Informe técnico a la Auditoría a los Sistema PREP y PREP Casilla

L.I. José Rómulo Bailón Barrón
Ing. Oscar Beltrán Gómez
M.I. Arión Ehécatl Juárez Menchaca
M.S.I. Sergio Antonio Talavera Carbajal

Índice

Introducción

El Programa de Resultados Estadísticos Preliminares (PREP) es el mecanismo de información electoral que provee los resultados preliminares y no definitivos, de carácter estrictamente informativo a través de la captura, digitalización y publicación de los datos asentados en las actas de escrutinio y cómputo de las casillas que se reciben en los centros de acopio y transmisión de datos autorizados por el Instituto Estatal Electoral (IEE).

En este marco de actividades se es necesaria la realización de una auditoría a la infraestructura del PREP y PREP Casilla, de conformidad con lo dispuesto en la sección cuarta, del capítulo II, título I, Libro Tercero del Reglamento de Elecciones del INE, así como del título II, de los Lineamientos del Programa de Resultados Electorales Preliminares (PREP), Anexo 13 de dicho Reglamento.

La auditoría de verificación y análisis de la infraestructura y del sistema informático que será utilizado en la implementación y operación del PREP y PREP Casilla, se deberán 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.

AUDITORÍA AL SISTEMA INFORMÁTICO Y A LA INFRAESTRUCTURA TECNOLÓGICA DEL PREP

En el marco de las actividades para la implementación y operación del Programa de Resultados Electorales Preliminares (PREP) y PREP Casilla para el Proceso Electoral 2021 en el estado de Chihuahua, se llevó a cabo la auditoría al sistema informático y a la infraestructura tecnológica del PREP, de conformidad con lo dispuesto en la sección cuarta, del capítulo II del Reglamento de Elecciones del INE, así como del título II, capítulo III, de su Anexo 13 relativo a los Lineamientos del PREP.

A continuación se presenta el trabajo realizado en la auditoría a los sistemas del PREP y PREP Casilla.

I. Análisis de vulnerabilidades a la infraestructura tecnológica

Introducción

El análisis de vulnerabilidades a la infraestructura tecnológica contempla desde la verificación de la red de comunicaciones y cableado eléctrico, hasta cuestiones de seguridad relacionadas con riesgos de penetración y sus posibles consecuencias, para lo cual, este sprint contempla:

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

Revisión de Infraestructura.

Para la auditoría a la infraestructura del OPL se realiza la visita a las oficinas centrales y al centro operativo, donde se puede establecer que en términos generales que la red de datos **CUMPLE SATISFACTORIAMENTE** con la evaluación basada en el cuestionario e inspección visual que se realizó como parte de esta auditoría, en los informes técnicos entregados al centro operativo del PREP se detalla las observaciones y procedimientos realizados para esta inspección.

Análisis de vulnerabilidades a la red interna del IEE de Chihuahua

Cualquier vulnerabilidad crea brechas en la integridad de la red que los atacantes pueden aprovechar para obtener acceso a la red. Una vez dentro de la red, un atacante puede realizar ataques malintencionados, robar datos confidenciales y causar daños importantes a los sistemas críticos.

Observaciones

Los resultados obtenidos a partir de la auditoría realizada informan que la infraestructura del Instituto Estatal Electoral (IEE) de Chihuahua **cumple satisfactoriamente** en términos generales de la auditoría y su revisión, haciendo notar en los informes técnicos las diferentes oportunidades de mejora.

Con respecto a las vulnerabilidades, estas no representan un riesgo alto en la seguridad del sistema y su funcionamiento, por lo que las condiciones para su operación son **aceptables**.

II. Pruebas de denegación de servicios al sistema PREP.

Introducción

Los ataques DDoS (por sus siglas en inglés, **D**istributed **D**enial **o**f **S**ervice) se utilizan para sobrecargar la infraestructura de red orientada a Internet y los servicios de los que dependen muchas empresas. Su habilidad para causar cortes en la red y un caos general en cualquier empresa y en su personal de seguridad de TI hace que los ataques DDoS sean un asunto particularmente problemático para las empresas de cualquier tamaño.

Los ataques DDoS están diseñados para evitar que los usuarios legítimos accedan al sitio web de una empresa o a sus servicios empresariales, separándolos con una cantidad desbordante de solicitudes, paquetes y datos ilegítimos, además de otros tipos de tráfico de red.

Aunque los ataques DDoS son, en su mayoría, generados por “Hackers” o personas maliciosas también se dan en pruebas de seguridad y de rendimiento, esto para garantizar el buen funcionamiento de las aplicaciones y sitios Web.

Actualmente tenemos un caso especial de ataque DDoS propiciado por la demanda legítima de usuarios interesados en las publicaciones y servicios de algún sitio Web, este ataque (que se apega más que nada al rendimiento del sitio) se le suele denominar “Pruebas de Estrés”; el IEE de Chihuahua entra en este último caso al publicar los resultados preliminares de las elecciones de este año.

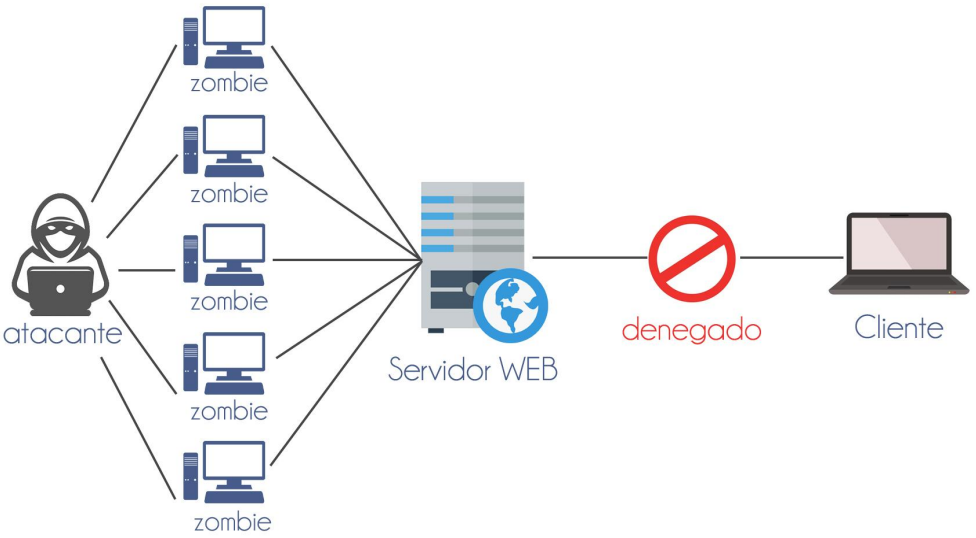

Imagen 2.1. Boceto de un ataque DDoS.

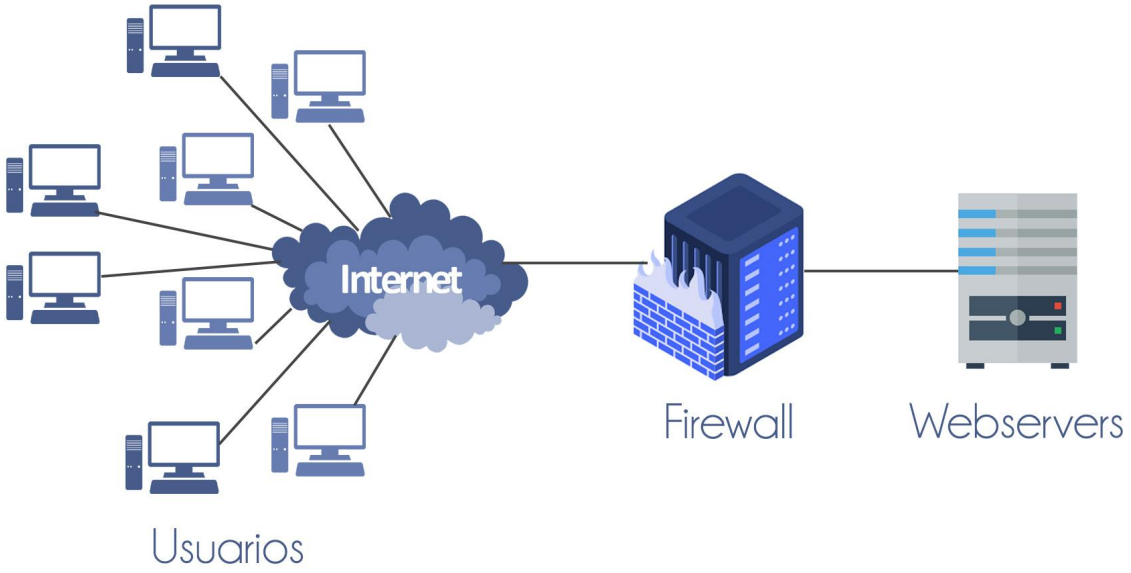

Imagen 2.2. Boceto de un ataque de Estrés.

Pruebas de estrés

Las pruebas de estrés fueron llevadas a cabo durante los simulacros programados los días 16, 23 y 30 de Mayo, para lo cual se utilizaron instalaciones de la Universidad Autónoma de Chihuahua así como del Instituto Tecnológico de Chihuahua 2 además de varias herramientas de software y scripts desarrollados ex profeso.

De acuerdo al horario establecido para los simulacros se realizaron varios periodos de pruebas entre las 16:00 y 18:00 hrs., durante los cuales fueron lanzados ataques simultáneos ejecutando las herramientas de software disponibles así como los scripts desde varios equipos ubicados en ambas locaciones.

Para el tercer simulacro se hacen notar las mejoras presentadas de acuerdo a la infraestructura que aloja el servicio de publicación de resultados del PREP.

Observaciones

A lo largo de los tres simulacros y de las pruebas a las que fue sometido el sitio de publicación del Prep 2021 se ha visto que:

- Son perceptibles las mejoras y el nivel de infraestructura del sitio, de acuerdo a los tres simulacros realizados.
- Los ajustes realizados dan un buen precedente del nivel técnico y del tiempo de respuesta por alguna contingencia.
- Los nombres de dominio dan seriedad al proceso, dado que podría darse el caso de sitios falsos que pudieran difundir datos erróneos.
- Las pruebas arrojaron resultados **satisfactorios** en los niveles de carga y estrés.

Los ajustes, pruebas y la configuración de los nombres de dominio generan un buen grado de certeza en el comportamiento del sitio de las publicaciones PREP en las futuras elecciones del 6 de Junio, sin embargo, y particularmente por la naturaleza tecnológica de los sitios Web, no es posible asegurar en un 100% que el sitio de publicación PREP así como cualquier otro sitio presente en Internet, se encuentre libre de ataques y posibles vulnerabilidades.

III. Validación del sistema informático del PREP y de sus bases de datos, ante un tercero con fé pública

Introducción

La auditoría de validación del sistema informático del PREP y de sus bases de datos que operará el día de las elecciones, tiene como objetivo verificar los sistemas que serán usados el día de la jornada electoral, así como validar que las bases de datos que almacenarán la información correspondiente al proceso de votación se encuentren sin registros adicionales y operen adecuadamente.

Validación y verificación de los sistemas informáticos PREP y PREP Casilla

Para la validación y verificación de los sistemas que serán utilizados el día de la jornada electoral, se llevaron a cabo los siguientes análisis:

Base de datos. Se realizó la verificación de la base de datos que contendrá la información del PREP.

Sistema PREP

En este apartado se realizan el registro del número de versión, las firmas digitales (Hash) del sistema PREP y de los archivos que se consideraron pertinentes para su revisión; el proceso anterior se realiza con el objetivo de hacer una comparación el día de la elección con los sistemas y archivos que se utilizarán, dando certeza al proceso ya que estos archivos serán los mismos que fueron auditados.

Asimismo se realiza el proceso en forma de simulacro que describe cómo será llevado a cabo el día de las elecciones, se revisa inicialmente que tanto la base de datos como el sitio Web de publicación no tenga información innecesaria y la base de datos se encuentre inicializada.

Sistema PREP Casilla

Después del análisis y auditoría del sistema instalado en los dispositivos móviles para la captura de las actas o PREP Casilla se obtienen **resultados favorables** en términos generales.

Observaciones

Los sistemas PREP y PREP Casilla **son aptos** para su operación durante la jornada electoral del 6 de junio de 2021. En general son sistemas estables que dan el resultado esperado en cuanto a las salidas con respecto a las entradas recibidas, sin embargo, en los informes técnicos entregados al IEE de Chihuahua se expusieron oportunidades de mejora para que los sistemas sean más eficientes y robustos.

IV. Pruebas funcionales de caja negra al sistema informático del PREP

Introducción

La auditoría de verificación y análisis del sistema informático que será utilizado en la implementación y operación del PREP, mediante la realización de pruebas funcionales de caja negra; 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.

A continuación se presenta el análisis y observaciones al proceso de operación del Programa de Resultados Estadísticos Preliminares (PREP) del Instituto Estatal Electoral (IEE) de Chihuahua que será utilizado durante la jornada electoral el día 6 de junio de 2021.

Pruebas funcionales de caja negra

Se realizan las pruebas funcionales de caja negra al sistema en el marco de la auditoría al PREP y PREP Casilla a las 11 horas del día 3 de junio de 2021, en el Centro de Acopio y Transmisión de Datos (CATD) ubicado en la Asamblea Municipal de Chihuahua.

Observaciones

La evaluación de caja negra a los sistemas (PREP y PREP Casilla) del Instituto Estatal Electoral de Chihuahua fue **satisfactoria**, los votos de las actas capturadas, fueron procesadas de manera correcta según sus particularidades, obteniendo los resultados esperados, así como su publicación de manera correcta.

Conclusiones

Los resultados de la Auditoría muestran que la infraestructura y el sistema PREP y PREP Casilla **son considerados aptos** para su funcionamiento en el proceso electoral del 6 de junio de 2021. Los detalles y reservas de esta auditoría son entregados al IEE de Chihuahua en los informes técnicos correspondientes.