junio	Resultado 24/Junio	Comentarios/Acciones
4.6.1 Comunicaciones Seguras: Controles de la Red	Confirmar que el área de captura y almacenamiento deberá estar segregado de otras áreas de TI.	NO EJECUTADA	NO EJECUTADA	ACEPTADO	Se confirmó que la segmentación contempla este escenario. Además el sistema del PREP se encuentra totalmente aislado de la infraestructura de TI del IEC.
4.6.2 Comunicaciones Seguras: Seguridad de los servicios de red	Validar la existencia de control de protocolos no permitidos. Tener una lista de servicios/protocolos permitidos.	NO EJECUTADA	NO EJECUTADA	ACEPTADO	Se valida que la lista de los protocolos no utilizados se encuentran bloqueados. Se utiliza política: denegar todo, permitir únicamente lo que se necesita.
4.6.3 Comunicaciones Seguras: Segregación en redes	Confirmar que se tiene un esquema de direccionamiento con evidencia de la segregación.	NO EJECUTADA	NO EJECUTADA	ACEPTADO	Se confirma esquema de topología y configuración que confirma la segregación de la red.
4.6.4 Comunicaciones Seguras: Transferencia de información	Confirmar que se tienen canales seguros de transmisión de estaciones de captura hasta sistema .	NO EJECUTADA	NO EJECUTADA	ACEPTADO	Se confirmó que en el app móvil se cuenta con autenticación de múltiples factores y SSL. Para el escáner se cuenta con la transmisión mediante VPN. Las estaciones de captura se encuentran bajo el dominio del firewall y sólo tienen acceso local.

Análisis de Vulnerabilidades: Del Escaneo y Revisión de Configuraciones

Prueba	Criterio Para Aceptación	Resultado 10/Junio	Resultado 17/Junio	Resultado 24/Junio	Comentarios/Acciones
4.7 Escaneo a infraestructura de computo	Confirmar que en el escaneo no haya ninguna vulnerabilidad nivel alta o crítica.	NO EJECUTADA	NO EJECUTADA	ACEPTADO	Se confirmó mediante varios escaneos y no se encuentran vulnerabilidades críticas.
4.8 Escaneo de infraestructura de comunicaciones	Validar que en el escaneo no haya ninguna vulnerabilidad nivel alta o crítica.	NO EJECUTADA	NO EJECUTADA	ACEPTADO	Se validó que hay una vulnerabilidad alta que puede ser explotada mediante un protocolo en particular el cual no aplica y no es usado por los equipos del PREP y se encuentra bloqueado.
4.9 Revisión de configuración de infraestructura de comunicaciones					
4.9.1 Revisión de configuración Switches LAN	Revisar la configuración de la infraestructura de switches cumpliendo los requerimientos de mejores prácticas y proporcionar recomendaciones sobre este	NO EJECUTADA	NO EJECUTADA	NO EJECUTADA	El tipo de switch utilizado para interconexión de las máquinas está limitado en funcionalidades para validar un “hardening”, se da peso a la seguridad física del edificio y la restricción de uso y asociación de la computadora.
4.9.2 Revisión de configuración Router	Validar la configuración de la infraestructura de router cumpliendo los requerimientos de mejores prácticas	NO EJECUTADA	NO EJECUTADA	ACEPTADO	Se valida que la configuración del ruteador es seguro y sigue las mejores prácticas del fabricante.
4.9.3 Revisión de configuración Firewall	Validar la configuración de la infraestructura de Firewall cumpliendo los requerimientos de mejores prácticas	NO EJECUTADA	NO EJECUTADA	ACEPTADO	Se valida que la configuración del firewall es seguro y sigue las mejores prácticas del fabricante.

Glosario

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