UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MÉXICO

FACULTAD DE INGENIERÍA

IMPLEMENTACIÓN DE SEGURIDAD EN LA INFRAESTRUCTURA DE RED PARA LA DIFUSIÓN DEL PROGRAMA DE RESULTADOS ELECTORALES PRELIMINARES 2017 EN EL ESTADO DE MÉXICO BAJO LA NORMA ISO/IEC 27001:2013

TESINA

QUE PARA OBTENER EL TÍTULO DE

INGENIERA EN COMPUTACIÓN

PRESENTA:

GABRIELA PIÑA REMIGIO

ASESOR:

DR. MARCELO ROMERO HUERTAS

TOLUCA, MÉXICO ABRIL 2018

RESUMEN

Esta tesina muestra una descripción general del proceso de difusión de los resultados electorales del Programa de Resultados Electorales Preliminares del Instituto Electoral del Estado de México realizado el 4 de junio de 2017 para la elección de Gobernador en el Estado de México.

Específicamente se describe como se implementó seguridad en la Infraestructura que se utilizó para la difusión de los resultados electorales. Así mismo, se detalla la infraestructura que operó para la difusión del PREP, la cual estaba compuesta del hosteo del servicio web en un centro de datos que cuenta con el nivel Tier IV e International Computer Room Expert Association (ICREA) nivel 5. Además, el servicio de hosteo contó con seguridad en la web a través de la implementación de un firewall del tipo Web Application Firewall (WAF), el cual se utilizó principalmente para bloquear los ataques del tipo Distributed Denial of Service (DDoS). La infraestructura del PREP contaba con un ancho de banda a internet de 6 Gbps.

El PREP en el IEEM está certificado bajo la norma ISO 27001:2013, por lo que esta infraestructura fue implementada para cumplir con los objetivos de seguridad de la información, además como una solución de mejora continua (ISO, 2016).

Las pruebas realizadas a la infraestructura fueron pruebas de estrés y un ataque de Denial of Service (DoS). Estas pruebas sirvieron para identificar algunas vulnerabilidades en la infraestructura, con el fin de que el día de la Jornada Electoral se garantizara el cumplimiento de los objetivos de seguridad propuestos por el IEEM.

En particular, las pruebas de estrés se realizaron para cuantificar la capacidad y disponibilidad que ofrecía la infraestructura, para validar los requerimientos de rendimiento y la escalabilidad de la plataforma “difusión del PREP”. Con lo cual se verificó que la página se mantuvo en línea en los tiempos comprometidos, sin embargo, se observó que los tiempos de recarga de la página web se fueron incrementando.

De igual manera, en las pruebas se incluyó un ataque de Denial of Service (DoS), para monitorear el consumo de ancho de banda o sobrecarga de los recursos disponibles, con ello se incrementó el tiempo de espera de la página web, aunque siempre se mantuvo en línea. Este fenómeno tuvo presencia el día de la Jornada Electoral.

Contenido

INTRODUCCIÓN

Siempre que se habla de elecciones en un país o estado, resulta un tema importante e interesante, ya que en ella se elegirá a un representante que gobernará un determinado lugar por cierto tiempo, así mismo la ciudadanía involucrada le interesa conocer de cerca los resultados de cada candidato.

Hoy en día, gracias al avance de la tecnología e implementación de las TIC es posible conocer en tiempo y forma el progreso de una elección, de esta forma la ciudadanía podrá seguir los resultados y estará informada de la evolución del proceso electoral.

En México existen Organismos Públicos Locales (OPL) que son los encargados de organizar las elecciones en sus entidades federativas. El Instituto Electoral del Estado de México (IEEM) es un OPL que, de manera conjunta con el Instituto Nacional Electoral, tiene a su cargo la función estatal de la organización de las elecciones en el Estado de México (IEEM, 2015).

El IEEM es una Institución de carácter permanente, y profesional en su desempeño que se rige por los principios de certeza, imparcialidad, independencia, legalidad, máxima publicidad y objetividad (IEEM, 2015).

Como OPL el IEEM debe implementar el Programa de Resultados Electorales Preliminares (PREP) para dar cumplimiento a lo establecido en el artículo 1°, fracción I, de los Lineamientos del Programa de Resultados Electorales Preliminares del Reglamento de Elecciones emitido por el Instituto Nacional Electoral, en el código Electoral del Estado de México, y en los Lineamientos Operativos del Programa de Resultados Electorales Preliminares 2017 emitidos por el IEEM. (IEEM, 2017)

Así mismo, el IEEM cuenta con la Unidad de Informática y Estadística quien es el área responsable de la implementación y operación del PREP en el proceso electoral 2016-2017 (IEEM, 2016), de tal manera que, como última parte del proceso de PREP

se tiene la publicación o difusión de los resultados electorales, el cual tiene como propósito el presente trabajo de tesina.

El día de la Jornada Electoral el IEEM debe difundir los resultados de la elección en su página web, de tal forma que, la información que se difunda debe contar con una disponibilidad alta, de igual manera, la información se debe presentar en tiempo y forma para que puedan ser consultadas por los Integrantes del Consejo General, por los medios de comunicación y por la sociedad interesada en el Estado de México.

Por otra parte, los resultados deben estar disponibles en un lapso de veinticuatro horas, iniciando a las 18:00 horas del día de la Jornada Electoral y terminando el día siguiente a las 18:00 horas (INE, 2016).

Específicamente, ésta tesina muestra cómo se implementó la seguridad en la infraestructura de red para la difusión del Programa de Resultados Electorales Preliminares 2017 en el Estado de México bajo la norma ISO/IEC 27001:2013.

Para el PREP la información es uno de los insumos importantes, es por ello, que se debe garantizar la transparencia, la confidencialidad, la credibilidad y la integridad de la información que se difunde, en el tiempo que opera este programa.

Por lo tanto, el tema de seguridad de la información juega un papel importante, haciendo énfasis que las características que definen la seguridad de la información son cuatro: confidencialidad, integridad, autenticidad y disponibilidad. No todas estas características deben estar vigentes simultáneamente, ni tienen todas la misma importancia en todas las circunstancias, al contrario, las circunstancias en las que está inmerso el ciclo de retroalimentación determinan cuales de estas características son las importantes o deseables (Daltabuit, Hernández, Mallén, & Vázquez, 2007). En este caso para la difusión de los resultados electorales el objetivo de seguridad más importante es la disponibilidad ya que se debe garantizar que los resultados estarán disponibles las 24 horas que dura el PREP, sin embargo, la Integridad también se debe considerar ya que no se debe manipular dicha información.

Objetivo general

Documentar el diseño de la infraestructura de red para la difusión en Internet del Programa de Resultados Electorales Preliminares en el Estado de México, que permita alcanzar los objetivos de seguridad propuestos por el IEEM.

Alcance y limitaciones

En el Instituto donde se desarrolló el presente trabajo de titulación, existen varias unidades, específicamente se colaboró con la Unidad de Informática y Estadística en la subjefatura de Informática en Infraestructura, donde se llevó a cabo la difusión de los resultados de la jornada electoral del día 4 de junio de 2017 en el Estado de México.

El alcance de este trabajo fue determinado con base a los requerimientos estipulados en los lineamientos Operativos del Programa de Resultados Electorales Preliminares 2017, en la sección publicación de resultados.

Organización del documento

El contenido de este trabajo de tesina está estructurado de la siguiente forma:

*En el Capítulo I, s*e plantea la situación actual del IEEM, donde se abordan temas relacionados con el PREP, definición, características, objetivo y cómo se lleva a cabo el proceso en general. Además, se explica el proceso de la difusión de los resultados electorales como última parte del PREP. Para finalizar este capítulo, se realiza un análisis del PREP 2015 y se describen algunas alternativas de solución.

*En el Capítulo II, s*e describen las características de la Infraestructura que se utilizó y las tecnologías que se implementaron para cubrir la parte de seguridad de la información.

El Capítulo III. Se describen las pruebas que se realizaron, además se muestra el desempeño real y los hallazgos obtenidos el día de la Jornada Electoral.

Finalmente se presenta una sección de conclusiones donde se describen las generalidades del trabajo.

CAPÍTULO I. ANTECEDENTES

1.1. INSTITUTO ELECTORAL ESTADO DE MÉXICO

El Instituto Electoral del Estado de México, en términos de la base V del artículo 41 de la Constitución Política de los Estados Unidos Mexicanos, es un organismo público local que, de manera conjunta con el Instituto Nacional Electoral, tiene a su cargo la función estatal de la organización de las elecciones en el Estado de México (IEEM, 2015).

Conforme al artículo 116, fracción IV, inciso c, de la Constitución Política Federal, así como los diversos 11, párrafo primero de la Constitución Política del Estado Libre y Soberano de México el Organismo Público Electoral del Estado de México, y 168 del Código Electoral del Estado de México, se denomina Instituto Electoral del Estado de México, que se encuentra dotado de personalidad jurídica y patrimonio propio, autónomo en su funcionamiento e independiente en sus decisiones, responsable de la organización, desarrollo y vigilancia de los procesos electorales para las elecciones de Gobernador, Diputados a la Legislatura del Estado y miembros de Ayuntamientos, y cuya función la realiza a través del Instituto Nacional Electoral (IEEM, 2015).

Además, es una Institución de carácter permanente, y profesional en su desempeño que se rige por los principios de certeza, imparcialidad, independencia, legalidad, máxima publicidad y objetividad (IEEM, 2015).

Son algunas funciones del Instituto:

- Desarrollar y ejecutar los programas de educación cívica.
- Orientar a los ciudadanos para el ejercicio de sus derechos y cumplimiento de sus obligaciones político electorales.
- Llevar a cabo las actividades necesarias para la preparación de la jornada electoral

- Imprimir los documentos y producir los materiales electorales, en términos de los lineamientos que al efecto emita el Instituto Nacional Electoral.
- Efectuar el escrutinio y cómputo total de la elección para diputados, integrantes de los ayuntamientos, con base en los resultados consignados en las actas de cómputos distritales y municipales.
- Implementar y Operar el Programa de Resultados Electorales Preliminares de las elecciones locales, de conformidad con las reglas, lineamientos, criterios y formatos que para efecto emita el Instituto Nacional Electoral.
- Ordenar la realización de conteos rápidos, basados en las actas de escrutinio y cómputo de casillas a fin de conocer las tendencias de los resultados el día de la Jornada Electoral, de conformidad con los lineamientos que emita el Instituto Nacional Electoral.
- Organizar, desarrollar y realizar el cómputo de votos y declarar los resultados de los mecanismos de participación ciudadana en términos de este código.
- Supervisar las actividades que realicen los órganos distritales y municipales, durante el proceso electoral de que se trate.

El Instituto Electoral del Estado de México nace en el año 1996, a la fecha ha organizado 15 elecciones, desde el año 2000, el IEEM ha tenido a su cargo la Implementación y operación del Programa de Resultados Electorales Preliminares, misma que ha tenido lugar la difusión o publicación de los resultados, tema en el que se centra este trabajo (IEEM, 2015).

1.2. PROGRAMA DE RESULTADOS ELECTORALES PRELIMINARES

El PREP constituye el mecanismo de información electoral de carácter estrictamente informativo que se encarga de proveer los resultados preliminares y no definitivos de un proceso electoral, a través de la digitalización de las Actas de Escrutinio y Cómputo que se reciben de las mesas directivas de casillas en los Centros de Acopio y Transmisión de Datos (CATD), así como la transmisión, captura,

validación y publicación de los datos asentados en ellas en los Centros de Captura y Validación (CCapV) autorizados por el IEEM y su posterior difusión (IEEM, 2017).

Es un programa único, conformado por recursos humanos, materiales, procedimientos operativos, procedimientos de captura, digitalización y publicación por medio del uso de TIC, que garantiza la seguridad, la transparencia, la confiabilidad y la integridad de las elecciones estatales (IEEM, 2017).

En la Figura 1 se muestran gráficamente las Actividades y elementos del PREP:

- Identificación del Acta de Escrutinio y Cómputo (AEC) de cada casilla, colocándose una etiqueta de código de barras en cada una de las oficinas distritales en días previos a la Jornada Electoral. Las etiquetas serán enviadas por la Unidad de Informática y Estadística a la Dirección de Organización, quien las distribuirá en las Juntas Distritales para su colocación durante el armado de los paquetes electorales.
- Colocación de la primera copia del Acta de Escrutinio y Cómputo en el sobre-PREP, actividad que realizan los funcionarios de la Mesa Directiva de Casilla en presencia de los representantes; es el elemento generador de la información de los resultados electorales.
- Traslado de los paquetes electorales a los consejeros distritales y recepción de los paquetes y los sobres-PREP, esta actividad se lleva a cabo en la sede de los consejeros distritales ante la presencia de los representantes. Incluye la entrega del paquete electoral al pleno del Consejo Distrital correspondiente y la entrega del sobre-PREP a los CATD.
- Digitalización y Transmisión de la imagen del AEC; se registra la fecha y hora en la que ingresaron, para que posteriormente, se digitalicen y se transmitan al Centro Estatal de Cómputo (CEsCO).
- Captura y verificación; a partir de los datos de la imagen de las AEC, los resultados asentados en las AEC se transcribirán, utilizando para ello el sistema informático de registro de resultados preliminares, inmediatamente después se

verificarán los datos registrados y las imágenes de las AEC en el mismo sistema.

- Concentración de los resultados; la llegada de los datos vía red local, y las imágenes vía enlaces de telecomunicaciones al CEsCO, permitirá generar los concentrados estatales y distritales. Se confirmará que los datos provengan de lugares reconocidos y que correspondan a parámetros válidos.
- Presentación de resultados; a partir de los resultados concentrados, estos se difundirán a la Sala de Sesiones del Consejo General, los portales web de los difusores oficiales; así como al Centro de Comunicaciones, donde se ubicarán los representantes de los medios de comunicación acreditados para la jornada electoral.

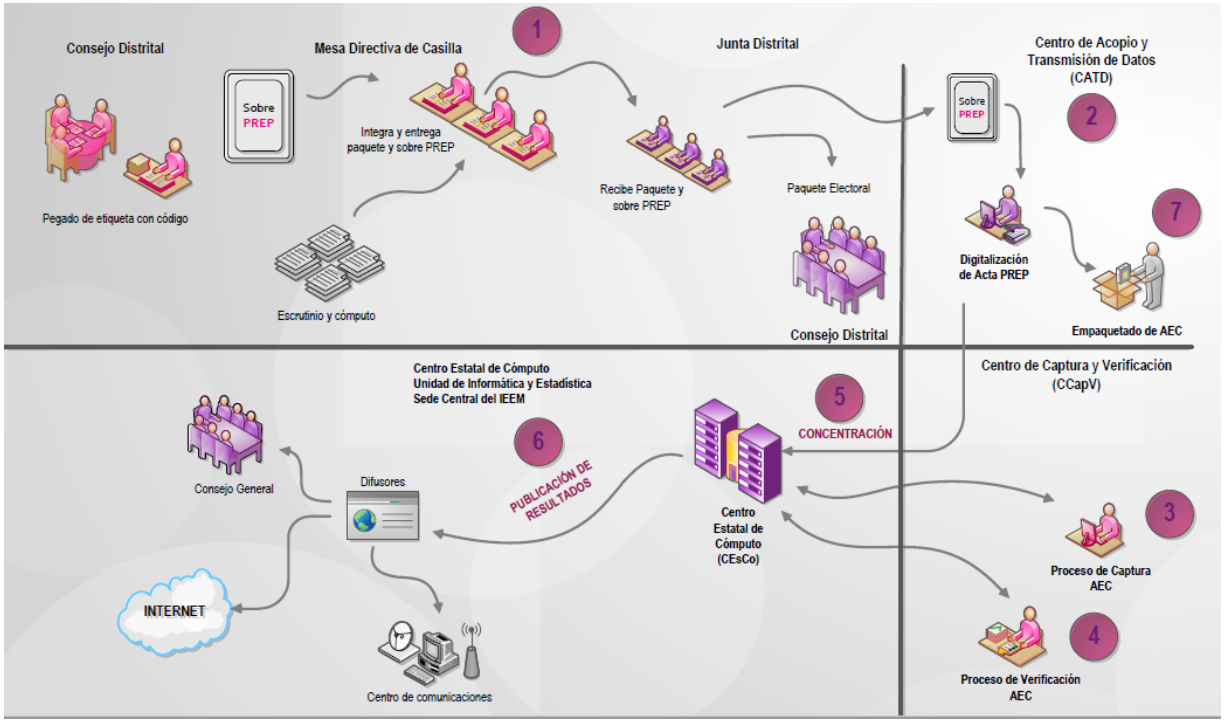


Figura 1. Actividades y elementos del PREP (IEEM, 2017)

El PREP tiene por objetivo principal, proporcionar información veraz y oportuna a los integrantes del Consejo General, a los medios de comunicación y a la sociedad interesada, de los resultados preliminares que se obtengan en las elecciones, cumpliendo en todo momento con los principios de certeza, legalidad, independencia,

imparcialidad, máxima publicidad y objetividad en lo relativo al diseño, operación e implementación del PREP (IEEM, 2017).

1.3. COMISIÓN ESPECIAL DEL PROGRAMA DE RESULTADOS ELECTORALES PRELIMINARES

La Comisión Especial para la atención del Programa de Resultados Electorales Preliminares, es una Comisión que auxilia al Consejo General en la Coordinación de las actividades relativas a la implementación y operación del Programa de Resultados Electorales Preliminares (IEEM, 2016).

La Comisión se integra por un Consejero (a) presidente (a), dos Consejeros (as) Electorales, un Secretario Técnico, un Secretario Técnico suplente, y los representantes de los partidos políticos. Así mismo la Comisión tiene los siguientes objetivos (IEEM, 2016).

- Proponer al Consejo General la designación de los órganos internos responsables de la coordinación de las actividades del Programa de Resultados Electorales Preliminares.
- Fungir como órgano auxiliar del Consejo General del Instituto, responsable de supervisar el desarrollo de las actividades del Programa de Resultados Electorales Preliminares.
- Verificar la aplicación del Reglamento de Elecciones del Instituto Nacional Electoral, en relación a la implementación del Programa de Resultados Electorales Preliminares.
- Dar seguimiento a los trabajos relativos a la implementación y operación del Programa de Resultados Electorales Preliminares.
- Supervisar la correcta integración y funcionamiento del Comité Técnico Asesor del Programa de Resultados Electorales Preliminares (COTAPREP).
- Vigilar que quienes operen el Programa de Resultados Electorales Preliminares garanticen su correcto funcionamiento para proporcionar a la

ciudadanía, información veraz y oportuna de los resultados preliminares de la elección de Titular del Ejecutivo del Estado de México.

- Resolver los aspectos no provistos en la normatividad aplicable.

1.4. COMITÉ TÉCNICO ASESOR DEL PROGRAMA DE RESULTADOS ELECTORALES PRELIMINARES

El Comité Técnico Asesor se crea para brindar asesoría técnica en materia de Resultados Electorales Preliminares a la Comisión Especial para la atención del Programa de Resultados Electorales Preliminares (IEEM, 2016).

El Comité Técnico Asesor tiene las siguientes funciones:

- Realizar análisis, estudios y propuestas, en el desarrollo y optimización del Programa de Resultados Electorales Preliminares, con la finalidad que éste cumpla con los objetivos y metas planteadas.
- Asesorar los trabajos propios del Programa de Resultados Electorales Preliminares en materia de tecnologías de la información y comunicaciones, investigación de operaciones, análisis estadístico, así como en aspectos logístico operativos.
- Asesorar y dar seguimiento a la implementación y operación de los mecanismos para llevar a cabo el Programa de Resultados Electorales Preliminares.
- Dar seguimiento a la coordinación y supervisión de la instalación y operación de los equipos de digitalización y captura, así como a la capacitación del personal o de los prestadores de servicios, en su caso, electores preliminares.
- Asesorar y dar seguimiento en el diseño y aplicación del sistema de digitalización, captura y verificación, del procedimiento de transmisión y recepción, así como las medidas de las medidas de seguridad y protección, consolidación, procesamiento y publicación de la información.
- Revisar y emitir recomendaciones sobre la forma en que será presentada la información del Programa de Resultados Electorales Preliminares en las diferentes pantallas de publicación.

- Realizar reuniones de trabajo con representantes de los partidos políticos y, en su caso, de los candidatos independientes ante el Consejo General, para dar a conocer el plan de trabajo, avances y seguimiento de la implementación y operación del Programa de Resultados Electorales Preliminares.
- Presenciar la ejecución de todos los simulacros del Programa de Resultados Electorales Preliminares, debiendo asistir a algún recinto donde se lleve a cabo el proceso técnico operativo de al menos un simulacro
- Elaborar un informa final de las actividades desempeñadas durante la vigencia del Comité Técnico Asesor del Programa de Resultados Electorales Preliminares.

1.5. PROBLEMÁTICA

La Unidad de Informática y Estadística es el área responsable del diseño e implementación del PREP, por lo que es el área encargada de difundir los resultados de las elecciones, y lo realiza por medio de la red informática denominada Internet, conforme a lo dispuesto en el Reglamento de elecciones del INE y a los lineamientos operativos del PREP 2017 emitidos por el IEEM.

El procedimiento de resultados preliminares consiste en acumular los votos obtenidos por cada partido político o coalición de las distintas casillas, y preparar las presentaciones en las que se darán a conocer los resultados y las imágenes de las Actas de Escrutinio y Cómputo (AEC). Dentro de este procesamiento se encuentra el total a nivel distrito y estatal. Esto se realiza cuando se vayan concentrado los datos, de forma tal que no haya retraso considerable entre la recepción y la presentación de los resultados. Este procesamiento tendrá la función de llevar a cabo la sumatoria de la elección y resguardar dicha información en los archivos que se diseñen para tal efecto.

A partir de los archivos generados para la presentación de resultados, se producirán otros archivos que contendrán la información en detalle y acumulados. Los diferentes formatos facilitarán el armado de las pantallas y reportes para la difusión.

Los datos de la presentación estatal se difundirán en los siguientes sitios: sala de sesiones del Consejo General y Centro de Comunicaciones del Instituto Electoral del Estado de México (Sala de Prensa), así como en los sitios web aprobados.
En la pantalla principal de salida se incluyen, entre otras, la siguiente leyenda: "*Los resultados electorales que aquí se presentan son preliminares, de carácter estrictamente informativo*" (IEEM, 2017).

Los resultados se presentan usando tecnología de tipo web. Además, los resultados se presentan en forma tabular y se incorporan elementos gráficos, se permite la consulta a nivel casilla, distrito local y estatal (IEEM, 2017).

Con el fin de que una mayor cantidad de ciudadanos tengan acceso a los resultados preliminares se puede convenir con instituciones educativas del Estado de México, así como con empresas periodísticas de circulación regional y/o nacional, para que coloquen en sus portales web los resultados electorales. Para ello el IEEM firma un convenio para entregar los resultados a las organizaciones interesadas, en este documento se advierte que los resultados no sean alterados, así con un previo cumplimiento de condiciones de seguridad para él envío y la recepción de los resultados (INE, 2016).

La difusión de los resultados electorales inicia a las 18:00 horas del día domingo 4 de junio de 2017, tal y como lo marca los Lineamientos Operativos del PREP 2017 emitidos por el IEEM, así mismo para dar cumplimiento en particular al artículo 39 de dichos lineamientos, los resultados preliminares se presentan en los siguientes sitios:

- En la sala de sesiones del Consejo General
- En las oficinas de los integrantes del Consejo General y de la Junta General.
- En los Centros de Comunicaciones (sala de prensa).
- En la página institucional (www.ieem.org.mx).
- En relación con los difusores externos, se convino con empresas periodísticas y con Instituciones educativas.

- En la página web se colocan las direcciones electrónicas (URL) para conectarse con los difusores, que en su caso también presentaron los resultados preliminares.

Las actualizaciones de los resultados se presentan mediante cortes de información cada 15 minutos, hasta cumplirse 24 horas a partir del inicio de la difusión, hasta las 18:00 horas del 5 de junio de 2017.

1.6. ALTERNATIVAS DE SOLUCIÓN

El PREP se encuentra certificado bajo la norma ISO 27001:2013, en los resultados del análisis de riesgos se muestra al proceso de la difusión de resultados con un nivel alto, esto debido a que en la difusión del PREP de la elección del año 2015 se presentó un ataque cibernético denominado Distributed Denial of Service (DDoS) en la infraestructura del ISP que el Instituto tenía contratado, este incidente se presentó a partir de las 20:00 horas, con una duración aproximada de cinco horas, tiempo en que la difusión de los resultados se vio disminuida, por tanto, afectó en la difusión a la ciudadanía, en el consejo y en la sala de prensa no tuvieron incidentes, este evento afectó la disponibilidad que se tenía comprometida en la difusión hacia Internet. Dicha información fue proporcionada por el ISP.

Con base en estos resultados y a los objetivos establecidos por el IEEM para el PREP 2016 – 2017, se definen los siguientes requerimientos para cumplir con los Lineamientos Operativos del PREP para la difusión de los resultados electorales:
Servicios

- Servidores web.
  - Servicio de cómputo para procesamiento de datos y/o aplicaciones críticas.
  - Servidores virtuales con capacidades de cómputo como mínimo CPU de 4 núcleos, 16GB en RAM y 50GB en disco duro.
  - Sistemas operativos Linux.
  - Conectividad redundante a Internet.

    - Respaldos.
- Protección perimetral.
- Seguridad de la Información.

Servicios administrados

- Nivel de disponibilidad en el servicio de al menos 99.5%.
- Entrega del Registro del número de control de cambios (RFC).
- Soporte de servicios de Tecnologías de la Información (TI) confiables.
- Operación en base a las mejores prácticas de TI.
- Atención a solicitudes de servicio, cambios y seguimiento a incidentes operativos.
- Configuración apropiada del sistema operativo, servicios, puertos y hardware del servidor.
- Contacto de primera línea con el fabricante del software.
- Entrega de reportes de disponibilidad y desempeño.
- Administración, operación, soporte y monitoreo de los sistemas operativos en un esquema de 7*24*365 bajo las mejores prácticas y por medio de personal especialista altamente calificado.
- Entrega de reporte de desempeño de los recursos (CPU, RAM, DISCO).

El Comité Técnico Asesor del PREP analiza dos alternativas de solución, de dos ISP (proveedores de servicios de telecomunicaciones) con soluciones de seguridad en la difusión de información en Internet, las cuales contienen las siguientes características.

SOLUCIÓN ISP 1

Este proveedor de servicios de telecomunicaciones propone dos elementos en su propuesta: 1) servicios y 2) servicios administrados y soporte.

1. **Servicios**

En la Tabla 1 se describen los servicios que ofrece el proveedor.

Cantidad	Descripción
14	Servidor web (4 núcleos, 14 GB, 200 SSD)
2	File replication (1 núcleo, 3.5 GB, 50 SSD)
2	VPN Servidor NG Firewall (1 núcleo, 3.5 GB, 50 GB SSD)
4	Servidor WAF (8 núcleos, 28 GB, 400 GB SSD)
2	Servicios de respaldo
2	Gestor de tráfico (DNS Querys / Health Check)
1	IP publica
1	DNS
22	1 TB de ancho de banda
1	Monitoreo de Infraestructura y sitios web
1	Simulación de carga (1 hora 250, 000 usuarios)

Tabla 1. Servicios ofrecidos por ISP 1

2. **Implementación de servicios y soporte**

En la Tabla 2 se describe como el proveedor implementa los servicios**.**

Descripción	Horas
WAFs	
Despliegue de cluster de WAFs	32
Configuración de seguridad de WAFs	60
Análisis de desempeño en pruebas de carga	16
Monitoreo de operación de WAFs durante los 3 simulacros	24
Monitoreo de operación de WAFs durante el proceso electoral	64
Reporte de incidentes registrados en WAFs	20
Monitoreo exterior el día de la elección	20

Tabla 2. Implementación de servicios por ISP 1

Descripción	Horas
Configuración de cluster de servidores web público	
Creación del Storage	2
Creación del servicio de nube	2
Creación de Máquina Virtual WEB1	4
Creación de Máquina Virtual WEB2	4
Creación de Máquina Virtual WEB3	4
Creación de Máquina Virtual WEB4	4
Creación de Máquina Virtual WEB5	4
Creación de Máquina Virtual WEB6	4
Configuración de máquina virtual de replicador HTML	16
Creación del conjunto de disponibilidad	3
Agregar extremos	5
Instalación y configuración del servicio de apache y FTP en cada uno de los servidores	24
Pruebas de acceso y redundancia a los servidores web y solución de problemas	16
Instalar monitoreo de infraestructura	30
Instalar replicación en cada servidor para contenido HTML	48
Monitoreo de operación web durante los 3 simulacros y dos pruebas	38
Monitoreo de operación web durante el proceso electoral	38
Reporte de incidentes registrados en web	20
Redes	
Diseño y creación de red	12
Creación de VPN	22
Soporte remoto para incidentes de instalaciones de cliente VPN en equipos	6
Monitoreo de operación de túneles durante los 3 simulacros	24
Monitoreo de operación de túneles durante el proceso electoral	24

Tabla 2. Implementación de Servicios por ISP 1 (cont')

Descripción	Horas
Portación de DNS	24
Activación del administrador de tráfico	16
Prueba de carga	
Diseño de patrón de carga de sitios web	32
Instalación de infraestructura de pruebas	8
Cuatro pruebas de carga portal exterior	16
Reporte de carga	16
Varios	
Preparación de subscripción y ambientes	30
Cierre de infraestructura y cierre de proyecto	40
Administración del proyecto	40
Documentación	20

Tabla 2. Implementación de Servicios por ISP 1 (cont')

SOLUCIÓN ISP 2

Este proveedor de servicios de telecomunicaciones propone seis elementos en su propuesta: 1) servicios, 2) servicios administrados, 3) respaldos, 4) reportes especiales, 5) seguridad perimetral compartida administrada y 6) seguridad de información.

1. **Servicios**

   En la Tabla 3 se describen los servicios ofrecidos por el proveedor.

Concepto	Balanceo		Servidor web		
	Balanceador	Balanceador	Servidor web 1	Servidor web 2	Servidor web3
Unidad virtual de procesamiento Linux.	1	1	1	1	1

Tabla 3. Servicios ofrecidos por ISP 2

Concepto	Balanceo		Servidor web		
vCPU	4 núcleos	4 núcleos	4 núcleos	4 núcleos	4 núcleos
vRAM	16GB	16GB	16GB	16GB	16GB
vDISK1	50GB	50 GB	50GB	50GB	50GB
Características generales					
Licenciamiento Linux RedHat v6					
Licenciamiento de Apache v2 freeware					
Conectividad redundante a Internet					
Monitoreo de Infraestructura 7*24					
Soporte técnico de: 5 sistemas operativos, 3 servidores web Apache v2 freeware					
Respaldos					
Actualización del servidor web a petición del cliente					
1 IP homologada por servidor virtual					
2 vNIC por servidor virtual					
Protección perimetral					

Tabla 3. Servicios ofrecidos por ISP 2 (cont')

2. **Servicios administrados**

   En la Tabla 4 se describe como se administran los servicios.

Nivel de disponibilidad
Nivel de disponibilidad en el servicio de al menos 99.5% mensual, no acumulable
Control de Cambios
Altas, bajas y cambios en la configuración lógica de la infraestructura de cómputo virtual
Reinstalación de Sistema Operativo
Apertura/cierre de puertos en los firewalls del servicio
Administración de Sistemas Operativos Linux RedHat **5 Sistemas Operativos**
Administración básica del Sistema Operativo
Aplicación de parches y actualizaciones

Tabla 4. Servicios administrados por ISP 2

Configuración de servicios, puertos y seguridad
Configuración y administración del hardware del servidor
Respaldo de configuración o estado del sistema
Solución de incidentes que se presenten en el Sistema Operativo
Reinstalación del Sistema Operativo
Monitoreo de los recursos (CPU, RAM, disco) y desempeño del servidor
Reporte de uso y desempeño del servidor
Entregables
Acta de entrega de servicio sobre cambios efectuados (RFC) en el sistema operativo del servidor
Memoria técnica
Reporte de causa raíz (Post-mortem) cuando se presente una falla o problema en el sistema administrado que ocasione afectaciones al servicio
Reporte de disponibilidad
Reporte de desempeño de recursos (CPU, RAM, disco)
Matriz de escalamiento
Acceso a portal web para visualización de reportes en línea
Servicios administrados de 3 Servidores web Apache
Creación de puntos de montaje de sitios web
Configuración y administración de servicio web
Administración de todos los procesos de los aplicativos webs y su ambiente de solución
Configuración y administración de FTP para que el cliente deposite los archivos a publicar
Atención a incidentes y problemas
Notificación de umbrales
Entregables
Utilización de procesamiento
Utilización de memoria
Disponibilidad del proceso de servidor web (HTTP)
Disponibilidad del puerto de publicación (TCP 80, 8080, 443)
Reportes Post-mortem

Tabla 4. Servicios administrados por ISP 2 (cont')

3. **Respaldos**

Dentro de la propuesta de solución, el proveedor contempla respaldos, en la Tabla 5 se describe cada cuanto se llevan a cabo estos respaldos y el alcance.

Periodicidad	Retención	Tipo
Semanal (domingos)	1 semana	Máquinas virtuales completas

Tabla 5. Respaldos por ISP 2

4. **Reportes especiales**

Se entrega de manera semanal reportes de los servicios del Servidor web, desempeño del servidor de producción.

5. **Seguridad perimetral compartida administrada**

El servicio de seguridad perimetral compartida administrada, considera implementar un firewall de alto desempeño y alta disponibilidad (a través de un contexto o Dominio virtual) que permite mantener una operación independiente de otros clientes, incluyendo políticas, reglas de firewall, objetos y reportes de operación y desempeño.

El servicio solo incluye la funcionalidad de firewall, no incluye las funcionalidades de Intrusion Prevention System (IPS), Web Content Filter, antivirus de red, VPN, etc.

El servicio contempla la conectividad a través de los puertos del servicio de colocación y/o conectividad Triara con transferencia de datos a Internet, la segmentación de las zonas es realizada a través de VLANs.

6. **Seguridad de información**

Web Protection de Incapsula es una solución basada en la nube para la protección de sitios web y aplicaciones de las amenazas externas.

CAPÍTULO II. INFRAESTRUCTURA

En este capítulo se documenta la infraestructura utilizada para la difusión del Programa de Resultados Electorales Preliminares (PREP), incluyendo el estudio de viabilidad técnica, diseño de infraestructura y el proceso de difusión.

2.1. VIABILIDAD TÉCNICA

El Comité Técnico Asesor del PREP elige la propuesta de solución número 2, las dos propuestas de solución cumplen con lo solicitado para este servicio, sin embargo, la solución número 1, no fue seleccionada debido a que el Centro de Datos se encuentra fuera del país, en los Estados Unidos de América (EUA), por lo que el Comité resuelve que no es viable que los resultados electorales salgan del país por considerarse información confidencial e información sensible políticamente, esto debido a la efervescencia electoral en el país y principalmente en el Estado de México para la elección de Gobernador 2017.

Derivado de lo anterior, el Comité Técnico Asesor del PREP propone a la Comisión del PREP la solución número 2 para la difusión de los resultados electorales, la cual operaría el día de la Jornada Electoral, esta solución cumple con los requerimientos establecidos en los lineamientos operativos del PREP. La solución incluye los Centros de Datos ubicados en las ciudades de Querétaro y Monterrey, cumple con las certificaciones Tier IV, ICREA nivel 5 e ISO 27000, además cuenta con personal certificado para operar este proyecto, es de clase mundial y cuenta con una disponibilidad alta.

La solución tiene un costo aproximado de $1,500,000 MXN y consiste principalmente de un clúster de cinco servidores con Sistema Operativo Linux RedHat, que se encuentran hospedados en el Centro de Datos, de los cuales tres son servidores web Apache y dos son balanceadores de carga. El servicio cuenta con seguridad perimetral en la web a través de la implementación del servicio de

Imperva Incapsula (Web Application Firewall (WAF)), el cual se utiliza principalmente para bloquear ataques del tipo Distributed Denial of Service (DDoS) (IMPERVA, 2015). El ancho de banda a internet inicial es de 1 GB, creciendo hasta 6 Gbps en el punto más alto.

2.2. DISEÑO DE INFRAESTRUCTURA

Para llevar a cabo la difusión de manera segura y con una alta disponibilidad el día de la Jornada Electoral, a continuación, se describe la infraestructura y/o los servicios ofrecidos por el ISP para el proceso de difusión de los resultados electorales a Internet.

En la Tabla 6 se muestra las capacidades de cómputo virtual.

Concepto	Balanceo		Servidor Web		
	Balanceador	Balanceador	Servidor web	Servidor web	Servidor web
Unidad Virtual de Procesamiento Linux	1	1	1	1	1
vCPU:	4 núcleos	4 núcleos	4 núcleos	4 núcleos	4 núcleos
vRAM:	16GB	16GB	16GB	16GB	16GB
vDISK1:	50GB	50GB	50GB	50GB	50GB

Tabla 6. Capacidades de cómputo virtual por ISP 2

2.2.1. Servicio de administración de servidores web

El ISP ofrece el servicio de administración de servidores web hospedados en los Centros de Datos que cuentan con acceso a Internet o con una conexión hacia una Intranet donde se publica el sitio, como se puede apreciar en la Figura 2.

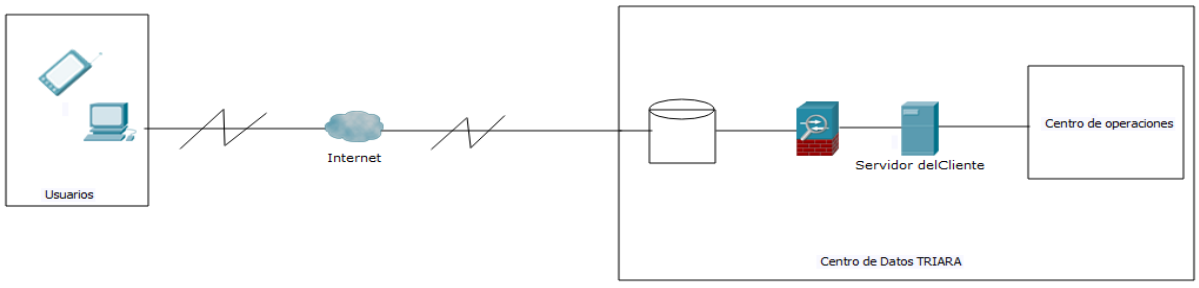


Figura 2. Servicios de administración de servidores web por ISP 2

2.2.2. Seguridad perimetral compartida administrada

El servicio de seguridad perimetral compartida administrada aprovecha la infraestructura del centro de datos Triara como se muestra en la Figura 3, y está diseñado para proveer los servicios de seguridad al IEEM. Incluye la funcionalidad del firewall de alto desempeño y alta disponibilidad (a través de un contexto o a través de Dominios Virtuales) que permite al IEEM mantener una operación independiente, incluyendo políticas, reglas de firewall, objetos y reportes de operación y desempeño.

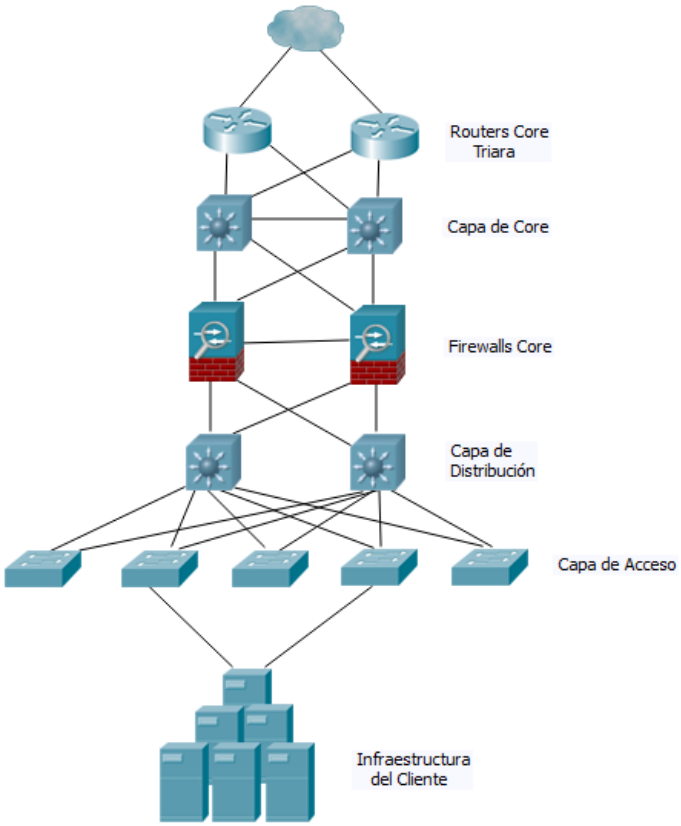


Figura 3. Servicio de Seguridad perimetral compartida administrada por ISP 2

2.2.3. DNS

El ISP implementa un DNS en su Infraestructura protegido por la solución de seguridad perimetral, de esta manera se evitan los ataques de Distributed Denial of Service **(**DDoS) al DNS del Instituto, y así esté disponible.

2.2.4. Seguridad de información

Esquema de seguridad que permite brindar protección a los portales del dominio ieem.org.mx de las amenazas informáticas existentes en la actualidad. Por lo tanto, para brindar seguridad a la información se tiene: Servicio en la nube WAF.

En el núcleo de la Nube de Protección Incapsula se encuentra una solución de Imperva de Proxy Reverso y el Firewall Aplicativo (WAF) en la nube, que se despliega a través de una red de distribución mundial CDN.

Esta solución funciona redireccionando el tráfico del sitio web a través de la nube de Incapsula mediante la realización de un simple cambio de DNS. Esto permite a la Nube de Incapsula inspeccionar todos y cada una de las solicitudes enviadas al sitio web y filtrar cualquier tipo de actividad maliciosa, tal como se muestra en la Figura 4.

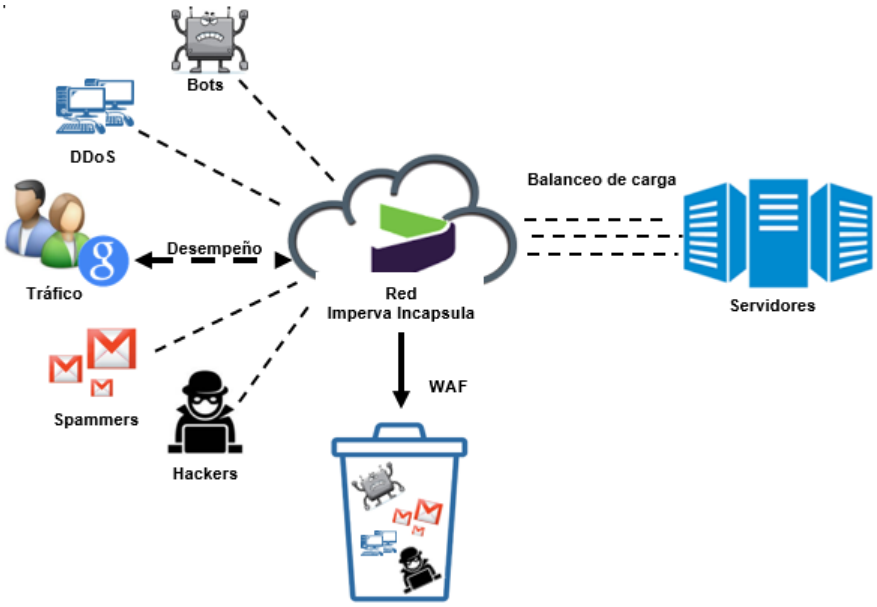


Figura 4. Servicio en la Nube WAF por ISP 2

El servicio en la Nube WAF brinda protección contra ataques de tipo DDoS sobre el dominio del Instituto, particularmente a los portales publicados (www.ieem.org.mx y www.prepieem.org.mx).

2.3. PROCESO DE DIFUSIÓN

De acuerdo con los lineamientos Operativos del PREP, en el artículo número 40, se elaboran convenios de colaboración con empresas periodísticas, e instancias de educación superior públicas donde solamente participa la UAEM para que apoyen en la difusión de los resultados electorales.

Por ello, 18 empresas participan como difusores oficiales los cuales son: Noticieros Televisa, Grupo Imagen, adn40, Métrica, Heraldo Estado de México, Impulso Estado de México, El Sol de Toluca, Grupo Milenio, Aristegui Noticias, El Universal, Hoy Estado de México, Canal Once, Portal, Proceso, Político.mx, La Jornada y la Universidad Autónoma del Estado de México.

La Unidad de Informática y Estadística es el área responsable de enviar la información a los difusores, se diseña el esquema de seguridad para el envío de la información a los difusores donde la Unidad realiza los envíos y los difusores no pueden entrar a la infraestructura del IEEM por los resultados (ver Figura 5).

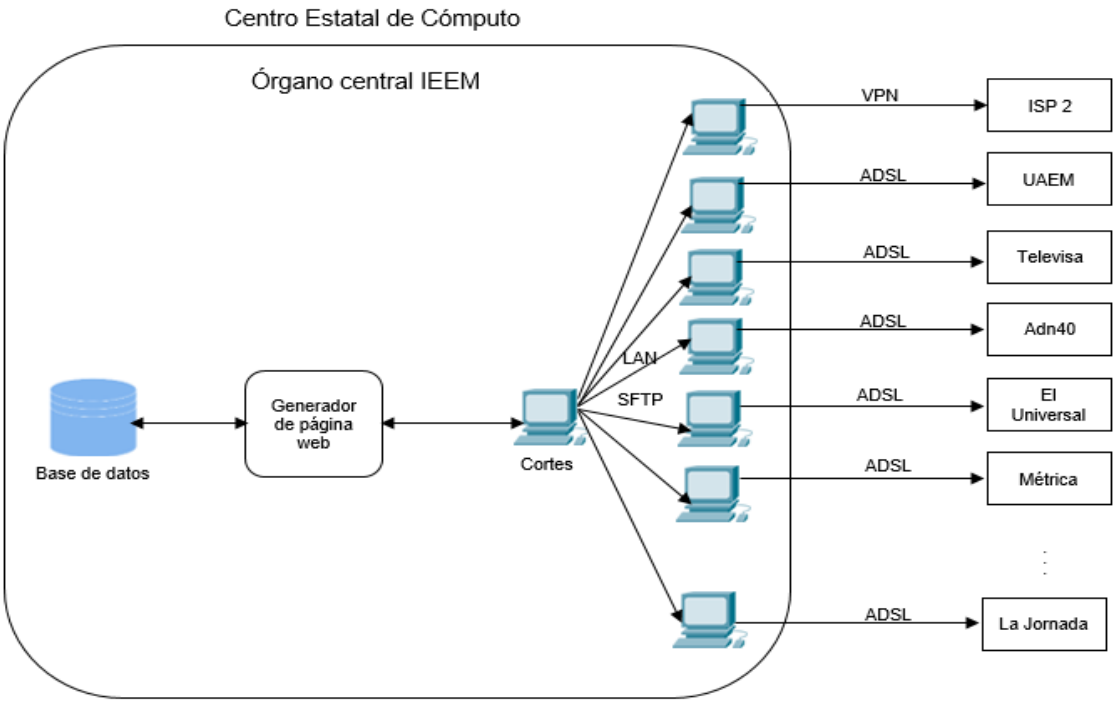


Figura 5. Proceso de difusión

Los equipos de cómputo para difundir los resultados electorales cumplen con un nivel de seguridad que se adquiere a través de un proceso de hardening para evitar cualquier ataque. Además, los equipos de cómputo cuentan con el Sistema Operativo Ubuntu 16.04 LTS el cual tiene instalado los siguientes programas:

- Secure Shell (SSH)
- Cliente FTP Filezilla
- Navegador web

Estos programas son necesarios para llevar a cabo el proceso de difusión, es por ello que no se tiene instalado ningún otro programa que no se utilice para cumplir con este objetivo.

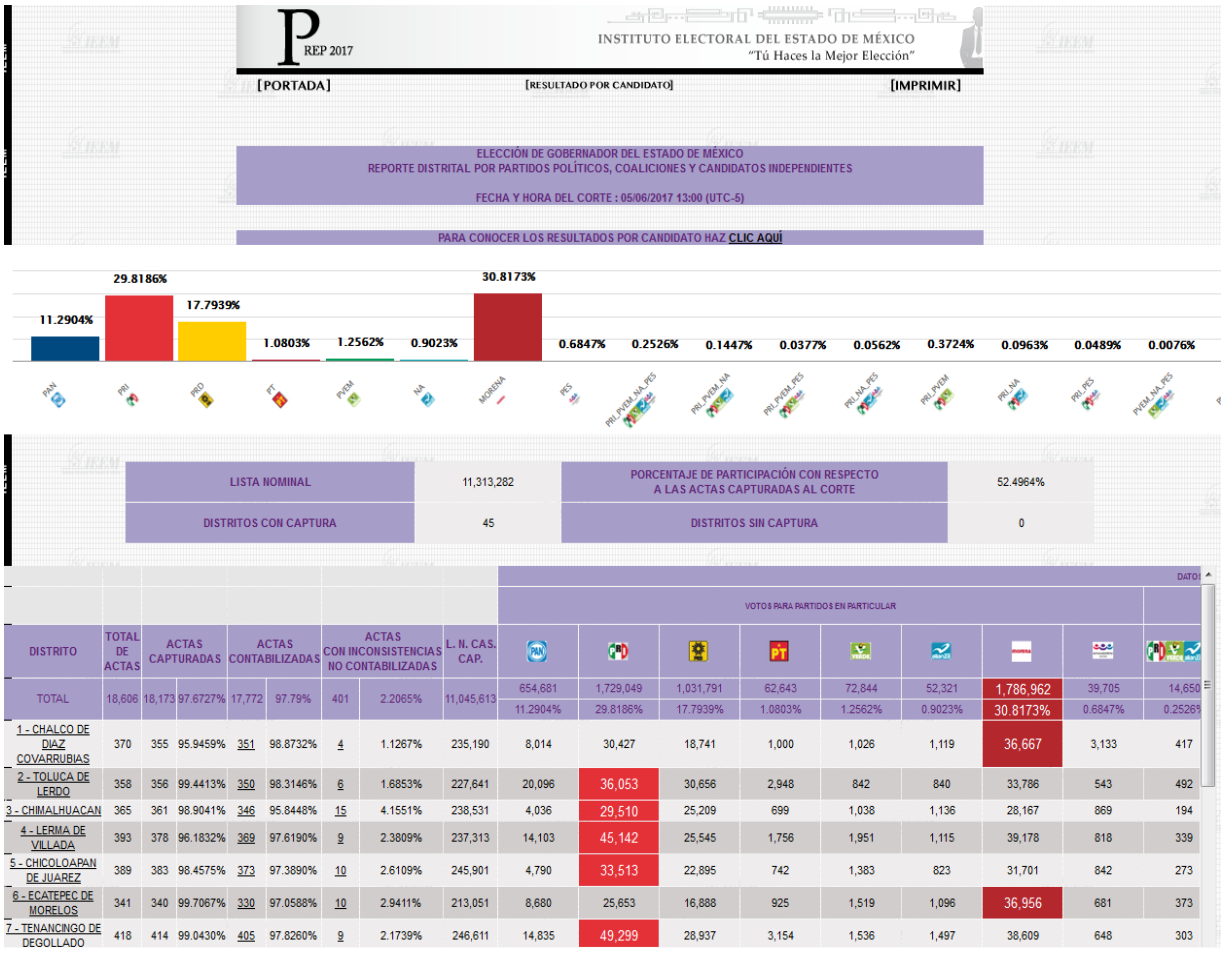
Por otro lado, se tienen enlaces ADSL de 100 Mbps y un enlace simétrico a Internet de 50 Mbps, los primeros se utilizan para difundir los resultados a cada difusor y el último se utiliza para difundir los resultados al ISP 2.

El inicio a la difusión de los resultados electorales es el día 4 de junio de 2017 a las 18:00 horas, a partir de esta hora cada quince minutos el sistema genera un corte con los últimos datos que se tiene en la base de datos, estos cortes contienes los archivos necesarios para construir una página web simple (html, css, imágenes, archivos, etc.).

Una vez que ya se tiene el corte, éste se deposita en una carpeta compartida en un equipo de cómputo. Posteriormente la persona encargada de difundir los resultados toma el corte, y a través de una conexión SFTP se transfiere el corte a una carpeta que indica el difusor con permiso de lectura y escritura, una vez que el corte se encuentra en el equipo del difusor, mediante una conexión SSH se descomprime el corte en el momento exacto a los quince minutos.

El ISP es el difusor oficial del IEEM, para este caso, se construye una VPN que crea un canal de comunicación segura. A través de dicho canal la persona encargada de difundir los resultados establece una conexión SSH al servidor del ISP para descomprimir los cortes cada quince minutos.

Posterior a que se descomprimen los cortes, se actualiza la página web, donde se tienen publicados los resultados electorales en forma tabular (ver Figura 6), para que la ciudadanía interesada, principalmente en el Estado de México vea reflejado cada quince minutos los nuevos valores de la elección.



PREP 2017

INSTITUTO ELECTORAL DEL ESTADO DE MÉXICO
"Tú Haces la Mejor Elección"

[PORTADA] [RESULTADO POR CANDIDATO] [IMPRIMIR]

ELECCIÓN DE GOBERNADOR DEL ESTADO DE MÉXICO
REPORTE DISTRITAL POR PARTIDOS POLÍTICOS, COALICIONES Y CANDIDATOS INDEPENDIENTES

FECHA Y HORA DEL CORTE : 05/06/2017 13:00 (UTC-5)

PARA CONOCER LOS RESULTADOS POR CANDIDATO HAZ CLIC AQUÍ

LISTA NOMINAL	11,313,282	PORCENTAJE DE PARTICIPACIÓN CON RESPECTO A LAS ACTAS CAPTURADAS AL CORTE	52.4964%
DISTRITOS CON CAPTURA	45	DISTRITOS SIN CAPTURA	0

DISTRITO	TOTAL DE ACTAS	ACTAS CAPTURADAS		ACTAS CONTABILIZADAS		ACTAS CON INCONSISTENCIAS NO CONTABILIZADAS		L. N. CAS. CAP.	VOTOS PARA PARTIDOS EN PARTICULAR								
TOTAL	18,606	18,173	97.6727%	17,772	97.79%	401	2.2065%	11,045,613	654,681	1,729,049	1,031,791	62,643	72,844	52,321	1,786,962	39,705	14,650
									11.2904%	29.8186%	17.7939%	1.0803%	1.2562%	0.9023%	30.8173%	0.6847%	0.2526%
1 - CHALCO DE DIAZ COVARRUBIAS	370	355	95.9459%	351	98.8732%	4	1.1267%	235,190	8,014	30,427	18,741	1,000	1,026	1,119	36,667	3,133	417
2 - TOLUCA DE LERDO	358	356	99.4413%	350	98.3146%	6	1.6853%	227,641	20,096	36,053	30,656	2,948	842	840	33,786	543	492
3 - CHIMALHUACAN	365	361	98.9041%	346	95.8448%	15	4.1551%	238,531	4,036	29,510	25,209	699	1,038	1,136	28,167	869	194
4 - LERMA DE VILLADA	393	378	96.1832%	369	97.6190%	9	2.3809%	237,313	14,103	45,142	25,545	1,756	1,951	1,115	39,178	818	339
5 - CHICOLOAPAN DE JUAREZ	389	383	98.4575%	373	97.3890%	10	2.6109%	245,901	4,790	33,513	22,895	742	1,383	823	31,701	842	273
6 - ECATEPEC DE MORELOS	341	340	99.7067%	330	97.0588%	10	2.9411%	213,051	8,680	25,653	16,888	925	1,519	1,096	36,956	681	373
7 - TENANCINGO DE DEGOLLADO	418	414	99.0430%	405	97.8260%	9	2.1739%	246,611	14,835	49,299	28,937	3,154	1,536	1,497	38,609	648	303

Figura 6. Resultados electorales en forma tabular (IEEM, 2017)

En la infraestructura del difusor oficial del IEEM, se encuentra la página web Institucional (http://www.ieem.org.mx), en la cual se tienen una página html y en ella se tienen las ligas hacia los diferentes sitios de difusión y quien encabeza la lista de los difusores es el mismo difusor oficial, como se muestra en la Figura 7.

Figura 7. Página HTML con las ligas hacia los difusores del PREP (IEEM, 2017)

La razón por la cual los difusores del PREP no pueden entrar a la infraestructura del IEEM, y cada uno cuente con su infraestructura es, que, si en algún momento el difusor oficial del IEEM deja de funcionar, se tengan otras alternativas para seguir difundiendo los resultados electorales.

CAPÍTULO III. PRUEBAS

En este capítulo se documentan las pruebas que se realiza a la Infraestructura para la difusión del Programa de Resultados Electorales Preliminares los cuales incluyen un Ataque de DoS y pruebas de estrés. Además, se documenta el desempeño real y los hallazgos obtenidos el día de la Jornada Electoral.

3.1. ATAQUE DoS

Esta prueba la realiza el ente auditor externo del PREP con 10 equipos con IP´s públicas y con un ancho de banda de 1Gb. Se diseña un ataque con el cual se simulan cientos o miles de peticiones consecutivas al servidor de difusión de resultados del sistema PREP para obtener parte del tráfico usual del día de la elección.

Tras iniciar la prueba, se comienza a monitorear el sitio web para observar su comportamiento. Aproximadamente un minuto después de haber iniciado el ataque se observa que el sitio deja de responder peticiones por espacio de un minuto, tras lo cual, el balanceador de carga entra en operación, permitiendo nuevamente la navegación (si bien más lenta de lo usual) a través del difusor del PREP.

Tras mantener el nivel de peticiones por unos diez minutos, se procede a aumentar el volumen de dichas peticiones, dejando pasar unos minutos entre el primer y el segundo ataque, para intentar dejar sin servicio. Sin embargo, esta vez no se logra saturar al servidor.

Análisis de resultados

Esto demuestra que la infraestructura utilizada para la difusión de los resultados electorales soporta ataque de Denegación de Servicio de baja o mediana intensidad, aunque cabe mencionar que ninguna plataforma está exenta de riesgo cuando el

ataque se realiza con una gran cantidad de computadoras, que pueden llegar a varios miles de equipos. En resumen, se puede afirmar que la infraestructura de la difusión está razonablemente protegida contra ataques de Denegación de Servicio.

3.2. PRUEBAS DE ESTRÉS

En estas pruebas se cuantifica la capacidad en infraestructura, se validan los requerimientos de desempeño, la escalabilidad de la plataforma y la difusión de los resultados.

De esta manera se puede conocer que cantidad de usuarios simultáneos soporta el sistema PREP, con tiempos y datos razonables sobre la infraestructura y las plataformas propuestas para el sistema. Así mismo, se evalúa la suficiencia de los recursos del sistema para soportar el nivel propuesto a los escenarios para el sistema PREP.

TIPOS DE PRUEBAS

Prueba de Carga

Consiste en la simulación de las cargas de trabajo típicas de múltiples usuarios realizando procesos típicos para el sistema. Indican y validan la respuesta de la aplicación al ser sometida a una carga de usuarios y/o transacciones esperada en el escenario adecuado.

Prueba de Estrés

Consiste en cargar el sistema o los componentes del sistema hasta que llegan a los límites de funcionamiento. Permite encontrar el volumen de datos (o el tiempo) en que la aplicación deja de ser capaz de responder a las peticiones como se espera. Se tiene por lo menos dos escenarios como se muestra en la Tabla 7, uno con carga suficiente para mantener el servidor atendiendo peticiones sin exceder su capacidad. El segundo escenario es rebasar la capacidad del servidor y verificar que puede

responder a las peticiones utilizando distintos mecanismos como el uso de balanceadores de carga. Más adelante se presenta mediante gráficas el detalle que proporciona la herramienta JMeter que se utiliza para la prueba.

	Respuesta en los primeros 10 ciclos	Respuesta entre los 20 y 30 ciclos	Respuesta después de los 30 ciclos
Carga suficiente	Respuesta inmediata	Respuesta inmediata	Respuesta inmediata
Sobrecarga	Respuesta inmediata	Se pasma unos segundos, posteriormente resuelve las peticiones con el balanceador.	Esporádicamente hay que esperar para cargar nuevamente la página y envía un mensaje de error code 20.

Tabla 7. Dos escenarios de la prueba de estrés

Durante el ataque al sistema, el sitio web se mantiene en línea, aunque la velocidad de carga se ve ligeramente afectada y en dos ocasiones esporádicas en una hora que dura el ataque muestra el código de error 20 (ver Tabla 8), pero es importante señalar que este mensaje es enviado por el software de Incapsula y el sistema continua en operación.

www.prepieem.org.mx – Connection failed
Error code 20 The proxi failed to connect to the web server, due to TCP connection time out. ----------

Tabla 8. Código de error 20

También se observa, que cuando el software Incapsula detecta un comportamiento anómalo automáticamente bloquea una conexión y la restaura una vez que se deja de atacar como se presenta en la Tabla 9.

www.prepieem.org.mx – Access Denied
Error code 15 The request was blocked by the security rules. ----------

Tabla 9. Código de error 15

MÓDULO PUBLICADOR RESULTADOS

Prueba de estrés por candidato (escenario 1)

La prueba se realiza con base a la siguiente configuración (ver Figura 8):

- Dominio: www.prepieem.org.mx
- Ruta: /rptDistrital.html
- Escenario critico
- 3000 hilos * 1 segundo (30 ciclos) 21018 muestras

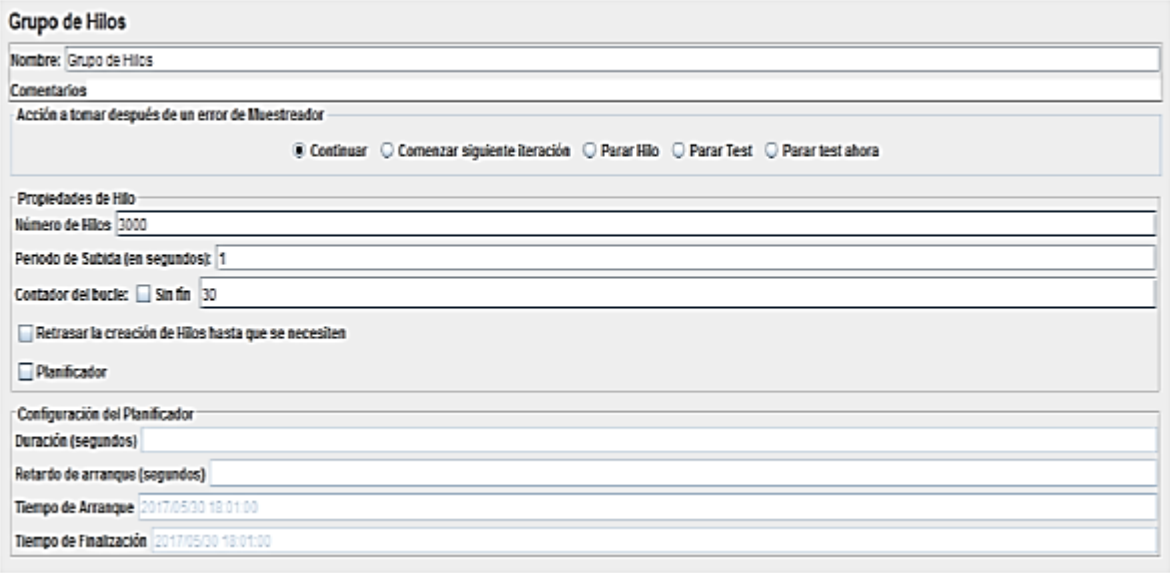


Figura 8. Configuración de la prueba de estrés por candidato (escenario 1) por ente auditor

Reporte de resumen

Se presenta la Figura 9 con la información que resulta de las peticiones HTTP, y que permite interpretar los resultados obtenidos y establecer comparaciones entre pruebas:

- Número de muestras
- Tiempo medio en milisegundos
- Tiempo mínimo en milisegundos
- Tiempo máximo en milisegundos

- Desviación típica
- Porcentaje de error
- Rendimiento
- Kb/segundo
- Media de Bytes recibidos

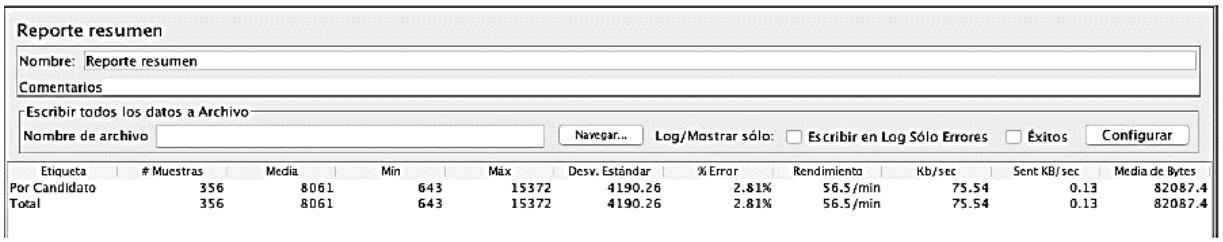


Figura 9. Información que resulta al ejecutar las peticiones HTTP por ente auditor

Gráfico de resultados

Se muestra en la Figura 10 los resultados obtenidos al ejecutar las peticiones HTTP especificadas ofreciendo en una gráfica de líneas los valores de tiempo en milisegundos, rendimiento, y los valores de media, mediana y desviación típica.

Figura 10. Grafica de líneas de los resultados obtenidos al ejecutar las peticiones HTTP por ente auditor

Árbol de resultados

En la Figura 11 se muestra a detalle cada petición HTTP realizada, analizando las cabeceras de la petición y de las respuestas obtenidas. De este modo, se puede monitorear que sucede a la hora de procesar cada petición.

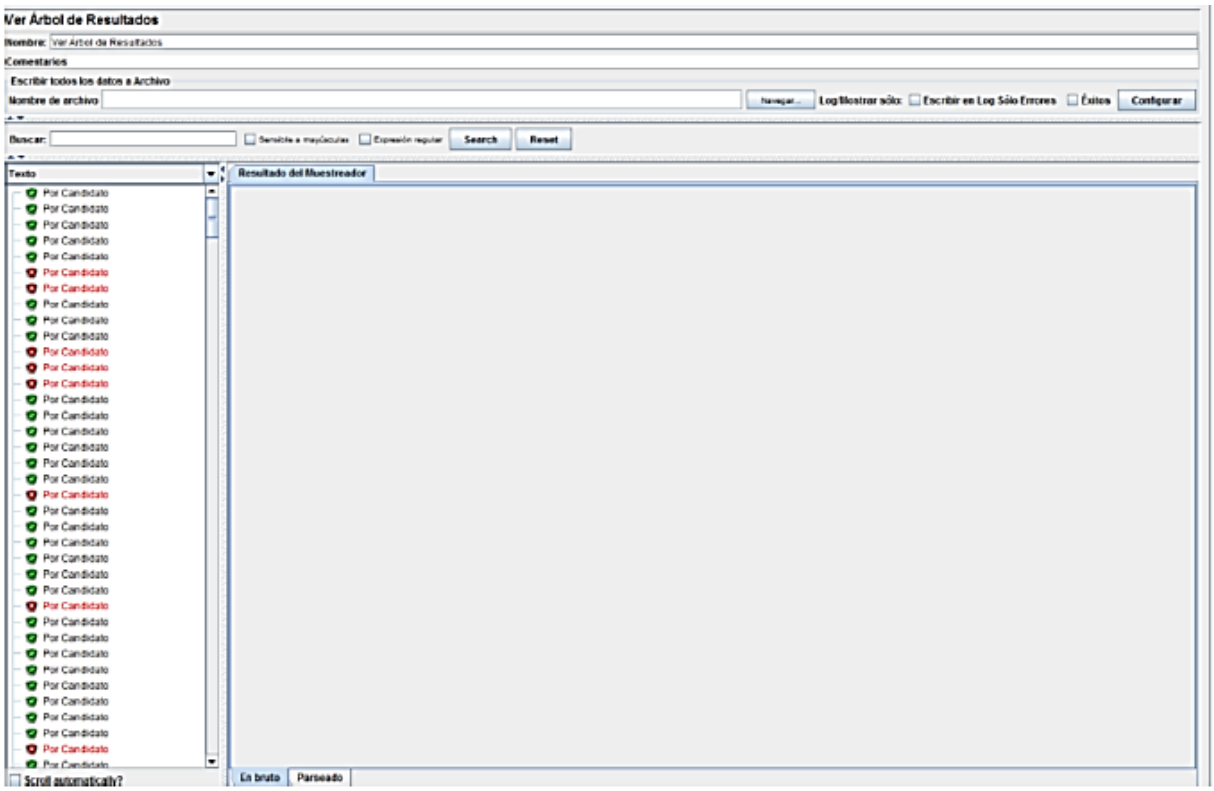


Figura 11. Árbol de resultados al ejecutar las peticiones HTTP por ente auditor

Resultados en árbol

Se muestra en la Figura 12 cada una de las peticiones HTTP que se realizan por el respectivo grupo de hilos, así como el estatus de atendida y no atendida según el caso, a detalle.

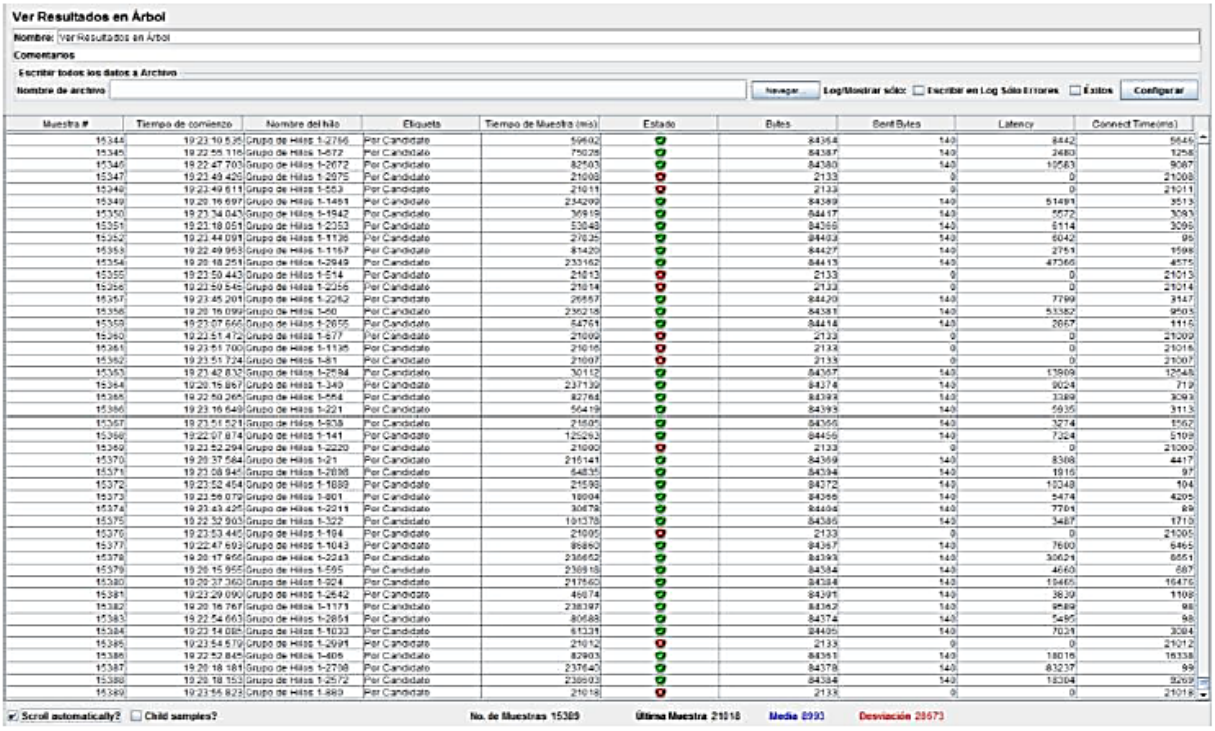


Figura 12. Resultados en árbol al ejecutar las peticiones HTTP por ente auditor

Resumen de prueba

Se muestra en la Tabla 10 un resumen de los resultados obtenidos al ejecutar la prueba de estrés por candidato escenario 1.

Modulo	No. Muestras	Media	Mín.	Máx.	% Error	Rendimiento	Kb/Sec
Publicación	76945	8993	0	350618	2.81%	56.5	75.74

Tabla 10. Resumen de los resultados al ejecutar la prueba de estrés por candidato (escenario 1) por ente auditor

Así mismo, se muestra en la Figura 13 el porcentaje de las peticiones HTTP resueltas y no resueltas, que resulta al ejecutar la prueba de estrés por candidato escenario 1.

Figura 13. Porcentaje de peticiones HTTP resultas y no resueltas de la prueba de estrés por candidato (escenario 1) por ente auditor

Prueba de estrés por candidato (escenario 2)

La prueba se realiza con base a la siguiente información

- Dominio: www.prepieem.org.mx
- Ruta: /rptDistrital
- Escenario critico
- 10000 hilos * 1 segundo (30 ciclos)

Reporte de resumen

Se presenta la Figura 14 la información que resulta de las peticiones HTTP, y que permite interpretar los resultados obtenidos y establecer comparaciones entre pruebas.

- Número de muestras
- Tiempo medio en milisegundos
- Tiempo mínimo en milisegundos
- Tiempo máximo en milisegundos
- Desviación típica
- Porcentaje de error
- Rendimiento
- Kb/segundo
- Media de Bytes recibidos

Figura 14. Información que resulta al ejecutar las peticiones HTTP por ente auditor

Gráfico de resultados

Se muestra en la Figura 15 los resultados obtenidos al ejecutar las peticiones HTTP especificadas ofreciendo en una gráfica de líneas los valores de tiempo en milisegundos, rendimiento y los valores de media, mediana y desviación típica.

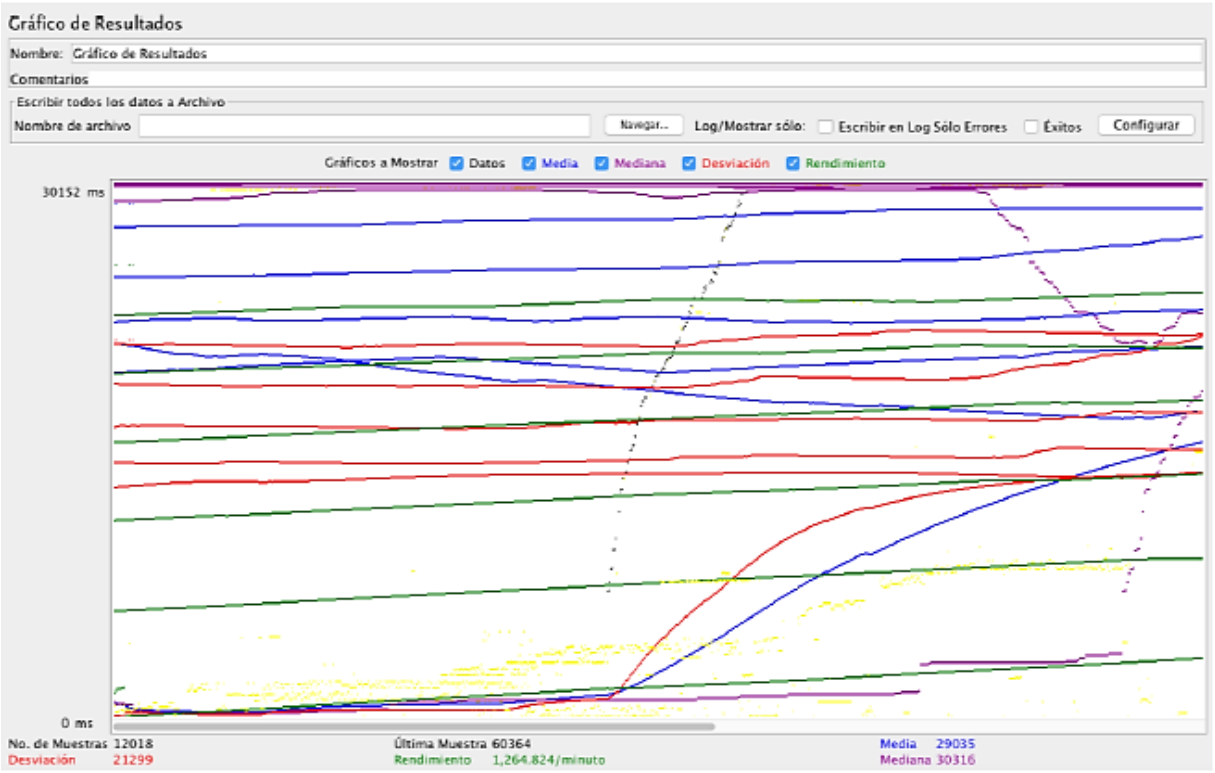


Figura 15. Gráfica de líneas de los resultados obtenidos al ejecutar las peticiones HTTP por ente auditor

Árbol de resultados

En la Figura 16 se muestra a detalle cada petición HTTP que se realiza, se analiza las cabeceras de la petición y de las respuestas obtenidas. De este modo, se puede monitorear que sucede a la hora de procesar cada petición.

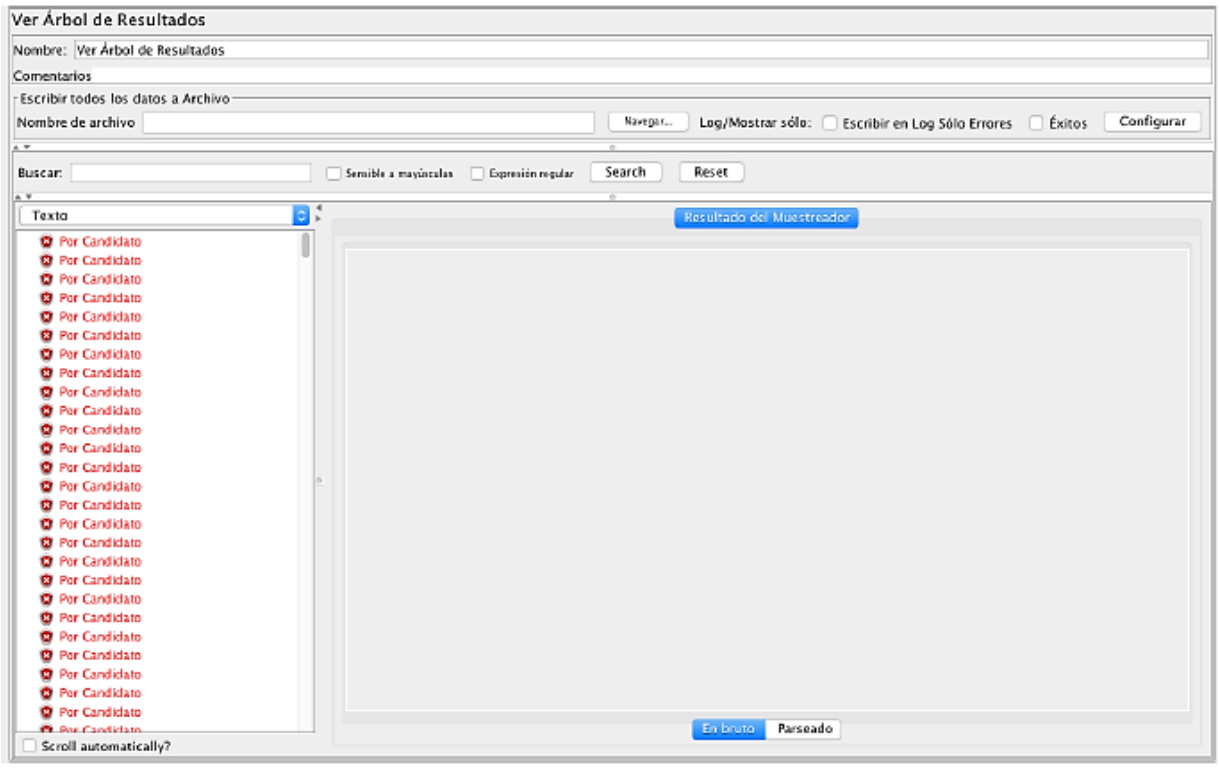


Figura 16. Árbol de resultados al ejecutar las peticiones HTTP por ente auditor

Resultados en árbol

Se muestra en la Figura 17 cada una de las peticiones HTTP que se realiza por el respectivo grupo de hilos, así como su estatus de atendida y no atendida según el caso, a detalle.

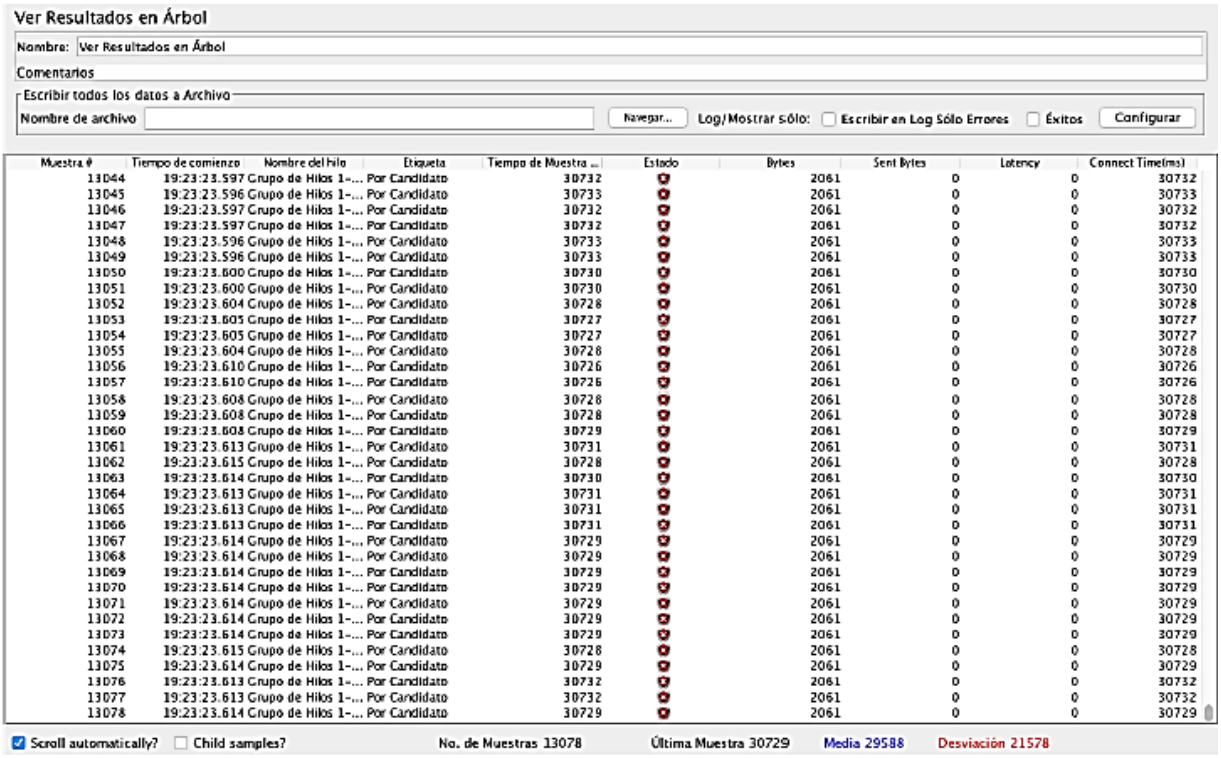


Figura 17. Resultados en árbol al ejecutar las peticiones HTTP por ente auditor

Resumen de prueba

Se muestra en la Tabla 11 un resumen de los resultados obtenidos al ejecutar la prueba de estrés por candidato escenario 2.

Modulo	No. Muestras	Media	Mín.	Máx.	% Error	Rendimiento	Kb/Sec
Publicación	21976	846	65	31983	0.09%	324.8/sec	1319.2

Tabla 11. Resumen de los resultados al ejecutar la prueba de estrés por candidato (escenario 1) por ente auditor

Así mismo, se muestra en la Figura 18 el porcentaje de las peticiones HTTP resueltas y no resueltas, que resulta al ejecutar la prueba de estrés por candidato escenario 2.

Figura 18. Porcentaje de peticiones HTTP resultas y no resueltas de la prueba de estrés por candidato (escenario 2) por ente auditor

Análisis de resultados

Durante las pruebas de estrés que dura una hora se puede observar que la tasa de error es de 0.09%, una tasa muy baja, es importante mencionar que los mismos se distribuyen, lo cual permite concluir que, aunque los tiempos de espera de recarga de la página se ven incrementados el sistema se mantuvo en línea durante las pruebas.

3.3. DESEMPEÑO REAL

A continuación, se muestra un reporte con el desempeño real obtenido el día de la Jornada Electoral con la implementación de Imperva Incapsula, el cual incluye la información del tráfico web monitoreado, información de seguridad y reporte de infraestructura y eventos presentados.

En la Figura 19 se muestra gráficamente el diagrama de red de alto nivel que estuvo operando el día de la Jornada Electoral.

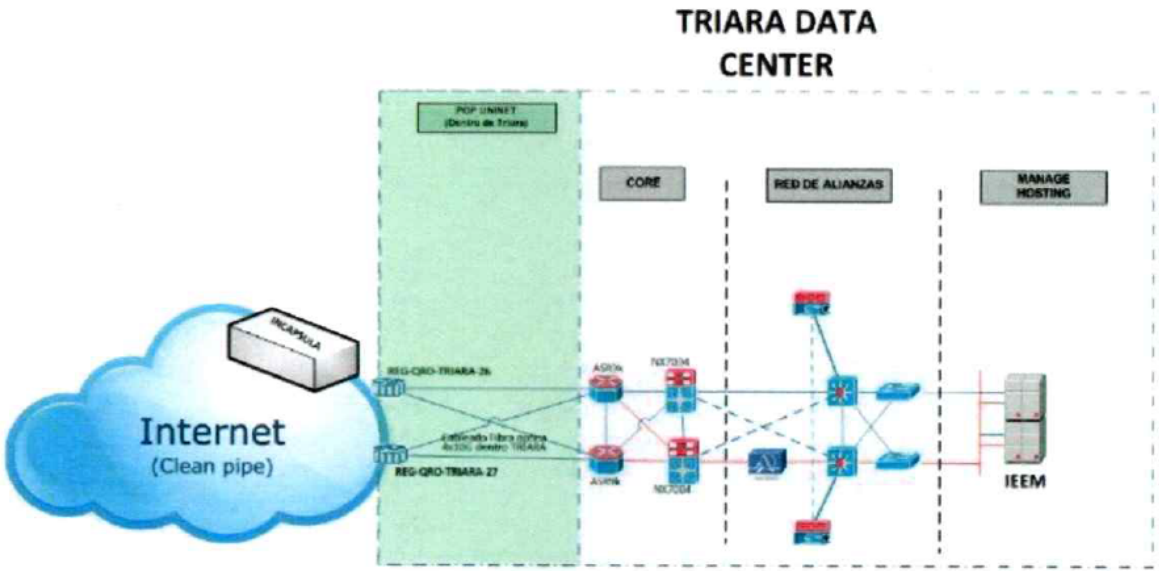


Figura 19. Diagrama de red de alto nivel por ISP 2

3.3.1. REPORTE WAF INCAPSULA

La solución Imperva Incapsula consta de una plataforma de entrega de aplicaciones basada en la nube. Mediante el uso de una red de entrega de contenido global que provee servicios de seguridad web, protección de ataques de DDoS y balanceo de carga.

Los portales web protegidos por Incapsula en el periodo del 4 al 5 de junio de 2017 (Jornada Electoral) son los siguientes:

- www.ieem.org.mx
- www.prepieem.org.mx

En la Figura 20 se muestran los portales protegidos configurados en Imperva Incapsula.

Figura 20. Portales protegidos configurados en Imperva Incapsula por ISP 2

3.3.1.1. Información del tráfico web monitoreado

A continuación, se muestra la información relevante sobre el tráfico web monitoreado dirigido hacia los sitios web protegidos por la solución Imperva Incapsula durante el periodo reportado.

Portal web: www.ieem.org.mx

En la Figura 21 se muestra el porcentaje de visitas realizadas por distintos países al portal web.

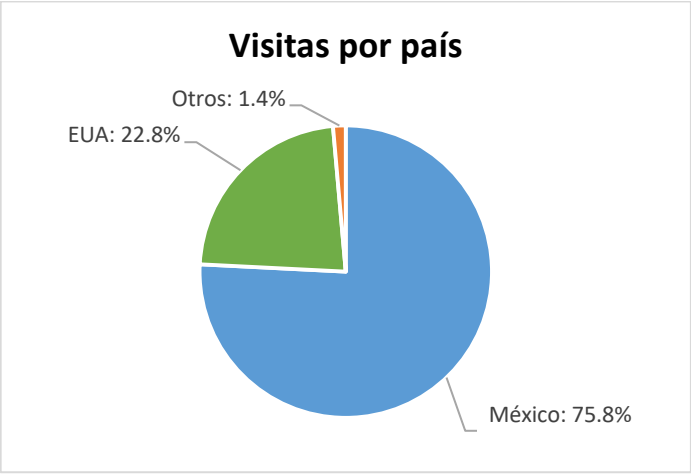


Figura 21. Porcentaje de visitas por distintos países al portal www.ieem.org.mx por ISP 2

Se muestra información general de acceso al portal web en la Tabla 12.

Información general	Totales	Promedio
Visitas Totales	918, 800 visitas	Humanos: 77.6% Bots: 22.4%
Hits totales (Clics totales)	17,000,000 clics	Clics por segundo: 98.6
Bits por segundo	Máximo: 80 Mbps	24 Mbps
Ancho de banda acumulado (04/06/2017 – 05/06/2017)	506.9 GB	

Tabla 12. Información general de acceso al portal web www.ieem.org.mx por ISP 2

Portal web: www.prepieem.org.mx

En la Figura 22 se muestra el porcentaje de visitas realizadas por distintos países al portal web.

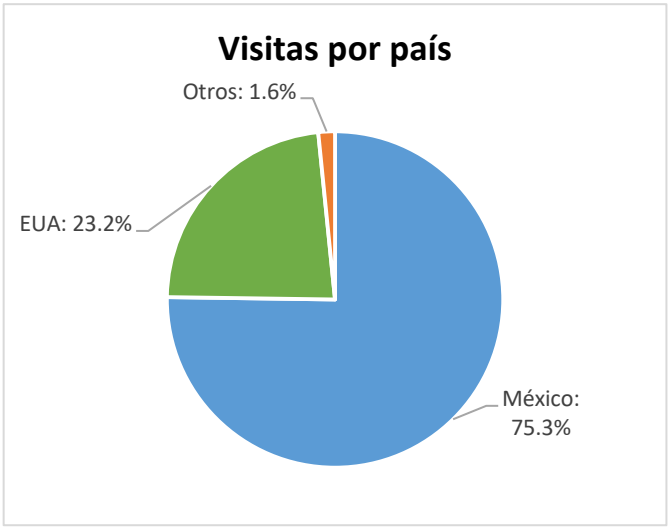


Figura 22. Porcentaje de visitas por distintos países al portal www.prepieem.org.mx por ISP 2

Se muestra información general de acceso al portal web en la Tabla 13.

Información general	Totales	Promedio
Visitas Totales	989, 900 visitas	Humanos: 76.6% Bots: 23.4%
Hits totales (Clics totales)	28,000,000 clics	Clics por segundo: 161.9
Bits por segundo	Máximo: 543 Mbps	71 Mbps
Ancho de banda acumulado (04/06/2017 – 05/06/2017)	1.5 TB	

Tabla 13. Información general de acceso al portal web www.prepieem.org.mx por el ISP 2

3.3.1.2. Información de Seguridad

A continuación, se muestra la información relevante de seguridad sobre el tráfico web monitoreado dirigido hacia los portales web protegidos por la solución Imperva Incapsula durante el periodo reportado.

Portal web: www.ieem.org.mx

Se muestra en la Tabla 14 información general sobre las alertas generadas en el periodo reportado para el portal web protegido.

Amenaza detectada	No. de alertas	Configuración
Visitantes de lista negra	n/a	No hay IPs origen en lista negra.
Visitantes de países en lista negra	n/a	No hay países en lista negra.

Tabla 14. Información sobre las alertas generadas para el portal web www.ieem.org.mx por ISP 2

Amenaza detectada	No. de alertas	Configuración
Visitantes de URLs en lista negra	n/a	No hay URLs en lista negra
Control de acceso de Bots	35,000	Este apartado muestra el conteo de los Bots o herramientas de análisis de vulnerabilidades automatizadas que fueron bloqueadas al intentar acceder al portal protegido. Incapsula puede distinguir entre un Bot convencional de uno maliciosos de acuerdo a su comportamiento, clasificación del cliente y reputación del origen. Esto permite realizar bloqueos y proteger el portal web sin perjudicar el funcionamiento de Bots benéficos. Este tipo de actividades son bloqueadas por la solución de seguridad Imperva Incapsula.
Bots sospechosos	2000	Los Bots maliciosos generan carga redundante en el portal web con la finalidad de obtener información que pudiera representar un riesgo y no aportan alguna funcionalidad o beneficio alguno. Incapsula analiza el comportamiento de los Bots que intentan acceder al portal web.

Tabla 14. Información sobre las alertas generadas para el portal web www.ieem.org.mx por ISP 2 (cont')

Amenaza detectada	No. de alertas	Configuración
Inclusión remota de archivos	0	Alerta cuando se detecta intento de realizar ataques Inclusión remota de archivos mediante herramientas especializadas y analizadores de vulnerabilidades.
SQL Injection	2	Genera una alerta cuando se detecta la inyección de código SQL en las transacciones web para explotar alguna vulnerabilidad en la validación de datos de entrada en el portal web que se conecta a una base de datos. Las peticiones categorizadas como SQL Injection fueron bloqueadas por las reglas de seguridad de Incapsula.
Cross Site Scripting	0	Genera alerta de seguridad cuando se detecta la inyección de código de programación (ej. Javascript) en las transacciones web para explotar vulnerabilidades de validación de datos en la aplicación y comprometer la información de la misma. Durante el periodo reportado no se detectó este tipo de amenaza.

Tabla 14. Información sobre las alertas generadas para el portal web www.ieem.org.mx por ISP 2 (cont')

Amenaza detectada	No. de alertas	Configuración
Acceso ilegal a recursos web	3	Alerta cuando se detecta intentos de acceder a páginas administrativas, ver o ejecutar archivos del sistema a través de la interfaz web. Es comúnmente realizado mediante adivinación de URLs, ataques de Directory Travesal y técnicas de inyección de comandos. Se detectaron intentos de acceso a URLs administrativas o privadas (algunas de estas podrían no existir y se trata de pruebas de solicitudes a URLs al azar para validar el comportamiento del portal web) Las peticiones categorizadas como acceso ilegal a recursos web fueron bloqueadas por las reglas de seguridad de Incapsula.
Denegación de Servicio Distribuido (DDoS)	0	Esta regla detecta cuando se presenta un ataque de Denegación de Servicio Distribuido, el cual es un tipo de ataque cuyo propósito es provocar la indisponibilidad de un recurso mediante su saturación y provocación de fallo (en este caso los portales web del IEEM) a través del uso de una gran cantidad de equipos atacantes.

Tabla 14. Información sobre las alertas generadas para el portal web www.ieem.org.mx por ISP 2 (cont')

Amenaza detectada	No. de alertas	Configuración
		La solución de seguridad Incapsula proporciona servicios de protección que absorben ataques de DDoS de hasta múltiples de Gigabytes de forma escalable de acuerdo a la demanda requerida. Adicionalmente Incapsula mitiga ataques enfocados al protocolo HTTP mediante el bloqueo de tráfico malicioso antes de que este llegue al servidor web, aplicando diferenciadores para usuarios validos y maliciosos. Finalmente, Incapsula también analiza el comportamiento de los visitantes de los portales web protegidos y realiza desafíos (pruebas de JavaScript, cookies, y CAPTCHAs) para validar que las peticiones provengan de orígenes humanos. Durante el periodo reportado no se detectó este tipo de amenaza.
Protección de puertas traseras (Backdoor)	0	Durante el periodo reportado no se detectó este tipo de amenaza.

Tabla 14. Información sobre las alertas generadas para el portal web www.ieem.org.mx por ISP 2 (cont')

En los datos presentados anteriormente se observa que el tipo de amenaza que se ha presentado con mayor frecuencia es "Control de Acceso a Bots".

Para el periodo reportado se llevaron a cabo 35,000 bloqueos que corresponden a la alerta "Control de Acceso de Bots".

Distribución de Incidentes por país

En la Figura 23 se muestra gráficamente el porcentaje de alertas generadas por distintos países al portal web.

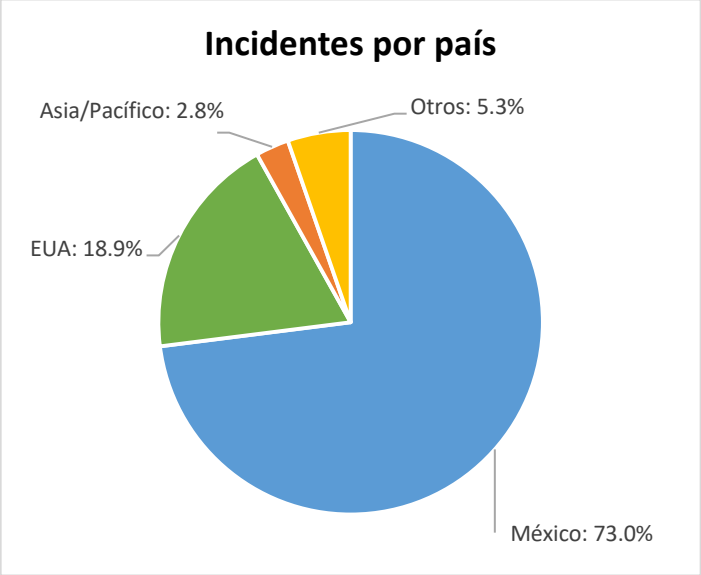


Figura 23. Porcentaje de alertas generadas por diversos países al portal www.ieem.org.mx por ISP 2

Se observa en la gráfica que el país extranjero con mayor cantidad de alertas generadas es Estados Unidos (US).

Portal web: www.prepieem.org.mx

A continuación, se muestra en la Tabla 15 información general sobre las alertas generadas en el periodo reportado para el portal web protegido.

Amenaza detectada	No. de alertas	Configuración
Visitantes de lista negra	n/a	No hay IPs en lista negra

Tabla 15. Información sobre las alertas generadas para el portal web www.prepieem.org.mx por ISP 2 (cont')

Amenaza detectada	No. de alertas	Configuración
Visitantes de países en lista negra	n/a	No hay países en lista negra
Visitantes de URLs en lista negra	n/a	No hay URLs en lista negra
Control de Acceso de Bots	29,000	Este apartado indica los Bots o herramientas de análisis de vulnerabilidades bloqueados al intentar acceder al portal web protegido. Este tipo de actividades son bloqueadas por la solución de Seguridad Imperva Incapsula.

Tabla 15. Información sobre las alertas generadas para el portal web www.prepieem.org.mx por ISP 2 (cont')

Amenaza detectada	No. de alertas	Configuración
Bots sospechosos	3,000	Los Bots maliciosos generan carga redundante en el portal web con la finalidad de obtener información que pudiera representar un riesgo y no aportan alguna funcionalidad o beneficio alguno, Incapsula analiza el comportamiento de los Bots que intentar acceder al portal web. Para este propósito Incapsula provee diversas opciones para el manejo de Bots maliciosos y sospechosos. Para el periodo reportado se configuró el método de comprobación de acceso humano mediante el envío de un desafío (Challenge).
Inclusión remota de archivos	0	Alerta cuando se detecta intento de realizar ataques de inclusión remota de archivos mediante herramientas especializadas y analizadores de vulnerabilidades. En el periodo no se reportaron este tipo de amenazas.

Tabla 15. Información sobre las alertas generadas para el portal web www.prepieem.org.mx por ISP 2 (cont')

Amenaza detectada	No. de alertas	Configuración
SQL Injection (SQLi)	1	Genera una alerta de seguridad cuando se detecta la inyección de código SQL en las transacciones web para explotar alguna vulnerabilidad en la validación de datos de entrada en el portal web que se conecta hacia una base de datos. Se detectó que se lanzó un análisis de vulnerabilidades al portal www.prepieem.org.mx con herramientas de seguridad como Acunetix y Arachni y este intento de exploración fue bloqueado por la solución de WAF de Incapsula. Las peticiones categorizadas como SQL Injection fueron bloqueadas por las reglas de seguridad de Incapsula.
Cross Site Scripting (XSS)	5	Genera alerta de seguridad cuando se detecta la inyección de código de programación (ej. Javascript) en las transacciones web para explotar vulnerabilidades de validación de datos de aplicación y comprometer la información de la misma.

Tabla 15. Información sobre las alertas generadas para el portal web www.prepieem.org.mx por ISP 2 (cont')

Amenaza detectada	No. de alertas	Configuración
		Se detectaron peticiones mal formadas las cuales incluían caracteres no válidos en las URLs, adicionalmente se observó que se intentó hacer pruebas de ejecución de código de programación dentro de los valores de cabeceras HTTP. Estas peticiones fueron bloqueadas por la solución WAF de Incapsula. Las peticiones categorizadas como Cross Site Scripting (XSS) fueron bloqueadas por las reglas de seguridad de Incapsula.
Acceso ilegal a recursos web	6	Alerta cuando se detecta intentos de acceder a páginas administrativas, ver o ejecutar archivos del sistema a través de la interfaz web. Es comúnmente realizado mediante adivinación de URLs, ataques de Directory Traversal y técnicas de inyección de comandos. Se detectó el uso de herramientas automatizadas para obtener información del portal web mediante la comprobación de URLs.

Tabla 15. Información sobre las alertas generadas para el portal web www.prepieem.org.mx por ISP 2 (cont')

Amenaza detectada	No. de alertas	Configuración
		En algunas URLs administrativas o privadas se detectaron alertas de seguridad (algunas de estas podrían no existir y se trata de pruebas de solicitudes a URLs al azar para validar el comportamiento del portal web). Las peticiones categorizadas como acceso ilegal a recursos web fueron bloqueadas por las reglas de seguridad de Incapsula.
Denegación de Servicio Distribuido (DDoS)	10,000	Esta regla detecta cuando se presenta un ataque de Denegación de Servicio Distribuido, el cual es un tipo de ataque cuyo propósito es provocar la indisponibilidad de un recurso mediante su saturación y provocación de fallo (en este caso los portales web del IEEM) a través del uso de una gran cantidad de equipos. La solución de seguridad Incapsula proporciona servicios de protección que absorben ataques de DDoS de hasta múltiples Gigabytes de forma escalable de acuerdo a la demanda requerida.

Tabla 15. Información sobre las alertas generadas para el portal web www.prepieem.org.mx por ISP 2 (cont')

Amenaza detectada	No. de alertas	Configuración
		Adicionalmente Incapsula mitiga ataques enfocados al protocolo HTTP mediante el bloqueo de tráfico malicioso antes de que este llegue al servidor web, aplicando diferenciadores para usos válidos y maliciosos. Finalmente, Incapsula también analiza el comportamiento de los visitantes de los portales web protegidos y realiza desafíos (pruebas de JavaScript, cookies y CAPTCHAs) para validar que las peticiones provengan de orígenes humanos. Las peticiones HTTP categorizadas como pertenecientes a un ataque de Denegación de Servicio (DDoS) fueron bloqueadas por las reglas de seguridad de Incapsula.
Protección de puertas traseras (Blackdoor)	0	Durante este periodo no se detectó ningún tipo de amenaza.

Tabla 15. Información sobre las alertas generadas para el portal web www.prepieem.org.mx por ISP 2 (cont')

En los datos presentados anteriormente se observa que el tipo de amenaza que se ha presentado con mayor frecuencia es "Control de Acceso de Bots".

Para este periodo se llevaron a cabo 29, 000 bloqueos que corresponden a la alerta "Control de Acceso de Bots".

Distribución de incidentes por país

En la Figura 24 se muestra gráficamente el porcentaje de alertas generadas por distintos países al portal web.

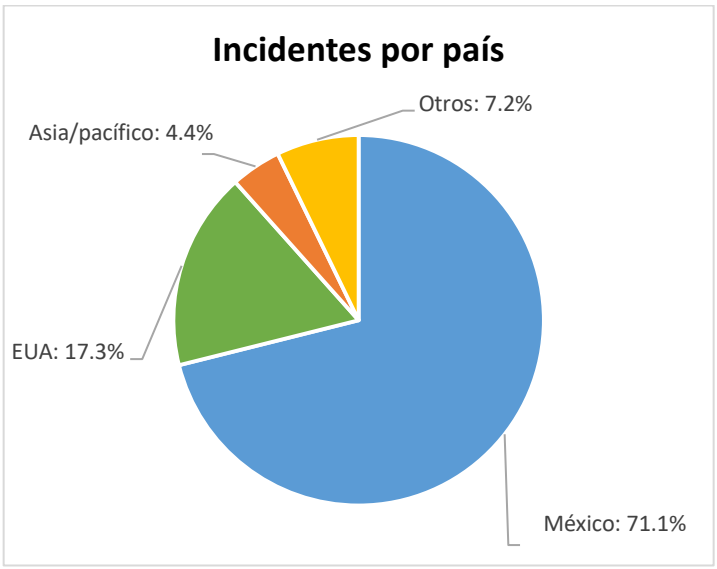


Figura 24. Porcentaje de alertas generadas por diversos países al portal *www.prepieem.org.mx por ISP 2*

Se observa en la gráfica que el país extranjero con mayor cantidad de alertas generadas es Estados Unidos.

3.3.1.3. Reporte de infraestructura y eventos presentados

A continuación, se presenta a través de gráficas el comportamiento de la infraestructura utilizada en la Jornada Electoral y algunos eventos presentados en el mismo, los cuales incluyen la carga de CPU, conexiones por segundo del servicio apache, utilización promedio de CPU, utilización promedio de memoria, utilización del sistema de archivos y el desempeño de servidores del IEEM.

Carga de CPU

La carga de CPU muestra la demanda del balanceador durante la Jornada Electoral, como se muestra en la Figura 25, de igual manera se puede observar en la gráfica un evento de mitigación.

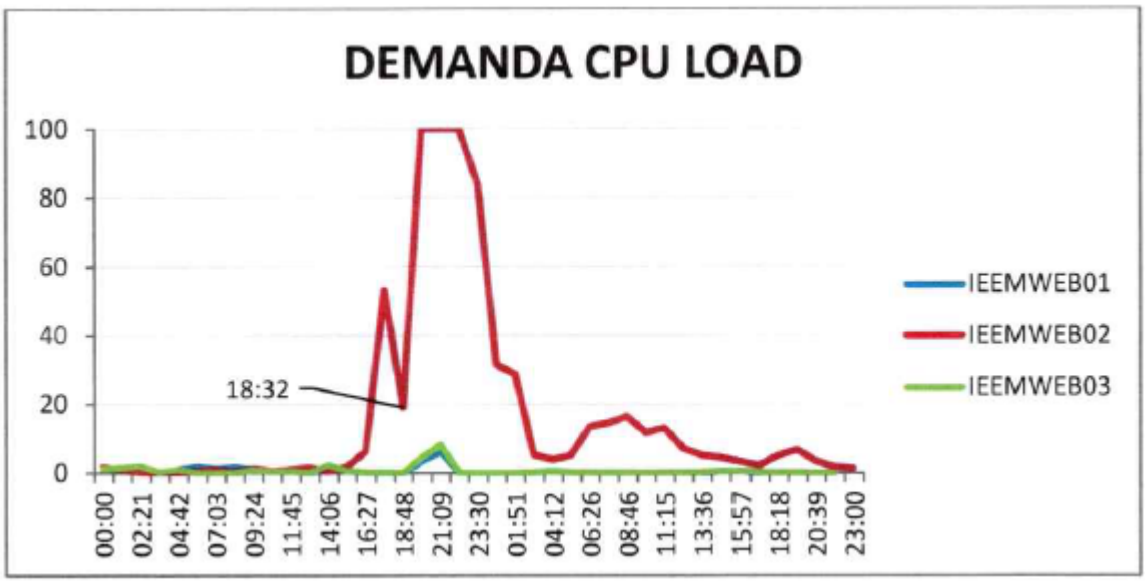


Figura 25. Carga de CPU por ISP 2

Evento de Mitigación, efecto sobre el balanceador (IEEMWEB02)

Se muestra la cronología del Evento de Mitigación realizado el 4 de junio y en la Tabla 16 se presenta un resumen sobre el evento.

Duración	IP destino	Máximo tráfico presentado	Objeto administrado
8 minutos	----	2.9 Mbps	IEEM-TRIARA-QRO

Tabla 16. Resumen del evento de mitigación por ISP 2

1. Se detecta una alerta, incrementando el nivel de severidad de bajo a alto, se procede con la aplicación de mitigación bloqueando el segmento de donde se detecta la alerta.

2. Se reporta “Error code 20” (este error es asociado a pérdida de paquetes entre INCAPSULA y los servidores web de IEEM).

3. Se detiene la mitigación

Conexiones por segundo Servicio Apache

En la Figura 26 se muestra el número de conexiones por segundo generadas hacia el Servicio Apache en los tres servidores web durante la Jornada Electoral.

Figura 26. Conexiones por segundo al servicio apache en los tres servidores web por ISP 2

Evento de Denegación de Servicio Distribuida (DDoS)

Lo siguiente es la cronología del evento de ataque DDoS detectado.

1. Se presenta el alto consumo de memoria y CPU en los tres servidores web del IEEM.
2. La página web del Instituto comienza a experimentar lentitud.

3. Se detecta un ataque de DDoS catalogado como alto sobre los equipos del IEEM.
4. Se reportan fallas de conexión en algunos puertos.
5. Ataque de código malicioso confirmado y mitigado eficientemente.
6. Se estabilizan conexiones en los servidores web y en los puertos en su totalidad.

Utilización promedio de CPU

En las siguientes Figuras 27 y 28 se muestra la utilización promedio de CPU de los servidores en la Jornada Electoral.

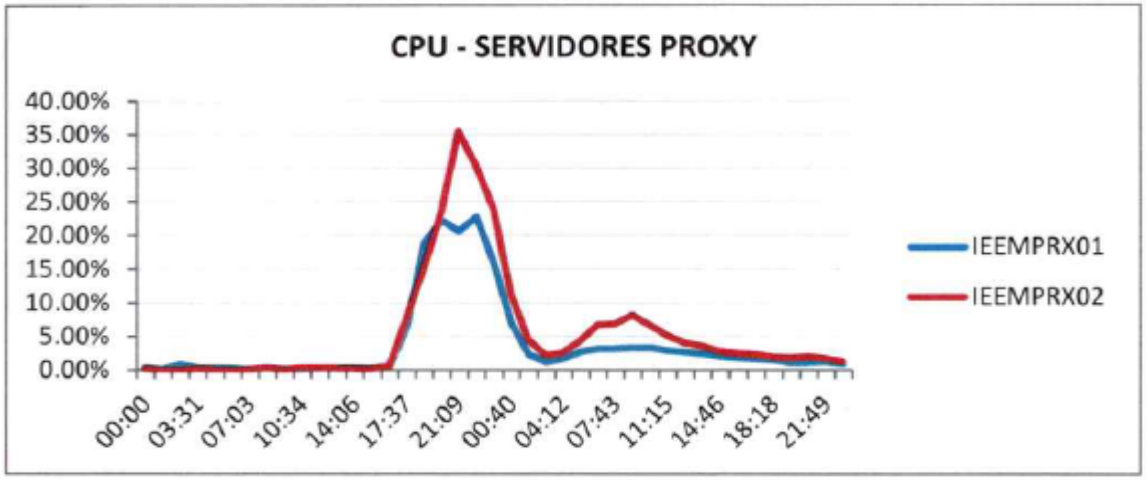


Figura 27. Utilización promedio de CPU de los servidores proxy por ISP 2

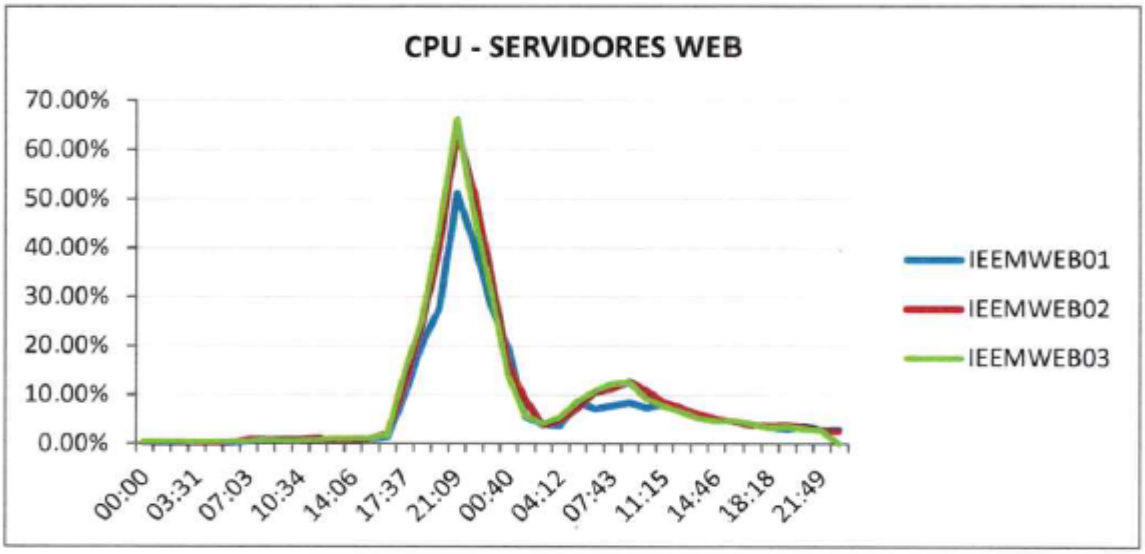


Figura 28. Utilización promedio de CPU de los servidores web por ISP 2

Ningún umbral de alarma de CPU fue rebasado durante la jornada electoral (los umbrales establecidos fueron 80% para advertencia y 90 % para excepción). El alto consumo reflejado en los CPU se debió al evento de Denegación de Servicio Distribuida (DDoS) mencionado.

Utilización promedio de memoria

En la Figura 29 se muestra la utilización promedio de memoria de los servidores proxy y web.

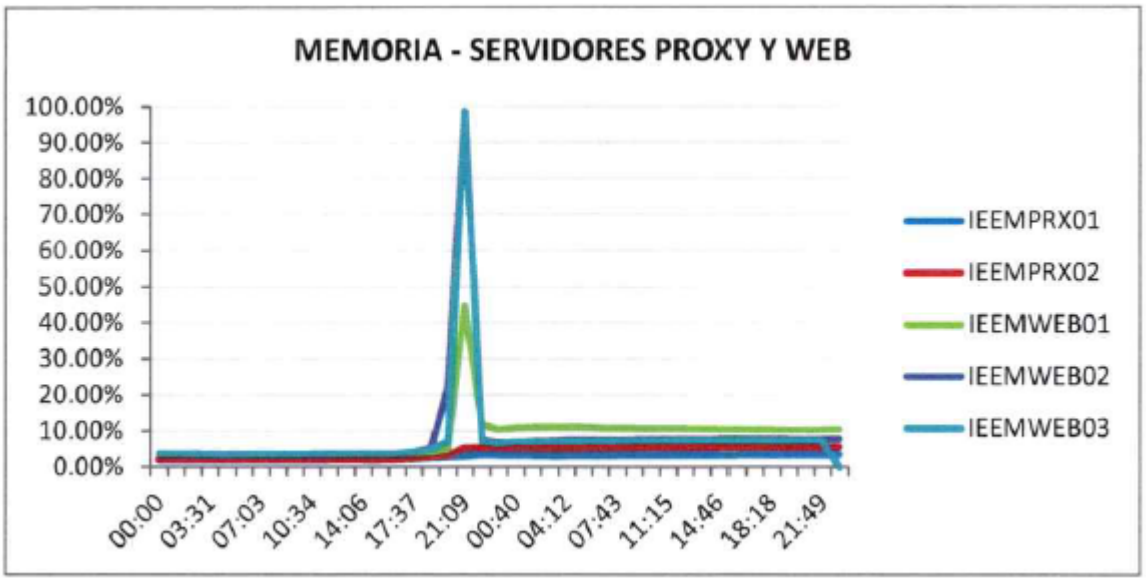


Figura 29. Utilización promedio de memoria de los servidores proxy y web por ISP 2

El umbral de alarma en memoria fue rebasado durante la Jornada Electoral (los umbrales establecidos fueron 80% para advertencia y 90% para excepción) debido al evento de Denegación de Servicio Distribuida mencionado por lo tanto se incrementó la memoria en los servidores web.

Uso del Sistema de Archivo

En la Figura 30 se muestra a través de una gráfica la utilización del sistema de archivos de los servidores proxy y web.

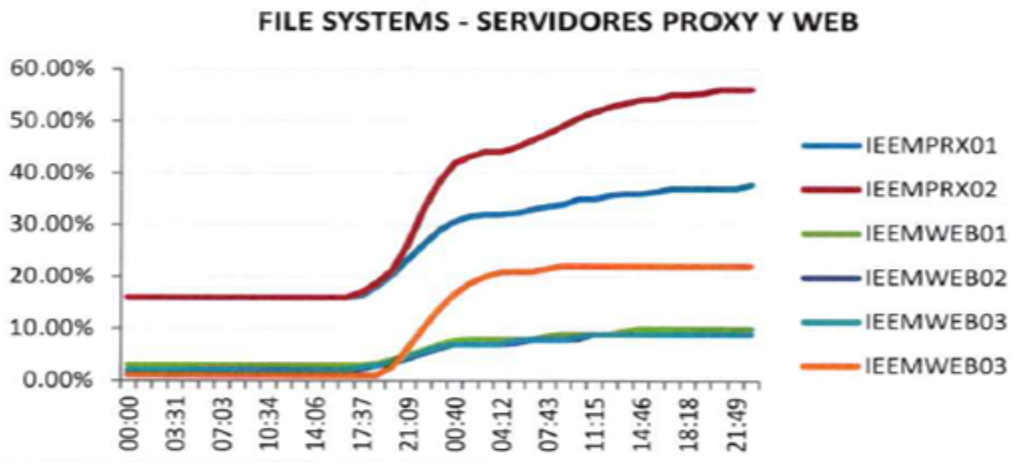


Figura 30. Utilización del sistema de archivos de los servidores proxy y web por ISP 2

Ningún umbral de alarma en el archivo de sistema fue rebasado durante la Jornada Electoral (Los umbrales establecidos fueron 80% para advertencia y 90% para excepción).

Los archivos del sistema no incluidos en la gráfica, no presentaron cambio en su utilización ni se encontraban en estado de alarma.

Desempeño de servidores IEEM

La Figura 31 muestra a través de una gráfica de barras el desempeño de los servidores a nivel de disponibilidad.

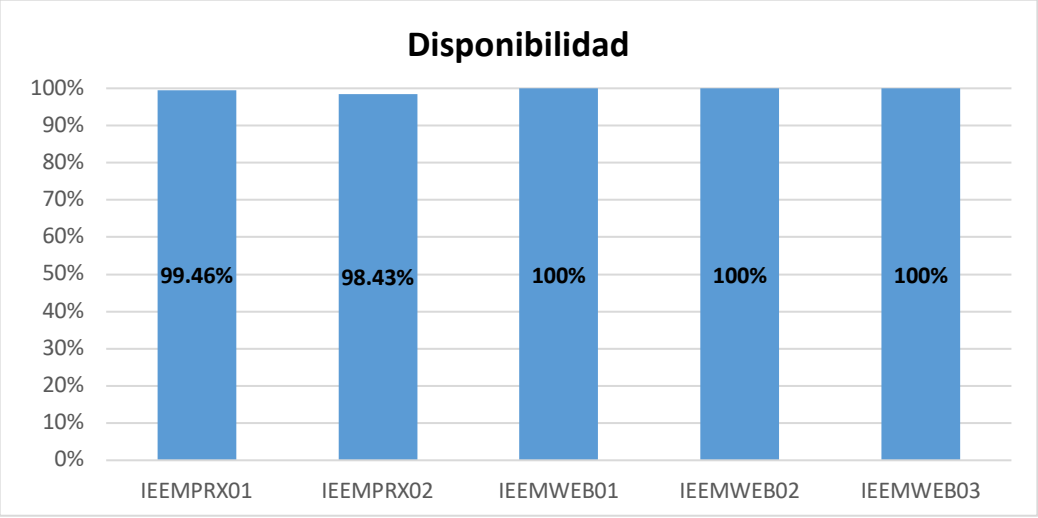


Figura 31. Desempeño a nivel de disponibilidad de los servidores del IEEM por ISP 2

La disponibilidad muestra el porcentaje de tiempo que los equipos fueron alcanzables por ping, durante las 48 horas contempladas en el evento (04/06/2017 00:00 – 05/06/2017 23:59).

La disponibilidad promedio de los 5 servidores fue de 99.57%. el porcentaje de disponibilidad de los servidores PROXY se vio afectado por el evento de DDoS y el error de Incapsula “Error code 20” (pérdida de paquetes).

Análisis de resultados

La solución WAF Incapsula se mantuvo activa y funcionando durante el periodo reportado.

Durante el periodo reportado se detectó que los portales web del Instituto Electoral del Estado de México (www.ieem.org.mx y www.prepieem.org.mx) fueron objetivo de diversos intentos de exploración maliciosa, de análisis de vulnerabilidades y ataques de Denegación de Servicio Distribuido (DDoS por sus siglas en inglés).
Este tipo de peticiones HTTP fueron bloqueadas por la solución de seguridad Incapsula mediante sus reglas de protección y su capacidad de mitigación de ataques volumétricos.

Durante el periodo reportado no se presentó ningún tipo de incidente de seguridad.

CONCLUSIONES

En la presente tesina se ha documentado el diseño de la infraestructura de red que operó en la Jornada Electoral para la difusión en Internet del Programa de Resultados Electorales Preliminares en el Estado de México en el proceso electoral 2016-2017, con lo cual se alcanzó el objetivo primordial para el Instituto Electoral del Estado de México que fue la disponibilidad, ya que se difundieron los resultados electorales en el tiempo comprometido y con ello se da cumplimiento a lo ordenado en el reglamento de elecciones del INE y a los Lineamientos Operativos del PREP 2017. Por lo tanto, se cumple con el objetivo general de esta tesina.

Adicionalmente, se puede decir lo siguiente:

El Programa de Resultados Electorales Preliminares en el Estado de México, es un programa robusto de carácter informativo que se encarga de proveer los resultados preliminares y no definitivos de un proceso electoral, su buen funcionamiento es importante ya que permite a la ciudanía interesada principalmente en el Estado de México, seguir de cerca los resultados de la elección, es por ello que se brindó seguridad a la información cuidando la disponibilidad y la integridad de la misma.

Se concluye que la solución que se implementó para dotar de seguridad de la información a la difusión del PREP, se mantuvo activa y funcionando durante la Jornada Electoral, aunque se detectaron diversos incidentes como intentos de exploración maliciosa, de análisis de vulnerabilidades y ataques de Denegación de Servicio Distribuido (DDoS por sus siglas en inglés), éstos fueron bloqueadas por la solución mediante la aplicación de reglas de protección a la capacidad de mitigación de ataques volumétricos.

Como resultado de las pruebas el ente auditor manifiesta que los servidores e infraestructura asociada a los procesos del PREP 2017 son razonablemente seguros y que su nivel de riesgo es muy bajo para la operación del mismo.

Por otro lado, el instituto realizó convenios con 18 difusores, por lo que se tuvieron otras alternativas para seguir difundiendo los resultados electorales y así cumplir con la disponibilidad comprometida.

Por último, la teoría que se tomó como fundamento para poder desarrollar este trabajo de investigación, en la presente tesina se ve aplicado en un proyecto real puesto que en él se aplican temas de Seguridad en Redes como lo es seguridad de la información, así como ataques de seguridad, políticas de seguridad, entre otros; e intervienen diversas tecnologías que hacen posible la implementación y operación del PREP, por lo que, aunque el PREP dura 24 horas, tiene un impacto importante políticamente ya que son los primeros resultados que se da a conocer a los partidos políticos, al Consejo General del IEEM y a la ciudadanía interesada principalmente en el Estado de México el día de la elección.

El proceso de difusión que se llevó a cabo para la elección de Gobernador en el Estado de México en el 2017, para el IEEM resultado favorable ya que se cumplió con los objetivos planteados, sin embargo, como una oportunidad de mejora para el proceso sería automatizar el envió de la información a los diferentes difusores, con esto se disminuye el riego del factor humano.

Finalmente, una oportunidad de mejora adicional sería que los enlaces ADSL fueran enlaces simétricos, con lo que se podría mejorar el tiempo de respuesta del sistema PREP.

GLOSARIO

AEC	Acta de Escrutinio y Cómputo es el documento que levantan los funcionarios de casilla al concluir el escrutinio y cómputo de cada una de las elecciones (Tribunal E., 2018).
ADSL	Asymetric Digital Subscriber Line, o Línea de Usuario Digital Asimétrica, se refiere a la tecnología que se sirve de las líneas telefónicas convencionales para crear una conexión a Internet (Maugard, 2017)
Balanceador de carga	Herramienta destinada a repartir (mediante el uso de algoritmos) el trabajo a realizar entre los nodos de un sistema en clúster (Cardador, 2014).
Bot	Es un tipo de programa que posee la capacidad de ejecutar acciones específicas (IIEMD, 2018).
CATD	Centro de Acopio y Transmisión de Datos.
CCapV	Centro de Captura y Validación. Espacio físico destinado para la captura y validación de las AEC, acondicionado en un lugar cercano al Centro Estatal de Cómputo (IEEM, 2017).
CEsCO	Centro Estatal de Cómputo.

Clúster	Grupo de computadoras completas e interconectadas, que trabajan juntas como un recurso de computación unificado y que pueden crear la ilusión de ser una única máquina (Stallings, 2006).
Cross Site Scripting	Es un ataque de inyección de código malicioso para su posterior ejecución que puede realizarse a sitios web, aplicaciones locales e incluso al propio navegador (UNAM, 2015).
DDoS	Ataque de Denegación de Servicio Distribuido es una forma de ataque en la que usuarios malintencionados intentan dejar recursos de red fuera de servicio para los usuarios a los que están destinados (Interoute, 2018).
DNS	Sistema de Nombres de Dominio es un sistema de bases de datos distribuidas que se utiliza para gestionar los nombres de los sistemas principales y sus direcciones IP (Protocolo de Internet) asociadas (IBM, 2018).
DoS	Ataque de Denegación de Servicio, inhabilita el uso de los recursos de una red o de un sistema por parte de los usuarios legítimos (Daltabuit, Hernández, Mallén, & Vázquez, 2007).
Firewall	Es un dispositivo de seguridad de la red que monitorea el tráfico de red entrante y saliente además decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad (Cisco, 2018).

FTP	Protocolo de Transferencia de Archivos, es un protocolo para la transferencia de archivos entre sistemas conectados a una red (Stallings, 2004).
Hardening	Configurar una computadora u otros dispositivo de red para resistir ataques (Sánchez, 2013).
HTTP	Protocolo de transferencia de hipertexto es el protocolo base del world wide web (www) y se puede utilizar en cualquier aplicación cliente – servidor que suponga la utilización de hipertexto (Stallings, 2004).
ICREA	Asociación Internacional sin fines de lucro formada por ingenieros especializados en el diseño, construcción, operación, administración, mantenimiento, adquisición, instalación y auditoría de centros de cómputo (ICREA, 2018).
IEEM	Instituto Electoral del Estado de México es un organismo público local que, de manera conjunta con el Instituto Nacional Electoral, tiene a su cargo la función estatal de la organización de las elecciones en el estado de México (IEEM, 2015).
IMPERVA	Empresa dedicada a la seguridad de la información (IMPERVA, 2010).
INCAPSULA	Protege aplicaciones web y sitios web con un Firewall de Aplicaciones Web (WAF) (IMPERVA, 2018).

INE	Instituto Nacional Electoral, organiza procesos electorales libres, equitativos y confiables para garantizar el ejercicio de los derechos político-electorales de la ciudadanía y contribuir al desarrollo de la vida democrática de México (INE, 2018).
IPS	Sistemas de Prevención de Intrusiones detectan y bloquean cualquier intento de intrusión, transmisión de código malicioso o amenazas a través de la red (Interoute, 2018).
ISO	Organización Internacional para la Estandarización, crea documentos que proporcionan requisitos, especificaciones, directrices o características que se pueden utilizar de forma coherente para garantizar que los materiales, productos, procesos y servicios sean adecuados para su propósito (ISO, 2018).
ISP	Proveedor de Servicios de Internet.
JMeter	Software de código abierto diseñado para hacer pruebas de carga de servidores, por ejemplo servidores web (JMeter, 2018).
OPL	Organismo Público Local, son los encargados de la organización de las elecciones en su entidad federativa para la designación de gobernadores, diputados locales, presidentes municipales, integrantes de ayuntamientos, jefes de delegaciones, jefe de gobierno, entre otros (INE, 2017).

PREP	Programa de Resultados Electorales Preliminares, constituye el mecanismo de información electoral de carácter estrictamente informativo que se encarga de proveer los resultados preliminares y no definitivos de un proceso electoral (IEEM, 2017).
Seguridad perimetral	Arquitectura y elementos de red que proveen de seguridad al perímetro de una red interna frente a otra que generalmente es internet (Ramos, 2011).
Servidor	Es un equipo informático que forma parte de una red y provee servicios a otros equipos cliente (onyx, 2016).
Servidor Proxy	Es un equipo informático su principal función es guardar en memoria caché las páginas web a las que acceden los usuarios de la red durante un cierto tiempo, de esta forma las siguientes veces que estos acceden al mismo contenido, la respuesta es más rápida (onyx, 2016).
SFPT	Es un Protocolo Seguro de Transferencia de Archivos. Se ejecuta sobre el protocolo SSH. Compatible con la funcionalidad completa de seguridad y autenticación de SSH (SSH, 2017).
Sobre PREP	Sobre traslucido en el que se guarda la primera copia del acta de escrutinio y cómputo de la casilla, se coloca por fuera del paquete electoral, en el costado (IEEM, 2017).

SQL Injection	consiste en la inserción o “inyección” de una consulta SQL por medio de los datos de entrada desde el cliente hacia la aplicación (owasp, 2012).
SSH	Secure Shell es un programa que sirve para autenticación segura, transferencia de archivos, ejecución de comandos en una máquina remota en una red insegura, igual para ejecución de programas gráficos remotos y respaldos seguros de redes. Es decir, es un programa que proporciona una conexión entre dos máquinas de forma segura (Daltabuit, Hernández, Mallén, & Vázquez, 2007).
TIC	Tecnologías de la Información y Comunicación son el conjunto de herramientas relacionadas con la transmisión, procesamiento y almacenamiento digitalizado de la información (Luna, 2018).
TIER	Mide el tiempo de disponibilidad de un centro de datos.
VPN	Red Privada Virtual es la extensión de una red privada que utiliza enlaces a través de redes públicas o compartidas, tales como Internet (Daltabuit, Hernández, Mallén, & Vázquez, 2007).
WAF	Firewall de Aplicaciones Web, protege a una aplicación web de ataques maliciosos (IMPERVA, 2018).

REFERENCIAS

Cardador, A. L. (2014). *Dimensionar, instalar y optimizar el hardware.* España: IC Editorial.

Cisco. (2018). *¿Qué es un firewall?* Obtenido de Cisco: https://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html

Daltabuit, E., Hernández, L., Mallén, G., & Vázquez, J. d. (2007). *La seguridad de la información.* México: Limusa.

IBM. (2018). *DNS (Sistema de nombres de dominio)*. Obtenido de IBM: https://www.ibm.com/support/knowledgecenter/es/ssw_i5_54/rzakk/rzakkkickoff.htm

ICREA. (2018). *Acerca de ICREA*. Obtenido de International Computer Room Experts Association: http://www.icrea-international.org/nuevoPortal/quienesSomos.asp

IEEM. (2015). *Historia*. Obtenido de Instituto Electoral del Estado de México: http://www.ieem.org.mx/acerca/historia.html

IEEM. (2015). *Sobre el IEEM*. Obtenido de Instituto Elecctoral del Estado de México: http://www.ieem.org.mx/acerca/definicion.html

IEEM. (22 de Septiembre de 2016). *Acuerdo N°. IEEM/CG/83/2016*. Obtenido de Instituto Electoral del Estado de México: http://www.ieem.org.mx/consejo_general/cg/2016/a083_16.pdf

IEEM. (4 de Noviembre de 2016). *Acuerdo N°. IEEM/CG/93/2016*. Obtenido de Instituto Electoral del Estado de México: http://www.ieem.org.mx/consejo_general/cg/2016/a093_16.pdf

IEEM. (4 de Noviembre de 2016). *Acuerdo N°. IEEM/CG/94/2016*. Obtenido de Instituto Electoral del Estado de México: http://www.ieem.org.mx/consejo_general/cg/2016/a094_16.pdf

IEEM. (2 de Febrero de 2017). *Lineamientos Operativos del Programa de Resultados Electorales Preliminares 2017*. Obtenido de Instituto Electoral del Estado de México: http://www.ieem.org.mx/consejo_general/cg/2017/acu_17/a036_17.pdf

IEEM. (4 de Junio de 2017). *PREP Elección de Gobernador/a del Estado de México*. Obtenido de Instituto Electoral del Estado de México: http://www.prepieem.org.mx/rptDistrital_part.html

IIEMD. (2018). *¿Qué es un bot?* Obtenido de Instituto Internacional Español de Marketing Digital: https://iiemd.com/bot/que-es-bot

IMPERVA. (2010). *La historia de Imperva*. Obtenido de IMPERVA: https://www.imperva.com/docs/Imperva_Company_Overview_ES_LATIN.pdf

IMPERVA. (2015). *Imperva Incapsula DDoS Protection*. Obtenido de IMPERVA INCAPSULA: https://www.imperva.com/docs/DS_Incapsula_DDoS_Protection.pdf

IMPERVA. (2018). *Firewall de aplicacion web*. Obtenido de Imperva: https://www.imperva.com/products/application-security/web-application-firewall-waf/)

IMPERVA. (2018). *Seguridad para sitios web*. Obtenido de IMPERVA INCAPSULA: https://www.incapsula.com/es/seguridad-web/

INE. (9 de Septiembre de 2016). *Reglamento de Elecciones*. Obtenido de Instituto Nacional Electoral: http://portalanterior.ine.mx/archivos3/portal/historico/recursos/IFE-v2/DS/DS-CG/DS-SesionesCG/CG-acuerdos/2016/09_Septiembre/CGex201609-07/CGex201609-7-ap-7-Reglamento.pdf

INE. (26 de Abril de 2017). *¿Qué son los OPL?* Obtenido de Instituto Nacional Electoral: https://www.ine.mx/que-son-los-opl/

INE. (2018). *Voto y Elecciones en México*. Obtenido de Instituto Nacional Electoral: https://www.ine.mx/

Interoute. (2018). *DDoS*. Obtenido de Interoute: https://www.interoute.es/unified-ict/hosting/servicios-gestionados/seguridad-gestionada/ddos

Interoute. (2018). *Sistema de prevención de intrusiones*. Obtenido de Interoute: https://www.interoute.es/hosting/servicios-gestionados/seguridad-gestionada/prevencion-de-intrusiones

ISO. (2016). *ISO/IEC 27001:2013 INFORMATION SECURITY*. Obtenido de ISO/IEC: https://www.iso.org/isoiec-27001-information-security.htm

ISO. (2018). *ISO desarrolla estándares*. Obtenido de Organización Internacional para la Estandarización: https://www.iso.org/standards.html

JMeter. (2018). *JMeter*. Obtenido de Apache JMeter: https://jmeter.apache.org/

Luna, N. (26 de Febrero de 2018). *¿Qué son las TICs?* Obtenido de Entrepreneur: https://www.entrepreneur.com/article/308917

Maugard, J. (2017). *Tecnología ADSL*. Obtenido de Kill my Bill: https://www.killmybill.es/tecnologia-adsl/

onyx. (2016). *¿Qué es un servidor?* Obtenido de onyx system: http://www.onyxsystems.es/que-es-un-servidor.html

owasp. (4 de Diciembre de 2012). *Inyección SQL*. Obtenido de owasp: https://www.owasp.org/index.php/Inyecci%C3%B3n_SQL

Ramos, A. (Febrero de 2011). *Seguridad perimetral*. Obtenido de intypedia: http://www.criptored.upm.es/intypedia/docs/es/video5/DiapositivasIntypedia005.pdf

Sánchez, E. (06 de 03 de 2013). *Hardening*. Obtenido de Magazcitum: http://www.magazcitum.com.mx/?p=2109#.WteHTC7wbcs

SSH. (10 de Octubre de 2017). *SFTP - SSH Secure File Transfer Protocol*. Obtenido de SSH Communications Security: https://www.ssh.com/ssh/sftp/

Stallings, W. (2004). *Comunicaciones y Redes de Computadoras.* Madrid: Pearson.

Stallings, W. (2006). *Sistemas operativos.* México: Pearson.

Tanembaun, A. S. (2012). *Redes de Computadoras.* México: Pearson.

Tribunal, E. (2018). *Acta de escrutinio y cómputo*. Obtenido de Tribunal Electoral del Poder Judicial de la Federación: http://te.gob.mx/taxonomy/term/26/0

UNAM. (21 de Agosto de 2015). *¿Qué es y cómo opera un ataque de Cross-Site Scripting (XSS)?* Obtenido de Coordinación de Seguridad de la Información: https://www.seguridad.unam.mx/historico/documento/index.html-id=35