Informe Final del Análisis de Vulnerabilidades a la Infraestructura Tecnológica del Programa de Resultados Electorales Preliminares en Quintana Roo 2022

PREP Quintana Roo 2022

Para dar cumplimiento a los Lineamientos del PREP 2022

Ernesto Guerrero Lara

2/junio/2022

Versión 1.0

Control de Documentación

Control de Configuración

Título:	Informe Final del Análisis de Vulnerabilidades a la Infraestructura del Programa de Resultados Electorales Preliminares en Quintana Roo 2022
Autor(es):	Israel Novelo Zel, Wilberth Pérez Segura, Sergio Cervera Loeza, Ernesto Guerrero Lara
Fecha:	2 de junio de 2022

Histórico de versiones

Versión	Fecha	Estado	Responsable	Nombre de archivo
1.0	2/junio/2022	A	Ernesto Guerrero Lara	Informe Final Auditoría.docx

Estado: (B)orrador, (R)evisión, (A)probado

Histórico de cambios

Versión	Fecha	Cambios
0.1	2/junio/2022	Ninguna, primera versión borrador

Tabla de contenido

1. Antecedentes

De conformidad con lo dispuesto en el artículo 347, numeral 1, incisos a) y b), del Reglamento de Elecciones, el **Instituto Electoral de Quintana Roo (IEQROO)** deberá someter su sistema informático a una auditoría técnica, para lo cual deberá designar un ente auditor. El alcance de la auditoria deberá cubrir el Análisis de Vulnerabilidades, considerando al menos pruebas de penetración y revisión de configuraciones a la infraestructura tecnológica del PREP.

En el anexo 13 "Lineamientos del Programa de Resultados Electorales Preliminares" del Reglamento de Elecciones emitido por el Instituto Nacional Electoral (INE) en su última modificación aprobada mediante acuerdo INE/CCOE004/2021 de fecha 11 de enero de 2021, en su Capítulo III "De la Auditoría del Sistema Informático" se indica que:

> *La auditoría de verificación y análisis del sistema informático que será utilizado en la implementación y operación del PREP, se deberá realizar con la finalidad de evaluar la integridad, disponibilidad y seguridad en el procesamiento de la información y la generación de los resultados conforme a la normativa aplicable y vigente.*

El IEQROO contrata a La Universidad Autónoma de Yucatán por medio de su Facultad de Matemáticas para realizar la Auditoría a la Infraestructura Tecnológica del Programa de Resultados Electorales Preliminares PREP, para el Proceso Electoral 2021-2022 en el estado de Quintana Roo de conformidad con lo establecido en los Lineamientos del PREP vigentes, aprobados mediante Acuerdo INE/CG661/2016 del Consejo General del Instituto Nacional Electoral de fecha 7 de septiembre de 2016 y su última modificación aprobada mediante acuerdo INE/CCOE004/2021 de fecha 11 de enero de 2021, para verificar los principios de certeza, legalidad, independencia, imparcialidad, máxima publicidad y objetividad del ejercicio de la función electoral relativa al diseño, operación e implementación del PREP dentro del Estado de Quintana Roo.

2. De la Auditoría

2.1. Alcance

La auditoría consideró las siguientes líneas de trabajo:

1. Análisis de Vulnerabilidades a la Infraestructura Tecnológica.
    a) Pruebas de Penetración
    b) Revisión de Configuraciones
2. Pruebas de denegación de servicios a los sitios Web del PREP, de Consulta y del IEQROO.

El trabajo de auditoría relacionado con las líneas anteriores concluyó el 2 de junio de 2022. A continuación se presenta el objetivo y alcance de cada línea.

2.2. Análisis de Vulnerabilidades a la Infraestructura Tecnológica

Los objetivos de esta línea de trabajo fueron:

- Identificar debilidades de seguridad en la infraestructura tecnológica mediante la ejecución de pruebas de penetración y revisión de configuraciones de seguridad.
- Clasificar el impacto y documentar las vulnerabilidades identificadas con el propósito de recomendar al IEQROO las posibles medidas para la mitigación de las vulnerabilidades que previamente fueron identificadas y documentadas.
- Verificar que las medidas implementadas por el IEQROO hayan atendido adecuadamente las vulnerabilidades reportadas.

2.2.1. Pruebas de Penetración

El objetivo fue realizar pruebas de penetración que permitan evaluar las medidas de seguridad de la infraestructura tecnológica del PREP, documentar los hallazgos para identificar oportunidades y emitir recomendaciones orientadas al fortalecimiento de ésta.

Las pruebas de penetración se llevaron a cabo tanto desde el interior como desde el exterior de la red de datos a examinar y se enfocaron en:

- Servidores físicos.
- Servidores virtuales.
- Equipos de telecomunicaciones.

La metodología que se utilizó incluyó pruebas de penetración y verificación de controles de seguridad de infraestructura y de aplicación, se basó en los estándares de seguridad Application Security Verification Standard (ASVS), la Testing Guide de la OWASP y el Critical Security Controls (CSC) del Center for Internet Security (CIS).

2.2.2. Revisión de Configuraciones

El objetivo fue analizar las configuraciones de los dispositivos que conforman la infraestructura tecnológica con base en mejores prácticas de seguridad informática para identificar oportunidades y emitir recomendaciones orientadas al fortalecimiento de ésta.

La revisión de configuraciones se realizó sobre:

- Servidores Virtuales y Físicos.
- Equipos de telecomunicaciones.
- Estaciones de trabajo.

Las revisiones de seguridad estuvieron basadas en los estándares de seguridad Application Security Verification Standard (ASVS) y Critical Security Controls (CSC).

2.2.3. Alcance

Se auditó el Centro de Comunicaciones y Cómputo (C3) principal y una muestra de nueve Centros de Acopio y Transmisión de Datos (CATD) seleccionados en común acuerdo con el IEQROO.

2.3. Pruebas de denegación de servicios

El objetivo fue realizar ataques de denegación de servicio que permitan identificar, evaluar y aplicar las medidas necesarias para asegurar la correcta y continua disponibilidad del servicio Web del sitio de publicación de resultados del PREP, del sitio de Consulta y del sitio principal del IEQROO, durante el periodo de operación del PREP y documentar los hallazgos detectados durante la realización de las pruebas.

2.3.1. Alcance

Las pruebas de denegación fueron de dos tipos:

- Tráfico no malintencionado.
- Tráfico de red malintencionado, consistente en paquetes de red malformados.

3. Resultados

Al concluir los trabajos de Auditoría, con fecha 2 de junio de 2022, se tienen los siguientes resultados.

3.1. Análisis de Vulnerabilidades a la Infraestructura Tecnológica

3.1.1. Pruebas de Penetración

Las pruebas de penetración a la infraestructura tecnológica de los Servidores que conforma el site principal del IEQROO y los servidores de la nube para Publicación y Consulta, indican que la infraestructura tecnológica del PREP cuenta con políticas y buenas prácticas de seguridad para garantizar la confidencialidad, integridad de la información y servicios a prestar durante la operación del PREP.

3.1.2. Revision de Configuraciones

La revisión de configuraciones a la infraestructura tecnológica que conforma el site principal del IEQROO y CATDs visitados indica que éstos cuentan con políticas y buenas prácticas de seguridad para garantizar la confidencialidad y disponibilidad de los servicios e información a prestar durante la operación del PREP.

3.2. Pruebas de denegación de servicio

Con base en los resultados de las pruebas de denegación de servicio a los sitios de publicación del PREP, Consulta y del IEQROO, el ente auditor establece que:

- El sitio de publicación del PREP y el sitio Consulta cuentan con la adopción e implementación de buenas prácticas de seguridad y disponibilidad del servicio para ser consultado continuamente por la Ciudadanía durante la operación del PREP.
- El sitio principal del IEQROO cuenta con la adopción e implementación de buenas prácticas de controles de disponibilidad del servicio para ser consultado continuamente por la Ciudadanía durante la operación del PREP.

MC Ernesto Antonio Guerrero Lara
Coordinador del Proyecto
Facultad de Matemáticas - UADY