SERVICIO DE AUDITORIA AL SISTEMA INFORMÁTICO Y A LA INFRAESTRUCTURA TECNOLÓGICA DEL PREP

INSTITUTO ELECTORAL Y DE PARTICIPACIÓN CIUDADANA DE JALISCO

Julio 2018

IJALTI
CLUSTER MANAGER

IJALTI
CLUSTER MANAGER

INSTITUTO ELECTORAL Y DE PARTICIPACIÓN CIUDADANA DE JALISCO (IEPC)
Servicio de Auditoria al Sistema Informático y
a La Infraestructura Tecnológica del PREP
JULIO 2018

PRUEBAS FUNCIONALES DE CAJA NEGRA AL SISTEMA INFORMATICO DEL PREP

IJALTI
CLUSTER MANAGER

PLAN DE PRUEBA

Información General	
Datos de la organización(cliente)	
Nombre	IEPC
Domicilio	Calle Florencia 2370, Italia Providencia, 44648 Guadalajara, Jal.
Gerente de Servicios de TI (o contacto principal)	Ramiro Garzón
Proyecto	
Nombre del producto evaluado	PREP
Fecha de recepción del Producto para su evaluación	09/05/2018
Nombre del documento (informe avance de pruebas)	PlanDePruebas_V1_0.docx
Ubicación	\iepc\Proyecto PREP
Fecha de creación	10/05/2018
Fecha de revisión	11/05/2018
Fecha último cambio	11/05/2018
Estatus de revisión	Aprobado
Autor	Erika Ramos
Dirección de Operaciones Recepción de comentarios	Aarón Moreno Erika Ramos: eramos@e-quallity.net

HISTORIAL DE CAMBIOS

Versión	Fecha	Autor	Función	Descripción del cambio(s)
1_0	21/06/2018	Erika Ramos, Adrian López	Líder de proyecto de pruebas	Versión inicial del documento

LISTA DE DISTRIBUCIÓN

Se distribuirá una copia del presente documento a las siguientes personas involucradas en el proyecto.

Nombre	Función
Aarón Moreno	Dirección de Operaciones
Ramiro Garzón	Gerente de TI

ÍNDICE

INTRODUCCIÓN

Este documento detalla el objetivo, alcance, estrategia y manejo de pruebas para el proyecto Sistema PREP (Programa de Resultados Electorales Preliminares).

El objetivo de este Plan de pruebas es servir como vinculo de comunicación entre los diferentes grupos involucrados en las pruebas de dicho proyecto.

Siendo un documento común, servirá también para asegurar que los diferentes equipos del proyecto entiendan sus dependencias e interacciones con otros equipos del proyecto, de manera que la información pueda fluir adecuadamente para tomar las decisiones correctas en el momento oportuno.

El equipo de pruebas de Test Sourcing realizará pruebas funcionales, performance, denegación de servicios y de comparación de código del proyecto PREP, este proyecto consiste en probar los requisitos listados en el alcance, mediante un proceso de análisis de requerimientos y documentación proporcionada por IEPC, el cual funge como insumo para aplicar la metodología de pruebas empleada por el equipo de Test Sourcing, a través de la cual se podrá definir la re-codificación y estructura necesaria por parte del equipo del IEPC, una vez que, aplicadas las pruebas de software, se encuentren, reporten y corrijan anomalías que afecten a la(s) aplicación(es) que conformarán el proyecto PREP.

Durante este proyecto, el equipo de pruebas de Test Sourcing trabajará con IEPC para conocer sus ambientes, analizar las aplicaciones, planear y efectuar las actividades de pruebas necesarias, para lo cual el IEPC proveerá a tiempo el ambiente necesario para efectuar las pruebas y todos los servicios relacionados requeridos.

OBJETIVOS

Las pruebas de software son una herramienta muy valiosa para prevenir posibles contingencias, protegerse de usuarios inexpertos o maliciosos mediante la corrección de posibles defectos que podrían originar fallas que aun cuando no alteran los resultados podrían ocasionar que los ciudadanos tuvieran una percepción de unas elecciones poco transparentes.

Dar a conocer las métricas de rendimiento y consumo de recursos de la aplicación “PREP”, antes de su paso a producción.

Identificar tiempos prolongados de respuesta, solicitudes y respuestas fallidas, exceso de envío o recepción de información por transacción.

Identificar posibles fallas al incrementar el número de peticiones realizadas al aplicativo que se pretende cargar.

Validar la configuración y desempeño de los mecanismos de seguridad (Firewall, Servidor de aplicaciones) en los servidores.

Observar el comportamiento de los servicios ejecutando una prueba de Performance durante la simulación de un ataque DOS (*Denegation Of Service*).

Generar una herramienta para validar que tanto la versión de código como la estructura de base de datos instaladas en el entorno de producción sean iguales a la última versión liberada.

ALCANCE

El proyecto consiste en un servicio de pruebas funcionales, pruebas de performance y pruebas de denegación de servicios que integran el sistema de captura y visualización de resultados de las elecciones en el Programa de Resultados Electorales Preliminarares (PREP) del estado de Jalisco.

Las pruebas funcionales implican el diseño y aplicación de casos de pruebas para los sistemas **1.0 PREP Casilla, 2.0 PREP Portal, 3.0 DigiCATD, 4.0 PREP Resultados;** los cuales forman parte del alcance del proyecto; que consisten en capturan los resultados plasmados en las actas de casillas entregados en los centros de captura; de igual forma se aplicarán las pruebas en la página web que será visualizada por los ciudadanos para revisar la evolución de los resultados obtenidos en la elecciones, se revisará que la información mostrada sea consistente, y que el comportamiento general del sistema cumpla con la especificación del mismo.

Las pruebas de performance implican, el diseño de scripts de prueba y su ejecución sobre el backend del PREP, el cual forma parte del alcance del proyecto; que consiste en simular una gran cantidad de usuarios virtuales realizando peticiones a la página del PREP.

Las pruebas de denegación de servicio implican dos ataques:
Simular un ataque de tipo TCP SYN ,mediante el envío masivo de paquetes SYN (synchronize) al servidor para iniciar la comunicación de acuerdo al protocolo TCP utilizando equipos especialmente configurados para generar un volumen de paquetes superior a los 600 mbps.

Simular un ataque de tipo DNS Amplification que consiste en hacer solicitudes de tipo DNS a servidores reales creando un paquete modificado donde se remplaza la IP de origen con la IP del servidor víctima, recibiendo este último todas las respuestas de las solicitudes realizadas generando un tráfico mayor a 1.2 gbps (El tráfico generado para realizar las consultas es mayor a 600 mbps pero se multiplica al recibir la respuesta de los servidores DNS).

Desarrollo de una serie de aplicaciones para generar y comparar firmas (Hash SHA1) tanto de la estructura de la base de datos cómo de los archivos de código fuente.

PRUEBAS A APLICAR

Pruebas funcionales: un ciclo de pruebas **progresivas** el cual consiste en la ejecución de los casos de pruebas diseñados y el registro de las anomalías detectas en los sistemas que conforman el proyecto; así como dos ciclos de prueba **regresivas**, que consisten en la verificación de las anomalías con estado "listas para probarse" y la ejecución de aquellos casos de pruebas que tienen impacto directo con la verificación. Para las pruebas de performance se aplicarán cuatro ciclos con simulación de diferentes cantidades de usuarios y con periodos de tiempos similares.

Pruebas de performance: las cuales consisten en ejecutar cuatro escenarios distintos, con la siguiente configuración: 15,000 usuarios, 10,000 usuarios, 5,000 usuarios, 8,400 usuarios.

Pruebas de denegación de servicios: Se realizarán dos tipos de ataques distintos, TCP SYN y DNS Amplification.

PLANEACIÓN DE LAS PRUEBAS

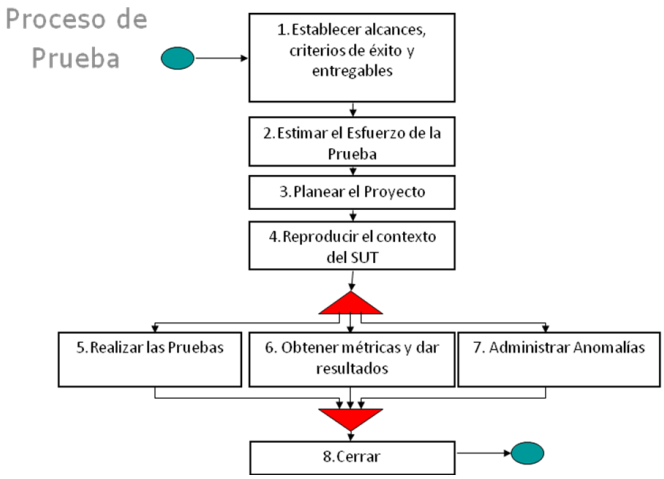
Estrategia de pruebas

Dentro de esta sección se profundiza en los detalles sobre la estrategia general de pruebas a seguir, especificando entre otros aspectos, la metodología, ciclos de prueba, tipos de prueba.

Metodología

En los proyectos de prueba que realizamos en nuestras instalaciones, **utilizamos un ciclo de vida que coincide** en buena medida con el conocido **Modelo-V**, y que incorpora actividades de administración de proyectos recomendadas por el **Project Management Institute**. Hemos desarrollado nuestro proceso de pruebas basado en dos modelos internacionales, obteniendo certificaciones como empresa, bajo dichos modelos especializados en prueba de Software: **TMM (Testing Maturity Model)** nivel 3 y **TPI (TestProcess Improvement)** Nivel Eficiente.

Para la documentación de nuestros procesos, **nuestro Grupo de Innovación y Desarrollo Tecnológico diseñó un Lenguaje formal de Especificación de Procesos**; con él definimos también actividades que involucran métricas, como la estimación necesaria para probar un sistema de ciertas características, o el establecimiento de criterios de aceptación de un producto en función de los resultados en las pruebas regresivas, o la definición de los elementos de información de los resultados de la prueba de software suficientes para la toma de decisiones gerenciales.



Ciclos de Prueba

El ciclo de prueba es la ejecución del proceso de pruebas, que se aplica a cada proyecto para obtener un resultado de la evaluación del sistema.

Ciclos de prueba	¿Aplica?
FUNCIONALES	
Pruebas Progresivas	✓
Pruebas Regresivas 1	✓
Pruebas Regresivas 2	✓
PERFORMANCE	
Simulación 15 000	✓
Simulación 10 000	✓
Simulación 8 400	✓
Simulación 5 000	✓
DENEGACIÓN DE SERVICIOS	
TCP SYN	✓
DNS Amplification	✓

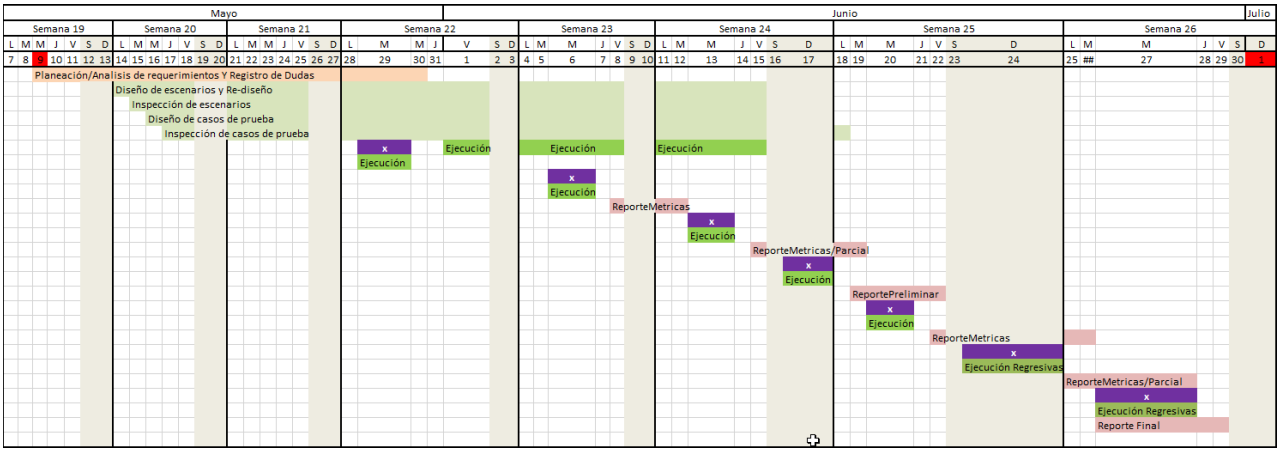
Tipos de prueba

Tipos de Pruebas	¿Aplica?
Pruebas Positivas	✓
Pruebas Negativas	✓
Pruebas de Caja Gris	✓
Pruebas Exploratorias	✓
Pruebas de Caja blanca	×
Pruebas de Performance	✓
Pruebas de Denegación de servicios	✓

Calendarios de Pruebas

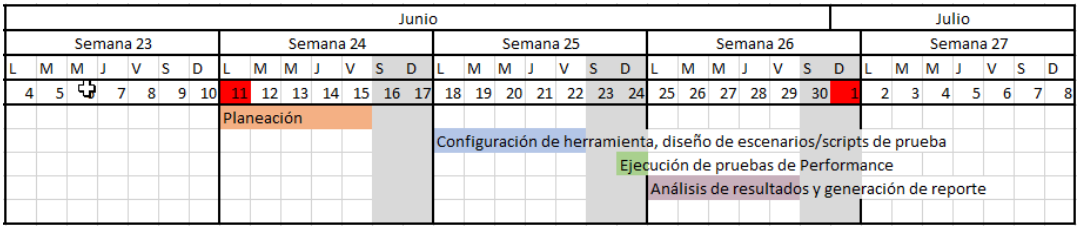
La siguiente sección muestra las actividades a realizar por el equipo de pruebas para el proyecto PREP en los tipos de pruebas funcionales, performance, denegación de servicios y herramienta de validación de código.

Plan de Pruebas Funcionales



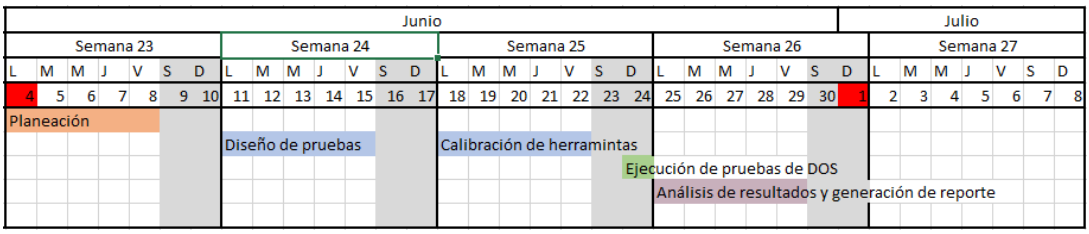
	Inicio/fin de proyecto.
	Planeación.
	Preparación de pruebas.
X	Simulacros del PREP.
	Ejecución de pruebas progresivas.
	Ejecución de pruebas regresivas.
	Reportes Metricas/Parcial/Final.
	No laborable.

Plan de Pruebas de Performance

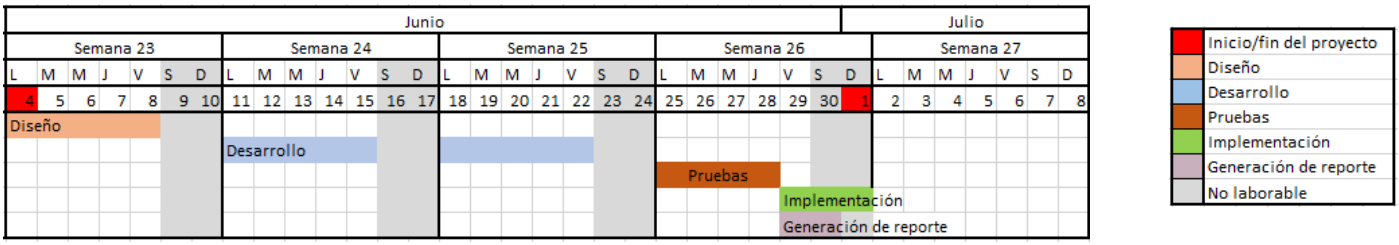


	Inicio/fin del proyecto
	Planeación
	Diseño de pruebas
	Ejecución de pruebas
	Generación de reporte
	No laborable

Plan de pruebas DOS



	Inicio/fin del proyecto
	Planeación
	Diseño de pruebas
	Ejecución de pruebas
	Generación de reporte
	No laborable



Las siguientes aplicaciones deben de encontrarse disponibles en su último nivel de código previo a la ejecución de las pruebas respectivas. La lista de hardware y software del proyecto se muestra en la siguiente tabla.

Hardware

- Celulares
- Escáner
- Laptop
- Computadora
- Miniprinter
- Lector CDD
- Servidores

Características de los Equipos						
Nombre de la Máquina	**SO**	**Procesador**	**Velocidad**	**Memoria RAM**	**Proyecto**	**Cantidad de Equipos**
LAPTOP-HC4UO8M0	Windows 10	INTEL CORE I5-7200U	2.50GHz	8GB	PREP Portal	1
LAPTOP-HC4UO8M0	Windows 10	INTEL CORE I5-7200U	2.50GHz	8GB	PREP Resultados	1
IEPCP320WS	Windows 10	INTEL XEON E3-1225	3.30GHz	8GB	DigiCATD	1
ZTE BLADE V8Q	Android 7.1.2	Snapdragon 435	1.4 GHz	2GB	PREP Casilla	5

Hardware			
Nombre	**Modelo**	**Proyecto**	**Cantidad de Equipos**
Miniprinter	Cognitive TPG A799	PREP Portal	1
Lector CDD	SC21803	PREP Portal	2
Escaner	HP ScanJet Enterprise Flow 7000 s3	DigiCATD	1

Performance

Características de los Equipos							
Nombre de la Máquina	Modelo	SO	Procesador	Velocidad	Memoria RAM	Proyecto	Cantidad de Equipos
Lenovo	ThinkPad T440p	Windows 10	Core i7	2.50GHz 2.49 GHz	12GB	Performance	1
HP	Zbook 15 G2	Windows 10	Core i7	2.60GHz	12GB	Performance	1

Características del Servidor						
Nombre de la Máquina	Modelo	SO	Procesador	Memoria RAM	Proyecto	Cantidad de Equipos
Lenovo	ThinkSystem SR550	Linux CentOS 7	4 Procesadores	8 GB	Performance	1

Software

- Prep Casilla
- Token IEPC
- DigiCATD
- Portal PREP
- PREP Resultados
- BD SQL Server 12.0.41

CASOS DE PRUEBA

Para el sistema PREP se planea generar un total de **279** casos de prueba, con los que se daría cobertura a las matrices de escenarios previamente diseñadas; dicho diseño de casos de prueba corresponde a los módulos mostrados a continuación.

Módulo	Casos de Prueba
1.0 PREP Casilla	40
2.0 PREP Portal	209
3.0 DigiCATD	30
4.0 PREP Resultados	Exploratorias

Para las pruebas de performance se planea generar un script de pruebas con dos configuraciones distintas, para simular una carga significativa sobre el servidor.

Usuarios	Tiempo
15000	3 min
10000	5 min

Para las pruebas de denegación de servicios se planea generar dos ataques sobre el servidor, con el envío de paquetes y la generación de tráfico durante el ataque.

Ataque	Trafico
TCP SYN	300 mbps y 800 mbps
DNS Amplification	N/A

Para las pruebas de comparación de código se utilizarán tres aplicaciones, para comparar la versión de código y la estructura de base de datos.

Nombre	Descripción
FileHashGen	Genera un archivo binario a partir de un directorio especificado donde por cada archivo encontrado almacena su nombre y una firma generada a partir de su contenido.
BDHashGen	Genera archivos binarios por tabla, vistas e índices primarios a partir de una conexión de base de datos para Microsoft SQL Server.
Comparador	Genera reportes en PDF con los resultados obtenidos de comparar los archivos generados por las aplicaciones anteriores.

DATOS DE PRUEBA

La estrategia a ser implementada consiste en definir y crear los tipos de usuario con el perfil requerido para ejecutar todas las funciones incluidas en cada uno de los módulos que conforman el proyecto PREP en los diferentes equipos que conforman el ambiente de pruebas.

Se utilizarán datos reales tanto como sea posible para validar el correcto comportamiento de la aplicación y sólo en casos especiales se hará uso de datos ficticios para simular ciertas tareas como la cantidad de votos, cantidad de votantes, actas para digitalización.

El equipo de pruebas generará internamente los scripts de prueba, matrices de escenarios, archivos binarios, acorde a las técnicas que apliquen para cada caso de prueba.

Aplicando los datos válidos e inválidos que puedan revelar anomalías de severidad alta y que afecten a la funcionalidad principal de los sistemas involucrados durante el proceso de recolección de información que se mostrará en la página del PREP.

CRITERIOS DE PRUEBA

Criterios de Entrada para todos los tipos de Pruebas

Criterios de entrada	Responsable
Funcionalidad de los sistemas (completa o por módulos) y disponible en un ambiente de pruebas.	**Equipo IEPC**
Calendario de liberación de módulos o del sistema completo para identificar el arranque de cada	

ejecución de pruebas (funcionales, performance y denegación de servicios)	
Datos, tablas, catálogos, actas que fuesen requeridos para las pruebas.	
Disponibilidad de datos reales para pruebas y soporte al equipo de pruebas de TestSourcing en el armado de conjunto de datos, en caso de ser requerido.	
Ambiente (configuración de hardware y software requeridos) y herramientas requeridas para pruebas disponibles.	
Resolución de dudas técnicas, funcionales, asignación de usuarios expertos para revisión de flujos.	
Personal capacitado para la ejecución de las pruebas.	**Equipo Test Sourcing**
Matrices de Escenarios de Prueba revisados y aprobados.	
Herramienta Mantis configurada para el reporte de anomalías.	

Criterios de Salida para todos los tipos de Pruebas

Criterios de salida	Responsable
Módulos estables, ninguna anomalía con severidad 1 'Muy Alta' ni severidad 2 'Alta', sin resolver.	**Equipo IEPC**
Sistema no resulta afectado severamente durante la ejecución de las pruebas de carga, permitiendo que pueda continuar atendiendo peticiones.	
Sistema no resulta afectado severamente durante las pruebas de denegación de servicios.	
Ejecución del 90% al 100% de Casos de Prueba	**Equipo Test Sourcing**
Ninguna anomalía en estado "Lista para probarse"	

ADMINISTRACIÓN DE RIESGOS

Durante el desarrollo de las pruebas es posible que se presenten situaciones especiales que pongan en riesgo el cumplimiento, avance o finalización de las actividades a desempeñar por parte del equipo pruebas. El objetivo de la siguiente tabla es identificar estos riesgos y prestar atención especial en ellos para evitar que se presenten aplicando el plan de contingencia mencionado o bien, en caso de presentarse alguno de ellos tener documentado un plan para mitigar el impacto del riesgo presentado.

	Descripción Riesgo	Plan de Contingencia	Plan de Mitigación
1	Retraso en instalación de aplicación (Manejo de "anomalías", problemas que no ha sido adecuadamente implementados)	En caso de existir algún asunto administrativo, se seguirá la línea de comunicación estipulada para el proyecto.	- Se adapta el plan. - Se habla con el cliente y se revisa la programación de fechas.

	Descripción Riesgo	Plan de Contingencia	Plan de Mitigación
2	Retraso en capacitación	El equipo de pruebas podría iniciar el diseño de casos de prueba, pero el Líder de Proyecto deberá enviar un correo especificando que sí aprueba el inicio de esa fase y acepta el riesgo de que exista posteriormente un re-trabajo excesivo que pueda retrasar las fechas de terminación de estos entregables y por ende, el inicio de la fase de ejecución.	- Se inicia con el diseño de entregables y se deja pendiente la información necesaria. - Se notifica al Líder de Proyecto que no se cuenta con la información de los procesos para complementar los entregables de pruebas. - Se solicita atención por parte del IEPC que pueda apoyar a explicar la funcionalidad pendiente. - Se notifica que el proceso quedará diseñado de manera general y se actualizará durante la ejecución de las pruebas, considerando que este re-trabajo es un tiempo a consumir en la ejecución de pruebas.
3	Falta de documentación (Requerimientos, cambios a requerimientos, no contar con la totalidad de documentación o prototipos de las aplicaciones a tiempo previo al inicio de diseño de matriz escenarios y diseño de casos de prueba)	Evaluar los cambios, el impacto y reprogramar las actividades de acuerdo a los cambios exclusivamente aprobados, que puedan ser “contenidos” o “manejables” para los tiempos del proyecto.	- Se inicia con el diseño de entregables de pruebas y se deja pendiente la información necesaria para complementarlos. - Se notifica al Líder de Proyecto que no se cuenta con la información de los procesos para complementar los entregables de pruebas. - Se solicita atención por parte de alguna área que pueda apoyar a explicar la funcionalidad pendiente. - Se notifica que el proceso quedará diseñado de manera general y se actualizará durante la ejecución de las pruebas, considerando que este re-trabajo es un tiempo a consumir en la ejecución de pruebas.
4	Retraso en contestar dudas	Contactar directamente a los responsables para aclaración de las dudas que bloqueen el avance de la documentación o ejecución de pruebas. Establecer sesiones específicas para cubrir el mayor número de pendientes.	- Se continúa con el proceso de pruebas y se mantiene la alerta. - Se establecen sesiones/juntas con los usuarios y líderes de proyecto para resolver las dudas más importantes. - Se contacta al Líder de Proyecto y se informa que las dudas pendientes se reflejarán en los entregables y dejarán

	Descripción Riesgo	Plan de Contingencia	Plan de Mitigación
			plasmadas para su identificación.
5	Retraso en tiempo de prueba (No contar con ambiente de pruebas listo.)	Posibilidad de crear un ambiente alterno en caso de existir dificultades en el servidor original.	- Se adapta el plan. - Se ingresan recursos adicionales para la ejecución de casos de pruebas. - Se reprograma el plan de ejecución de pruebas.
6	Retraso en tiempo de corrección (Cualquier anomalía detectada implicará tiempo para ser solucionada y por lo tanto podría afectar el calendario establecido.)	Revisiones diarias con el encargado de corrección de anomalías. Calificación de anomalías de acuerdo a su severidad y módulo.	- Se sigue el proceso de revisión de anomalías. - Se bloquea el módulo-sub-módulo y se deja para el siguiente Ciclo de Pruebas.
7	Falta de RH (equipo de trabajo, recursos críticos no disponibles a tiempo)	Preparar personal para su inclusión en el proyecto, en el momento que sea necesario. Notificar a los Líderes del Proyecto sobre los recursos para revisar el alcance y fechas de los proyectos.	- Se adapta el plan. - Trabajar tiempos extra por parte de los recursos disponibles. - Agregar más recursos al proyecto de áreas diferentes para cubrir los lugares críticos.

PLAN DE COMUNICACIÓN

Tipo de Comunicación	Objetivo de comunicación	Expositor	Receptor	Periodo	Medio	Formato
Externa (Cliente)	Dudas	Erika Ramos Aide Hernández Alma Estrada Leticia Rosales Karen Romo Adrian López Meinardo González	IEPC	Cada 10 dudas o semanal	Un correo enviado por Erika Ramos al contacto de IEPC. Las respuestas de las dudas se enviarán al líder del proyecto en periodos de 2 días hábiles.	Con la plantilla "DudasIEPC"
	Equipo para ambiente de pruebas	Erika Ramos	IEPC	Inicio del proyecto	Ir a las instalaciones del cliente por el equipo requerido y firmar una responsiva.	Responsiva del equipo

	Simulacros de la elección	Erika Ramos	IEPC	2 por semana	Por medio de un correo solicitar las fechas de simulacro y la autorización para ingresar al CATD del distrito	Correo electrónico
	Reportes Avance semanal	Erika Ramos	IEPC	Cada semana, a partir de la ejecución de las pruebas	Se enviará el reporte de avance cada semana al IEPC y si se cree conveniente, se realizará una junta para el desglose de dicho reporte.	ReporteAvance_ddmmaa_PREP_VX_X.xlsx
	Reporte preliminar	Erika Ramos	IEPC	Al finalizar las pruebas progresivas	Se enviará el reporte preliminar con los resultados de pruebas progresivas al IEPC y si se cree conveniente, se realizará una junta para el desglose de dicho reporte.	ReportePreliminar_PREP_VX_X.pdf
	Reporte de pruebas regresivas	Erika Ramos	IEPC	Al finalizar las pruebas regresivas	Se enviará el reporte de pruebas regresivas con los resultados de pruebas al IEPC y si se cree conveniente, se realizará una junta para el desglose de dicho reporte.	ReporteRegresivas_PREP_VX_X.pdf
	Reportes Finales	Erika Ramos Adrian López Meinardo González	IEPC	Una vez finalizado el proyecto.	Se enviarán a IEPC los reporte finales de cada tipo de prueba, una vez que haya concluido el proyecto. Se realizará	ReporteFinaldePruebasFuncionales_PREP_VX_X.pdf ReporteFinaldeResultadosPruebasPerformancePREP_VX_X.pdf ReporteFinaldeResultadosPruebasDOS_PREP_VX_X.pdf

					una junta con el Cliente al final del proyecto donde se le entregarán los resultados finales con las estadísticas de las Anomalías detectadas en todo el proyecto con sus respectivos estados.	
Interna (TestSourcing)	Reportes de Avance al director de operaciones	Erika Ramos	Aarón Moreno	Cada que se haga la entrega al cliente	Se enviará el reporte por correo previo a que se envíe al cliente	ReporteAvance_ddmmaa_PREP_VX_X.xlsx ReportePreliminar_PREP_VX_X.docx ReporteRegresivas_PREP_VX_X.docx
	Reportes Finales	Erika Ramos	Aarón Moreno	Una vez al final del proyecto	Se enviará el reporte final una vez que haya concluido el proyecto.	ReporteFinaldePruebasFuncionales_PREP_VX_X.pdf ReporteFinaldeResultadosPruebasPerformancePREP_VX_X.pdf ReporteFinaldeResultadosPruebasDOS_PREP_VX_X.pdf

ENTREGABLES

- Plan pruebas
- Reportes de resultados de avance
- Reporte preliminar de pruebas funcionales
- Reporte de pruebas regresivas
- Listado de anomalías documentados
- Reporte final de pruebas funcionales
- Reporte de pruebas de performance
- Reporte de pruebas de denegación de servicios
- Reporte de software de comparación de versiones

- **ANOMALÍA:** Es el defecto encontrado que no permite llegar a los criterios aceptados.

- **ESCENARIO DE PRUEBA:** Descripción general de los requerimientos como flujos de funcionalidad a un alto nivel.

- **CASO DE PRUEBA:** Una secuencia de instrucciones para verificar el buen o mal funcionamiento del sistema, en base al cumplimiento o no de una especificación del mismo.

- **MÓDULO:** Grano de sistema, opción, menú.

- **DOS:** Ataque de denegación de servicios.

REPORTE FINAL DE PRUEBAS FUNCIONALES

Información General	
Datos de la organización(cliente)	
Nombre	IEPC
Domicilio	Calle Florencia 2370, Italia Providencia, 44648 Guadalajara, Jal.
Gerente de Servicios de TI (o contacto principal)	Ramiro Garzón
Proyecto	
Nombre del producto evaluado	PREP
Fecha de recepción del Producto para su evaluación	09/05/2018
Nombre del documento (informe avance de pruebas)	ReportePreliminarDePruebasPREP_V1_0.docx
Ubicación	\iepc\Proyecto PREP
Fecha de creación	29/06/2018
Fecha de revision	29/06/2018
Fecha último cambio	29/06/2018
Estatus de revision	Aprobado
Autor	Erika Ramos
Director de Operaciones	Aarón Moreno
Recepción de comentarios (si los hubiera)	Erika Ramos: eramos@e-quallity.net

HISTORIAL DE CAMBIOS

Versión	Fecha	Autor	Función	Descripción del cambio(s)
1_0	29/06/2018	Erika Ramos	Líder de proyecto de pruebas	Versión inicial del documento

LISTA DISTRIBUCIÓN

Se distribuirá una copia del presente documento a las siguientes personas involucradas en el proyecto.

Nombre	Función
Aarón Moreno	Director de Operaciones
Ramiro Garzón	Gerente de TI

ÍNDICE

INT RODUCCIÓN

El Sistema PREP (Programa de Resultados Electorales Preliminares), es el mecanismo de información electoral que recaba los resultados preliminares y no definitivos, de carácter estrictamente informativo a través de la captura de los datos asentados en las actas de escrutinio y cómputo de las casillas que se reciben en los CATD (Centros de Acopio y Transmisión de Datos) autorizados.

El propósito del presente documento es dar a conocer los resultados finales de las pruebas funcionales en su ciclo de pruebas progresivas y regresivas obtenidos para el proyecto **PREP,** dentro del periodo que abarca del **9 de Mayo al 29 de Junio 2018**, así como también informar sobre las metodologías utilizadas en el proceso de pruebas de Test Sourcing y la clasificación empleada para las anomalías reportadas.

En este reporte se mostrará un resumen detallado de las actividades realizadas por el equipo de pruebas, desde planeación análisis documentación, diseño de escenarios, casos de prueba, reporte, y clasificaciones de anomalías detectadas y distribuidas por Módulo, según su Severidad, Prioridad, Tipo, Estado y Sistema Operativo.

Además, se detallarán los problemas presentados, las dependencias, riesgos y conclusiones, derivadas del seguimiento dado al proyecto en sus ciclos de pruebas progresivas y regresivas.

.

RESUMEN

El propósito del presente documento es dar a conocer el resultado final de pruebas funcionales, obtenido sobre el proyecto de pruebas del **sistema PREP**, durante el periodo: **del 09 de Mayo al 29 de Junio del 2018.**

Entre las principales actividades que se llevaron a cabo durante el periodo que abarca el presente documento, para el ciclo de pruebas Progresivas y Regresivas del sistema PREP, se destacan las siguientes:

Revisión de documentación de requerimientos del sistema, elaboración del desglose de funcionalidad, elaboración de las matrices de escenarios.

Registro, revisión y resolución de dudas expuestas por el equipo de pruebas de e-Quallity.

Generación de planes internos del proyecto, así como plan de actividades inicial.

Actividades generales de preparación del repositorio, adaptación de plantillas, entre otras y en general preparar el ambiente del proyecto de Pruebas.

Reuniones internas, entre ellas, reunión de arranque, reuniones de avance, capacitación de personal y forma de trabajo dentro del proyecto de pruebas.

Se diseñaron **44** Escenarios de prueba en base a los requerimientos proporcionados por el cliente, los cuales quedaron concentrados en un total de 4 matrices de escenarios de prueba.

Se realizó el diseño de técnicas para aplicarlas al desarrollo de casos de prueba.

Se llevó a cabo el diseño de casos de prueba para los módulos considerandos dentro del proyecto, obteniendo un total **281 Casos de prueba diseñados.**

El resultado obtenido de la ejecución del ciclo de **Pruebas progresivas** se llevó a cabo mediante la aplicación de los casos de prueba desarrollados para los módulos con un total de **281 casos ejecutados**, de los cuales se obtuvo como resultado: **221 Aprobados, 45 Desaprobados, 8 Por aplicar y 7 Bloqueados (por problemas derivados de anomalías reportadas).**

Se ejecutó el módulo 4 PREP Resultados con pruebas exploratorias y registrando los defectos encontrados los cuales están contemplados dentro de las estadísticas.

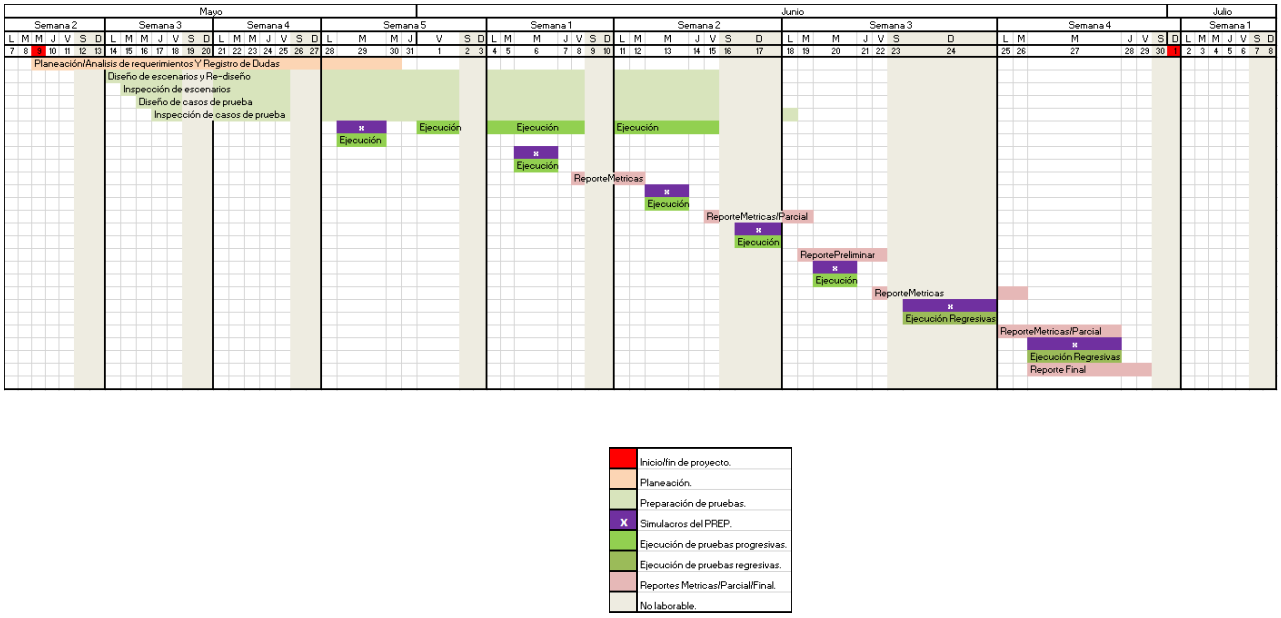
Se generaron reportes de pruebas progresivas del proyecto, con la finalidad de que se aplicaran las correcciones necesarias.

Se obtuvo capacitación por parte del cliente para explicar la funcionalidad de los cambios aplicados.

Se ejecutaron las pruebas regresivas, verificando las 50 anomalías, en la nueva versión del sistema PREP y se dio el seguimiento correspondiente. Durante este proceso se detectaron 11 anomalías nuevas que se incluyen en las estadísticas. Las métricas relacionadas serán detalladas en secciones posteriores.

El resultado obtenido en las **Pruebas regresivas** donde se verificaron las 61 anomalías dio como resultado: **47 Cerradas**, **5 En Proceso**, **7 Canceladas** y **2 No Atendidas**.

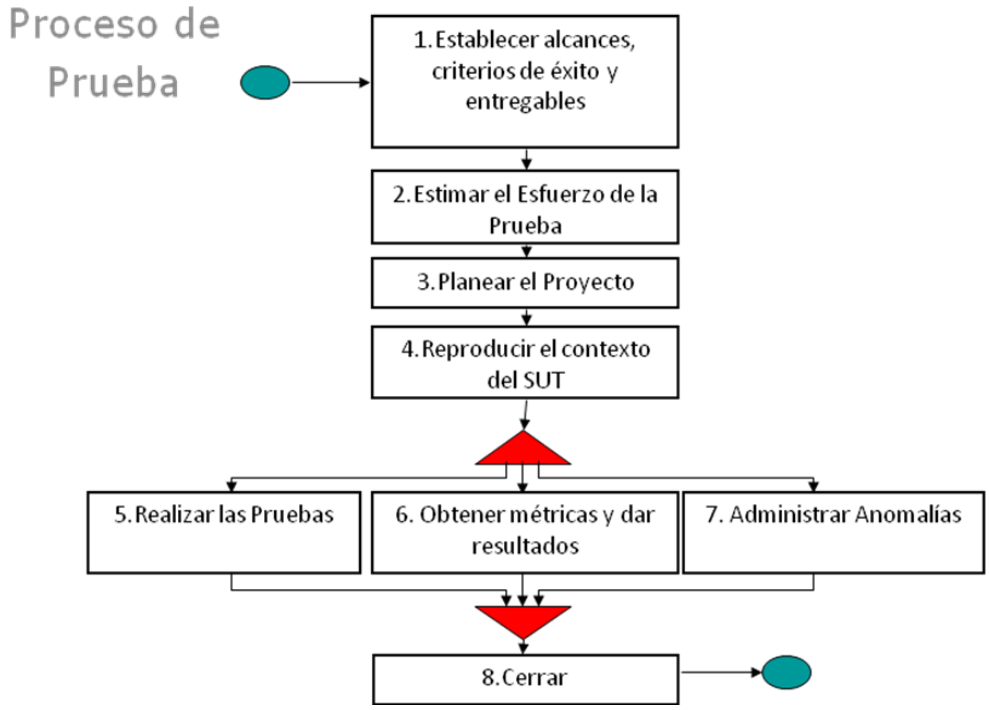
Siguiendo el siguiente cronograma de actividades del 09 de Mayo al 29 de Junio 2018.



METODOLOGÍA

En los proyectos de prueba que realizamos en nuestras instalaciones, **utilizamos un ciclo de vida que coincide** en buena medida con el conocido **Modelo-V**, y que incorpora actividades de administración de proyectos recomendadas por el **Project Management Institute**. Hemos desarrollado nuestro proceso de pruebas basado en dos modelos internacionales, obteniendo certificaciones como empresa, bajo dichos modelos especializados en prueba de Software: **TMM (Testing Maturity Model)** nivel 3 y **TPI (TestProcess Improvement)** Nivel Eficiente.

Para la documentación de nuestros procesos, **nuestro Grupo de Innovación y Desarrollo Tecnológico diseñó un Lenguaje formal de Especificación de Procesos**; con él definimos también actividades que involucran métricas, como la estimación necesaria para probar un sistema de ciertas características, o el establecimiento de criterios de aceptación de un producto en función de los resultados en las pruebas regresivas, o la definición de los elementos de información de los resultados de la prueba de software suficientes para la toma de decisiones gerenciales.



CRITERIOS UTILIZADOS PARA LA AUDITORIA

Escenarios prueba

Para el sistema **PREP** se diseñaron un total de **4 matrices de escenarios de prueba,** cuyos nombres para mayor referencia, se encuentran listados en la siguiente tabla; como contenido de las mismas, se tiene por el momento un total de **44** escenarios de pruebas correspondientes a los módulos: **1.0 PREP Casilla, 2.0 PREP Portal, 3.0 DigiCATD, 4.0 PREP Resultados;** los cuales forman parte del alcance del proyecto, los que a su vez se desprenden del análisis de la información/documentación fuente del sistema proporcionada al equipo de pruebas.

Módulos del Sistema	Nombre Matrices de Escenarios de Prueba	Escenarios Diseñados
1.0 PREP Casilla	MatrizEscenarios_PREP_Módulo_1_0_PREPCasilla_V1_0 (F29T04-01)	12
2.0 PREP Portal	MatrizEscenarios_PREP_Módulo_2_0_PREPPortal_V1_0 (F29T04-01)	25
3.0 DigiCATD	MatrizEscenarios_PREP_Módulo_3_0_DigiCATD_V1_0 (F29T04-01)	07
4.0 PREP Resultados	Pruebas exploratorias	00

Casos de prueba

Para el sistema PREP se generaron un total de **281** casos de prueba, con los que se dio cobertura a las matrices de escenarios previamente listadas; dicho diseño de casos de prueba corresponde a los módulos mostrados a continuación.

Módulo	Casos de Prueba Diseñados
1.0 PREP Casilla	51
2.0 PREP Portal	191
3.0 DigiCATD	39
4.0 PREP Resultados	Exploratorias

METODOLOGÍA PARA CLASIFICAR LOS HALLAZGOS

La metodología utilizada para la clasificación de defectos que implementamos está basada en métricas, características y estadísticas que nos permiten identificar con gran precisión el tipo de anomalía, a continuación, se describe los tipos de anomalías en los que se puede clasificar un defecto.

Clasificación	Descripción
Funcionalidad	Son anomalías referentes a que el sistema no cumple con la especificación del requerimiento, es decir, no realiza las funciones para las que fue creado o no las realiza adecuadamente (por ejemplo: cálculo, eliminación, generación, importar, etc.)
Validación	Verifica la información introducida por el usuario en el sistema, por ejemplo, tipos de datos, rangos, formatos, valores al límite (ej: RFC, CP, CURP, etc.), valores válidos/inválidos.

Integridad	Cuando no son del todo confiables los datos, no funcionan adecuadamente en conjunto, por ejemplo, si en un módulo se da de alta un registro, en un catálogo debe poderse utilizar la misma información o en cualquier otro módulo.
Seguridad	Problemas relacionados con no mantener protegidos los datos en una aplicación, problemas de confidencialidad, autenticación, autorización, disponibilidad del sistema o vulnerabilidades conocidas como facilidad de acceso a intrusos, entre otras.
Diseño	Significa que no se sigue el mismo estándar entre diferentes funcionalidades y pantallas del sistema.
Imagen	Se refiere a errores en el lenguaje, imágenes, redacción, etc.
Terminación inesperada	Indica que por alguna razón el sistema fue terminado sin que el usuario deseara hacerlo, por ejemplo, se cae el sistema (se colapsa), se bloquea, etc.

Además, se muestra una tabla con la descripción de la severidad que puede llegar a tener una anomalía.

Clasificación	Descripción
Muy Alta	El componente no puede ser usado o bloquea la prueba y la operación. No es posible continuar la prueba o continuar utilizando el sistema. No existe una solución alterna para continuar con la prueba.
Alta	Funciones críticas afectadas sin posibilidad de realizarlas de manera diferente, y que afectan a una cantidad considerable de Escenarios de prueba
Promedio	Funciones realizadas incorrectamente por el sistema. El componente puede ser usado, pero con restricciones, existe una solución alterna.
Baja	Son referentes a la apariencia del sistema, o causa inconvenientes y molestias a los usuarios, sin que el sistema se vea realmente afectado respecto a funcionalidad. Mejoras cosméticas que pueden ser solucionadas o diferidas a una nueva versión.
Mejora	No representa como tal una anomalía, desde el punto de vista crítico por no estar asociado a un requisito específico, pero es una propuesta para mejorar el sistema.

RESULTADOS DE LA EJECUCIÓN DE CASOS DE PRUEBA

Dentro de la presente sección se desglosa un resumen de la ejecución del ciclo de pruebas Progresivas para el sistema PREP, La ejecución de **Progresivas** fue de **281** casos de prueba diseñados y para la ejecución de pruebas **Regresivas** se **verificaron** las **61 anomalías** detectadas.

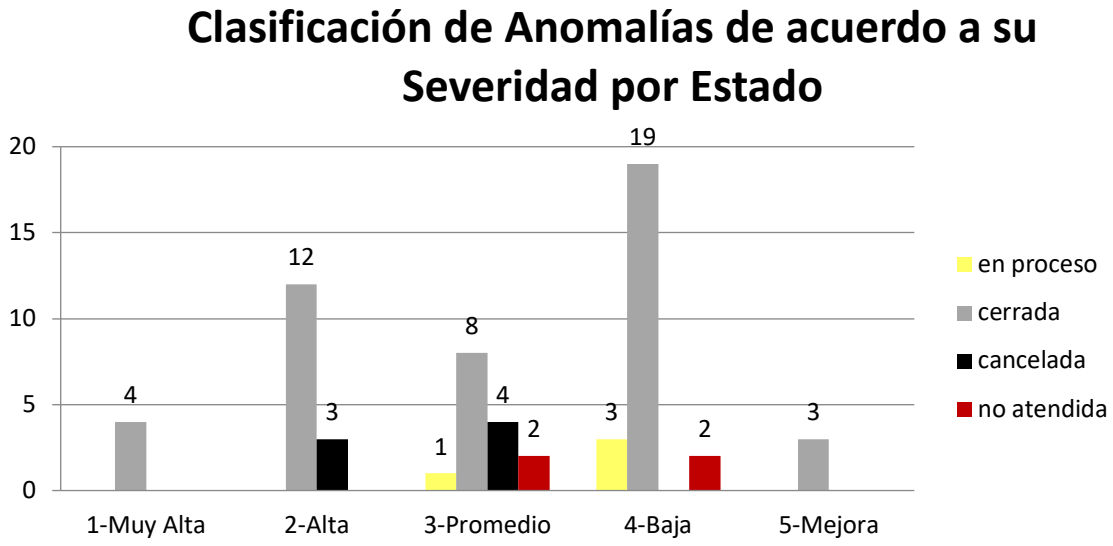
Proyecto Versión	PREP Progresivas					
Resultados Sobre Casos de Prueba	**Casos de Prueba Diseñados**	**Casos de Prueba Aplicados**	**Casos de Prueba Aprobados**	**Casos de Prueba Desaprobados**	**Casos de Prueba Bloqueados**	**Casos de prueba por Aplicar**
Funcionamiento (FN)	281	266	221	45	7	8
Porcentaje (%)	**100%**	**94.66%**	**78.65%**	**16.01%**	**2.49%**	**2.85%**

Proyecto Versión	PREP Progresivas					
Resultados Sobre Casos de Prueba	**Casos de Prueba Diseñados**	**Casos de Prueba Aplicados**	**Casos de Prueba Aprobados**	**Casos de Prueba Desaprobados**	**Casos de Prueba Bloqueados**	**Casos de prueba por Aplicar**
Funcionamiento (FN)	281	281	276	5	0	0
Porcentaje (%)	**100%**	**100%**	**98.22%**	**1.78%**	**0%**	**0%**

- **Casos de Prueba Reutilizados**: Se refiere a los casos de prueba que fueron seleccionados para ser ejecutados en la fase actual.
- **Casos de Prueba por Aplicar**: Son los casos de prueba que aún no se han ejecutado.
- **Casos de Prueba Aplicados**: Son los casos de prueba que ya se ejecutaron.
- **Casos de prueba Aprobados**: Son los casos en los que el sistema se comportó como se esperaba según los requisitos.
- **Casos de prueba Desaprobados:** Son los casos en los que el sistema NO se comportó como se esperaba según los requisitos.
- **Casos de Prueba Bloqueados**: Son los casos que quedaron pendientes por causas ajenas al equipo de prueba, por ejemplo, anomalías o dudas que no se resolvieron o respondieron.

CLASIFICACIÓN DE ANOMALÍAS POR SEVERIDAD POR ESTADO

El avance ejecución dio como resultado **61** anomalías las cuales están clasificadas mediante tablas y graficas de acuerdo con su **Severidad por Estado**.

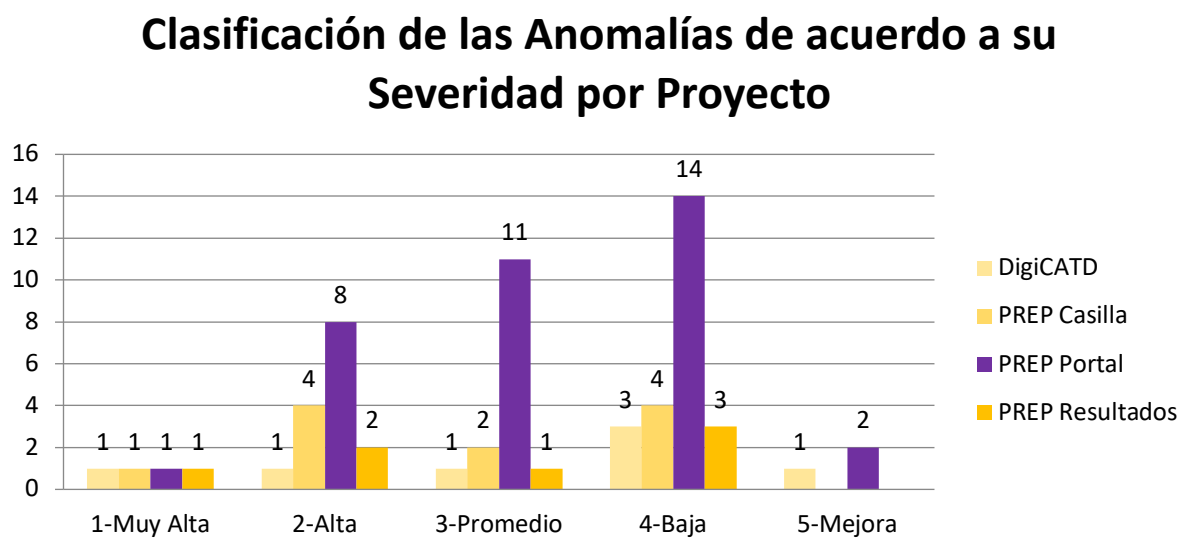


Severidad	En proceso	Cerrada	Cancelada	No atendida	Total general
Muy Alta	0	4	0	0	4
Alta	0	12	2	0	16
Promedio	1	8	4	2	14
Baja	3	19	0	2	24
Mejora	0	3	0	0	3
Total general	**4**	**46**	**7**	**4**	**61**

Se observa que 4 anomalía quedaron en proceso de revisión, estas anomalías son de severidad baja, por lo que no impacta en la funcionalidad de la aplicación; son anomalías que están relacionadas a aspectos de interfaz gráfica. y aplicar su corrección requiere de tiempo en proceso publicación y actualización de la app en los dispositivos móviles.

CLASIFICACIÓN DE ANOMALÍAS POR SEVERIDAD POR PROYECTO

El avance ejecución dio como resultado **61** anomalías las cuales están clasificadas mediante tablas y graficas de acuerdo a su **Severidad por Proyecto**, destacando con **36** anomalías reportadas para el proyecto **PREP Portal.**

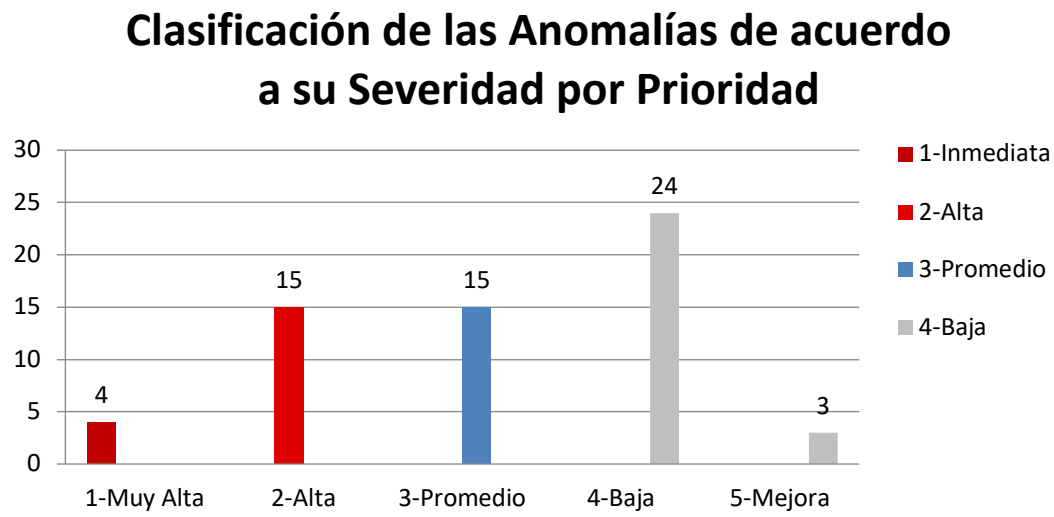


Severidad	DigiCATD	PREP Casilla	PREP Portal	PREP Resultados	Total general
Muy Alta	1	1	1	1	4
Alta	1	5	8	2	15
Promedio	1	1	11	1	14
Baja	3	4	14	3	24
Mejora	1	0	2	0	3
Total general	**7**	**11**	**36**	**7**	**61**

CLASIFICACIÓN DE ANOMALÍAS POR SEVERIDAD POR PRIORIDAD

Las **61** anomalías reportadas están clasificadas a continuación, mediante tablas y graficas de acuerdo con su **Severidad por Prioridad**, los datos son mostrados tanto en cantidad como en porcentaje**.**

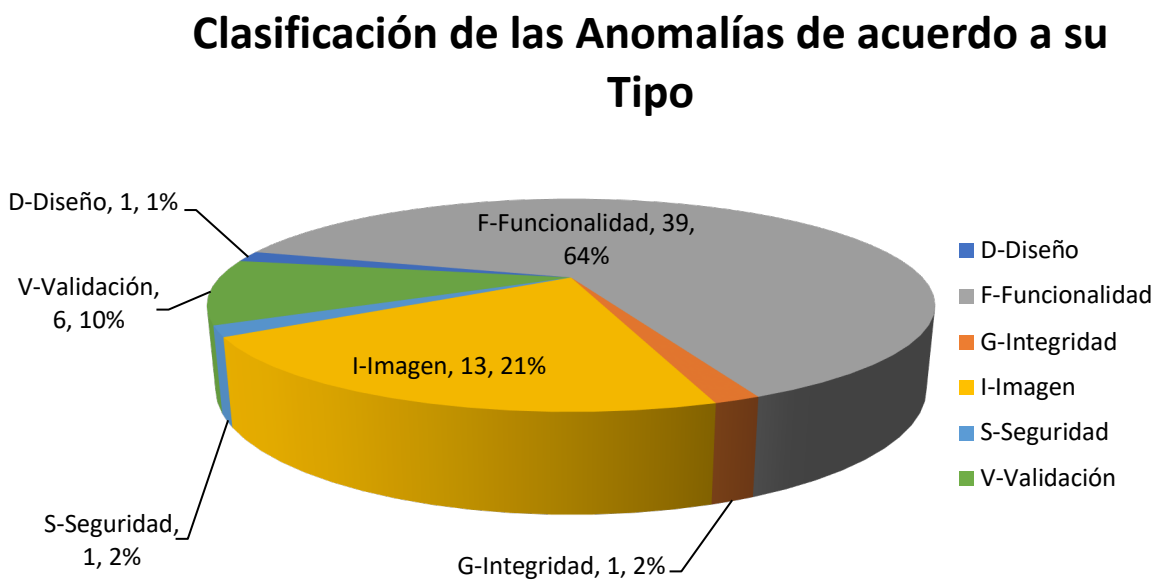
Clasificación	Descripción
Inmediata	Resolver inmediatamente, en cuanto se reporte.
Alta	Dar alta atención. Se puede resolver en la siguiente liberación interna
Promedio	Atención normal. Resolver al menos antes de la entrega al cliente
Baja	Baja Prioridad. Deseable que se corrija para la entrega al cliente



Severidad	Inmediata	Alta	Promedio	Baja	Total general
Muy Alta	4	0	0	0	4
Alta	0	15	0	0	15
Promedio	0	0	15	0	15
Baja	0	0	0	24	24
Mejora	0	0	0	3	3
Total general	**4**	**15**	**15**	**27**	**61**

CLASIFICACIÓN DE ANOMALÍAS POR SU TIPO

La tabla y gráfica siguientes muestran el total de las **61** anomalías encontradas en el proyecto **PREP**, clasificadas de acuerdo con su **Tipo**, destacando con 64% las anomalías clasificadas de **Funcionalidad;** los datos son mostrados tanto en cantidad como en porcentaje.



Tipo	Cantidad	Porcentaje
Funcionalidad	39	64%
Imagen	13	21%
Validación	6	10%
Seguridad	1	2%
Diseño	1	2%
Total general	**61**	**100%**

RIESGOS

Algunos de los riesgos que se estuvieron monitoreando a lo largo del proyecto, son:

Folio	Fecha registro	Descripción	Forma de mitigarlo	Impacto	Estado/Comentarios
R01	2018/05/14	No contar con la totalidad de la documentación	Llegar a un acuerdo (y cumplirlo) respecto a las entregas de la documentación.	Desfase en los tiempos planeados.	**Cerrado.**
R02	2018/05/15	Retraso en la respuesta de las dudas documentadas durante el proyecto.	Enviar recordatorio medio día antes de la fecha limite	Desfase en diseño y ejecución	**Cerrado.**
R03	2018/05/16	Recursos materiales incompletos (Terminales, impresora, escáner, maquinas, aplicaciones, página de distribuidor).	Llegar a un acuerdo (y cumplirlo) respecto a las entregas del recurso.	Desfase en tiempos planeados de ejecución	**Cerrado.**
R04	2018/05/18	Retraso y re-trabajo en las actividades de diseño y ejecución de casos de prueba por falta de documentación y equipos.	Ajustar tiempo en actividades	Retraso en las actividades del proyecto.	**Cerrado.**
R05	2018/06/18	Actualización de los datos de la página del PREP	Solicitar una actualización cada que sea necesaria	Retraso en ejecución y verificación de información	**Cerrado.**

CONCLUSIONES

Dentro del ciclo de Pruebas **Progresivas,** se diseñaron pruebas funcionales fundamentadas en base a la documentación recibida y resolución de dudas. Definidas y diseñadas las pruebas, fueron aplicadas al sistema, lo cual dio como resultado la detección y reporte de anomalías en cada uno de los módulos evaluados (**PREP Casilla, PREP Portal, DigiCATD, PREP Resultados**). Algunos de los puntos que destacar respecto a la ejecución del presente proyecto son:

Diseño de pruebas:

- *Diseño/Actualización/Corrección de escenarios de prueba* aplicando cambios basados en la documentación y retroalimentación del equipo del IPEC, dando como resultado un total de **44 escenarios de prueba**.
- *Diseño/Actualización/Corrección de casos de prueba* aplicando cambios basados en la documentación recibida en su última versión. Dando como resultado **281 casos de prueba** totales.

Ejecución de pruebas Progresivas:

- ***221** casos de prueba aprobados***.** Los cuales a través de su ejecución permitieron comprobar que el sistema se comporta como se esperaba.
- ***45** casos de prueba desaprobados***.** Los cuales al ejecutarse, identificaron anomalías en el funcionamiento del sistema.
- ***7** casos de prueba bloqueados***.** Los cuales que quedaron bloqueados ya que están relacionados con alguna anomalía que no ha sido solucionada por el equipo del IEPC.
- ***8** casos de prueba pendientes***.** Por cambios de los requerimientos, los cuales no están bien definidos.

Los resultados obtenidos en la ejecución del ciclo de pruebas Progresivas evidenciaron anomalías de funcionalidad, validación e interfaz gráfica.

- Al concluir la ejecución del ciclo de pruebas progresivas, se obtuvo un total de **50** anomalías detectadas, las cuales fueron documentadas en Mantis.
- Algunos detalles que conviene destacar, de las **50** anomalías, **4** son de **severidad "Muy alta"** y **11** con severidad **"Alta".**
- Otro dato importante a considerar es que, de las **50** anomalías, **32** son de Funcionalidad, **11** anomalías de **Imagen, 5** anomalías de **Validación, 1** anomalía de **Seguridad** y **1** anomalía de **Integridad.**

Ejecución de pruebas Regresivas:

- ***230** casos de prueba aprobados***.** Los cuales a través de su ejecución permitieron comprobar que el sistema se comporta como se esperaba.
- ***51** casos de prueba desaprobados***.** Los cuales, al ejecutarse, identificaron anomalías en el funcionamiento del sistema; Durante la verificación de las **51** casos de prueba desaprobados, **39** se aprobaron con la corrección de anomalías, **7** se cancelaron por cambio de requerimientos y **4** no atendida

porque se acepta, ya que es una anomalía de severidad baja, que no impacta en el funcionamiento.

Los resultados obtenidos en la ejecución del ciclo de pruebas Progresivas evidenciaron anomalías de funcionalidad, validación e interfaz gráfica.

- Al concluir la ejecución del ciclo de pruebas regresivas y verificación, se obtuvo un total de **61** anomalías detectadas, las cuales fueron documentadas en Mantis.
- Algunos detalles que conviene destacar, de las **61** anomalías, **4** son de **severidad "Muy alta"** y **15** con severidad **"Alta".**

ANEXO

Se agrega el documento confidencial con el reporte de las 61 anomalías detectadas durante el proceso de pruebas funcionales.

- Anexo 1. Anomalías_Pruebas_Funcionales

CONCEPTOS UTILIZADOS

- **ANOMALÍA:** Es el defecto encontrado que no permite llegar a los criterios aceptados.

- **ESCENARIO DE PRUEBA:** Descripción general de los requerimientos como flujos de funcionalidad a un alto nivel.

- **CASO DE PRUEBA:** Una secuencia de instrucciones para verificar el buen o mal funcionamiento del sistema, en base al cumplimiento o no de una especificación del mismo.

- **MÓDULO:** Grano de sistema, opción, menú.

VALIDACIÓN DEL SISTEMA INFORMATICO DEL PREP Y DE SUS BASES DE DATOS

IJALTI
CLUSTER MANAGER

Información General	
Datos de la organización(cliente)	
Nombre	IEPC
Domicilio	Calle Florencia 2370, Italia Providencia, 44648 Guadalajara, Jal.
Gerente de Servicios de TI (o contacto principal)	Ramiro Garzón
Proyecto	
Nombre del producto evaluado	PREP
Nombre del documento	Reporte Aplicación de Comparacion de Versiones_TestSourcing
Ubicación	\iepc\Proyecto PREP\DOS
Fecha de creación	29/Junio /2018
Fecha de revision	29/Junio/2018
Fecha último cambio	29/Junio/2018
Estatus de revision	Aprobado
Autor	Meinardo González Muñoz
Gerente de cuenta Test Sourcing	Aarón Moreno
Dirección de Operaciones Test Sourcing	Aarón Moreno

Historial de cambios

Versión	Fecha	Autor	Función	Descripción del cambio(s)
1.0	29/06/2018	Meinardo González	Senior Technical Test Analyst	Versión inicial del documento.

Lista de Distribución

Se distribuirá una copia del presente documento a las siguientes personas involucradas en el proyecto.

Nombre	Función
Ramiro Garzón	Gerente de Servicios de TI
Aarón Moreno	Dirección de Operaciones Test Sourcing

Aprobaciones Requeridas

Es indispensable la aprobación de las siguientes personas acerca de este Reporte Final de Resultados de Pruebas de Performance. Cualquier modificación al documento después de su aprobación, deberá ser nuevamente autorizada por:

Nombre	Función
Ramiro Garzón	Gerente de Servicios de TI
Aarón Moreno	Dirección de Operaciones – Test Sourcing

Revisores

El presente documento ha sido enviado para su información y revisión a las siguientes personas:

Nombre	Función
Aarón Moreno	Dirección de Operaciones – Test Sourcing

Manejo de Copias Obsoletas

Es responsabilidad del usuario de este documento asegurarse de que se está usando la última versión, es decir, la versión más reciente que está en el repositorio de documentos. Si el usuario requiere imprimir este documento, de la misma manera, deberá asegurarse de usar siempre la versión más reciente.

ÍNDICE

INTRODUCCIÓN

El sistema PREP (Programa de Resultados Electorales Preliminares) es el mecanismo de información electoral que recaba los resultados preliminares y no definitivos, de carácter estrictamente informativo a través de la captura de los datos asentados en las actas de escrutinio y cómputo de las casillas que se reciben en los CATD (Centros de Acopio y Transmisión de Datos) autorizados.

La finalidad del presente documento es describir el diseño y funcionalidad del software que realizará la comparación de versiones tanto de código como de estructura de base de datos entre la versión liberada y la versión implementada en producción.

TECNOLOGIAS

Lenguaje: Java Development Kit 8
Librerías: MSSQL JDBC 4.2

OBJETIVOS DEL SOFTWARE

El *Software* tiene cómo objetivo validar que tanto la versión de código como la estructura de base de datos instaladas en el entorno de producción sean iguales a la última versión liberada.

DISEÑO

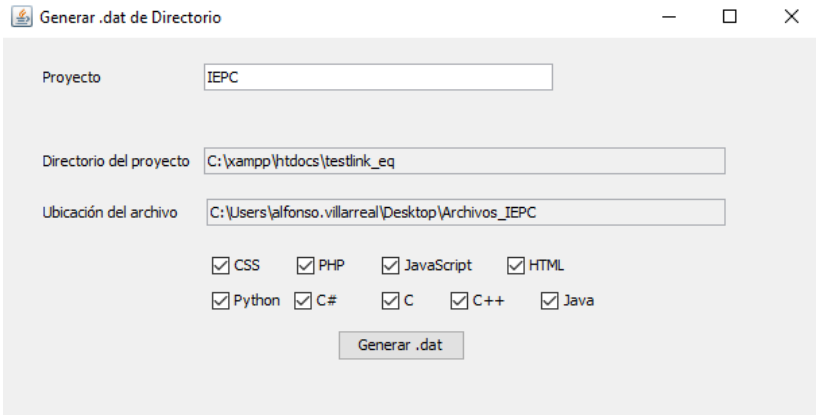
El Software está dividido en las siguientes tres aplicaciones.

Aplicaciones

Nombre	Descripción
FileHashGen	Genera un archivo binario a partir de un directorio especificado donde por cada archivo encontrado almacena su nombre y una firma generada a partir de su contenido.
BDHashGen	Genera archivos binarios por tabla, vistas e índices primarios a partir de una conexión de base de datos para Microsoft SQL Server.
Comparador	Genera reportes en PDF con los resultados obtenidos de comparar los archivos generados por las aplicaciones anteriores

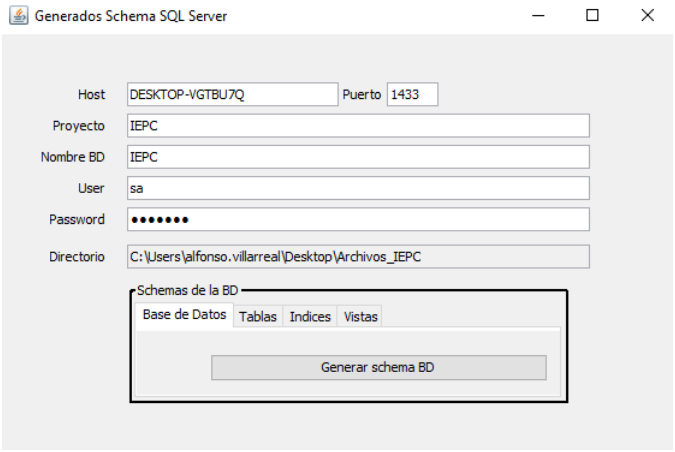
FileHashGen

Esta aplicación recorre cada subdirectorio de un directorio determinado, generando un hash por cada archivo encontrado, esta información se guarda en un archivo con formato binario.



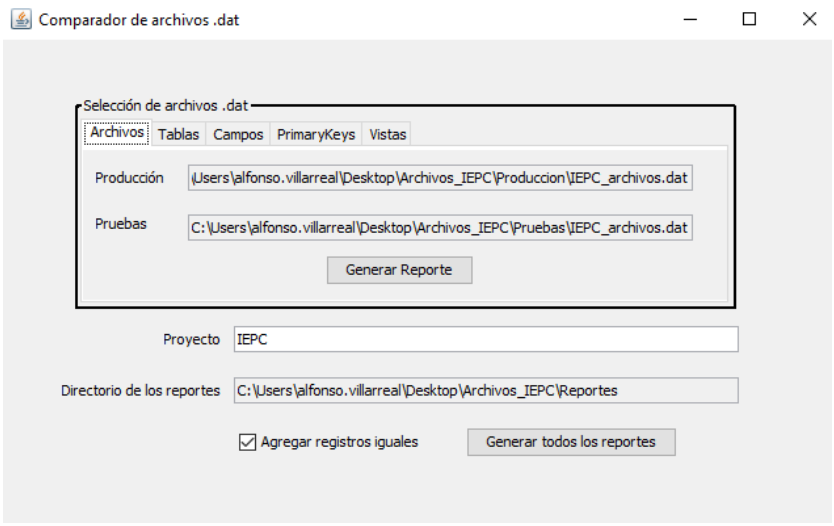
BDHashGen

Esta aplicación se conecta a una base de datos y analiza la estructura, permite generar archivos con información sobre la estructura de tablas, vistas e índices primarios.



Comparador

Esta aplicación lee los archivos generados por las aplicaciones **FileHashGen** y BDHashGen y hace comparaciones entre ellos generando un reporte como resultado.



Pruebas de Performance

Información General	
Datos de la organización(cliente)	
Nombre	IEPC
Domicilio	
Gerente de Servicios de TI (o contacto principal)	Ramiro Garzón
Proyecto	
Nombre del producto evaluado	PREP
Versión del product	PREP
Nombre del document	Reporte_Final_de_Resultados_Pruebas Performance_TestSourcing_PREP
Ubicación	\iepc\Proyecto PREP\Performance
Fecha de creación	25/Junio/2018
Fecha de revision	27/Junio/2018
Fecha último cambio	28/Junio/2018
Estatus de revision	Aprobado
Autor	Equipo Performance
Gerente de cuenta e-Quallity	Aarón Moreno
Dirección de Operaciones e-Quallity	Aarón Moreno

Historial de cambios

Versión	Fecha	Autor	Función	Descripción del cambio(s)
1.0	25/06/2018	Adrian López Alberto Gutiérrez	Pruebas Performance	Versión inicial del documento.
1.1	28/06/2018	Adrian López	Pruebas Performance	Se actualizaron las conclusiones.

Lista de Distribución

Se distribuirá una copia del presente documento a las siguientes personas involucradas en el proyecto.

Nombre	Función
Ramiro Garzón	Gerente de Servicios de TI
Aarón Moreno	Director de Operaciones TestSoucing

Aprobaciones Requeridas

Es indispensable la aprobación de las siguientes personas acerca de este Reporte Final de Resultados de Pruebas de Performance. Cualquier modificación al documento después de su aprobación, deberá ser nuevamente autorizada por:

Nombre	Función
Ramiro Garzón	Gerente de Servicios de TI
Aarón Moreno	Director de Operaciones – TestSourcing

Revisores

El presente documento ha sido enviado para su información y revisión a las siguientes personas:

Nombre	Función
Aarón Moreno	Dirección de Operaciones TestSourcing

Manejo de Copias Obsoletas

Es responsabilidad del usuario de este documento asegurarse que está usando la última versión, es decir, la versión que está en línea en el repositorio de documentos. Si el usuario requiere imprimir este documento, de la misma manera, deberá asegurarse de usar siempre la versión más reciente.

ÍNDICE

• INTRODUCCIÓN

El sistema PREP (Programa de Resultados Electorales Preliminares) es el mecanismo de información electoral que recaba los resultados preliminares y no definitivos, de carácter estrictamente informativo a través de la captura de los datos asentados en las actas de escrutinio y cómputo de las casillas que se reciben en los CATD (Centros de Acopio y Transmisión de Datos) autorizados.

La finalidad del presente documento es exponer un resumen detallado de las actividades realizadas durante las pruebas de carga, efectuadas sobre la aplicación “PREP”, las cuales van desde el diseño de scripts de pruebas, hasta los resultados obtenidos de la ejecución de los mismos. Los resultados serán mostrados visualmente mediante gráficas e interpretados para que puedan ser de utilidad para los interesados.

Las pruebas de performance permiten verificar el desempeño de las aplicaciones, identifican los riesgos y problemas relacionados con el desempeño ineficiente de las aplicaciones en los entornos productivos, y una vez que los problemas son identificados, se pueden realizar las correcciones necesarias antes de llevar el producto a producción.

• AMBIENTE

Aplicación: http://api.iepcjalisco.org.mx/stress-test

Base de Datos: SQLServer 12.0.41

Servidor:
Lenovo
Modelo: ThinkSystem SR550
Procesador (VM): 4 Procesadores
Memoria RAM(VM): 8 GB
Sistema Operativo (VM)**:** Linux CentOS 7

Enlace: 300 Mbps

Pruebas

Equipo1:	Lenovo
Modelo:	Lenovo ThinkPad T440p
Procesador:	Procesador: Core i7
Memoria:	12 GB

Equipo2:	HP
Modelo:	ZBook 15 G2
Procesador:	Procesador: Core i7
Memoria:	12 GB

• OBJETIVOS DE LAS PRUEBAS

Los objetivos de las pruebas de performance para el “PREP” son:

- Dar a conocer las métricas de rendimiento y consumo de recursos de la aplicación “PREP”, antes de su paso a producción.
- Identificar tiempos prolongados de respuesta, solicitudes y respuestas fallidas, exceso de envío o recepción de información por transacción.
- Identificar posibles fallas al incrementar el número de peticiones realizadas al aplicativo que se pretende cargar.
- Obtener gráficas que ilustren claramente las tendencias de cada una de las métricas, conforme avanza el tiempo de la ejecución de las pruebas de performance.
- Identificar problemas de la aplicación ejecutando las pruebas de manera coordinada con el equipo de desarrollo de IEPC.

• FUNCIONALIDAD PROBADA

Envío de petición

Nombre	Ruta	Justificación
Envío de petición	http://api.iepcjalisco.org.mx/stress-test	Obligatorio

• ANTECEDENTES DE PRUEBAS.

Fecha de ejecución
2018-06-24

De acuerdo al objetivo de la aplicación, se espera que en el entorno de producción reciba una gran cantidad de peticiones en poco tiempo. El rendimiento de la aplicación dependerá de dos factores: la infraestructura sobre la que será ejecutada la aplicación y el comportamiento de la aplicación durante su ejecución.

Para anticipar el comportamiento de la aplicación y confirmar que el rendimiento no se degrada durante la ejecución se debe realizar una prueba controlada que realice peticiones de forma constante durante un tiempo determinado y permita analizar la

cantidad de información enviada y recibida, así como los tiempos de respuesta de cada petición.

- ## EJECUCIÓN DE LAS PRUEBAS

Scripts de prueba

Se diseñó **un script** para realizar las pruebas de carga, el cual cubre con la carga total de la información proporcionada por la respuesta.

Script de prueba
IEPC-STRESS-TEST

Interpretación del flujo: Se realiza una petición a la url https://api.iepcjalisco.org.mx/stress-test y se obtiene la respuesta.

.1 ESCENARIOS DE PRUEBA EJECUTADOS

La ejecución del script de pruebas de performance se llevó a cabo mediante dos equipos de cómputo (generadores de carga). El script se ejecutó bajo las siguientes condiciones:

- 15,000 usuarios distribuidos en 3 minutos
- 10,000 usuarios distribuidos en 3 minutos
- 5,000 usuarios distribuidos en 3 minutos
- 8,400 usuarios distribuidos en 5 minutos

Escenario 1: Se definieron 15,000 usuarios, de los cuales se iniciaron 83 usuarios por segundo durante 3 minutos.

Resultado Ejecución:
Duración: 3 minutos y 11 segundos.
20:57:03 – 21:00:14

Resumen de estadísticas:

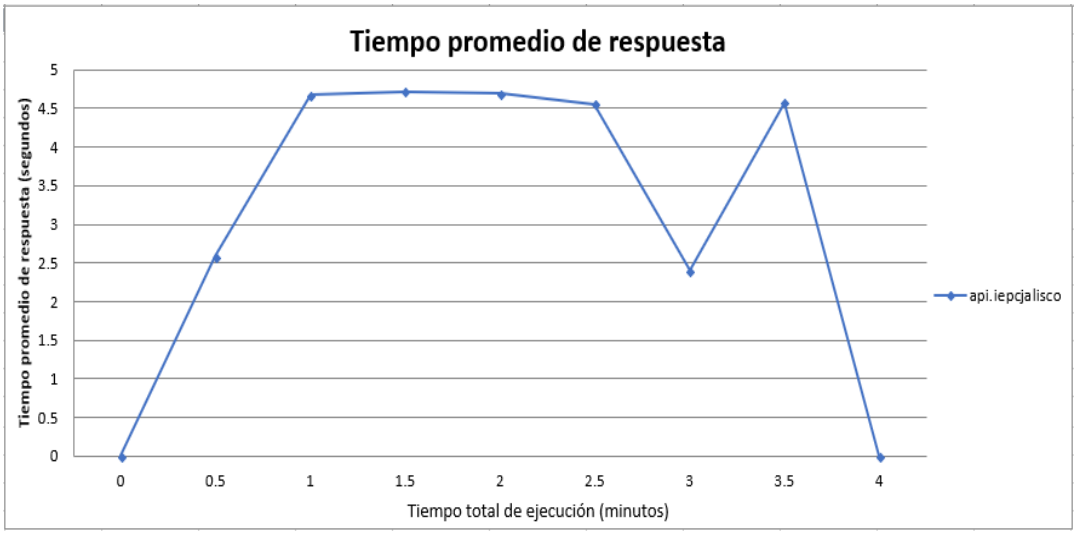
Total rendimiento (bytes):	2,331,008,997
Promedio rendimiento (bytes/seg):	12,204,236
Total peticiones (Hits):	15,000
Promedio peticiones por segundo:	83
Total Errores:	8533

Tras ejecutar el script de prueba con una cantidad de 15,000 usuarios durante 3 minutos (promedio de 83 peticiones por segundo), se observaron errores en un total de 8533 peticiones (56.8%) lo cual comprende más de la mitad de las peticiones totales realizadas (15,000).

En cuanto al tiempo de respuesta, se observó un comportamiento similar durante los minutos del 1 al 2.5 de la ejecución, registrando un promedio de 4.24 segundos en la respuesta, además de encontrarse en el minuto 3 el tiempo de respuesta más bajo registrando 2.40 segundos, no obstante, este resultado se debe a que en ese minuto se encontraron 1878 errores en las peticiones solicitadas (22% de los errores totales encontrados durante esta ejecución), por lo cual la respuesta fue un código de error 502 (ver gráfica Código de respuesta ejecución con 15,000 usuarios).

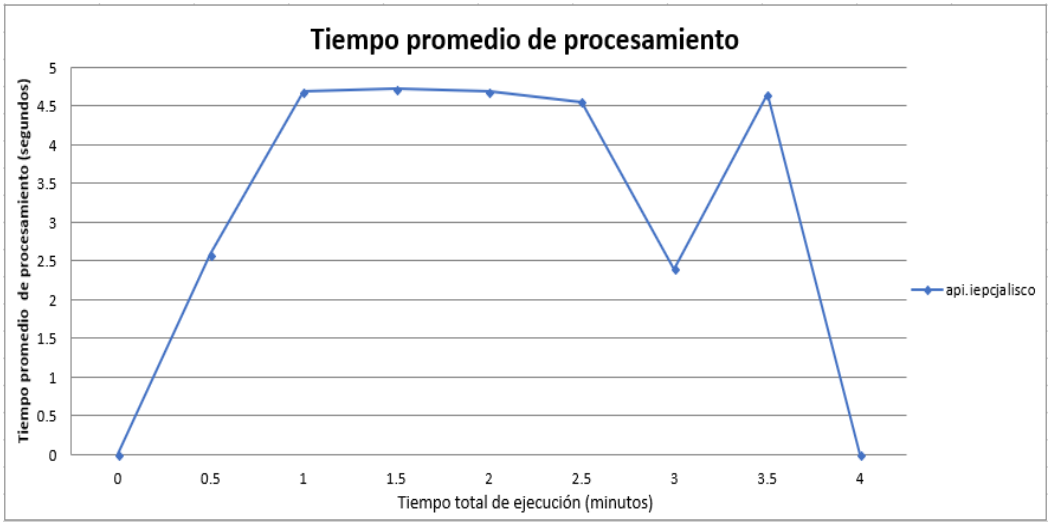
En la gráfica se muestra el tiempo promedio de respuesta de los elementos dentro del período de tiempo de ejecución de la prueba.

Tiempo promedio de respuesta	
Tiempo	api.iepcjalisco
0	0
0.5	2.581744422
1	4.675040519
1.5	4.721929469
2	4.689919355
2.5	4.556546413
3	2.402513174
3.5	4.578571429
4	0



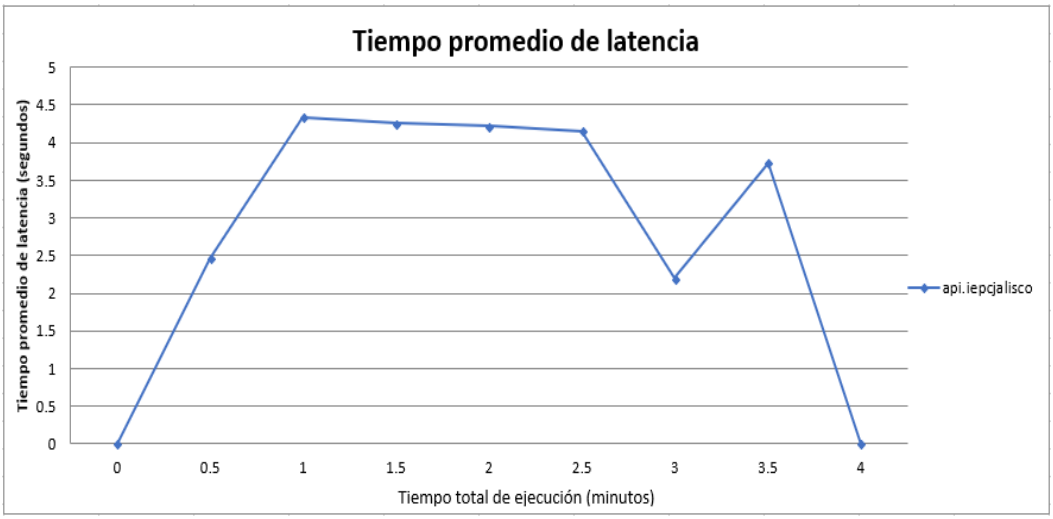
En la gráfica se muestra el tiempo promedio de procesamiento dentro del período de tiempo de ejecución de la prueba.

Tiempo promedio de procesamiento	
Tiempo	api.iepcjalisco
0	0
0.5	2.583828398
1	4.684598055
1.5	4.718568707
2	4.687822177
2.5	4.55811593
3	2.398523713
3.5	4.651935714
4	0



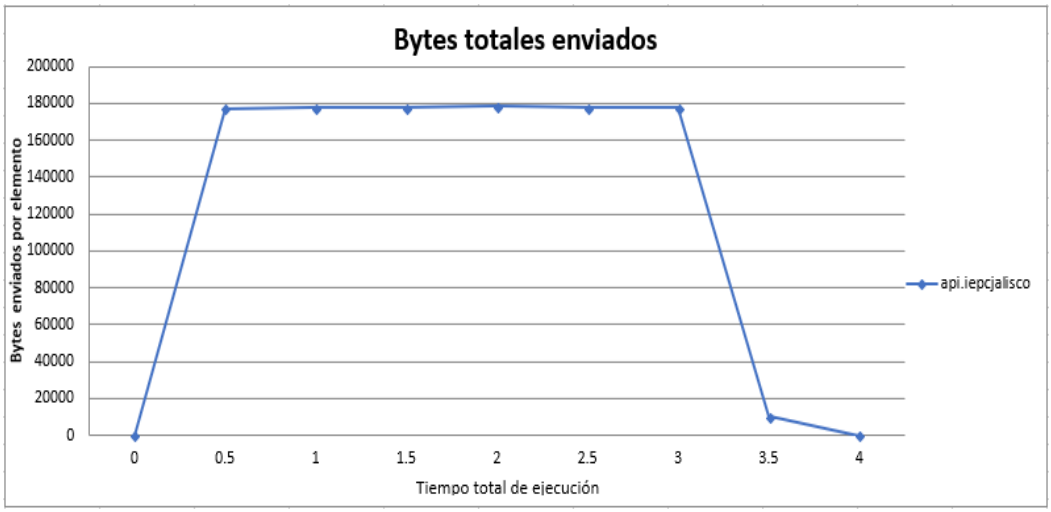
En la gráfica se muestra el tiempo promedio de latencia dentro del período de tiempo de ejecución de la prueba.

Tiempo promedio de latencia	
Tiempo	api.iepcjalisco
0	0
0.5	2.468905071
1	4.34278201
1.5	4.258877179
2	4.216833468
2.5	4.150685853
3	2.197596676
3.5	3.7315
4	0



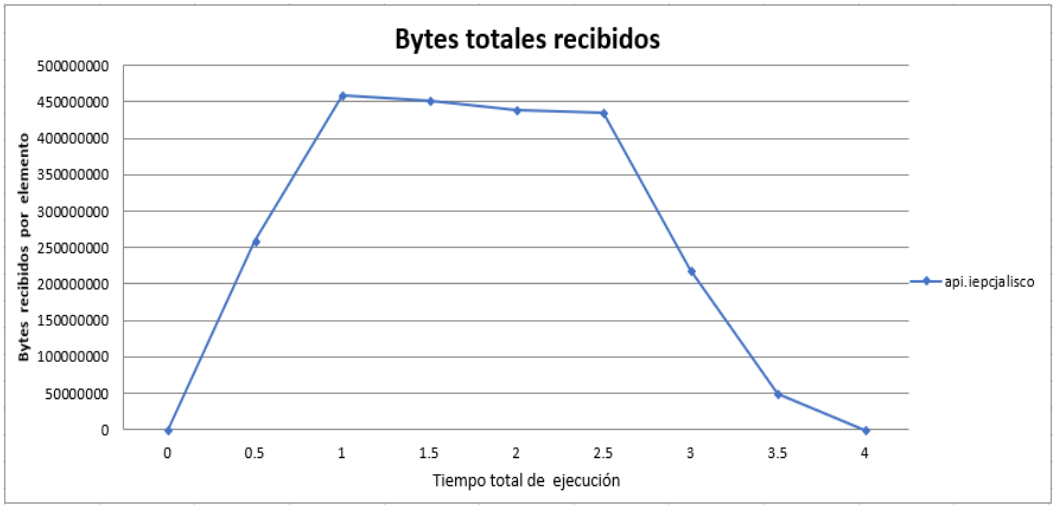
La gráfica muestra el volumen de información en bytes enviados por las peticiones durante la ejecución.

Bytes totales enviados	
Tiempo	api.iepcjalisco
0	0
0.5	177480
1	177696
1.5	177624
2	178560
2.5	177624
3	177624
3.5	10080
4	0



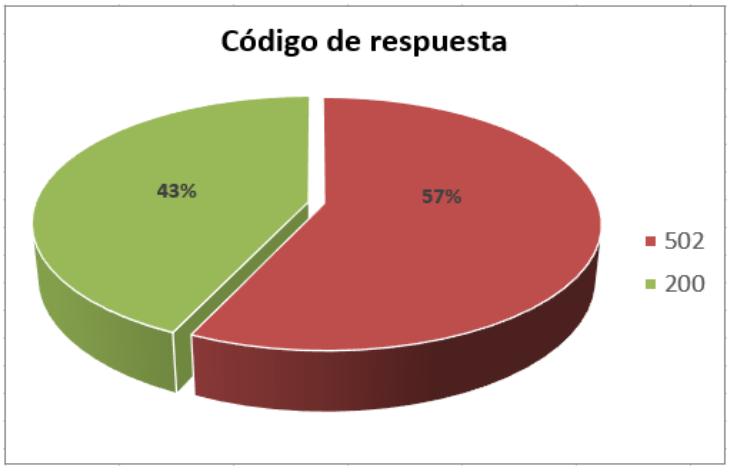
La gráfica muestra el volumen de información en bytes recibidos durante la ejecución.

Bytes totales recibidos	
Tiempo	api.iepcjalisco
0	0
0.5	259466333
1	459443147
1.5	452041269
2	439432545
2.5	435159954
3	219380352
3.5	49740370
4	0



La gráfica muestra los códigos de respuesta obtenidos durante la ejecución.

Código de respuesta		
Código	Cantidad	Porcentaje
502	8533	57%
200	6467	43%
Total	15000	100%



Escenario 2: Se definieron 10,000 usuarios, de los cuales se iniciaron 55 usuarios por segundo durante 3 minutos.

Resultado Ejecución:

Duración: 3 minutos y 25 segundos.

21:02:33 – 21:05:58

Resumen de estadísticas:

Total rendimiento (bytes):	2,377,845,559
Promedio rendimiento (bytes/seg):	11,599,247
Total peticiones (Hits):	10,000
Promedio peticiones por segundo:	55
Total Errores:	3344

Tras ejecutar el script de la prueba con una cantidad de 10,000 usuarios durante 3 minutos (promedio de 55 peticiones por segundo), se observaron errores en un total de 3344 peticiones (33% del total de las peticiones totales realizadas).

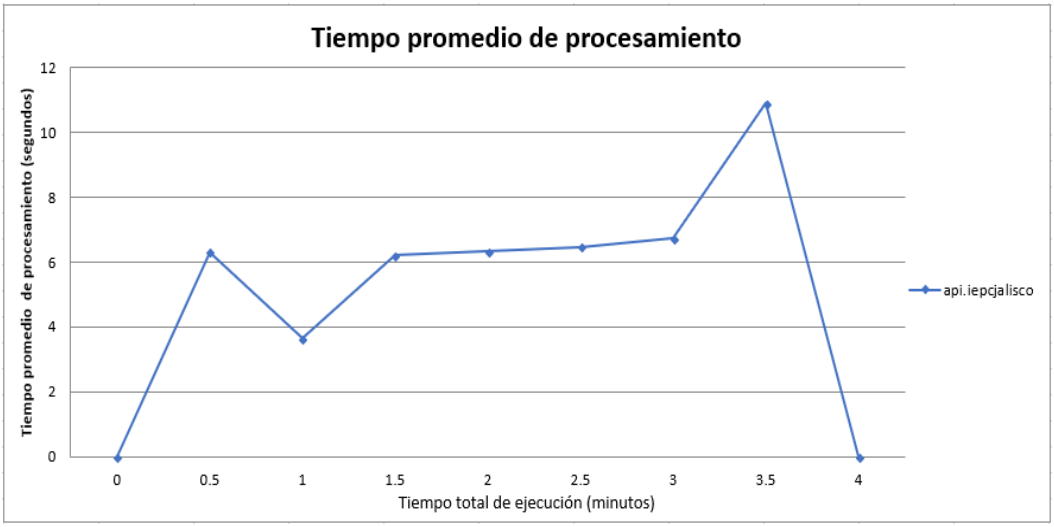
En cuanto al tiempo de respuesta, se observó un comportamiento similar durante los minutos del 1.5 al 3 de la ejecución, registrando un promedio de 6.42 segundos en la respuesta, además de encontrarse en el minuto 1 el tiempo de respuesta más bajo registrando 3.65 segundos, no obstante, este resultado se debe a que en ese minuto se encontraron 1062 errores en las peticiones solicitadas (31.7% de los errores totales encontrados durante esta ejecución), por lo cual la respuesta fue un código de error 502 (ver gráfica Código de respuesta ejecución con 10,000 usuarios).

En la gráfica se muestra el tiempo promedio de respuesta de los elementos dentro del período de tiempo de ejecución de la prueba.

Tiempo promedio de respuesta	
Tiempo	api.iepcjalisco
0	0
0.5	6.302794224
1	3.648123485
1.5	6.207611115
2	6.318341805
2.5	6.45991525
3	6.724572548
3.5	10.90328205
4	0

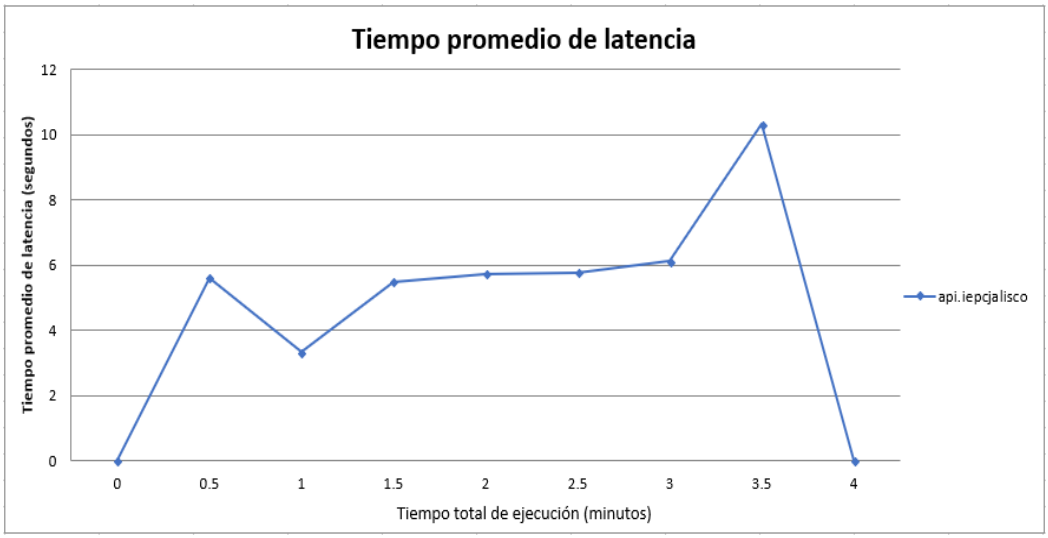
En la gráfica se muestra el tiempo promedio de procesamiento dentro del período de tiempo de ejecución de la prueba.

Tiempo promedio de procesamiento	
Tiempo	api.iepcjalisco
0	0
0.5	6.302794226
1	3.648123487
1.5	6.207611111
2	6.318341803
2.5	6.459915254
3	6.724572551
3.5	10.90328205
4	0



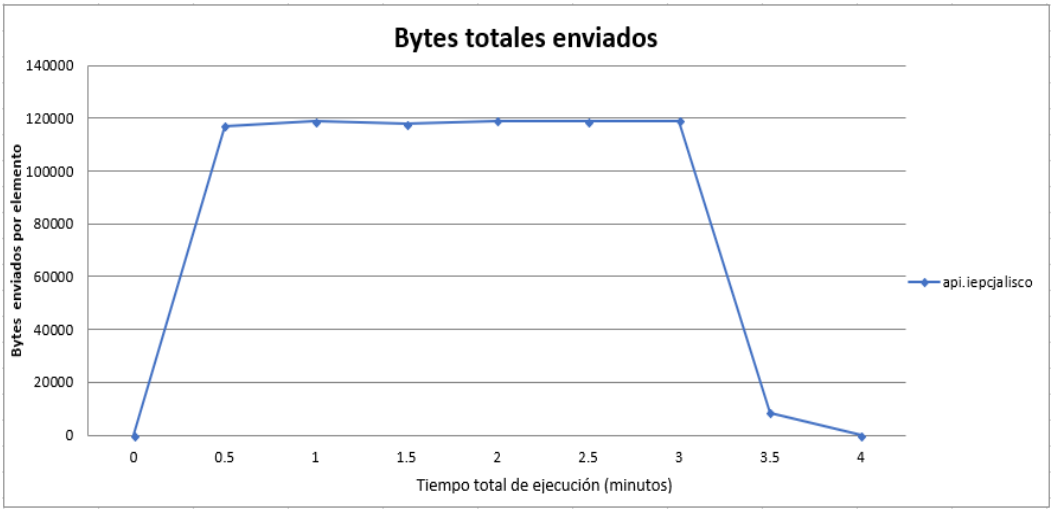
En la gráfica se muestra el tiempo promedio de latencia dentro del período de tiempo de ejecución de la prueba.

Tiempo promedio de latencia	
Tiempo	api.iepcjalisco
0	0
0.5	5.620351351
1	3.33198728
1.5	5.490360806
2	5.724626739
2.5	5.763845642
3	6.115909311
3.5	10.33005983
4	0



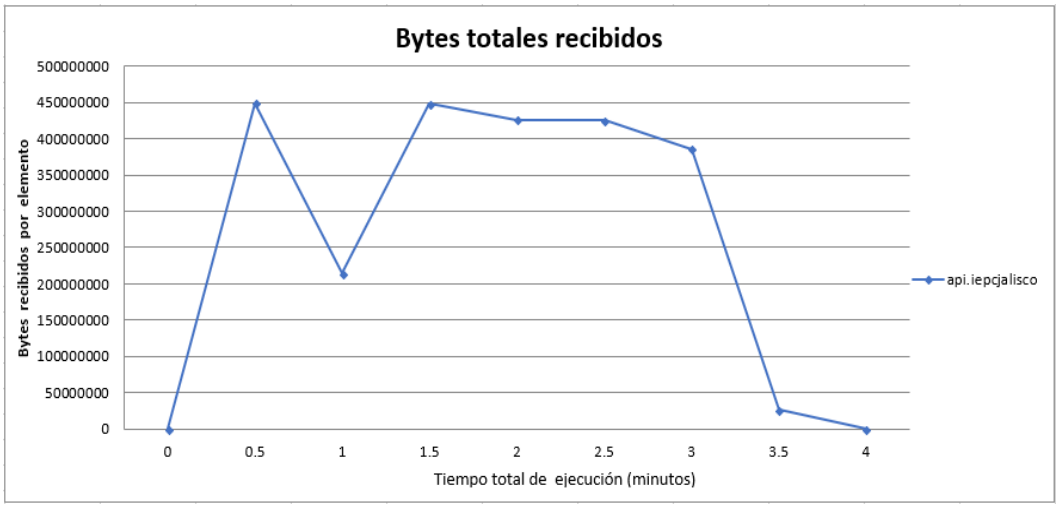
La gráfica muestra el volumen de información en bytes enviados durante la ejecución.

Bytes totales enviados	
Tiempo	api.iepcjalisco
0	0
0.5	117216
1	118944
1.5	117936
2	119016
2.5	118944
3	119088
3.5	8424
4	0



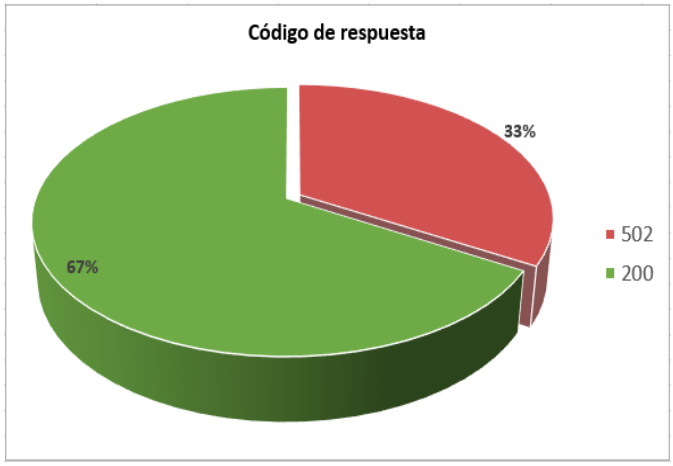
La gráfica muestra el volumen de información en bytes recibidos por las peticiones durante la ejecución.

Bytes totales recibidos	
Tiempo	api.iepcjalisco
0	0
0.5	448762769
1	214455104
1.5	448435137
2	426007381
2.5	425296110
3	385947038
3.5	26810244
4	0



La gráfica muestra los códigos de respuesta obtenidos durante la ejecución.

Código de respuesta		
Código	Cantidad	Porcentaje
502	3344	33%
200	6656	67%
Total	15000	100%



Escenario 3: Se definieron 5,000 usuarios, de los cuales se iniciaron 28 usuarios por segundo durante 3 minutos.

Resultado Ejecución:
Duración: 3 minutos y 9 segundos.
21:07:54 – 21:11:03
Resumen de estadísticas:

Total rendimiento (bytes):	1,723,730,496
Promedio rendimiento (bytes/seg):	9,120,267
Total peticiones (Hits):	5,000
Promedio peticiones por segundo:	28
Total Errores:	150

Después de la ejecución del script de la prueba con una cantidad de 5,000 usuarios durante 3 minutos (promedio de 28 peticiones por segundo), se observaron errores en un total de 150 peticiones (3% del total de las peticiones totales realizadas).

En cuanto al tiempo de respuesta, se observó un comportamiento similar durante los minutos del 0.5 al 1 y 2 al 2.5 de la ejecución, registrando un promedio de 1.24 segundos y 4.10 segundos respectivamente en la respuesta.

Se encontró en el minuto 0.5 y 1 los tiempos de respuesta más bajos, registrando en promedio 1.24 segundos.

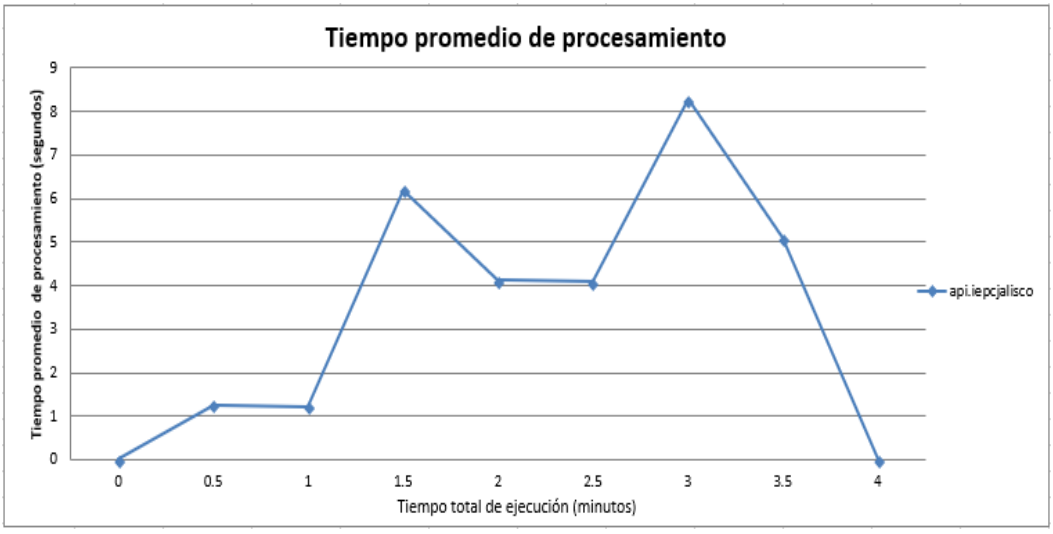
Con relación a los errores, en el minuto 1.5 se encontró la mayoría de estos, registrando 148 errores (98.6% del total de errores encontrados para esta prueba), esto generó un promedio de tiempo de respuesta de 6.20 segundos durante ese período.

En la gráfica se muestra el tiempo promedio de respuesta de los elementos dentro del período de tiempo de ejecución de la prueba.

Tiempo promedio de respuesta	
Tiempo	api.iepcjalisco
0	0
0.5	1.262828883
1	1.224399519
1.5	6.201833737
2	4.122321689
2.5	4.081925887
3	8.271119565
3.5	5.102666663
4	0

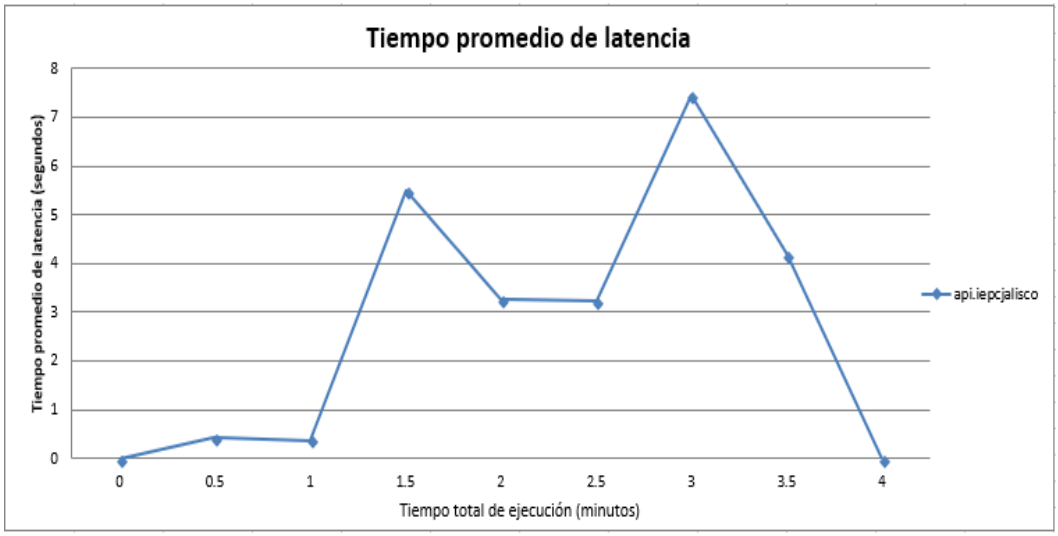
En la gráfica se muestra el tiempo promedio de procesamiento dentro del período de tiempo de ejecución de la prueba.

Tiempo promedio de procesamiento	
Tiempo	api.iepcjalisco
0	0
0.5	1.262828883
1	1.224399516
1.5	6.201833735
2	4.122321687
2.5	4.081925881
3	8.271119565
3.5	5.102666667
4	0



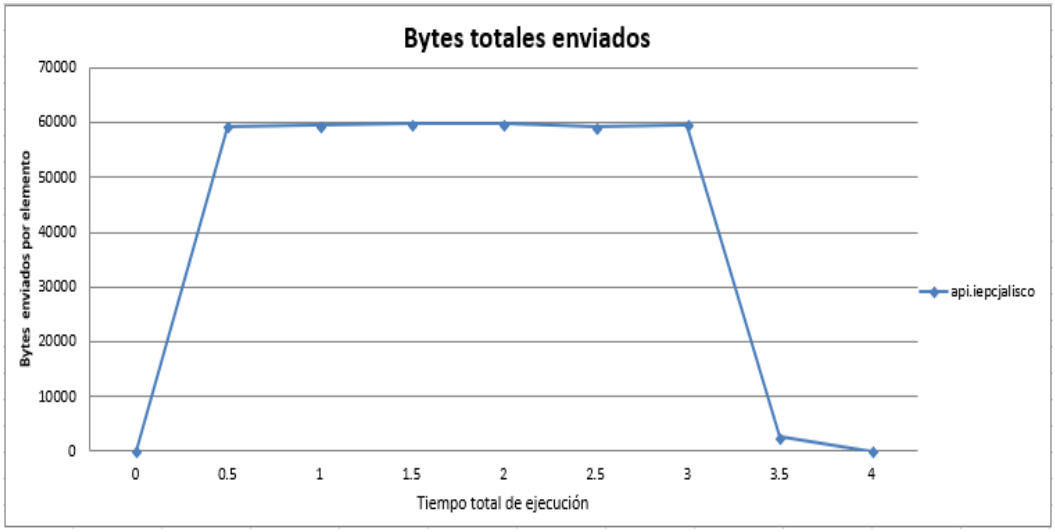
En la gráfica se muestra el tiempo promedio de latencia dentro del período de tiempo de ejecución de la prueba.

Tiempo promedio de latencia	
Tiempo	api.iepcjalisco
0	0
0.5	0.420253641
1	0.382696126
1.5	5.480709639
2	3.27533012
2.5	3.230675577
3	7.458660628
3.5	4.163694444
4	0



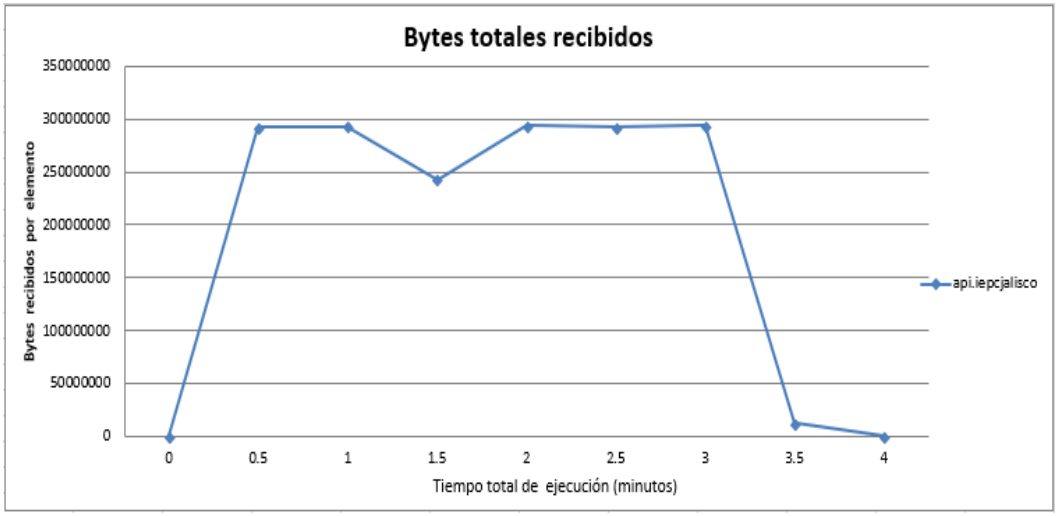
La gráfica muestra el volumen de información en bytes enviados durante la ejecución.

Bytes totales enviados	
Tiempo	api.iepcjalisco
0	0
0.5	59328
1	59472
1.5	59760
2	59760
2.5	59256
3	59616
3.5	2592
4	0



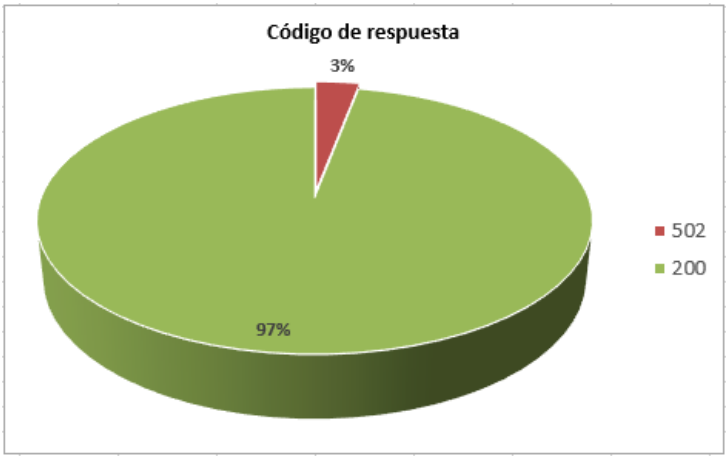
La gráfica muestra el volumen de información en bytes recibidos por las peticiones durante la ejecución.

Bytes totales recibidos	
Tiempo	api.iepcjalisco
0	0
0.5	292754202
1	293464678
1.5	242885844
2	294187263
2.5	292400344
3	294181836
3.5	12790494
4	0



La gráfica muestra los códigos de respuesta obtenidos durante la ejecución.

Código de respuesta		
Código	Cantidad	Porcentaje
502	150	3%
200	4850	97%
Total	5000	100%



Escenario 4: Se definieron 8,400 usuarios, de los cuales se iniciaron 28 usuarios por segundo durante 5 minutos. (Esta prueba se ejecutó en conjunto con la de denegación de servicios)

Resultado Ejecución:
Duración: 5 minutos y 10 segundos.
21:24:05 – 21:29:15
Resumen de estadísticas:

Total rendimiento (bytes):	2,536,079,881
Promedio rendimiento (bytes/seg):	8,180,903
Total peticiones (Hits):	8,400
Promedio peticiones por segundo:	28
Total Errores:	1276

Tras ejecutar el script de la prueba con una cantidad de 8,400 usuarios durante 5 minutos (promedio de 28 peticiones por segundo), se observaron errores en un total de 1276 peticiones (15% del total de peticiones totales realizadas).

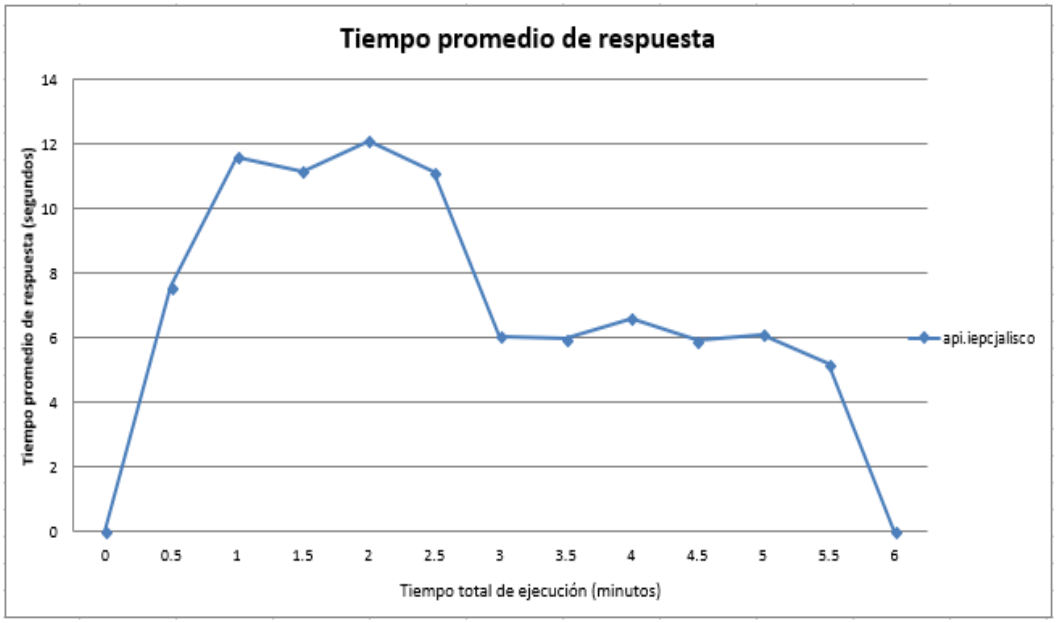
En cuanto al tiempo de respuesta, se observó un comportamiento similar durante los minutos del 3 al 5.5 de la ejecución, registrando un promedio de 5.98 segundos en la respuesta.

Con relación a los errores, en el minuto 3 se encontraron la mayoría de estos registrando 395 errores (30.9% del total de los errores encontrados durante esta prueba), esto genero un promedio de tiempo de respuesta de 5.97 segundos durante este período.

Se encontró en los minutos del 3.5 al 4.5 los tiempos de respuesta más bajos, registrando en promedio 4.95 segundos (los minutos finales de la prueba).

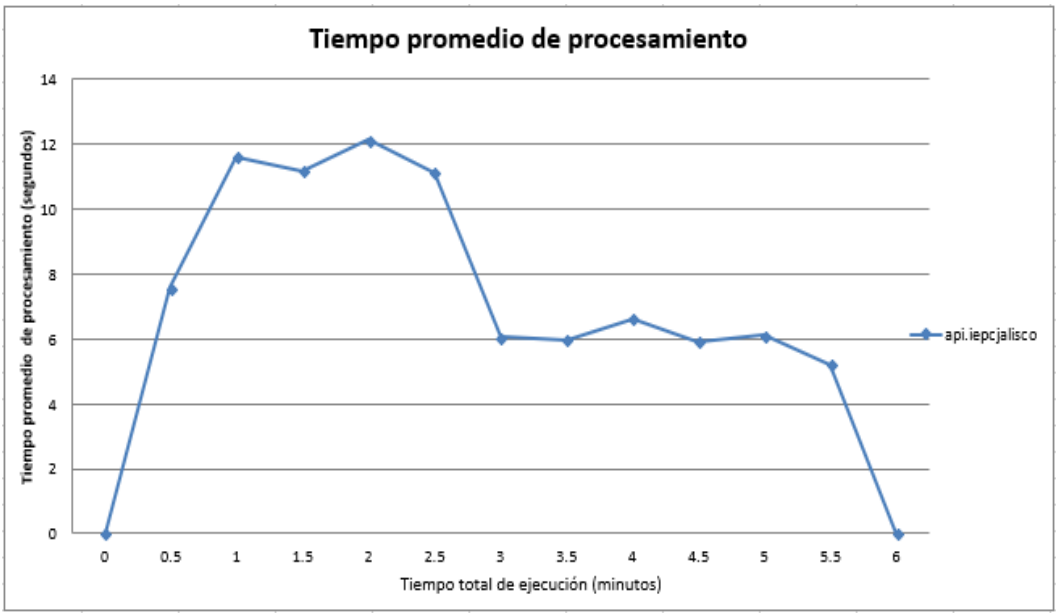
En la gráfica se muestra el tiempo promedio de respuesta de los elementos dentro del período de tiempo de ejecución de la prueba.

Tiempo promedio de respuesta	
Tiempo	api.iepcjalisco
0	0
0.5	7.58535018
1	11.6125675
1.5	11.17631146
2	12.12836635
2.5	11.13726348
3	6.058305389
3.5	5.972742239
4	6.627547194
4.5	5.921225807
5	6.117132461
5.5	5.209028557
6	0



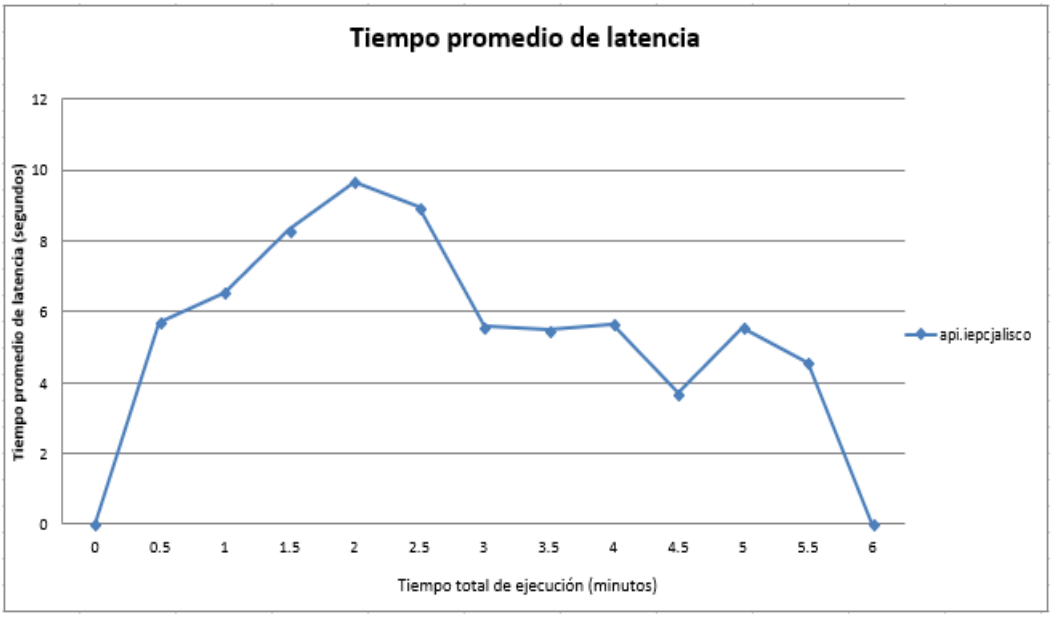
En la gráfica se muestra el tiempo promedio de procesamiento dentro del período de tiempo de ejecución de la prueba.

Tiempo promedio de procesamiento	
Tiempo	api.iepcjalisco
0	0
0.5	7.585350181
1	11.6125675
1.5	11.17631146
2	12.12836635
2.5	11.13726347
3	6.058305389
3.5	5.972742243
4	6.627547192
4.5	5.921225806
5	6.117132458
5.5	5.209028571
6	0



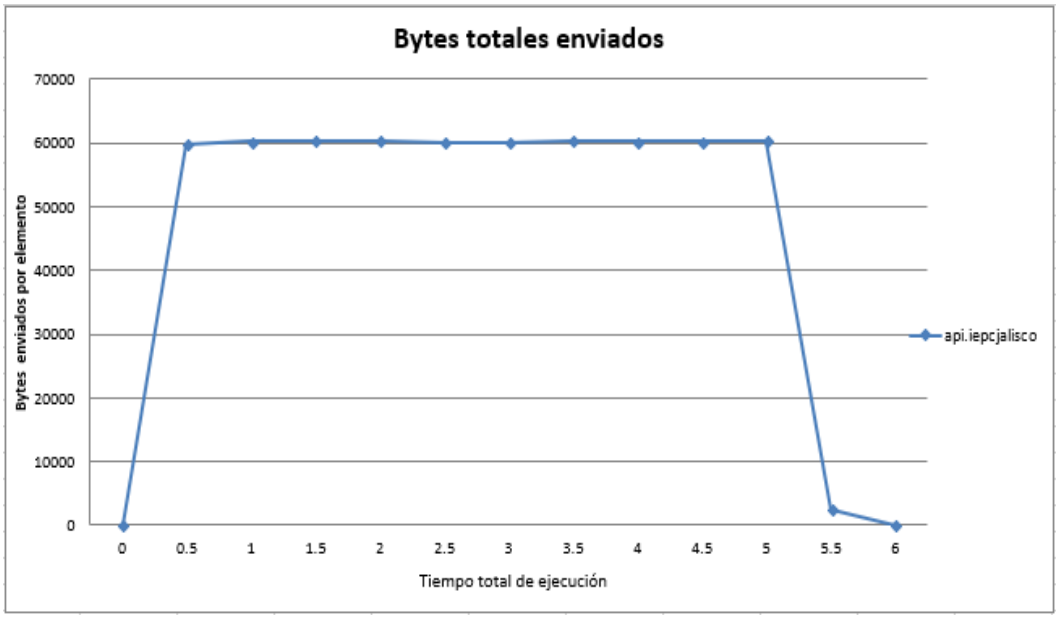
En la gráfica se muestra el tiempo promedio de latencia dentro del período de tiempo de ejecución de la prueba.

Tiempo promedio de latencia	
Tiempo	api.iepcjalisco
0	0
0.5	5.716188929
1	6.556316607
1.5	8.317436754
2	9.664994033
2.5	8.949368862
3	5.577014371
3.5	5.483843675
4	5.666747909
4.5	3.711072879
5	5.561958234
5.5	4.564
6	0



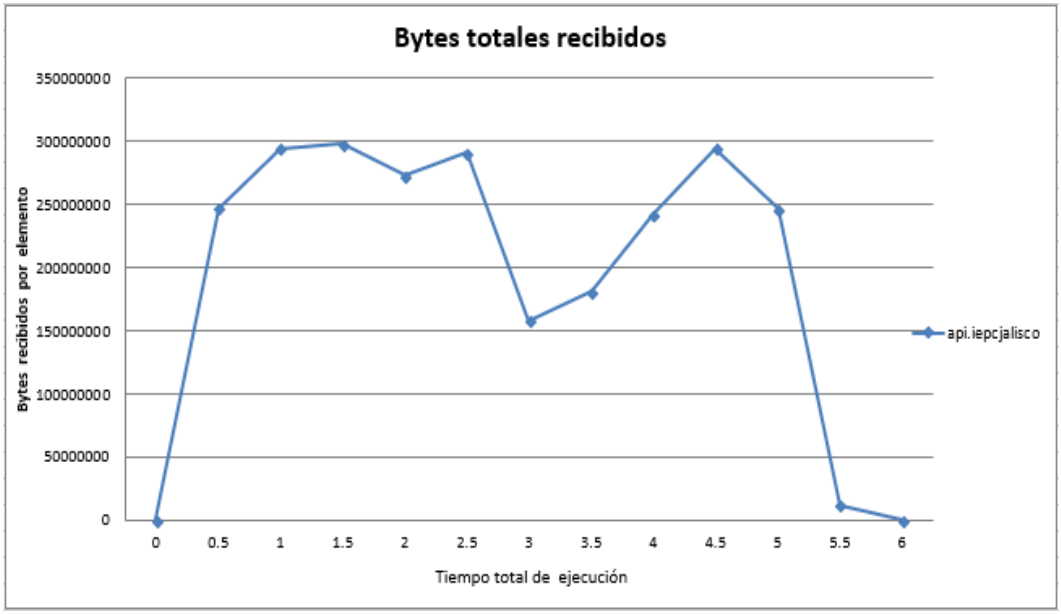
La gráfica muestra el volumen de información en bytes enviados durante la ejecución.

Bytes totales enviados	
Tiempo	api.iepcjalisco
0	0
0.5	59832
1	60264
1.5	60336
2	60336
2.5	60120
3	60120
3.5	60336
4	60264
4.5	60264
5	60336
5.5	2520
6	0



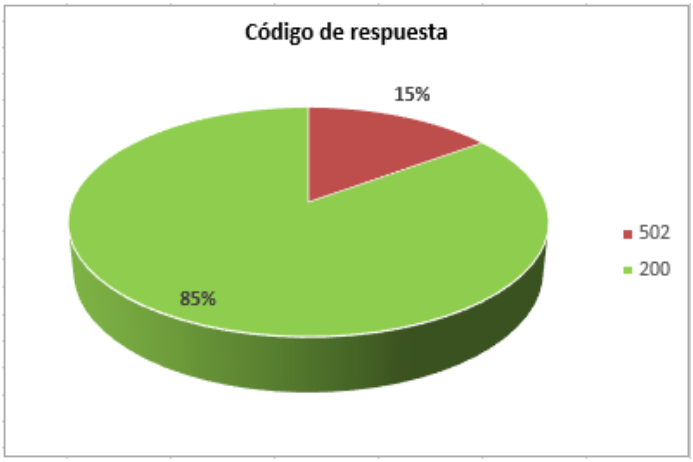
La gráfica muestra el volumen de información en bytes recibidos por las peticiones durante la ejecución.

Bytes totales recibidos	
Tiempo	api.iepcjalisco
0	0
0.5	246753142
1	294562419
1.5	297728448
2	272780158
2.5	290692842
3	157867620
3.5	181074791
4	241868936
4.5	294562932
5	246452457
5.5	11380851
6	0



La gráfica muestra los códigos de respuesta obtenidos durante la ejecución.

Código de respuesta		
Código	Cantidad	Porcentaje
502	1276	15%
200	7124	85%
Total	8400	100%



- **CONCLUSIONES**

Durante la ejecución de la prueba con una carga de 28 peticiones por segundo (5,000 usuarios durante 3 minutos), se observó un comportamiento aceptable en la aplicación, respondiendo un total de 1,723,730,496 bytes en 3 minutos con 9 segundos manteniendo una velocidad de respuesta promedio de 4.3 segundos. En esta ejecución se lanzaron 5,000 peticiones al servidor, resultando 150 (3%) peticiones fallidas con código de respuesta 502.

Al incrementar la carga a 55 peticiones por segundo (10,000 usuarios durante 3 minutos), se observó un aumento en el tiempo de respuesta, siendo el promedio de este de 6.6 segundos, además de presentar un 33% de peticiones fallidas, lo cual representa un incremento con relación a lo mencionado en el punto anterior.

La prueba en la que se realizaron 28 peticiones por segundo (8,400 usuarios durante 5 minutos) se ejecutó en conjunto con la prueba de denegación de servicios. En los resultados se observa un tiempo de respuesta de 8.1 segundos y se obtuvo un total del 15% de peticiones fallidas.

En la ejecución de la prueba con una carga de 83 peticiones por segundo (15,000 usuarios durante 3 minutos), se recibieron 2,331,008,997 bytes en 3 minutos con 11

segundos manteniendo una velocidad promedio de respuesta de 4.0 segundos. De un total de 15,000 peticiones enviadas se obtuvo como resultado un 57% de peticiones fallidas. Aún cuando la carga de esta ejecución es más alta que las anteriores, se obtuvo un tiempo promedio de respuesta más bajo, esto se debe a que las peticiones falladas eran respondidas en menor tiempo que las peticiones exitosas.

- **GLOSARIO DE TÉRMINOS**

Latencia: Tiempo de espera hasta el primer byte de la respuesta recibida.

Bytes recibidos: Cantidad de bytes recibidos en la respuesta.

Bytes enviados: Cantidad de bytes enviados en la solicitud.

Tiempo de procesamiento: Tiempo en que es cargada la respuesta.

Tiempo de respuesta: Tiempo total de la transacción.

Código 200: Ok, Respuesta estándar para peticiones correctas.

Código 502: Bad Gateway, El servidor está actuando de proxy o Gateway y ha recibido una repuesta inválida de otro servidor, por lo que no puede responder adecuadamente a la petición del navegador.

ANÁLISIS DE VULNERABILIDAD A LA INFRAESTRUCTURA TECNOLÓGICA

IJALTI
CLUSTER MANAGER

PLAN DE TRABAJO
Auditoría a la Infraestructura Tecnológica
del PREP 2018 del Estado de Jalisco

INTRODUCCION

Análisis de vulnerabilidades en la infraestructura tecnológica del PREP, incluyendo pruebas de inyección de código malicioso y pruebas de acceso a los diversos recursos del sistema informático en dos evaluaciones una al inicio de la cual se entrega un reporte de los hallazgos encontrados y la forma de solucionarlos. Una evaluación posterior donde se verifica que se hayan resueltos los hallazgos peligrosos encontrados.

OBJETIVOS

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

PARTICIPANTES

Jorge Haro Covarrubias (JH). Director de Tecnologías, Medios Tecnológicos Inteligentes s.a. de c.v.
Heriberto Villareal García (HV).Ingeniero de proyecto Medios Tecnológicos Inteligentes s.a. de c.v.
Ramiro Garzón Contreras. Jefe de la Unidad de Informática del IEPC Jalisco.
Personal de cada área que designe el Jefe de la unidad de informática del IEPC Jalisco.

REQUERIMIENTOS

Para realizar las actividades que se listan a continuación es necesario contar con lo siguiente:

- Acceso físico a las áreas de trabajo de la unidad de informática del IEPC Jalisco.
- Acceso al dominio(os) a auditar.
- Segmentos de la red a auditar.
- Acceso a Servidor(res).
- Direcciones Ip dentro de la red a evaluar
- Estaciones de trabajo involucradas.
- Acceso a las bases de datos a evaluar.
- Nodo con salida a internet.
- Dominio, equipos, segmentos de red etc. que no participan en la auditoría.
- Dos lugares de trabajo (mesa, silla etc.)

Las actividades que se listan a continuación se realizarán en el mes de junio de 2018.

MATRIZ DE PROGRAMACION DE ACTIVIDADES Y TAREAS PRIMERA PARTE DE LA AUDITORIA

ACTIVIDAD	TAREAS	CRONOGRAMA POR DIA				REQURIMIENTOS	RESPONSABLES		
		12	13	14	15		MTI	IEPC	
Pentest interno	Servidor(es)	*	*			Acceso a servidores vía red	JH		
	Aplicaciones Web		*	*		Acceso al dominio	JH		
	Equipos de telecomunicaciones			*	*	Acceso al segmento de red a analizar	JH		
	Estaciones de trabajo			*	*	Acceso a las estaciones de trabajo	JH		
Pentest Externo	Aplicaciones Web		*	*		Acceso al dominio	HV		
	Equipos de telecomunicaciones		*	*	*		HV		
Pruebas de Denegación del Servicio	**TAREAS**	**18**	**19**	**20**					
	Ataques volumétricos		*	*			JH/HV		

Cabe mencionar que conforme se vayan realizando las evaluaciones se entregarán reportes preliminares con el fin de que el ICPC Jalisco, pueda iniciar con la verificación y corrección en su caso de las vulnerabilidades encontradas.

MATRIZ DE PROGRAMACION DE ACTIVIDADES Y TAREAS, SEGUNDA PARTE DE LA AUDITORIA

ACTIVIDAD	TAREAS	CRONOGRAMA POR DIA				REQURIMIENTOS	RESPONSABLES		
		18	19	20	21		MTI	IEPC	
Pentest interno	Servidor(es)	*	*			Acceso a servidores vía red	JH		
	Aplicaciones Web		*	*		Acceso al dominio	JH		
	Equipos de telecomunicaciones			*	*	Acceso al segmento de red a analizar	JH		
	Estaciones de trabajo			*	*	Acceso a las estaciones de trabajo	JH		

Pentest Externo	Aplicaciones Web		*	*		Acceso al dominio	HV		
	Equipos de telecomunicaciones		*	*	*		HV		
Pruebas de Denegación del Servicio	**TAREAS**	**18**	**19**	**20**					
	Ataques volumétricos		*	*			JH/HV		

ÍNDICE

ANEXOS

1. REPORTE DE EVALUACIÓN

Reporte Servicios de Análisis de Seguridad

	Instituto Electoral y de Participación Ciudadana de Jalisco (IEPC)
Cliente:	
Proyecto:	**Evaluación de la Seguridad de las Aplicaciones Involucradas en el Prep 2018**
Responsable Cliente:	**Ramiro Garzón**
Fecha:	**Junio de 2018**
Documento:	Reporte IEPC 2018 V4

1.1 Objetivos del proyecto

Analizar y evaluar las particularidades la seguridad de la información con la que cuenta el **Instituto Electoral y de Participación Ciudadana de Jalisco (IEPC) PREP 2018.**

1.2 Plazo de ejecución

El plazo de ejecución se extendió por 4 semanas terminando.

1.3 Metodología

El análisis y la evaluación se llevaron a cabo desde 2 puntos diferentes siendo la primera fase un ataque desde fuera y sin conocimiento de la red y la segunda fue desde dentro de la red. Basado en las metodologías conocidas como ISSAF; OSWAP y la experiencia de nuestros expertos.

Cubre los siguientes puntos:

1) Evaluación y pruebas de penetración.
2) Identificación de Vulnerabilidades.
3) Penetración.
4) Evaluación de la seguridad de la red en Firewall.
5) Evaluación de la seguridad en Webservers
6) Evaluación de la seguridad en Web applicatios.

Notas importantes:

1 Este reporte es un reporte parcial que cubre solo las fases de pruebas “externas” y solo algunas internas (que se describen) de las evaluaciones mencionadas en los puntos anteriores.

1 Introducción.

La política de seguridad de la información muestra la dirección y el compromiso de la organización con la seguridad la información.

La política de seguridad tecnológica de la coordinación de sistemas debe embonar perfectamente en la política de seguridad del IEPC jalisco, ya que debe ser apoyada en algunos casos por personal fuera de la coordinación como es la entrada o salida de equipo, ingreso a las áreas exclusivas para personal de la coordinación de sistemas, trabajos en

instalaciones realizados por terceros etc.

2. PRUEBAS DE PENETRACIÓN Y VULNERABILIDADES

2.1 Introducción

La metodología ***Issaf*** para las pruebas de penetración está diseñada para evaluar la red, sistemas y la aplicación de controles. Consisten en tres fases de aproximación. Esta parte incluye tres fases siguientes:

• Fase - I: Planificación y Preparación.
• Fase - II: Evaluación.
• Fase - III: Presentación de Informes.

FASE - I: PLANIFICACIÓN Y PREPARACIÓN:

Esta fase comprende los pasos para el intercambio de información inicial, planificar y prepararse para la prueba. Las siguientes actividades están previstas:

• Identificación de las personas de contacto de ambos lados.
• Reunión de ***kick-off*** para confirmar el alcance, enfoque y la metodología.

FASE - II: EVALUACIÓN:

Esta es la fase en la que realmente llevan a cabo la prueba de penetración. En la fase de evaluación se aplica un enfoque por capas, como se muestra a continuación cada capa representa un mayor nivel de acceso a sus activos de información:

2.2 Recopilación de información

La recopilación de información es esencialmente el uso de Internet para encontrar toda la información posible sobre el objetivo (empresa o persona) usando tanto técnicas ***(DNS / WHOIS,*** motores de búsqueda, grupos de noticias, listas de correo, etc.). Al realizar cualquier tipo de prueba en un sistema de información, la información de minería y la recolección de datos es esencial y proporciona toda la información posible para continuar con la evaluación. Se Intenta explorar por todas las vías posibles para ganar más comprensión de su destino y sus recursos. Cualquier cosa que puede conseguir en esta etapa de la prueba es útil: folletos, tarjetas, anuncios en periódicos, documentos internos, y así sucesivamente.

2.3 Mapeo de la red y/o sistemas

Después de la primera sección, cuando toda la información posible sobre el objetivo se ha adquirido, un enfoque más técnico conocido como la "huella" de la red" y los recursos de que se trate. La información de la red específica de la sección anterior se toma y se amplia para producir una topología de red. Muchas herramientas y aplicaciones se pueden utilizar en esta etapa para ayudar al descubrimiento de la técnica información sobre los hosts y redes que participan en la prueba.

• Encontrar los ***host*** vivos.
• Barrido de puertos.

• Perímetro de asignación de red ***(router,firewall*** etc.).
• Identificación de los servicios críticos.
• Sistema operativo ***(fingerprint).***

2.4 Identificación de vulnerabilidades

Antes de iniciar esta sección, el auditor selecciona los puntos específicos de la prueba y la manera de prueba. Durante la identificación de la vulnerabilidad, el evaluador realizará varias actividades para la detección de explotación de los puntos débiles.

Estas actividades incluyen:

• Identificar los servicios vulnerables mediante banners servicio.
• Realizar análisis de vulnerabilidad para buscar vulnerabilidades conocidas. La información relativa a las vulnerabilidades conocidas se pueden obtener de anuncios de seguridad de los proveedores, o de bases de datos públicas, como ***SecurityFocus, nessus, CVE*** o avisos del ***CERT*** etc.
• Realizar la verificación falsos positivos y falsos negativos (por ejemplo, mediante la correlación de vulnerabilidades entre sí y con la información previamente adquirida).
• Enumerar las vulnerabilidades descubiertas.
• Estimar el impacto probable (clasificación de las vulnerabilidades encontradas).

2.5 Penetración

En esta sección el objetivo es el mismo de todo el capítulo:

“El evaluador trata de obtener acceso no autorizado eludiendo las medidas de seguridad y trata de llegar al mayor nivel de acceso como sea posible.”.

2.6 Obtener acceso y escalada de privilegios

En cualquier situación dada, un sistema se puede enumerar más. Las actividades en esta sección permitirá a los evaluadores para confirmar y documentar la intrusión probable y / o propagación de ataques automatizados. Esto permite una mejor evaluación del impacto para la organización en su conjunto.
Obtener un acceso con privilegios posible gracias a la obtención de acceso a las cuentas a través de varios medios, entre ellos:

• Descubrimiento de las combinaciones de nombre de usuario / contraseña (por ejemplo, ataques de diccionario, ataques de “*fuerza bruta”*)..
• Descubrimiento de la contraseña en blanco o contraseñas por defecto en el sistema de cuentas.
• Explotar configuración de proveedor por defecto (como los parámetros de configuración de red, contraseñas y otros).

2.7 Enumerar

Obtener las contraseñas ***encriptadas*** (por ejemplo por el dumping de la ***SAM*** en los sistemas Windows, o copiar ***/ etc / passwd y / etc / shadow de un sistema Linux***)

• Obtener la contraseña (texto claro o cifrado) mediante ***snnifing*** u otras técnicas.
• El ***snnif*** de tráfico y analizarlo.
• Reunir las ***cookies*** y utilizarlos para explotar las sesiones y de ataques de contraseña.

2.8 Comprometer de usuarios remotos / Sitios

"Un solo agujero es suficiente para exponer toda la red", independientemente el aseguramiento de la red perimetral. Cualquier sistema es tan fuerte como la más débil de sus partes.
Las comunicaciones entre usuarios remotos, sitios y redes de organización deben ser siempre con autenticación y el cifrado, tales como ***VPN***, para garantizar que los datos en tránsito por la red no se puede ser escuchados, sin embargo, esto no garantiza que los extremos de la comunicación no han sido comprometidos (por ejemplo los).

2.9 Mantenimiento del Acceso

El uso de canales cubiertos ***(vpns)***, explotación de ***back-doors, rootkits*** permiten ganar acceso en las aplicaciones o equipos claves en la red.

2.10 Reporte de hallazgos

Se reportan los hallazgos encontrados en las evaluaciones en este documento y en un documento final.

2.11 Objetivo de la sección

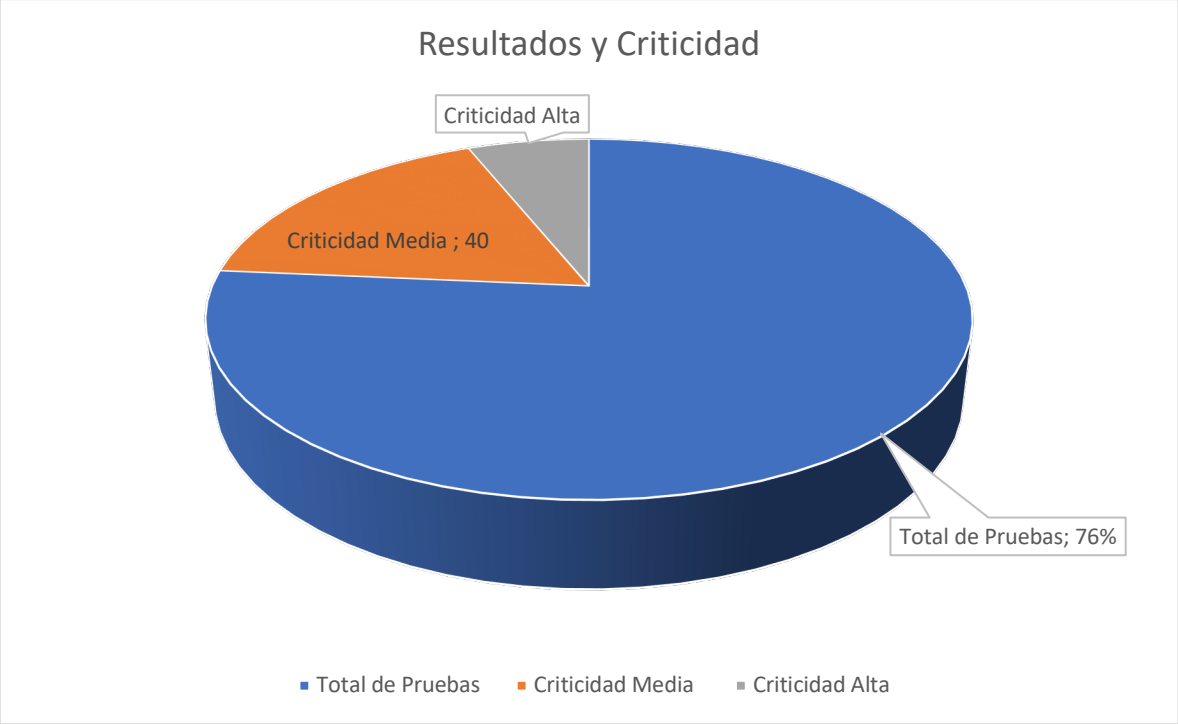
El evaluador trata de obtener acceso no autorizado eludiendo las medidas de seguridad y trata de llegar al mayor nivel de acceso como sea posible.

2.12 Procedimiento

A la fecha se realizaron las pruebas de penetración donde fue posible realizar las siguientes pruebas con los resultados que se muestran:

Resumen

Evaluación	Total	Mediano impacto	Alto impacto
Pruebas de penetración y vulnerabilidades	**25**	**4**	**4**
Pruebas a equipo firewall/ids	**10**	**0**	**----**
Pruebas a infraestructura	**50**	**18**	**7**
Pruebas a Web Applications	**90**	**18**	**3**
Total	**175**	**40**	**14**



PRUEBAS DE NEGACIÓN DE SERVICIO A SITIOS WEB DEL PREP Y AL SITIO PRINCIPAL OPL

IJALTI
CLUSTER MANAGER

Aprobaciones Requeridas

Es indispensable la aprobación de las siguientes personas acerca de este Reporte Final de Resultados de Pruebas de Performance. Cualquier modificación al documento después de su aprobación, deberá ser nuevamente autorizada por:

Nombre	Función
Ramiro Garzón	Gerente de Servicios de TI
Aarón Moreno	Dirección de Operaciones – Test Sourcing

Revisores

El presente documento ha sido enviado para su información y revisión a las siguientes personas:

Nombre	Función
Aarón Moreno	Dirección de Operaciones – Test Sourcing

Manejo de Copias Obsoletas

Es responsabilidad del usuario de este documento asegurarse de que se está usando la última versión, es decir, la versión más reciente que está en el repositorio de documentos. Si el usuario requiere imprimir este documento, de la misma manera, deberá asegurarse de usar siempre la versión más reciente.

ÍNDICE

IJALTI
CLUSTER MANAGER

INSTITUTO ELECTORAL Y DE PARTICIPACIÓN CIUDADANA DE JALISCO (IEPC)
Servicio de Auditoria al Sistema Informático y
a La Infraestructura Tecnológica del PREP
JULIO 2018

INTRODUCCIÓN

El sistema PREP (Programa de Resultados Electorales Preliminares) es el mecanismo de información electoral que recaba los resultados preliminares y no definitivos, de carácter estrictamente informativo a través de la captura de los datos asentados en las actas de escrutinio y cómputo de las casillas que se reciben en los CATD (Centros de Acopio y Transmisión de Datos) autorizados.

La finalidad del presente documento es exponer un resumen detallado de las actividades realizadas durante las pruebas de denegación de servicios (DOS), efectuadas sobre los servidores que ejecutan la aplicación "PREP", las cuales van desde la configuración y ejecución de herramientas, hasta el análisis de los resultados obtenidos. Los resultados serán mostrados visualmente mediante gráficas e interpretados para que puedan ser de utilidad para los interesados.

Las pruebas de DOS permiten verificar el comportamiento de los servidores durante la simulación de un ataque, identifican algunos riesgos y problemas relacionados con la seguridad y el desempeño de servicios, esto permite validar si la configuración es adecuada para la ejecución de los servicios en un entorno real además de anticipar el posible comportamiento que tendrán los servidores en caso de un ataque real.

AMBIENTE

Objetivo: api.iepcjalisco.org.mx

Servidor:
Lenovo
Modelo: ThinkSystem SR550
Procesador (VM): 4 Procesadores
Memoria RAM(VM): 8 GB
Sistema Operativo (VM)**:** Linux CentOS 7

Enlace: 300 Mbps

Pruebas:

Equipos:
Modelo: HP ZBook 15 G3 Workstation
Procesaror: Intel Core i7-6700HQ 2.60GHz
Memoria: 16 GB
Sistema Operativo: Linux Fedora 27

Enlace: 1 Gbps

OBJETIVOS DE LAS PRUEBAS

Los objetivos de las pruebas de denegación de servicios para el “PREP” son:

- Validar la configuración y desempeño de los mecanismos de seguridad (Firewall, Servidor de aplicaciones, etc.) en los servidores.
- Observar el comportamiento de los servicios durante la simulación de un ataque.
- Encontrar problemas de seguridad relacionados a la denegación de servicios.
- Conocer las posibles afectaciones en servidores durante un ataque.
- Contrastar el rendimiento de los servicios con los resultados de las pruebas de Performance

FUNCIONALIDAD PROBADA

La ejecución de las pruebas de seguridad se realizará en paralelo con ejecuciones de pruebas de performance que nos permitan observar el comportamiento de los servicios durante la simulación del ataque.

La funcionalidad a probar en las pruebas de performance será la carga de información al consultar la URL proporcionada por el departamento de sistemas del IEPC.

Envío de petición

Nombre	Ruta	Justificación
Envío de petición	http://api.iepcjalisco.org.mx/stress-test	Obligatorio

ANTECEDENTES DE PRUEBAS

Fecha de ejecución:
2018-06-24

La ejecución de pruebas de DOS se realizó con dos tipos diferentes de ataque:

El primer ataque es conocido cómo ***TCP SYN***, en el que se envían paquetes SYN (*synchronize*) al servidor para iniciar la comunicación de acuerdo al protocolo TCP, pero la comunicación nunca se concluye ya que se ignoran las respuestas del servidor. La intención es crear procesos en el servidor que esperan una respuesta del cliente, estos procesos tardan un tiempo en ser terminados al no recibir una respuesta valida. Un ataque a gran escala podría crear procesos suficientes para afectar el rendimiento de un servidor.

El segundo ataque se llama ***DNS Amplification***, este ataque consiste en hacer solicitudes de tipo DNS a servidores reales creando un paquete modificado donde se remplaza la IP de origen con la IP del servidor víctima, de esta manera los servidores DNS envían la respuesta al servidor que es objetivo del ataque, aunque este no haya realizado la solicitud. El trafico DNS por ser común y sencillo suele pasar inadvertido para la mayoría de los sistemas de seguridad.

Durante la ejecución de los ataques se utilizaron dos equipos para generar el tráfico de red necesario, estos equipos se identifican con las IPs 170.244.108.146 y 170.244.108.147. Además, se realizó una ejecución de performance en paralelo con la intención de monitorear el funcionamiento del servicio. La configuración de los equipos fue diseñada de forma exclusiva para la ejecución de la prueba. Los equipos que simularon el ataque tenían *GNU/Linux* como sistema operativo y se utilizó la herramienta *nload* para monitorear el ancho de banda utilizado durante la ejecución.

La ejecución del script de pruebas de performance se llevó a cabo mediante dos equipos de cómputo (generadores de carga). En cada prueba el script se ejecutó bajo las siguientes condiciones:

- 8,400 usuarios distribuidos en 5 minutos

EJECUCIÓN DE LAS PRUEBAS

Scripts de prueba

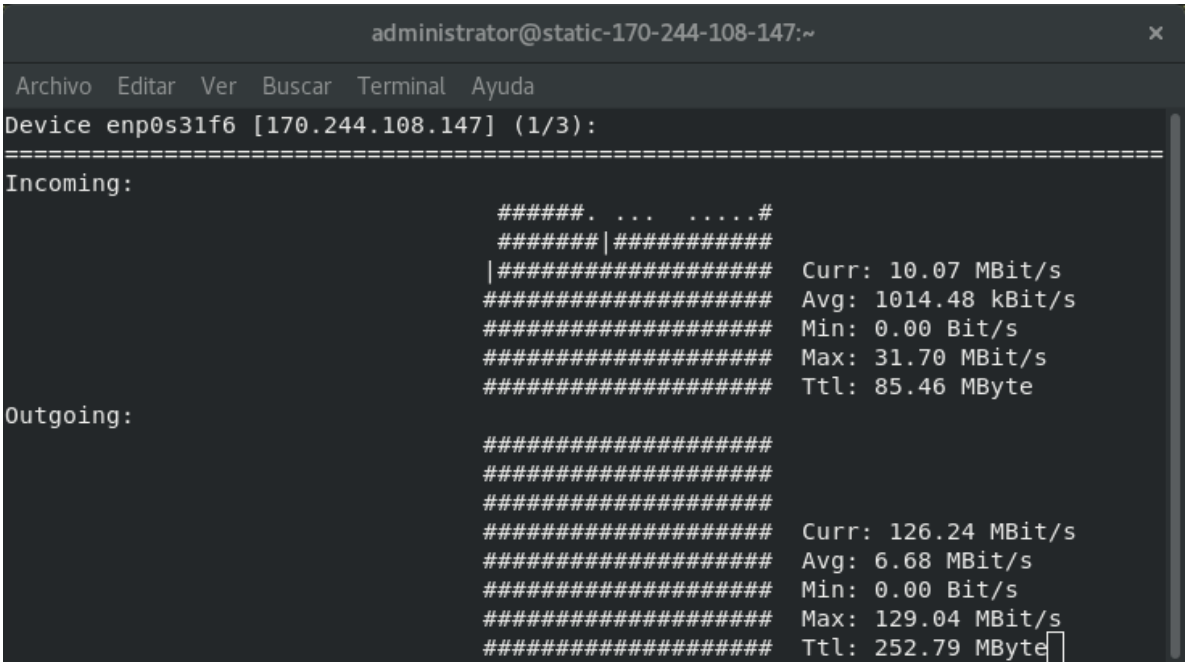
Se utilizó el script diseñado para las pruebas de carga el cual cubre con la carga total de la información proporcionada por la respuesta a la petición.

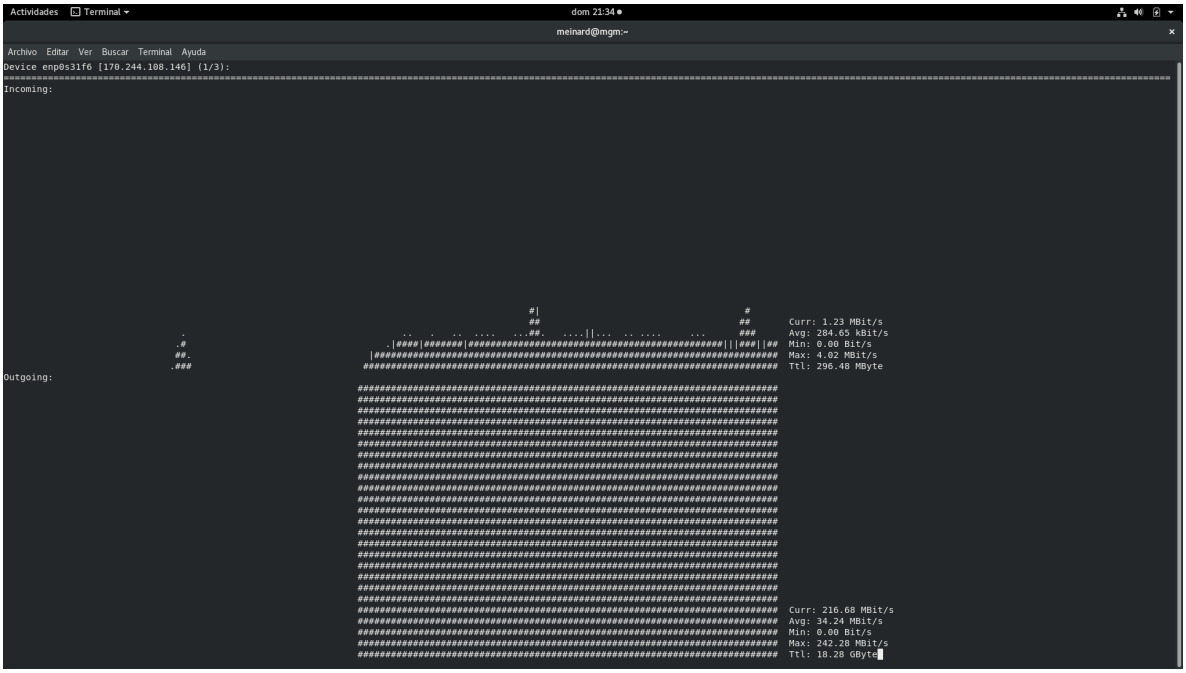
Script de prueba
IEPC-STRESS-TEST

TCP SYN

Durante la ejecución del ataque se enviaron paquetes de tipo SYN a la dirección api.iepcjalisco.org.mx durante dos minutos, después se detuvo la simulación del ataque para ver la reacción del sistema.

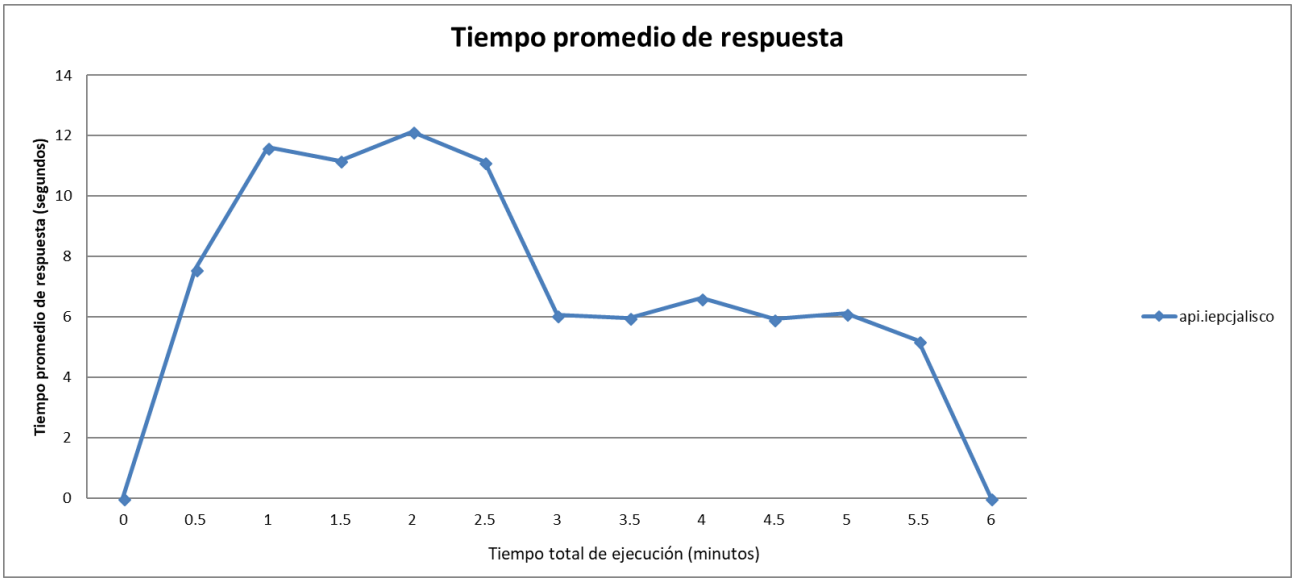
Durante la ejecución se generó tráfico por más de 300mbps entre los dos equipos que simularían el ataque.





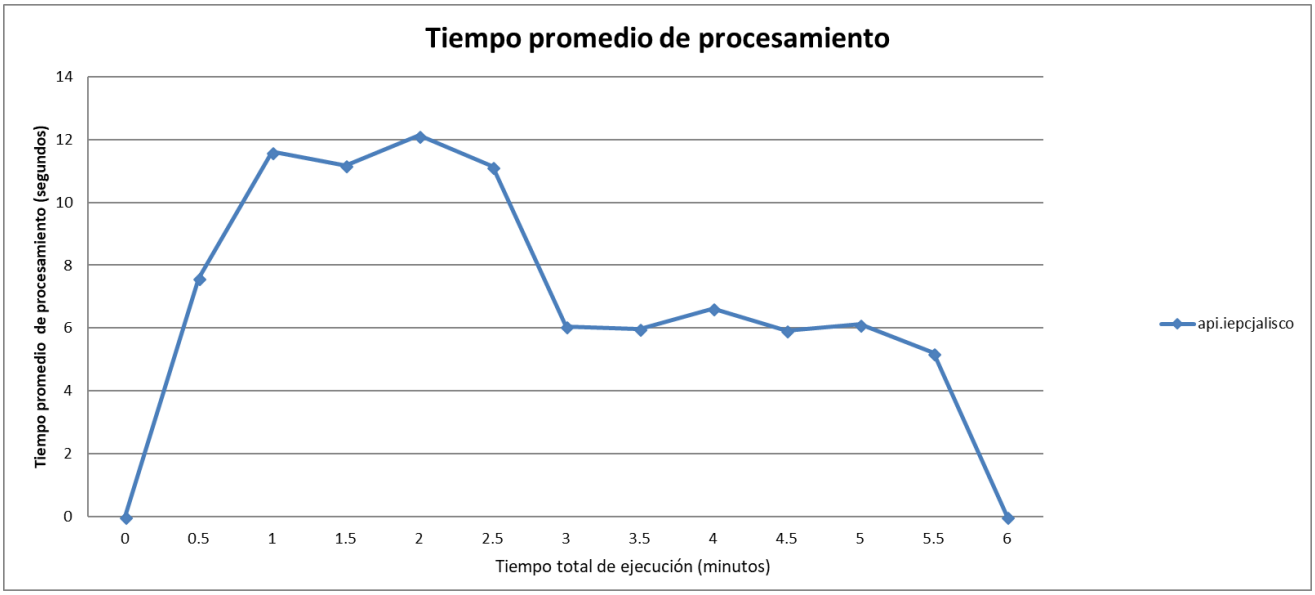
En la graficas siguientes se puede ver como en los primeros minutos se incrementan los tiempos de respuesta en las peticiones del servicio y como estos comienzan a disminuir después de los dos minutos y medio que es el momento en que se detiene la generación de tráfico.

En la gráfica se muestra el tiempo promedio de respuesta de los elementos dentro del periodo de tiempo de ejecución de la prueba.

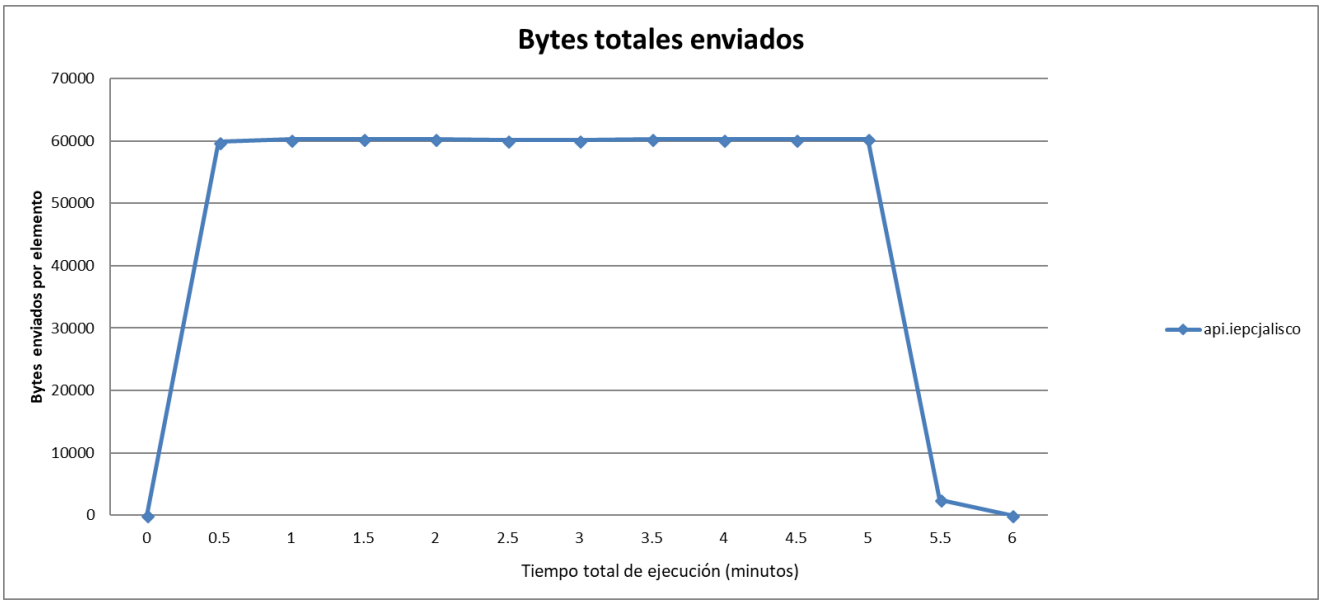


Tiempo promedio de respuesta	
Tiempo(min)	api.iepcjalisco
0	0
0.5	7.58535018
1	11.6125675
1.5	11.17631146
2	12.12836635
2.5	11.13726348
3	6.058305389
3.5	5.972742239
4	6.627547194
4.5	5.921225807
5	6.117132461
5.5	5.209028557
6	0

En la gráfica se muestra el tiempo promedio de procesamiento dentro del periodo de tiempo de ejecución de la prueba.



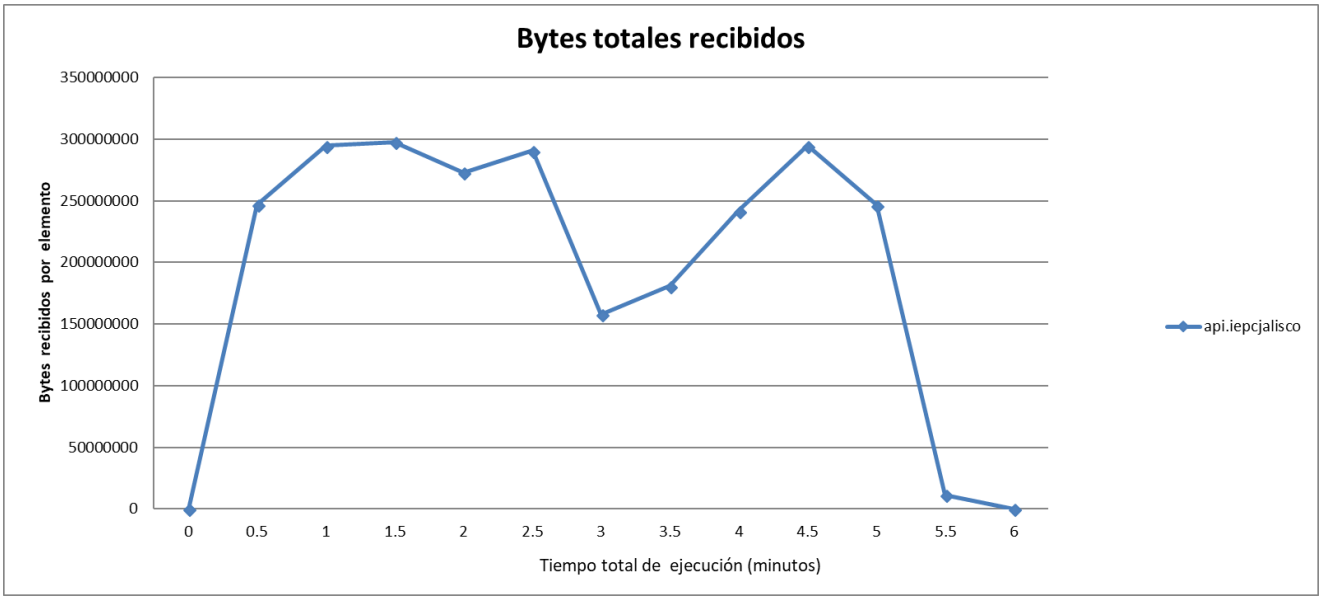
La gráfica muestra el volumen de información en bytes enviados por las peticiones durante la ejecución.



Tiempo promedio de procesamiento	
Tiempo(min)	api.iepcjalisco
0	0
0.5	7.585350181
1	11.6125675
1.5	11.17631146
2	12.12836635
2.5	11.13726347
3	6.058305389
3.5	5.972742243
4	6.627547192
4.5	5.921225806
5	6.117132458
5.5	5.209028571
6	0

Bytes totales enviados	
Tiempo(min)	api.iepcjalisco
0	0
0.5	59832
1	60264
1.5	60336
2	60336
2.5	60120
3	60120
3.5	60336
4	60264
4.5	60264
5	60336
5.5	2520
6	0

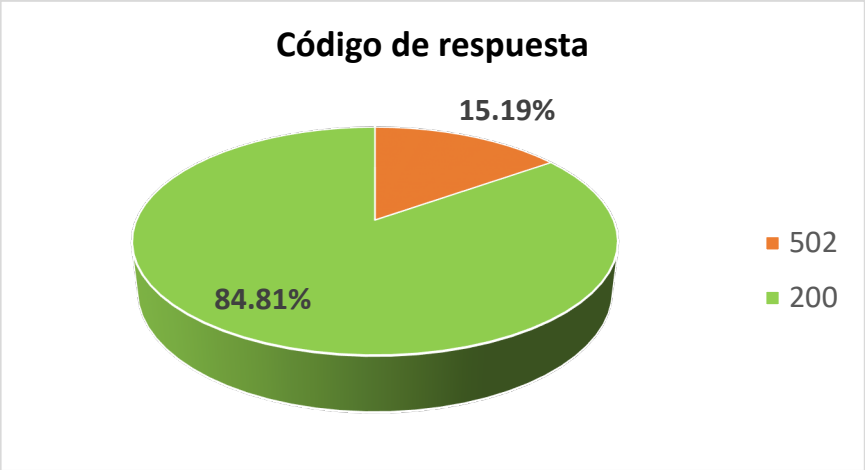
La gráfica muestra el volumen de información en bytes recibidos durante la ejecución.



Bytes totales recibidos	
Tiempo(min)	api.iepcjalisco
0	0
0.5	246753142
1	294562419
1.5	297728448
2	272780158
2.5	290692842
3	157867620
3.5	181074791
4	241868936
4.5	294562932
5	246452457
5.5	11380851
6	0

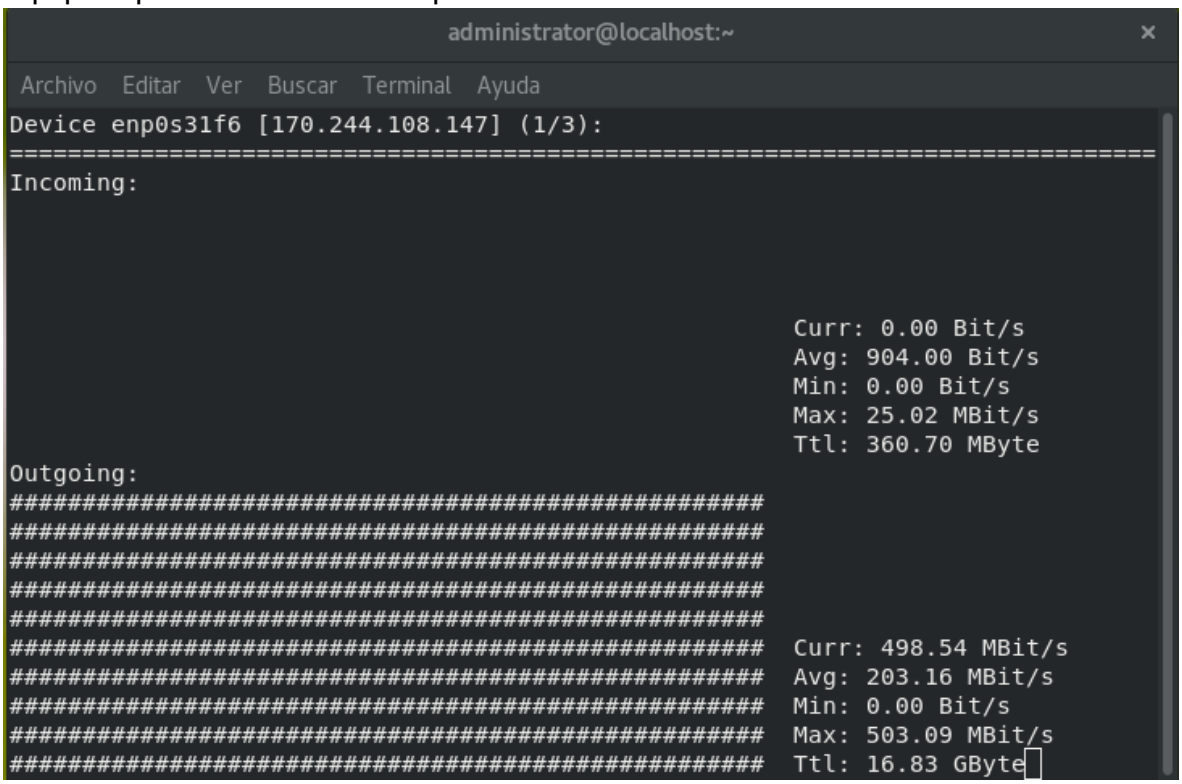
La gráfica muestra los códigos de respuesta obtenidos durante la ejecución.

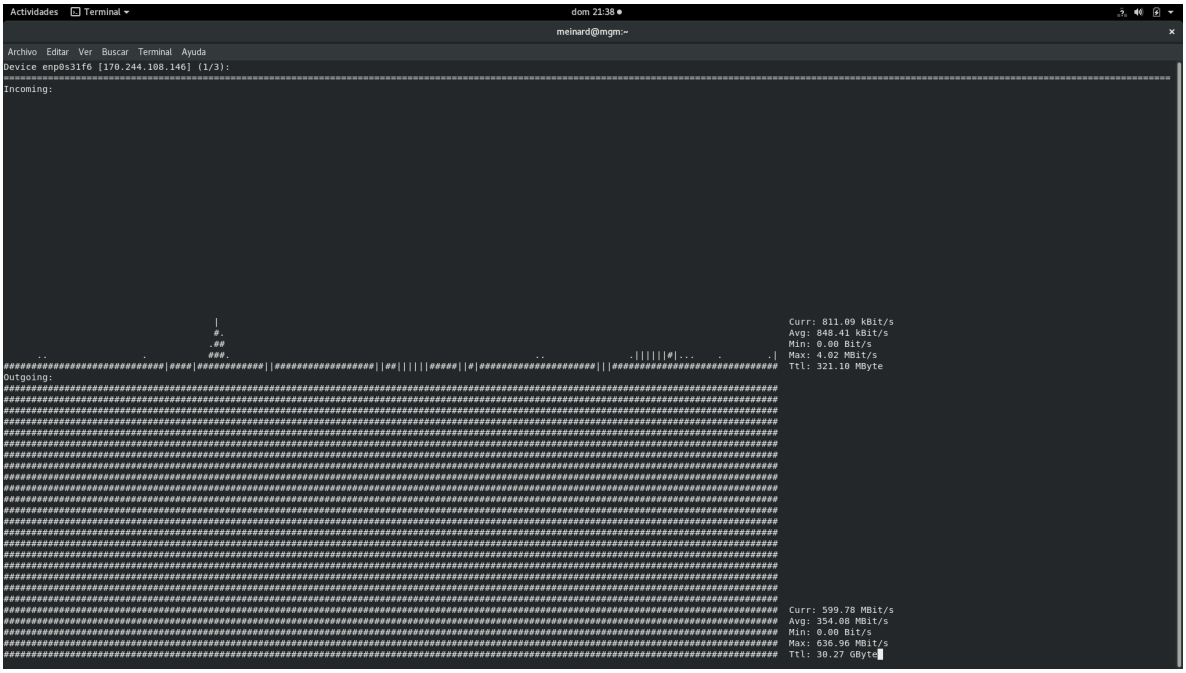
Código de respuesta		
Código	Cantidad	Porcentaje
502	1276	15.19%
200	7124	84.81%
Total	15000	100%



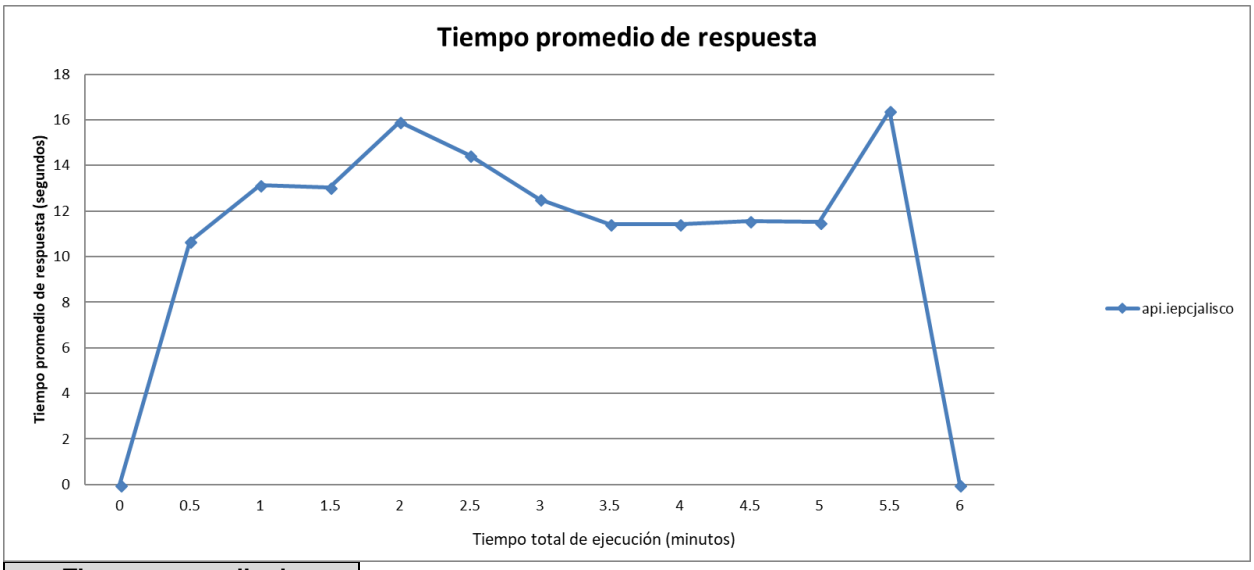
Segunda ejecución TCP SYN

Durante la segunda ejecución se generó tráfico por más de 800mbps entre los dos equipos que simularían el ataque.



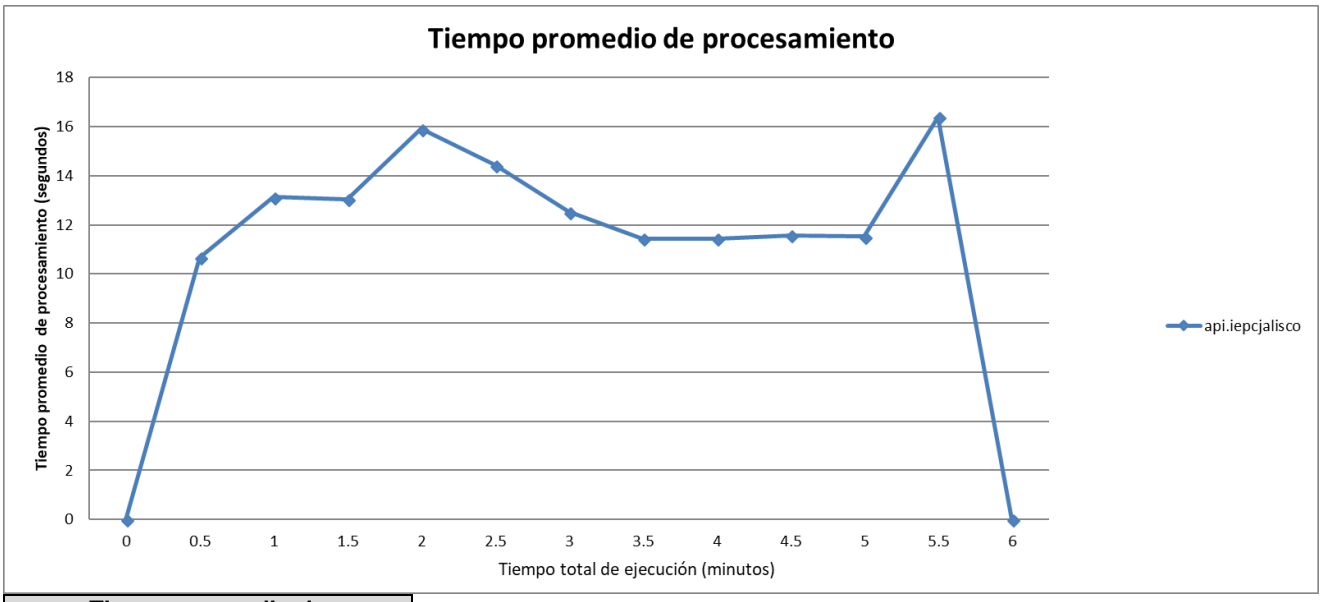


En la gráfica se muestra el tiempo promedio de respuesta de los elementos dentro del periodo de tiempo de ejecución de la prueba.



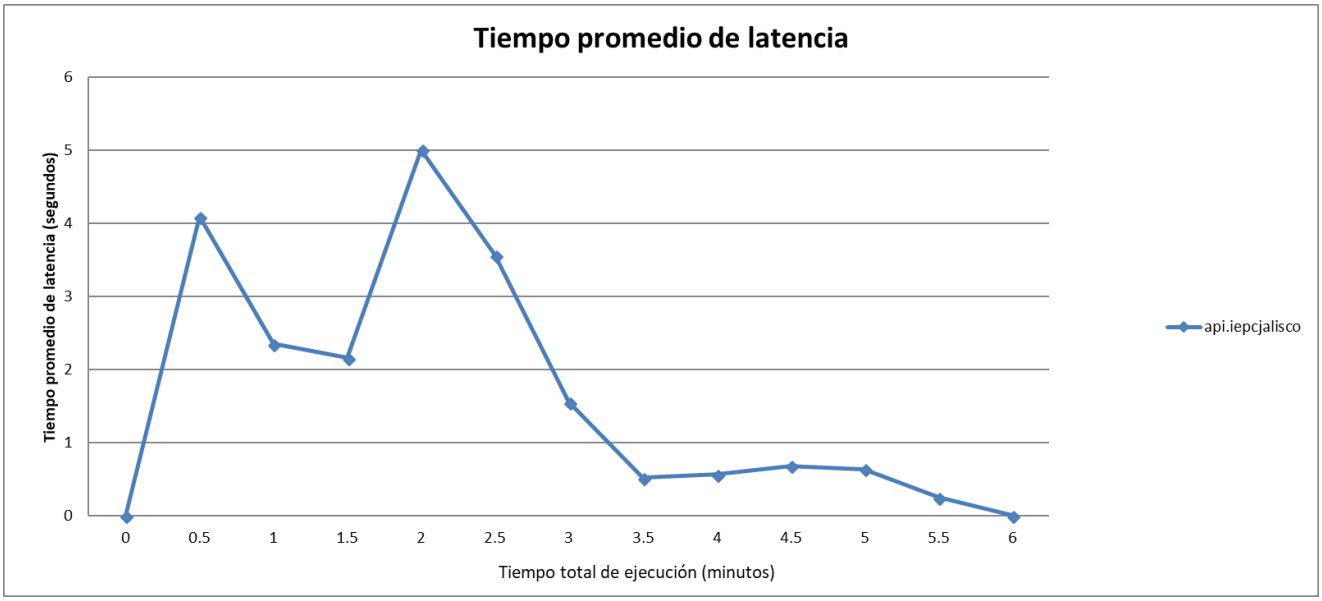
Tiempo promedio de respuesta	
Tiempo(min)	api.iepcjalisco
0	0
0.5	7.58535018
1	11.6125675
1.5	11.17631146
2	12.12836635
2.5	11.13726348
3	6.058305389
3.5	5.972742239
4	6.627547194
4.5	5.921225807
5	6.117132461
5.5	5.209028557
6	0

En la gráfica se muestra el tiempo promedio de procesamiento dentro del periodo de tiempo de ejecución de la prueba.



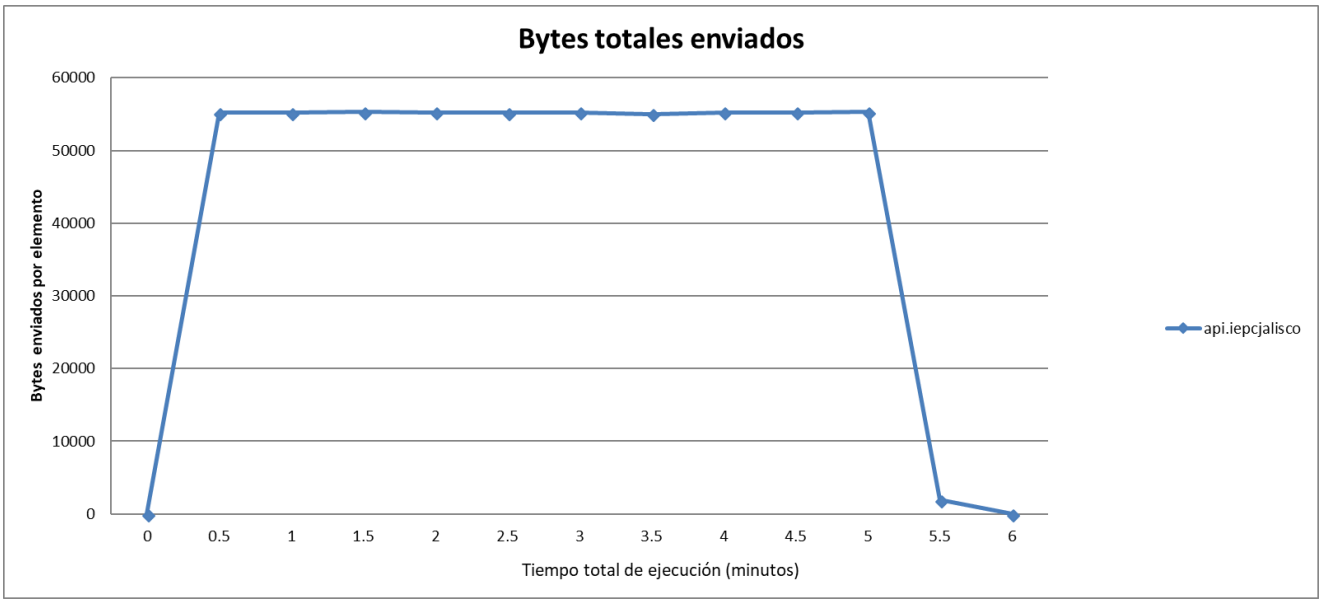
Tiempo promedio de procesamiento	
Tiempo(min)	api.iepcjalisco
0	0
0.5	7.585350181
1	11.6125675
1.5	11.17631146
2	12.12836635
2.5	11.13726347
3	6.058305389
3.5	5.972742243
4	6.627547192
4.5	5.921225806
5	6.117132458
5.5	5.209028571
6	0

En la gráfica se muestra el tiempo promedio de latencia dentro del periodo de tiempo de ejecución de la prueba.



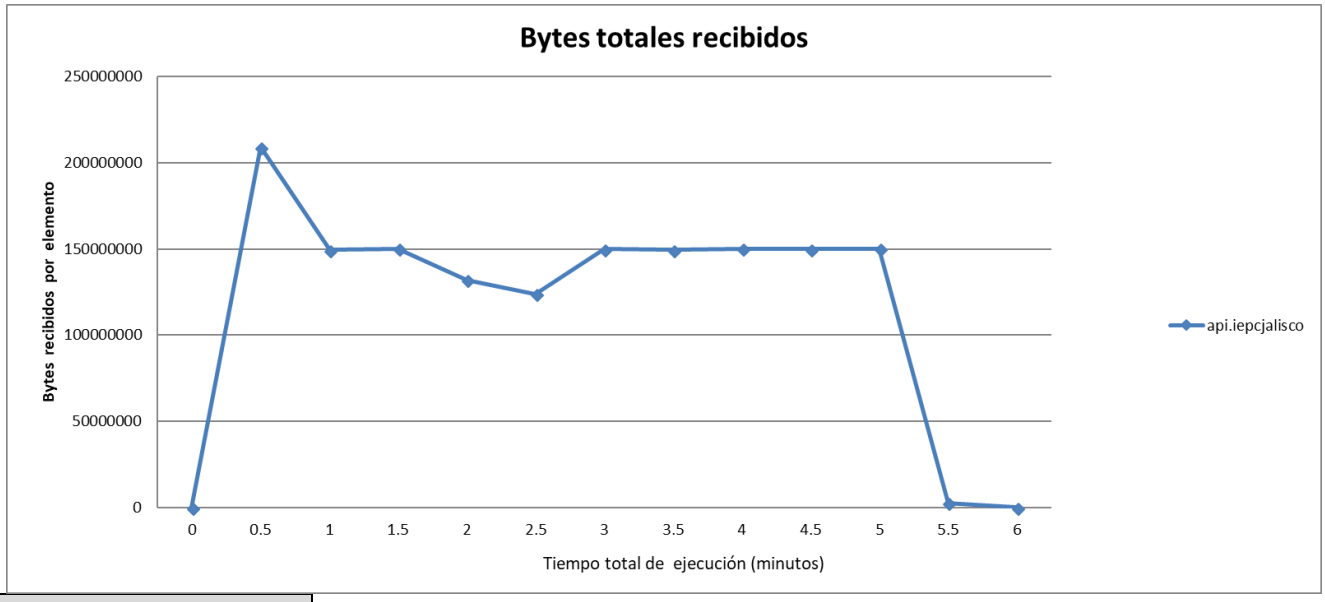
Tiempo promedio de latencia	
Tiempo(min)	api.iepcjalisco
0	0
0.5	5.716188929
1	6.556316607
1.5	8.317436754
2	9.664994033
2.5	8.949368862
3	5.577014371
3.5	5.483843675
4	5.666747909
4.5	3.711072879
5	5.561958234
5.5	4.564
6	0

La gráfica muestra el volumen de información en bytes enviados durante la ejecución.



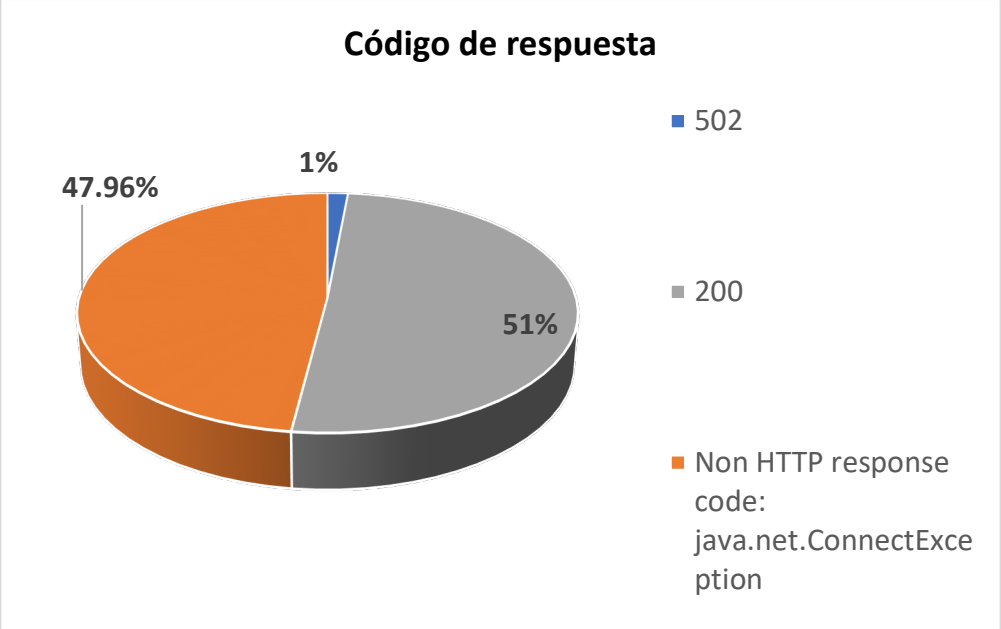
Bytes totales enviados	
Tiempo(min)	api.iepcjalisco
0	0
0.5	59832
1	60264
1.5	60336
2	60336
2.5	60120
3	60120
3.5	60336
4	60264
4.5	60264
5	60336
5.5	2520
6	0

La gráfica muestra el volumen de información en bytes recibidos por las peticiones durante la ejecución.



Bytes totales recibidos	
Tiempo(min)	api.iepcjalisco
0	0
0.5	246753142
1	294562419
1.5	297728448
2	272780158
2.5	290692842
3	157867620
3.5	181074791
4	241868936
4.5	294562932
5	246452457
5.5	11380851
6	0

La gráfica muestra los códigos de respuesta obtenidos durante la ejecución.



Código de respuesta		
Código	Cantidad	Porcentaje
502	125	1.49%
200	4246	50.55%
Non HTTP response code: java.net.ConnectException	4029	47.96
Total	15000	100%

DNS Amplification

Durante la ejecución del ataque se consultaron los siguientes dominios:

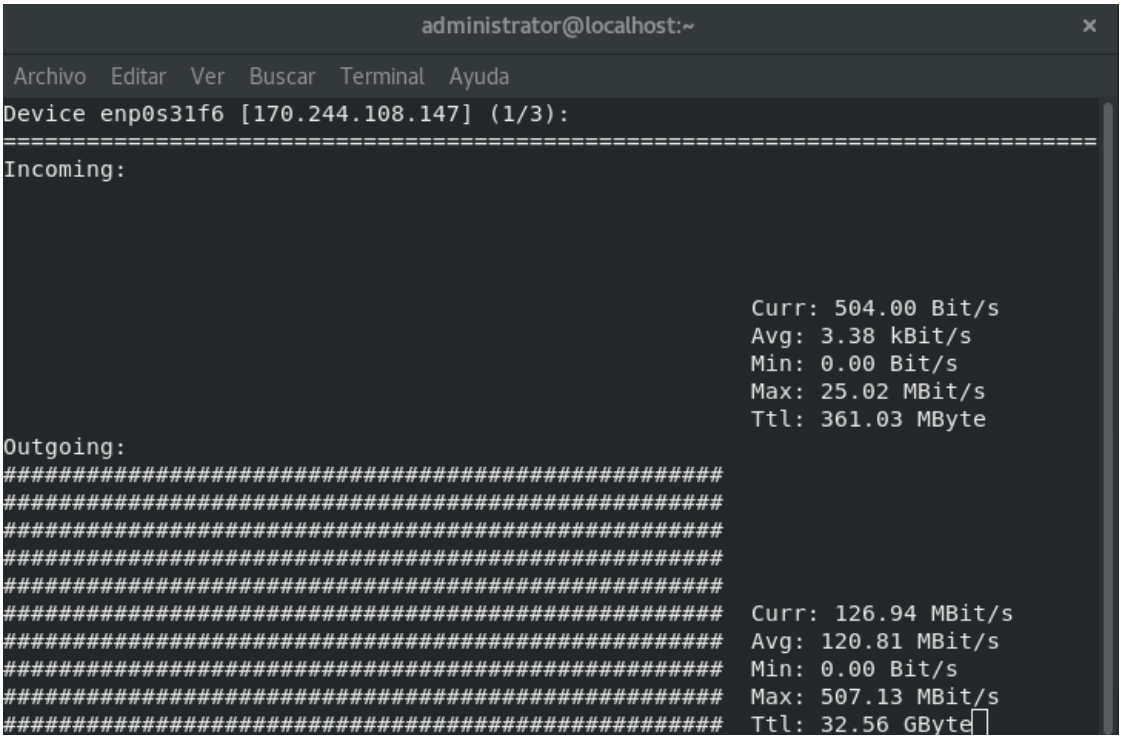
cinemex.com
google.com
liverpool.com
cinemex.com
google.com
liverpool.com
cinecolombia.com
bookmyshow.com
ligabancomer.mx
banamex.com
bancomer.com
vivaaerobus.com
calvinklein.mx
chevrolet.com
renault.com
honda.mx
intel.la
estafeta.com
canon.com
epson.com
jbl.com
vento.com
keeway.mx
suzuki.com
brp.com
totalplay.com
ducati.com
kawasaki.com
OCCmundial.com
x-tremo.mx
axtelpaquetes.mx
axtelcorp.mx
axtel.com
totalplay.com
mitotalplay.com
megacable.com
izzy.mx
izzyprecios.mx
sky.com
cablemas.com
tudecide.com
telecoms.mx
att.com
bmv.com
investing.com
kioski.net
eluniversal.com
assetel.com
milenio.com
securitic.com
pepsico.com
pepsicojobs.com
hoytocapepsi.com
minutemaid.com
cokeconsolidated.com
jnj.com
jnjmexico.com
scjohnson.com
tentulogo.com
milenio.com
jnj.ch
bmv.com
expansion.mx
generalmills.com
generalmills.es
eleconomista.com
cinecolombia.com
bookmyshow.com
ligabancomer.mx
banamex.com
bancomer.com
vivaaerobus.com
calvinklein.mx
chevrolet.com
renault.com
honda.mx
intel.la
estafeta.com
canon.com
epson.com
jbl.com
vento.com
keeway.mx
suzuki.com
brp.com
totalplay.com
ducati.com
kawasaki.com
OCCmundial.com
x-tremo.mx
axtelpaquetes.mx
axtelcorp.mx
axtel.com
totalplay.com
mitotalplay.com
megacable.com
izzy.mx
izzyprecios.mx
sky.com
cablemas.com
tudecide.com
telecoms.mx
att.com
bmv.com
investing.com
kioski.net
eluniversal.com
assetel.com
milenio.com
securitic.com
pepsico.com
pepsicojobs.com
hoytocapepsi.com
minutemaid.com
cokeconsolidated.com
jnj.com
jnjmexico.com
scjohnson.com
tentulogo.com
milenio.com
jnj.ch
bmv.com
expansion.mx
generalmills.com
generalmills.es
eleconomista.com

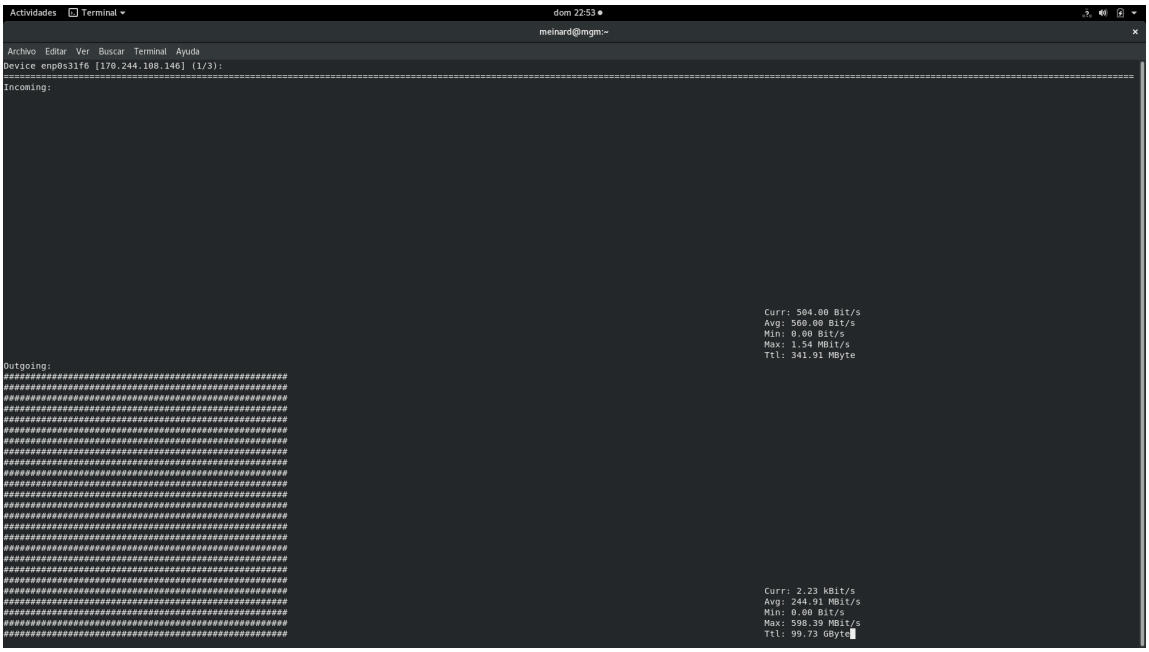
A continuación, se muestra la lista de servidores DNS a donde se enviaron las peticiones:

208.67.222.222
84.200.69.80
8.8.8.8
64.6.64.6
8.26.56.26
199.85.126.10
199.85.126.20
199.85.126.30
209.244.0.3
216.146.35.35
208.67.220.220
84.200.70.40
8.8.4.4
64.6.65.6
8.20.247.20
199.85.127.10
199.85.127.20
199.85.127.30
209.244.0.4
216.146.36.36
207.248.224.72
207.248.224.71
200.57.2.108
148.235.12.161
187.216.83.129
187.174.84.104
187.130.239.5
201.144.18.82
200.56.193.2
201.174.25.131
201.149.26.54
200.76.185.129
201.149.23.167
201.149.39.107
201.117.40.129
200.79.8.37
201.174.28.254
201.134.103.165
200.79.66.140
201.163.38.227

187.210.228.241
207.249.157.35
148.243.155.160
189.211.179.48
201.144.217.53
187.210.47.139
200.34.169.2
187.141.134.99
187.210.47.136
148.243.170.68
148.233.179.84
201.163.43.62
200.56.117.252
187.217.232.49
200.57.190.131
201.96.236.89
187.160.252.188
189.254.149.228
187.160.242.187
200.77.120.154
189.206.255.206
200.94.17.243
187.218.153.25
201.144.133.135
201.144.230.228
200.36.46.8
200.36.46.5
189.212.132.210
187.217.227.181
207.249.157.119

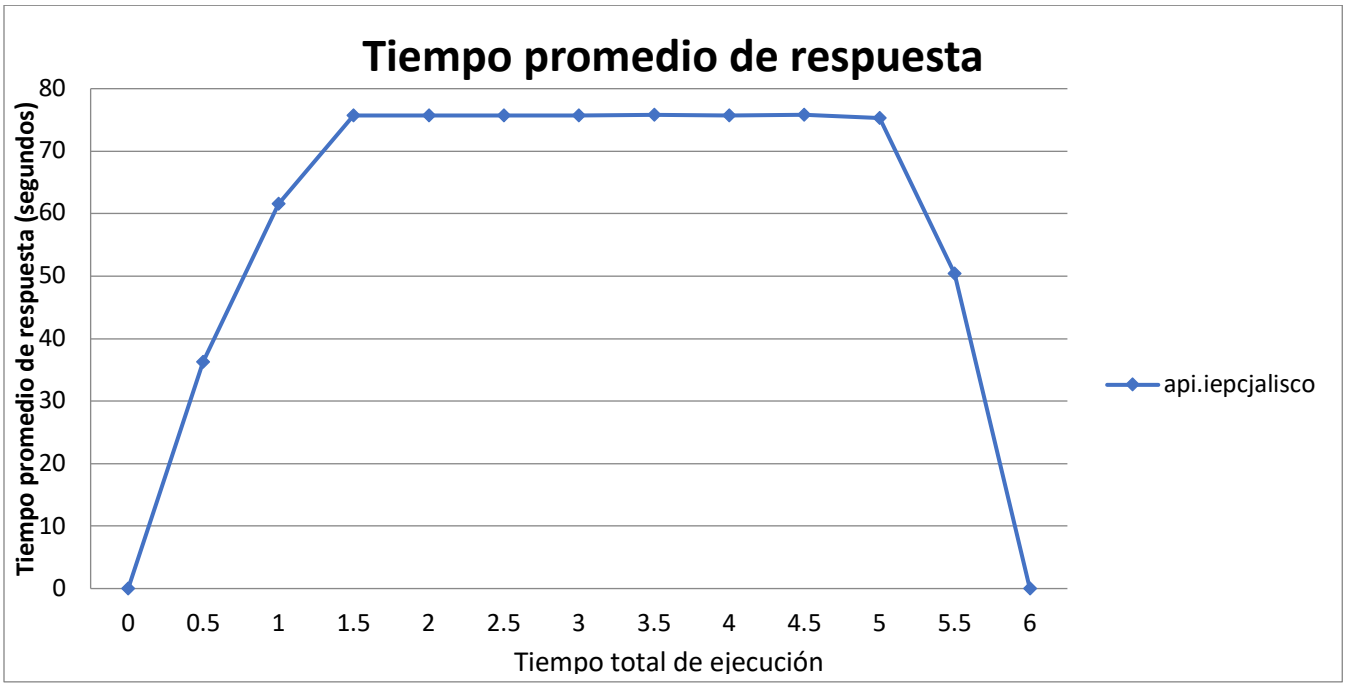
La ejecución se llevo a cabo con un ancho de banda de más de 600 mbps.





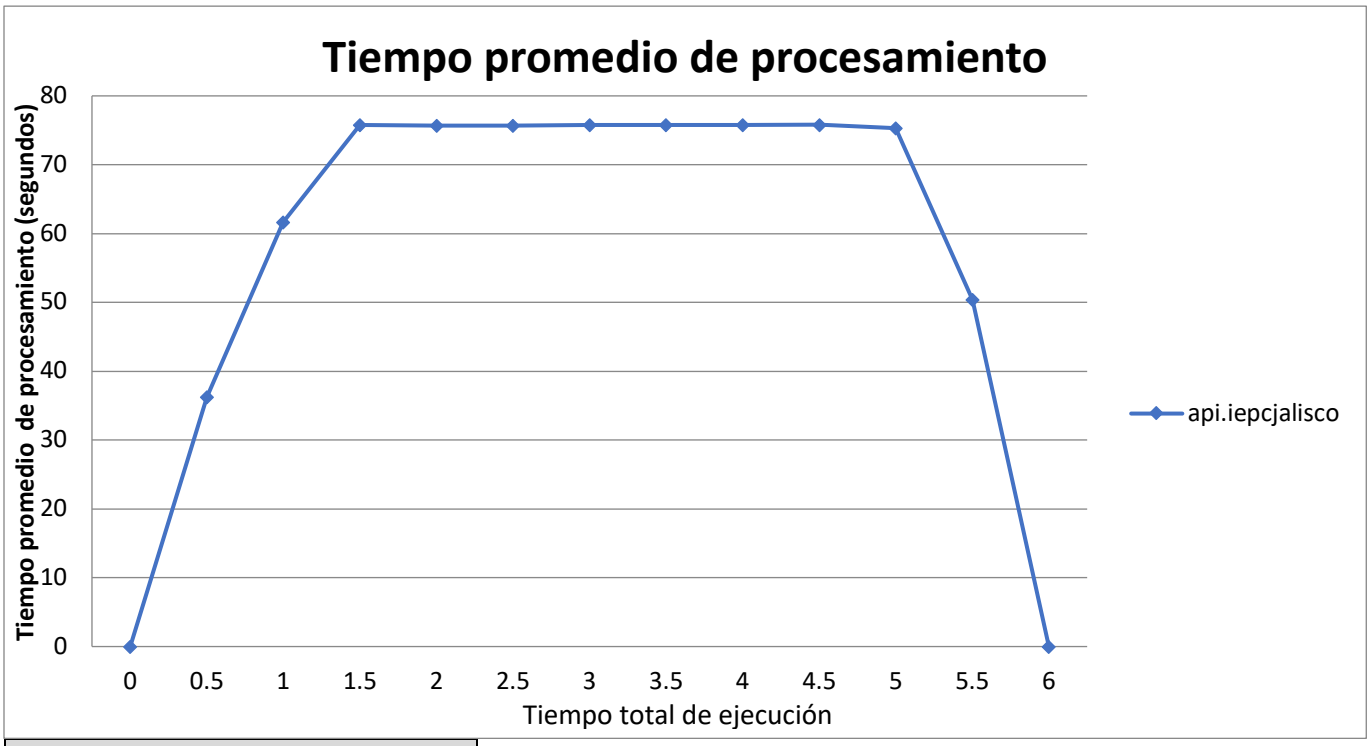
En las siguientes graficas se muestra el comportamiento de la aplicación durante la ejecución. Algo notable en esta ejecución es que además de incrementarse los tiempos de respuesta también se incrementó la cantidad de peticiones que fallaron.

En la gráfica se muestra el tiempo promedio de respuesta de los elementos dentro del periodo de tiempo de ejecución de la prueba.



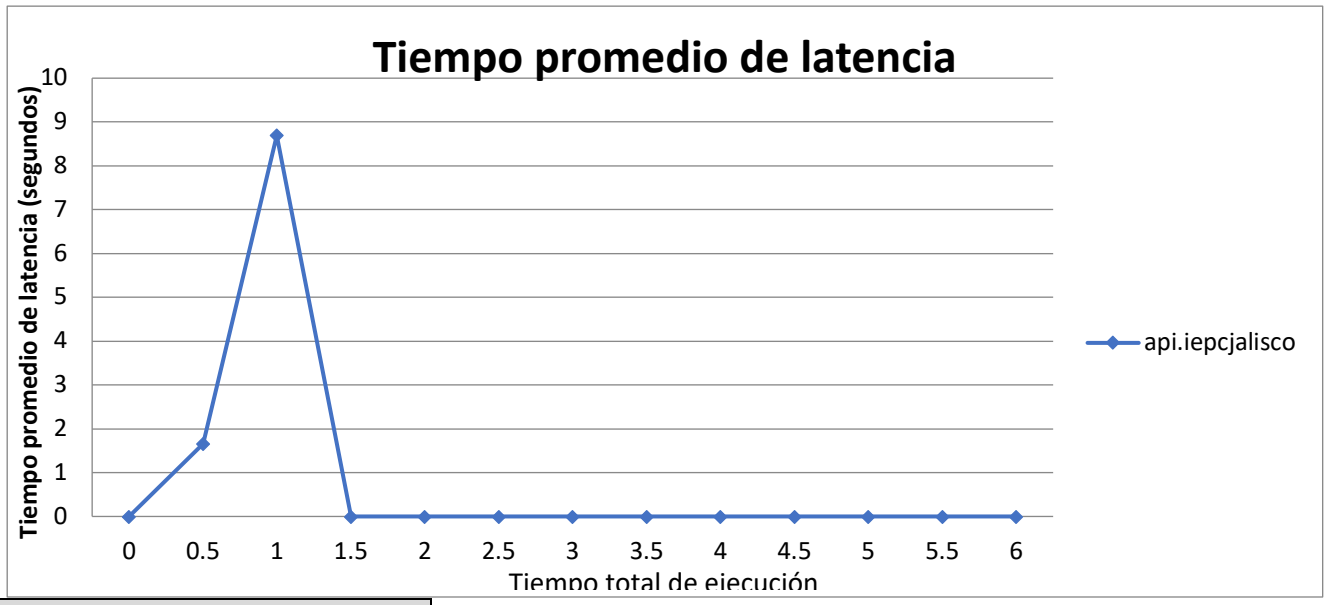
Tiempo promedio de respuesta	
Tiempo(min)	api.iepcjalisco
0	0
0.5	7.58535018
1	11.6125675
1.5	11.17631146
2	12.12836635
2.5	11.13726348
3	6.058305389
3.5	5.972742239
4	6.627547194
4.5	5.921225807
5	6.117132461
5.5	5.209028557
6	0

En la gráfica se muestra el tiempo promedio de procesamiento dentro del periodo de tiempo de ejecución de la prueba.



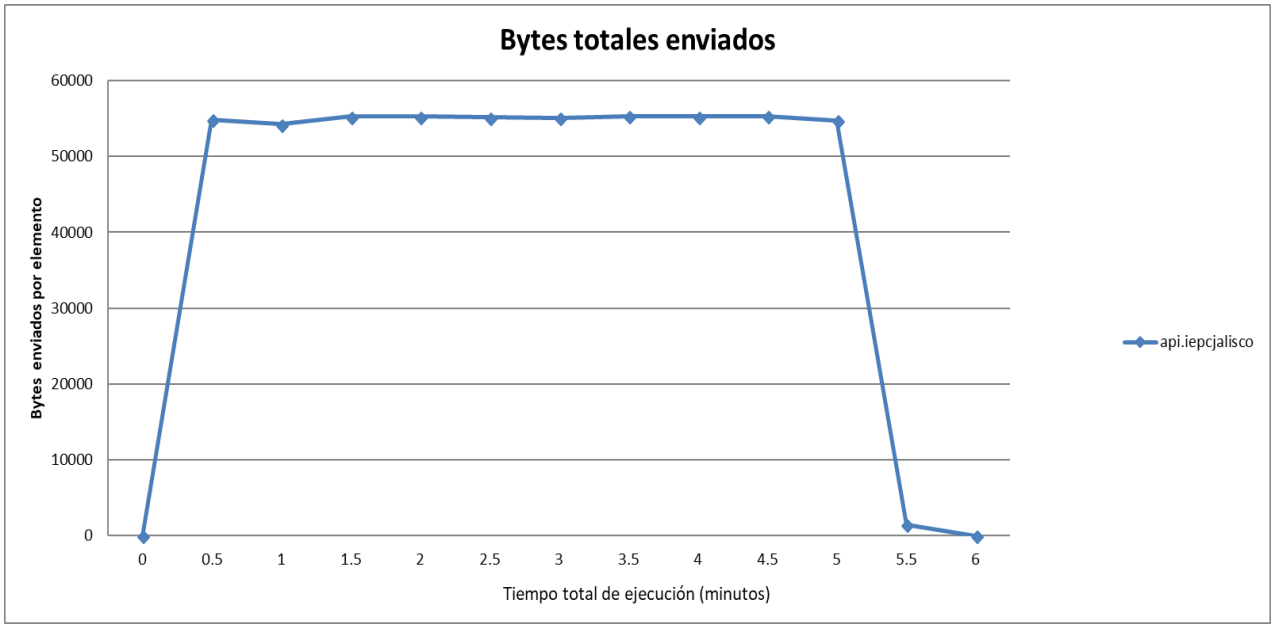
Tiempo promedio de procesamiento	
Tiempo(min)	api.iepcjalisco
0	0
0.5	7.585350181
1	11.6125675
1.5	11.17631146
2	12.12836635
2.5	11.13726347
3	6.058305389
3.5	5.972742243
4	6.627547192
4.5	5.921225806
5	6.117132458
5.5	5.209028571
6	0

En la gráfica se muestra el tiempo promedio de latencia dentro del periodo de tiempo de ejecución de la prueba.



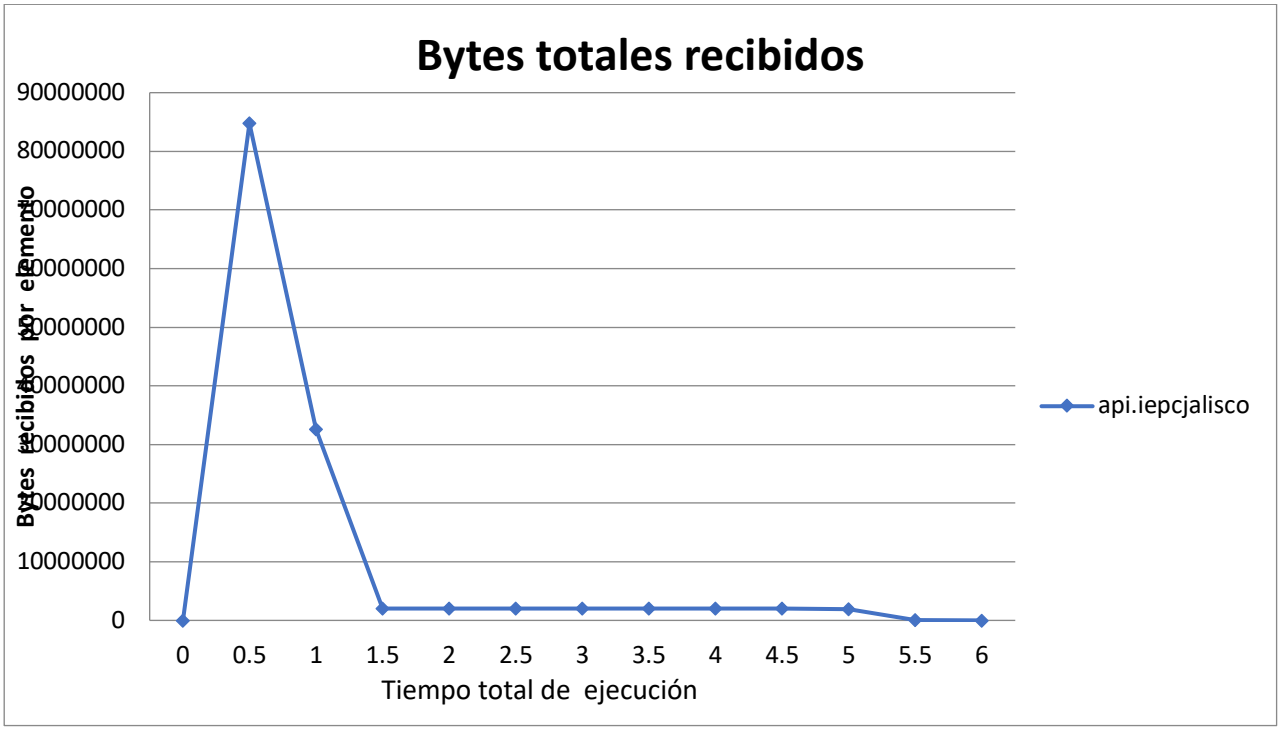
Tiempo promedio de latencia	
Tiempo(min)	api.iepcjalisco
0	0
0.5	5.716188929
1	6.556316607
1.5	8.317436754
2	9.664994033
2.5	8.949368862
3	5.577014371
3.5	5.483843675
4	5.666747909
4.5	3.711072879
5	5.561958234
5.5	4.564
6	0

La gráfica muestra el volumen de información en bytes enviados durante la ejecución.



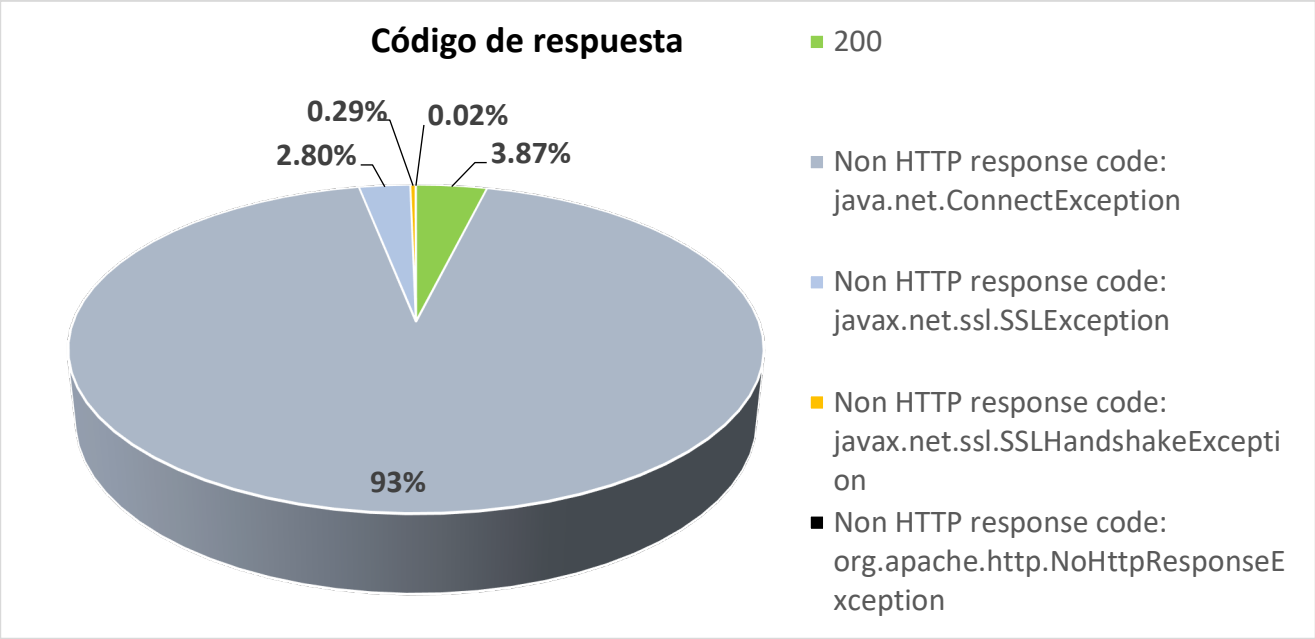
Bytes totales enviados	
Tiempo(min)	api.iepcjalisco
0	0
0.5	59832
1	60264
1.5	60336
2	60336
2.5	60120
3	60120
3.5	60336
4	60264
4.5	60264
5	60336
5.5	2520
6	0

La gráfica muestra el volumen de información en bytes recibidos por las peticiones durante la ejecución.



Bytes totales recibidos	
Tiempo(min)	api.iepcjalisco
0	0
0.5	246753142
1	294562419
1.5	297728448
2	272780158
2.5	290692842
3	157867620
3.5	181074791
4	241868936
4.5	294562932
5	246452457
5.5	11380851
6	0

La gráfica muestra los códigos de respuesta obtenidos durante la ejecución.



Código de respuesta		
Código	Cantidad	Porcentaje
200	324	3.87%
Non HTTP response code: java.net.ConnectException	7786	93.02%
Non HTTP response code: javax.net.ssl.SSLException	234	2.80%
Non HTTP response code: javax.net.ssl.SSLHandshakeException	24	0.29%
Non HTTP response code: org.apache.http.NoHttpResponseException	2	0.02%
Total	8370	100%

Ejecución coordinada con IEPC

Después de las ejecuciones en paralelo con pruebas de Performance se realizó una ejecución corta de tipo TCP SYN en coordinación con el IEPC en la que se confirmó con el área de sistemas el incremento de uso de recursos de procesamiento durante la prueba. Pero no se reportó afectación en el funcionamiento de las aplicaciones lo que podría indicar que el servidor de aplicaciones reaccionó adecuadamente ante el ataque.

CONCLUSIONES

Durante la ejecución de los ataques TCP SYN se mostró una degradación en los tiempos de respuesta, pero la mayoría de las peticiones se respondieron adecuadamente. En cambio, durante la ejecución del ataque DNS Amplification se mostró un incremento considerable en los tiempos de respuesta y en la cantidad de peticiones que se respondieron con error. Esto nos demuestra que el ataque saturó el ancho de banda que utilizan los servidores que atendían las peticiones e impidió que la herramienta de performance creara nuevas conexiones. Sin embargo, esto no afectó la respuesta del servicio desde otras ubicaciones lo que indica que algún mecanismo de seguridad aisló correctamente el tráfico perteneciente al ataque del tráfico normal.