INSTITUTO INTERAMERICANO DE DERECHOS HUMANOS
CENTRO DE ASESORÍA Y PROMOCIÓN ELECTORAL

INFORME DEL SEGUIMIENTO DE RECOMENDACIONES FORMULADAS EN EL INFORME PRELIMINAR No. 001-2024 - JUNTA CENTRAL ELECTORAL(JCE)

INFORME No. A-SR-2024 – INFORME DE SEGUIMIENTO DE RECOMENDACIONES DE AUDITORÍA.

PERÍODO COMPRENDIDO
DEL 11 AL 19 DE ENERO DE 2024.

CONTENIDO

CAPÍTULO I

INFORMACIÓN INTRODUCTORIA

MOTIVOS DE LA AUDITORÍA.

La presente auditoría se practicó en cumplimiento al Convenio de Cooperación internacional entre la Junta Central Electoral (JCE) y el Instituto Interamericano de Derechos Humanos (IIDH)/Centro de Asesoría y Promoción Electoral (CAPEL), el cual tiene como objetivo principal realizar una auditoría al sistema informático de Escrutinio, Digitalización, Escaneo y Transmisión de resultados (EDET) dispuesto para las elecciones municipales del 18 de febrero de 2024.

FINALIDAD.

Esta etapa o auditoría de seguimiento de las recomendaciones tiene como fin verificar el cumplimiento de las recomendaciones de remediación emitidas en el Informe No.001-2024-JUNTA CENTRAL ELECTORAL(JCE).

OBJETIVOS DE LA AUDITORÍA.

1. Objetivos Generales

Verificar sí se han ejecutado por parte de la Gerencia de Informática de la Junta Central Electoral (JCE) las recomendaciones emitidas en el Informe No.001-2024-JUNTA CENTRAL ELECTORAL(JCE).

2. Objetivos específicos

- Comprobar el estado de las recomendaciones emitidas en el Informe No.001-2024-JUNTA CENTRAL ELECTORAL(JCE).

- Determinar las causas por lo que no se han cumplido las recomendaciones emitidas en el Informe No.001-2024-JUNTA CENTRAL ELECTORAL(JCE).

- Verificar que las recomendaciones cumplidas cuenten con toda la evidencia y documentación soporte.

ALCANCE DE LA AUDITORÍA

La evaluación comprendió la revisión y verificación de la implementación de las recomendaciones planteadas en el informe No.001-2024-JUNTA CENTRAL ELECTORAL(JCE) y comprobar, sí han elaborado y aplicado el plan de acción para el cumplimiento de estas recomendaciones de remediación por parte de los funcionarios principales responsables de su corrección.

Durante el proceso del monitoreo y verificación del cumplimiento de las recomendaciones para una adecuada mejora y funcionamiento del EDET para llevar a cabo las elecciones municipales, se comprobó que en un 79% se encuentran cumplidas y el 8% se encuentran en proceso de ser cumplidas y el 13% no se cumplieron con las recomendaciones.

CAPÍTULO II

ANTECEDENTES

El Centro de Asesoría y Promoción Electoral (CAPEL) es un programa especializado del Instituto Interamericano de Derechos Humanos (IIDH). Fue creado en 1983 e inició sus labores en el mes de febrero de 1985.

El Estatuto del Centro establece que sus fines serán la asesoría técnica electoral y la promoción de las elecciones, con un enfoque multidisciplinario, labor que ha realizado con organismos electorales, poderes legislativos, organizaciones de la sociedad civil y partidos políticos. Establece también que el IIDH/CAPEL sustentará su acción en "*el principio de las elecciones libres como parte esencial de la teoría y práctica de los derechos humanos, condición de la democracia y fundamento del derecho a la libre determinación y de la paz en la convivencia nacional e internacional*". En la actualidad CAPEL ejecuta los programas relacionados con derechos y participación políticos que acoge el Instituto Interamericano de Derechos Humanos (IIDH).

El IIDH/CAPEL ha contribuido a fortalecer los procesos democráticos del Continente Americano, privilegiando, como un mecanismo para acompañar la reinserción de sus países a los procesos electorales, el fortalecimiento de los organismos electorales, a través de programas de asistencia técnica, de cooperación horizontal entre estos organismos y de campañas cívicas para el desarrollo de una cultura política democrática.

CAPEL ha propiciado el establecimiento de políticas de intercambio y transmisión de experiencias y conocimientos, lo cual permitió acuñar la expresión y desarrollar el instrumento de la cooperación horizontal en materia de asistencia técnica, de cuya utilidad han sido testigos y beneficiarios los representantes de los organismos electorales miembros de las Asociaciones Protocolo de Tikal, Protocolo de Quito y la Unión Interamericana.

El 10 de noviembre de 2023 se firmó el Convenio de cooperación sobre el sistema informático de Escrutinio, Digitalización, Escaneo y Transmisión de resultados (EDET) dispuesto para las elecciones municipales del 18 de febrero de 2024.

El alcance del proyecto corresponde a la realización de una auditoría técnica de rigor internacional sobre el sistema informático de Escrutinio, Digitalización, Escaneo y Transmisión de resultados (EDET) que se utilizará en las Elecciones Municipales, organizada en 4 etapas, planificación, trabajo de campo, presentación de informe de hallazgos y recomendaciones y seguimiento a través del acompañamiento hasta las elecciones municipales. En cada una de las etapas participará un grupo de especialistas seleccionados de acuerdo con su perfil profesional y experiencia en procesos electorales de diversos países del continente americano.

Realizada la evaluación y el seguimiento de las recomendaciones con el propósito de comprobar el cumplimiento de las recomendaciones planteadas en el informe preliminar de auditoría, los resultados se presentan en este informe con una descripción amplia y los hechos o remediaciones realizadas por la Junta Central Electoral fueron verificadas, al igual que su cumplimiento.

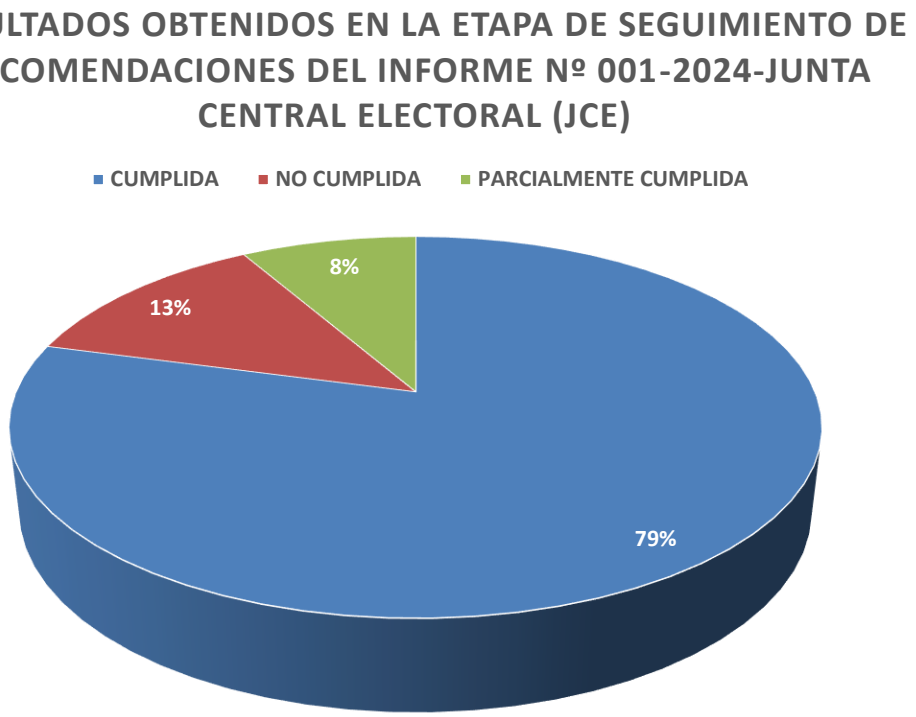
CAPÍTULO III

RESULTADOS OBTENIDOS EN LA ETAPA DE SEGUIMIENTO DE RECOMENDACIONES DEL INFORME No.001-2024-JUNTA CENTRAL ELECTORAL (JCE)

Se realizó el seguimiento de las recomendaciones de remediación emitidas en el Informe No.001-2024-JUNTA CENTRAL ELECTORAL(JCE), donde se obtuvieron los siguientes resultados:

CUADRO RESUMEN DEL CUMPLIMIENTO DE LAS RECOMENDACIONES AL 19 DE ENERO DE 2024

RECOMENDACIONES EMITIDAS	RECOMENDACIONES		
	CUMPLIDAS	PARCIALMENTE CUMPLIDAS	NO CUMPLIDAS
24	19	2	3



Según se detalla en el grafico anterior de las recomendaciones establecidas en el informe No.001-2024-JUNTA CENTRAL ELECTORAL (JCE), se cumplieron diez y nueve (19) recomendaciones que representan un 79%, dos (2) parcialmente cumplidas que representan un 8% y tres (3) no cumplidas que representan un 13% del total de las recomendaciones formuladas.

RECOMENDACIONES CUMPLIDAS

A continuación, se detallan las observaciones de remediación cumplidas:

MATRIZ DE SEGUIMIENTO DE LOS HALLAZGOS DE LA AUDITORIA

No. Ref. del Hallazgo	Hallazgo	Acciones Recomendadas	Acciones Realizadas por el Reponsable de Tecnología de la JCE	Cumplimiento	Comentarios
1	El SISTEMA OPERATIVO DEL EDET CUENTA CON UNA AUTENTICACIÓN INAPROPIADA.	Deshabilitar el inicio de sesión automático para cuentas con privilegios de administrador. Implementar un rol de usuario limitado para que inicie sesión 41 Pruebas de Intrusión - Sistema de Escrutinio Digitalización Escaneo y Transmisión de Resultados automática e inmediatamente arranque el software de EDET.	Se eliminaron privilegios de administración local y al usuario del EDET se le dio solo acceso únicamente a las Apis de Windows necesarias para la ejecución de la aplicación en modo Kiosco.	Cumplida	Al eliminar los privilegios de administración local y limitar los del usuario EDET se elimina esta vulnerabilidad
2	El SISTEMA OPERATIVO DEL EDET CUENTA CON MÚLTIPLES VULNERABILIDADES.	Aplicar inmediatamente todos los parches de seguridad pendientes. Considerar el uso de herramientas de gestión de parches para automatizar este proceso. Modificar el sistema operativo, de tal manera que se garantice que solo el software mínimo necesario se encuentra instalado,	Se aplicaron todas los parches de seguridad y acumulativos actualizados por Microsoft hasta el 27 de diciembre del 2023. Se tiene previsto realizar una nueva actualización previa a la clonación de los equipos que se utilizaran para las elecciones de febrero que	Cumplida	Con la actualización de los parches requeridos se eliminó esta vulnerabilidad
3	LA BASE DE DATOS LOCAL DEL EDET CUENTA CON UNA AUTENTICACIÓN INAPROPIADA.	Configurar la base de datos para que requiera credenciales específicas, independientes de las del sistema operativo. Esto implica implementar un sistema de autenticación propio de la base de datos. Desinstalar las herramientas de gestión de base de datos, instalar el MYSQL en un formato mínimo, contemplando la factibilidad de instalar únicamente el motor de base de datos sin ninguna herramienta adicional.	Se eliminaron los accesos a la base de datos para que los usuarios locales no puedan conectarse, quedando así únicamente acceso al usuario de la aplicación y se instalaron las actualizaciones de seguridad en el SQL Server.	Cumplida	Coin la eliminación de los accesos de los usuarios locales a la base de datos, se eliminó el riesgo
6	FALTA DE RESTRICCIONES EN EL ACCESO AL HARDWARE DEL EDET.	Configurar una contraseña en el BIOS para restringir el acceso y cambios en la configuración del hardware.	Se realizó el cifrado de el BIOS de todos los equipos con un password de alta complejidad con longitud de 15 caracteres; además, se realizó el cifrado de todos los discos duros con la herramienta BLocker, finalmente también se aplico un control para restringir la conexión de dispositivos USB	Cumplida	Con la realización del cifrado del BIOS y el manejo de claves complejas, se eliminó este riesgo

MATRIZ DE SEGUIMIENTO DE LOS HALLAZGOS DE LA AUDITORIA

No. Ref. del Hallazgo	Hallazgo	Acciones Recomendadas	Acciones Realizadas por el Reponsable de Tecnología de la JCE	Cumplimiento	Comentarios
9	FALTA DE CONTROLES PARA EVITAR LA EJECUCIÓN DE UN PROGRAMA DISTINTA AL SOFTWARE DEL EDET.	Establecer políticas de Lista Blanca (Whitelisting) para permitir solo la ejecución de software aprobado (como EDET) y bloquear todo lo demás.	Se instaló en los equipos un cliente del Antivirus Defender en la versión 3.6.5 con funcionalidades de antimalware y un control que impide la instalación de aplicaciones y la ejecución de scripts.	Cumplida	Con la aplicación de los controles que impiden la instalción de aplicaciones y la ejecución de scrips esta vulnerabilidad estaria eliminada
10	FALTA DE CONTROLES PARA EVITAR LA CONEXIÓN DE DISPOSITIVOS NO AUTORIZADOS AL HARDWARE DEL EDET.	Implementar controles que restrinjan el uso de puertos USB a dispositivos autorizados.	Se aplico un control para restringir la conexión de dispositivos USB mediante una lista blanca de acceso.	Cumplida	Con la aplicación de la lista blanca de dispositivos autorizados para su conexión, se elimina esta vulnerabilidad
11	BASES DE DATOS CENTRAL O PRINCIPAL DEL EDET CUENTA CON MÚLTIPLES VULNERABILIDADES.	Instalación de la actualización acumulativa 23 (CU23) para SQL Server 2019, además, observar los boletines de Microsoft para garantizar que todos los parches estén instalados para el día de las elecciones.	Se aplicaron los parches de seguridad actualizados del Microsoft SQL Server con el último CU disponible	Cumplida	Con la aplicación de los parches de seguridad de la base de datos, se elimina esta vulnerabilidad.
12	FALTA DE CONTROLES QUE PERMITEN LA CONEXIÓN DE CUALQUIER CLIENTE A LA BASE DE DATOS CENTRAL O PRINCIPAL DEL EDET. (Prueba realizada en la red interna ambiente QA).	Restringir las conexiones a la base de datos solo desde orígenes confiables y conocidos. Implementar listas de control de acceso por IP, implementar métodos de control que permitan establecer los clientes de base de datos autorizados, de tal manera que se establezcan reglas para que con el usuario recintos la conexión sea solo desde la aplicación EDET, estas capacidades están disponibles en un firewall de base de datos.	Se realizo un proceso de segmentación de la red y se crearon dos APN distintos para separar los ambientes. Se creo el APN JC1 para los ambientes de producción y JC2 para el ambiente de QA y Entrenamientos. Se identificaron los módems que se utilizarían para QA y pruebas (módems de color negro) los cuales se desactivarían el día de las	Cumplida	Con las acciones realizadas para la segmentación de la red y la creación de los dos distintos APNs, se elimina esta vulnerabilidad.
13	EXISTENCIA DE INFORMACIÓN SENSIBLE EN EL CÓDIGO FUENTE DEL SOFTWARE DEL EDET.	Eliminar las credenciales codificadas de los archivos de código fuente. Es esencial que toda información sensible sea manejada de manera segura, preferiblemente a través de mecanismos de almacenamiento y recuperación seguros, en lugar de estar codificada directamente en el código del software.	Se reviso el codigo y se eliminaron las referencias de conexión y las claves quemadas en codigo.	Cumplida	Se verifico el codigo y se confirmó la eliminación de las referencias y las claves qwuemadas en código, eliminando asi esta vulneravilidad.

MATRIZ DE SEGUIMIENTO DE LOS HALLAZGOS DE LA AUDITORIA

No. Ref. del Hallazgo	Hallazgo	Acciones Recomendadas	Acciones Realizadas por el Reponsable de Tecnología de la JCE	Cumplimiento	Comentarios
14	ACCESO A LOS DATOS DE LA BASE DE DATOS CENTRAL O PRINCIPAL DE PRODUCCIÓN DEL PROCESO DE LAS ELECCIONES.	Establecer políticas y controles de acceso que restrinjan la visibilidad entre diferentes entornos (producción, desarrollo, QA), asegurando que solo personal autorizado tenga acceso a datos sensibles de cada entorno. Revisar y documentar los enlaces de confianza de la base de datos que se usará el día de la elección.	Se realizo un proceso de segmentación de la red separando los ambientes de producción y QA y se eliminaron los enlaces de confianza con la base de datos.	Cumplida	Con las acciones realizadas para la separación de los ambientes y la segmentación de la red, se eliminó el riesgo
15	NO EXISTE UNA ESTANDARIZACIÓN EN EL PROCESO DE DESARROLLO DEL SOFTWARE DEL EDET.	Adoptar una metodología de desarrollo de software que les permita contar con un marco de trabajo para estructurar, planificar y controlar el proceso de desarrollo de sistemas de información.	Se inicio el trabajo de incorporar el desarrollo del software del EDET a la metodología de desarrollo existente.	Cumplida	Se pudo constatar que existe una metodología de desarrollo formalmente aceptada por la Dirección de Tecnología y si bien se verificó que esta metodología no se aplicó en una pequeña parte del desarrollo del EDET como es el caso del agente denominado TRXRecinto que se encarga de validar si existen datos para transmitir; además, tomando en cuenta que el Director de Tecnología de la Junta Central Electoral, dispuso a su personal que todos los desarrollos concernientes al Software EDET se incorporen a la metodología de desarrollo existente; con estos criterios, se consideraria esta vulnerabilidad como eliminada.

MATRIZ DE SEGUIMIENTO DE LOS HALLAZGOS DE LA AUDITORIA

No. Ref. del Hallazgo	Hallazgo	Acciones Recomendadas	Acciones Realizadas por el Reponsable de Tecnología de la JCE	Cumplimiento	Comentarios
16	INSUFICIENTE DOCUMENTACIÓN TÉCNICA DEL SOFTWARE DEL EDET.	Elaborar la documentación necesaria para que exista una comprensión adecuada del software del EDET.	Existe documentación actualizada con el detalle de técnico del software del EDET con todos sus módulos.	Cumplida	Se presento documentación técnica actualizada del sistema, solventando asi este hallazgo.
17	NO EXISTE UN PLAN DE TRANSFERENCIA DE CONOCIMIENTOS PARA EL SOFTWARE DEL EDET.	Elaborar y llevar a cabo un plan de transferencia de conocimientos para el software del EDET.	Se dispuso un proceso de transferencia de conocimiento del desarrollo del software del EDET, el cual finalizará previamente a la elección.	Cumplida	Con la disposición realizada por el Director de Tecnología, instruyendo al personal responsable del desarrollo del software EDET la planificación de la transferencia de conocimiento al resto de personal de desarrollo, y al tener una fecha maxima de ejecución previa a las elecciones, se estaría eliminando esta vulnerabilidad.
18	LA BITÁCORA DEL SISTEMA DEL EDET NO CONTIENE TODA LA INFORMACIÓN DE LA TRAZABILIDAD DE LAS ACCIONES REALIZADAS.	Incluir todas las acciones realizadas en la bitácora del sistema del EDET.	Se habilitaron campos en el log de auditoria del sistema para que quede registrada todas las acciones que se realicen y se pueda obtener la trazabilidad completa de las acciones realizadas por un usuario en la	Cumplida	Revisado el archivo de log del sistema se constato que se implementaron nuevos campos que permiten tener la trazasbilidad completa de las acciones realizadas en el EDET
19	EXISTENCIA DE PUNTOS DE MEJORA PARA LA GUÍA RÁPIDA DE INSTALACIÓN DE ELECCIONES MUNICIPALES 2024.	a) Utilizar precintos numerados y registrar el número de precinto con el que sale la maleta y proveer dos precintos adicionales para: b) Agregar en la maleta formularios con el detalle e identificación de los componentes para que el técnico firme y certifique en las instancias de: c) Indicar el peso de la maleta en forma visible para alertar de riesgos en el esfuerzo de quien la manipule y posibles daños por la caída ante un sobreesfuerzo. d) Se recomienda complementar instrucciones	Se actualizó la documentación de instalación con las recomendaciones realizadas y se espera tener una nueva versión para el jueves 18 de enero del 2024 con las novedades presentadas en la prueba regional del sábado 13 de enero del 2024.	Cumplida	Al momento se tiene ya las versiones finales de los documentos con las observaciones recibidas de la prueba regional

MATRIZ DE SEGUIMIENTO DE LOS HALLAZGOS DE LA AUDITORIA

No. Ref. del Hallazgo	Hallazgo	Acciones Recomendadas	Acciones Realizadas por el Reponsable de Tecnología de la JCE	Cumplimiento	Comentarios
20	EXISTENCIA DE DEBILIDADES LOS PROCEDIMIENTOS DE PERSONALIZACIÓN, QC, INSTALACIÓN DEL TÉCNICO DEL RECINTO.	Realizar las recomendaciones descritas en el componente de evaluación de procesos.	Se actualizó la documentación de clonado con las recomendaciones realizadas para en base a la misma los técnicos realicen los procesos de instalación y personalización y se espera tener una nueva versión para el jueves 18 de enero del 2024 con las novedades presentadas en la	Cumplida	Al momento se tiene ya documentado el procedimiento final de clonado con las observaciones recibidas de la prueba regional
21	MECANISMO DE AUTENTICACIÓN INSEGURO UTILIZADO PARA LA TRANSMISIÓN DE RESULTADOS DEL EDET.	Utilizar un token de llave pública privada en el lugar de el MAC address como mecanismo de autenticación	Se modificó el control de autenticación de un dispositivo eliminando el control por la macadress y cambiándolo por el serial de la tarjeta madre del computador controlando el acceso a través de una lista blanca que contiene los seriales de los equipos	Cumplida	Con el cambio realizado al control de los equipos con una lista blanca con los seriales de los equipos autorizados, se eliminó esta vulnerabilidad.
22	EL MODEM MÓVIL UTILIZADO POR EL EDET TIENE LA CONTRASEÑA POE DEFECTO.	Establecer contraseñas completas en todos los modem móviles.	Se está realizando un proceso de cambio de claves de acceso a los módems que estarán activos para las elecciones. Al momento se encuentra un 80% de cumplimiento de este	Cumplida	Se realizó el cambio de claves en la totalidad de los modems que se utilizan en la elección
23	INSUFICIENTES MEDIDAS DE SEGURIDAD EN LA RED INFORMÁTICA.(Prueba realizada en la red interna ambiente QA)	a) Fortalecer las medidas de seguridad con la implementación de equipos y software de monitoreo de amenazas en tiempo real. b) Activar las notificaciones del sistema de monitoreo con un sistema de escalado para evitar falsos positivos	Se implemento un logo on trigger para la identificación de los equipos que pueden autentificarse en la red controlandolos a través de una lista blanca que contiene los seriales de los de equipos que pueden conectarse a la red.	Cumplida	Con la segmentación de la red, la creación de los APNs que separan los ambientes de producción y QA, además de la impkementación del control para la autenticación de los equipos autorizados para su conexión, esta vulnerabilidad quedaría eliminada.

RECOMENDACIONES PARCIALMENTE CUMPLIDAS

A continuación, se detallan las observaciones de remediación parcialmente cumplidas:

MATRIZ DE SEGUIMIENTO DE LOS HALLAZGOS DE LA AUDITORIA

No. Ref. del Hallazgo	Hallazgo	Acciones Recomendadas	Acciones Realizadas por el Reponsable de Tecnología de la JCE	Cumplimiento	Comentarios
7	El SOFTWARE DEL EDET SIN FIRMA DE CÓDIGO.	Desarrollar y aplicar una política estricta de firma de código. Configurar las políticas del sistema operativo para permitir la ejecución solo de aplicaciones que estén firmadas por el certificado de desarrollo.	Se realizó un procedimiento de verificación del software del edet y cuando este se ejecuta, se autoverifica comparando con el hash guardado en base de datos	Parcialmente cumplida	El procedimiento realizado es una verificación de la integridad del ejecutable. Una vez compilada la version del ejecutable se calcula un hash que es almacenado en la base de datos y este es verificado cada vez que el sistema arranca, si el hash concide con el guardado en la base de datos, se establece conexión, caso contrario no se conecta a la base de datos. Si bien no se han implementado firmas digitales en los ejecutables, los controles adoptados proporcionan una capa de seguridad adicional. Estos controles compensatorios reducen significativamente el riesgo de que ejecutables no autorizados sean copiados o ejecutados en el equipo EDET. Por lo que esta vulnerabilidad estaría parcialmente mitigada.

MATRIZ DE SEGUIMIENTO DE LOS HALLAZGOS DE LA AUDITORIA

No. Ref. del Hallazgo	Hallazgo	Acciones Recomendadas	Acciones Realizadas por el Reponsable de Tecnología de la JCE	Cumplimiento	Comentarios
8	PROTECCIÓN INSUFICIENTE DEL SOFTWARE DEL EDET CONTRA PROGRAMAS MALICIOSOS (MALWARE)	Instalar y configurar una solución antimalware avanzada, que ofrezca protección más allá de las capacidades del antivirus por defecto de Windows.	Se instaló en los equipos un cliente del Antivirus Defender en la versión 3.6.5 con funcionalidades de antimalware y un control que impide la instalación de aplicaciones y la ejecución de scripts.	Parcialmente cumplida	Se observó que, aunque no se ha instalado un antivirus distinto al que viene por defecto en Windows, los controles aplicados proporcionan una capa de seguridad adicional. Estos controles compensatorios reducen significativamente el riesgo de que ejecutables con malware sean copiados o ejecutados en el equipo EDET. Por lo tanto, este hallazgo se considera mitigado parcialmente, dado que las medidas implementadas ofrecen una solución que, aunque no elimina completamente la vulnerabilidad, sí reduce su impacto y probabilidad de ocurrencia.

RECOMENDACIONES NO CUMPLIDAS

A continuación, se detallan las observaciones de remediación no cumplidas:

MATRIZ DE SEGUIMIENTO DE LOS HALLAZGOS DE LA AUDITORIA

No. Ref. del Hallazgo	Hallazgo	Acciones Recomendadas	Acciones Realizadas por el Reponsable de Tecnología de la JCE	Cumplimiento	Comentarios
4	CREDENCIALES EXPUESTAS DE LA BASE DE DATOS LOCAL DEL EDET.	Implementar técnicas de cifrado en memoria y realizar una revisión de los procesos que pueden acceder a la memoria para identificar y mitigar la exposición de claves.	Se implementó un control de validación de conexión que únicamente autoriza la interacción a la base de datos local mediante un software que cuente con el hash de seguridad de la JCE previamente registrado en la misma Base de datos. Por tanto, aun ante el escenario de que un atacante obtuviera los credenciales de la base de datos local, estos credenciales serían totalmente inútiles, sino se utiliza con un software previamente registrado por la JCE..	No cumplida	Es importante destacar que, la vulnerabilidad encontrada no ha sido remediada. Si bien al aplicar los procedimientos de endurecimiento de los equipos del EDET, elevaron enormemente la dificultad para llegar a obtener el ejecutable del sistema, disminuyendo así la probabilidad de su explotación. Sin embargo, puede ser posible obtener el ejecutable de otras fuentes y explotar esta vulnerabilidad para ver las credenciales de la base de datos en el binario. En consecuencia, este hallazgo se considera aún no remediado, aunque su severidad haya disminuido.

MATRIZ DE SEGUIMIENTO DE LOS HALLAZGOS DE LA AUDITORIA

No. Ref. del Hallazgo	Hallazgo	Acciones Recomendadas	Acciones Realizadas por el Reponsable de Tecnología de la JCE	Cumplimiento	Comentarios
5	CREDENCIALES EXPUESTAS DEL USUARIO QUE UTILIZA EL EDET PARA CONECTARSE A LA BASE DE DATOS CENTRAL O PRINCIPAL.	Implementar técnicas de cifrado en memoria y realizar una revisión de los procesos que pueden acceder a la memoria para identificar y mitigar la exposición de claves.	Se implementaron una serie de controles compensatorios que impiden que se pueda utilizar las credenciales como único recurso para establecer una conexión no autorizada a la base de datos, debido a que el sistema utiliza métodos de autorización multifactorial, que se describen a continuación: Autorización de medios de comunicación (APN) Autorización de dispositivos de comunicación (MODEM) Autorización de equipo EDET (hardware registrado) Por tanto, aun ante el escenario de que un atacante obtenga los credenciales, si no cuenta con los otros factores de autorización no podría establecer conexión a la base de datos.	**No cumplida**	Een este caso la vulnerabilidad encontrada no ha sido remediada. Si bien al aplicar los procedimientos de endurecimiento de los equipos del EDET, elevaron enormemente la dificultad para llegar a obtener el ejecutable del sistema, disminuyendo así la probabilidad de su explotación. Sin embargo, puede ser posible obtener el ejecutable de otras fuentes y explotar esta vulnerabilidad para ver las credenciales en el binario. En consecuencia, este hallazgo se considera aún no remediado, aunque su severidad haya disminuido.
24	PUERTO EXPUESTO DEL SERVIDOR DE BASE DE DATOS CENTRAL O PRINCIPAL DEL EDET.	Crear una arquitectura basada en APIs, así los clientes solo interactúan con el API y no directamente con el motor de la base de datos	Se implementaron medidas que mitigan este riesgo como el control para la autenticación de equipos mediante una lista blanca, sin embargo queda un riesgo residual que sería aceptado ya que por el tiempo y lo complejo de cambiar la arquitectura de la aplicación no se pudiera realizar al momento.	**No cumplida**	Si bien se implementaron medidas compensatorias que limitan la conección a la base de datos, la solución definitiva es el cambio de arquitectura de la aplicación lo cual por tema de tiempo y complejidad no es posible hacerlo por el momento.