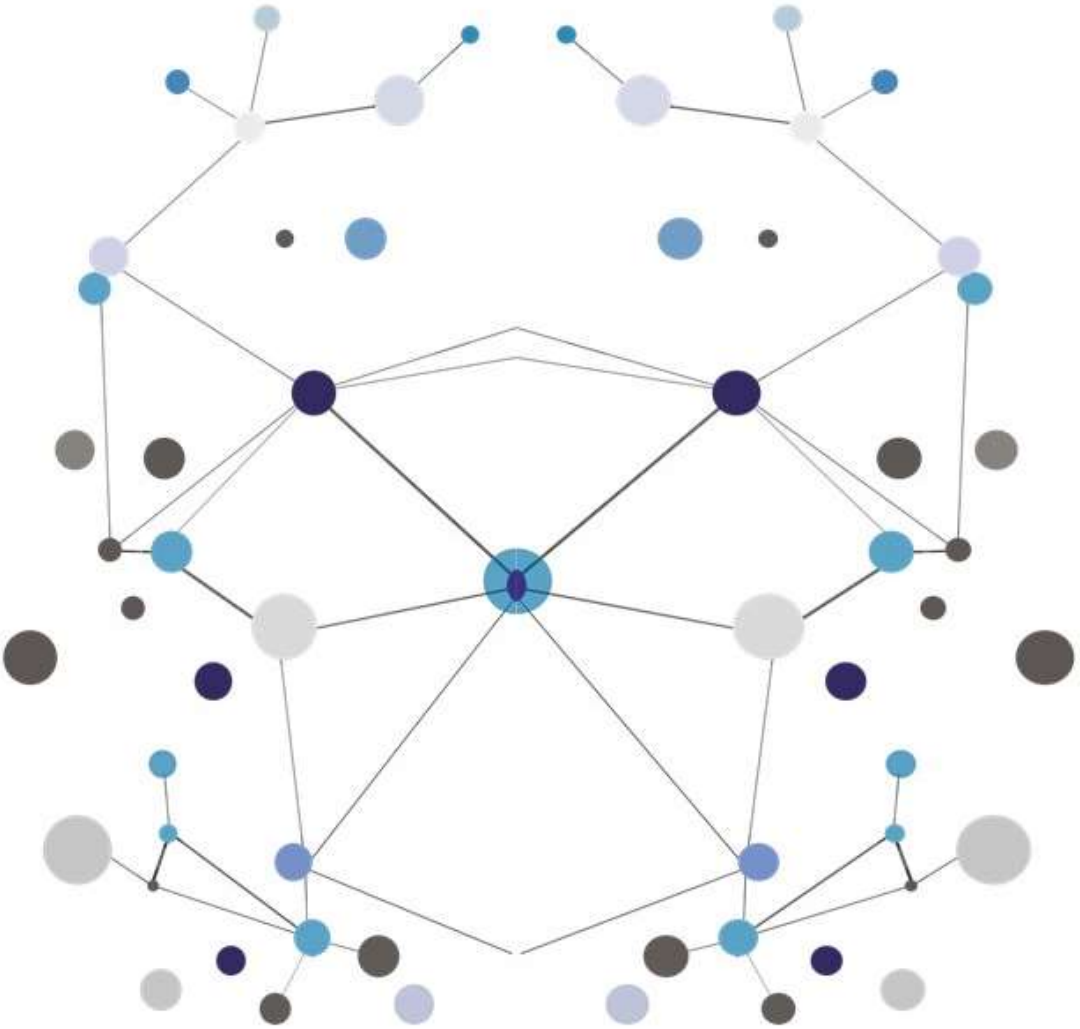


ATRIBUTOS DEL DOCUMENTO			
RESUMEN	Evaluación del proyecto ante un ataque con el fin de encontrar algún riesgo que impida que sea lanzado a producción.		
EMPRESA AUDITORA	SOFTWORLD		
AUTOR(ES)	L. S. C. Salvador Pereyra A	**LICENCIA**	SFTW19902018
PERIODO DE PRUEBAS	17/Junio/2018	**A**	17/Junio/2018
REVISADO/APROVADO	-	**FECHA DE APROBACIÓN**	-

RESULTADOS DEL SITIO: prepcampeche2018.mx

ACTIVIDADES

- **Ataques volumétricos por protocolo TCP**
  - **400 mbps de throughput**
  - **Syn Flood**
- **Ataque Volumétrico por UDP**
  - **400 mbps**
  - **DNS Amplification**
- **Ataque volumétrico por protocolo ICMP**
  - **400 mbps**
  - **ICMP Flood**
- **Ataque en la capa de aplicación HTTP**
  - **Slowloris Attack**

ENTREGABLES	Número de Copias
Informe preliminar de los ataques anteriormente mencionados.	1 de
Información extra:	

17 de jun. de 18

- **Ataque volumétrico por protocolo TCP**
- **Ataque Volumétrico por UDP**
- **Ataque volumétrico por protocolo ICMP**
- **Ataque en la capa de aplicación HTTP**

JUNIO

d	l	m	m	j	v	s
27	28	29	30	31	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30

Contenido

RESUMEN EJECUTIVO

SoftWorld México en colaboración con el **Instituto Tecnológico Superior de Calkiní**, ejecutó un ataque DDoS utilizando diferentes métodos mencionados con anterioridad a la WEB del **Instituto Electoral del Estado de Campeche** identificando debilidades en las configuraciones del software que mantiene operativo los sistemas de información de la organización.

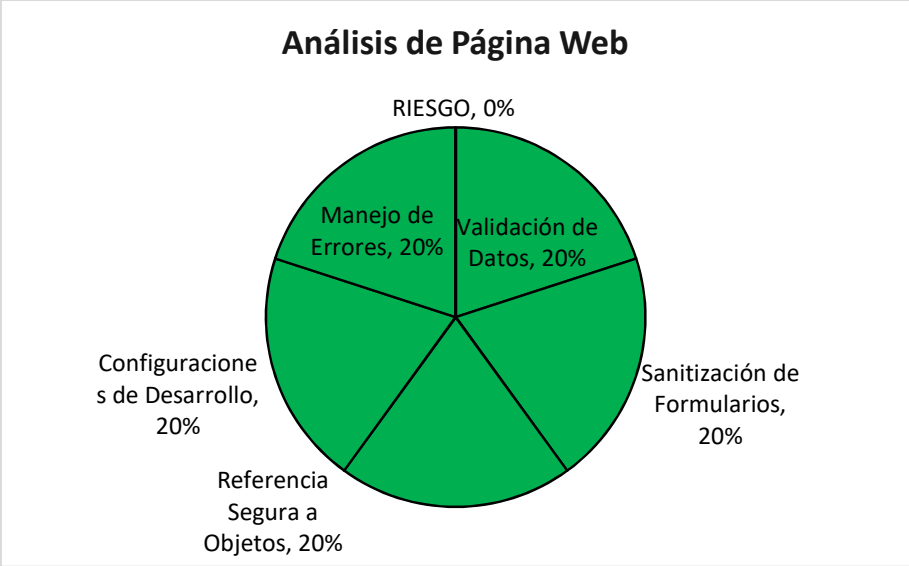
De lo anterior, en esta sección se documenta el resumen ejecutivo en donde se pretende plasmar en una visión holística el nivel de vulnerabilidad, riesgo e impacto a los que **Instituto Electoral del Estado de Campeche** se encuentra expuesta mediante los servicios evaluados y analizados, mismos que se encuentran publicados en Internet.

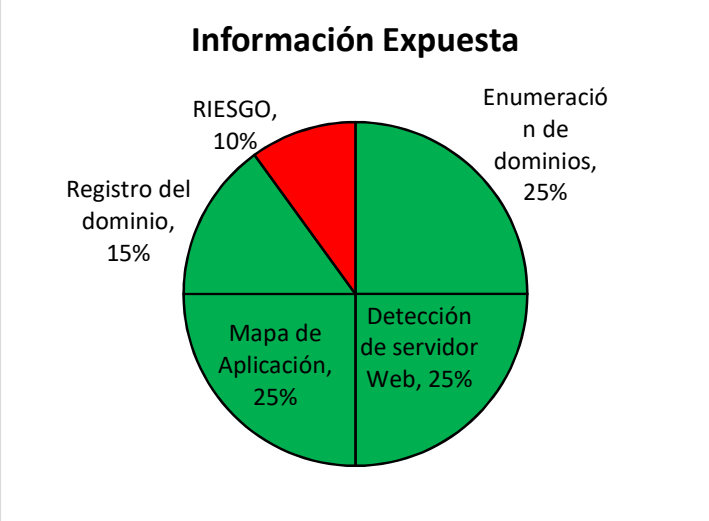
Agradecemos la confianza y la oportunidad que **Instituto Electoral del Estado de Campeche** nos brinda al permitirnos formar parte de tan importante organización posicionándonos como un asesor y socio de negocios en cuanto a servicios de ciber seguridad se refiere. **SoftWorld** tu compañía de ciberseguridad.

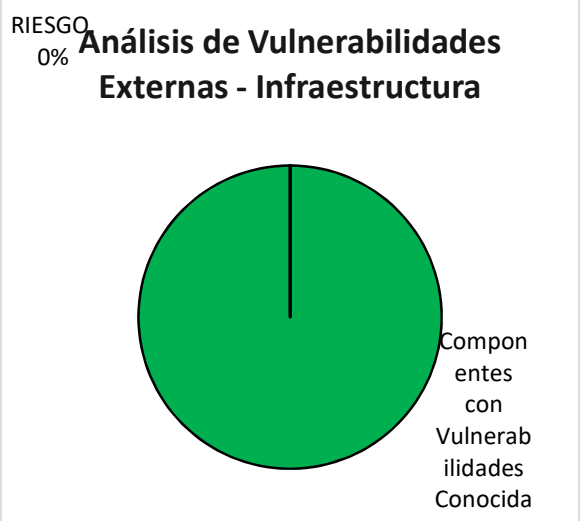
Clasificación de Vulnerabilidades

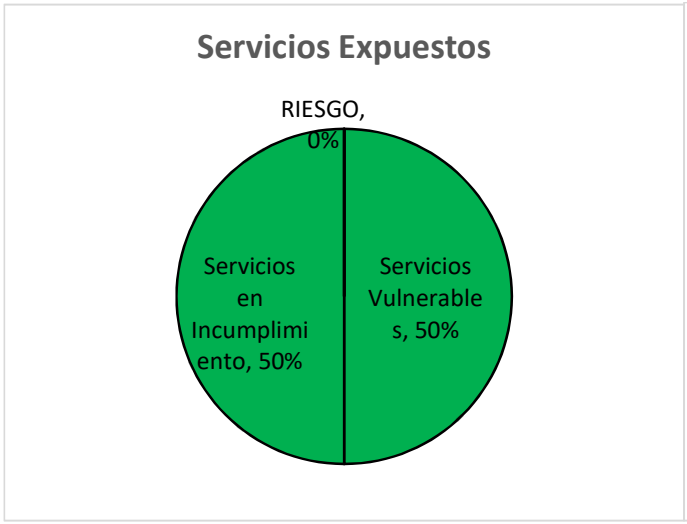
GRAVEDAD	DESCRIPCIÓN
ALTA	Las vulnerabilidades altas proporcionan a los intrusos remotos funcionalidades de root o de administrador. Con estas vulnerabilidades pueden comprometer el sistema por completo proporcionando acceso y ejecución de forma. La presencia de puertas traseras o troyanos también se clasifica como vulnerabilidad urgente.
MEDIA	Las vulnerabilidades de riesgo medio proporcionan acceso a información almacenada en el host, incluyendo configuraciones de seguridad. Algunos ejemplos de vulnerabilidades de riesgo alto son fuga parcial de contenidos, acceso a ciertos ficheros del host, navegación por los directorios, fuga de información de las reglas de filtrado y mecanismos de seguridad, posibilidad de ataques de DoS, y uso no autorizado de los servicios como envío de mail no autorizado.
BAJA	Son aquellas vulnerabilidades con calificación menor a 3.9. son consideradas satisfactorias durante una revisión, sin embargo, se propone a las organizaciones corregir estas vulnerabilidades para minimizar la superficie de riesgo al mínimo. **No requerido**.

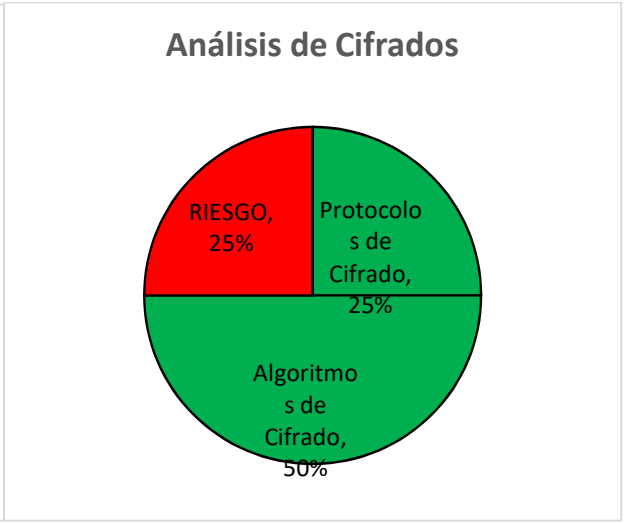
INDICADORES DE SEGURIDAD











ALCANCE

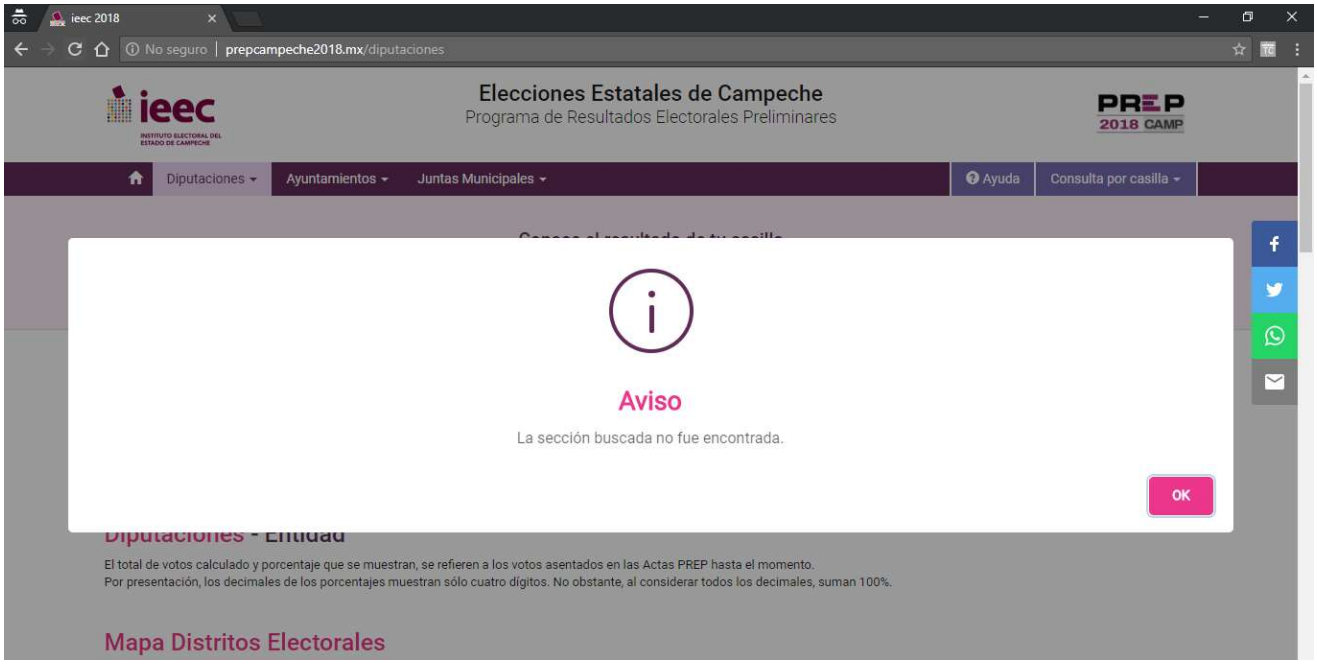
El presente reporte presenta un resumen de las vulnerabilidades identificadas y confirmadas por parte de los auditores del departamento de Seguridad de SoftWorld, en los sitios y aplicaciones Web evaluados y analizados, mismas que tuvieron por alcance las siguientes direcciones URL:

Sitio Web Auditado	IP
prepcampeche2018.mx	**104.20.93.168**

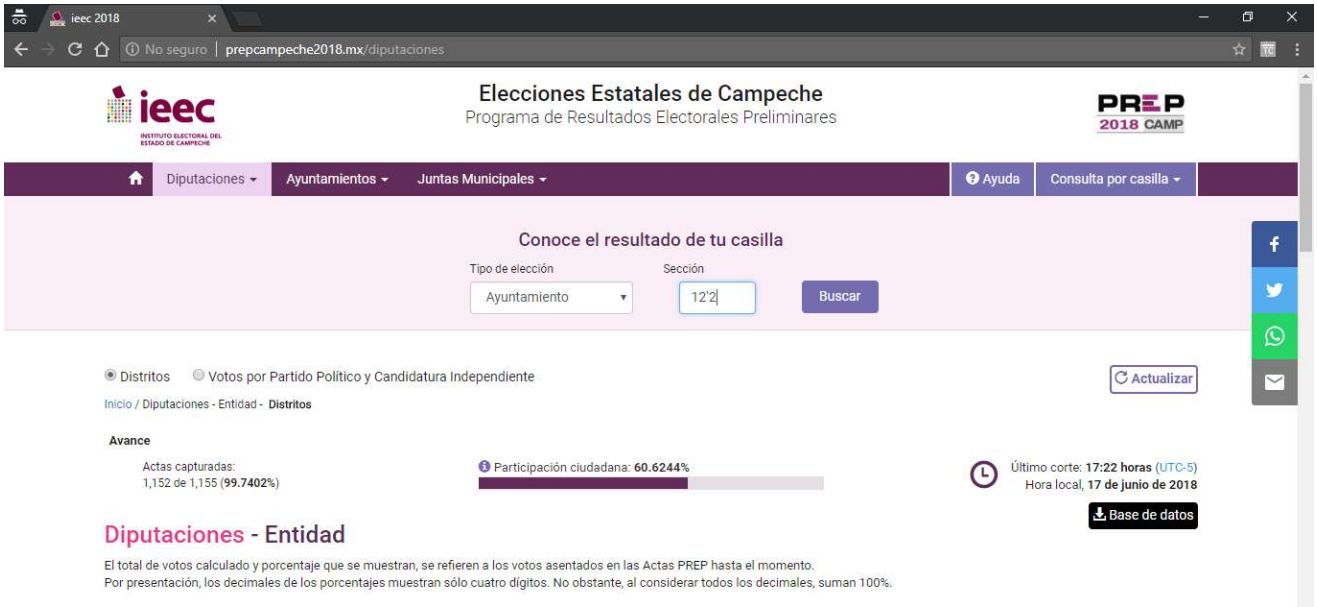
RESULTADO DE LAS PRUEBAS

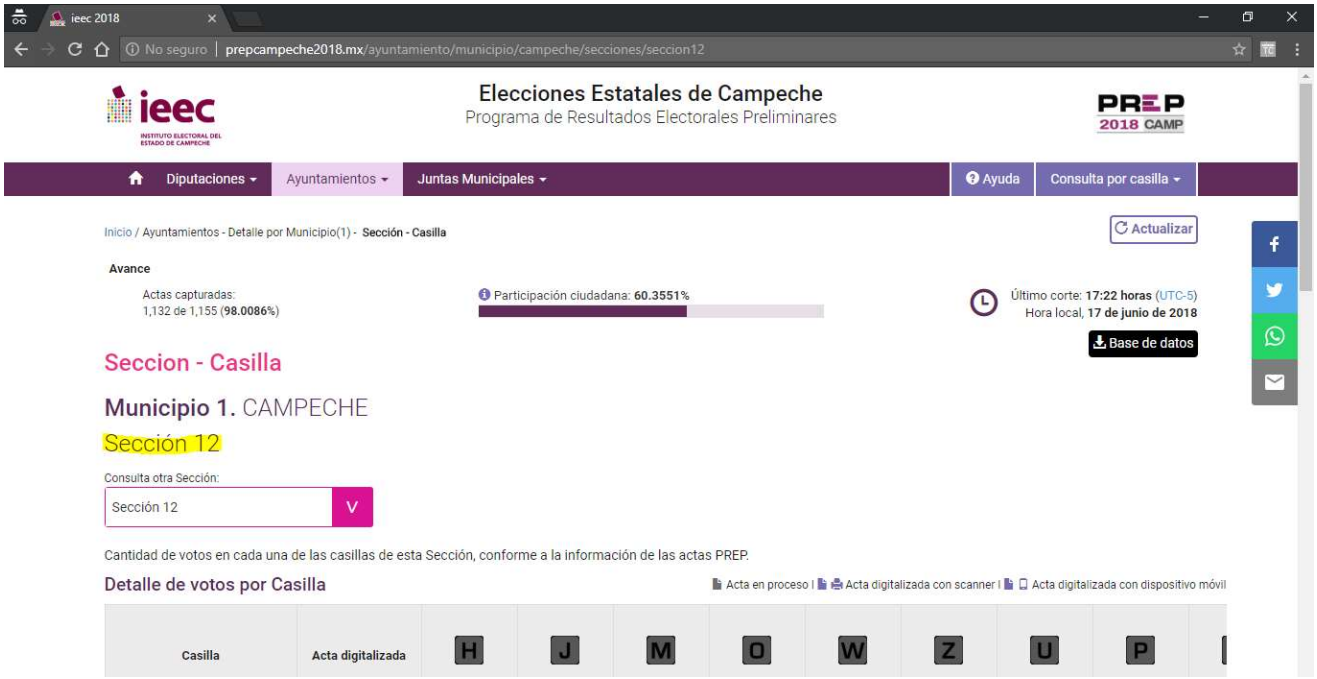
Análisis de Página Web

Validación de Datos – Sin Riesgo

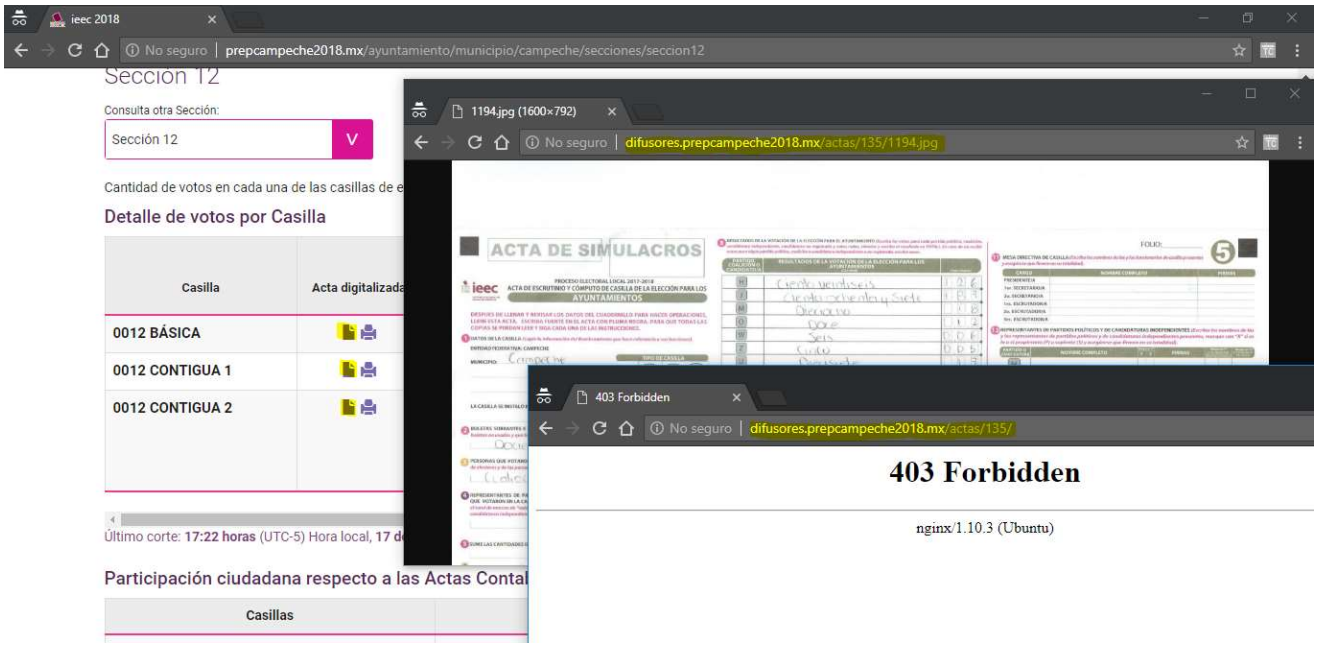


Sanitización de Formularios – Sin Riesgo

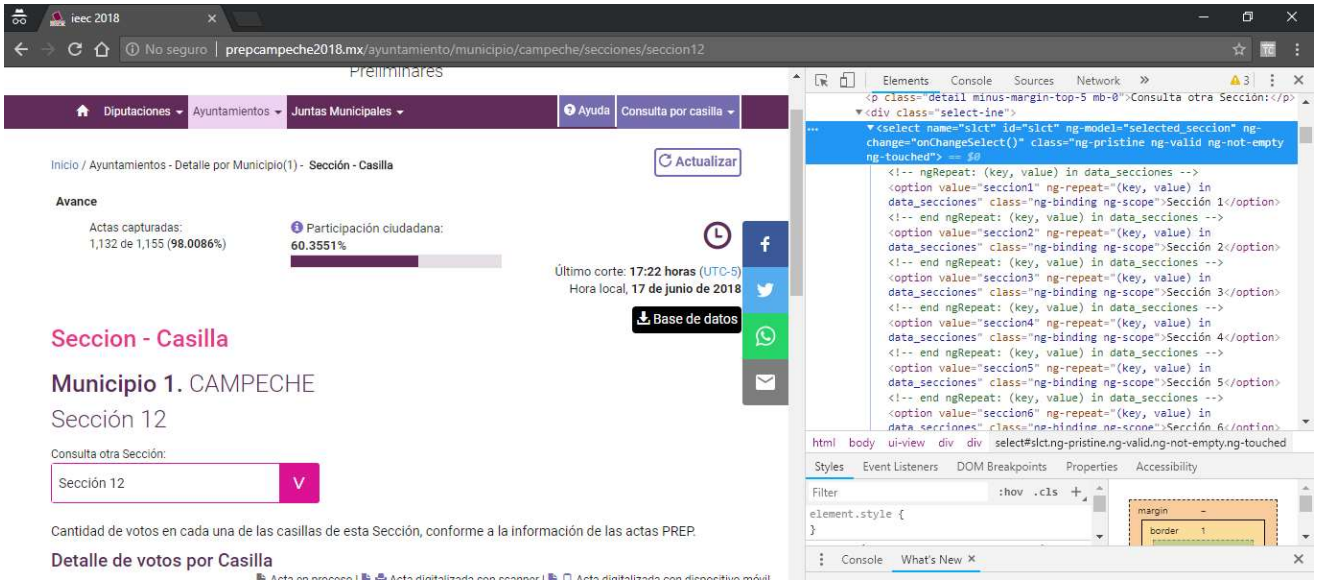




Referencia Segura a Objetos – Sin Riesgo



Configuraciones de Desarrollo – Sin Riesgo



Manejo de Errores – Sin Riesgo

Análisis de Vulnerabilidades Externas – Infraestructura

Componentes con Vulnerabilidades Conocidas – Sin Riesgo

104.20.93.168

Summary

Critical	High	Medium	Low	Info	Total
0	0	3	0	19	22

Details

Severity	Plugin Id	Name
Medium (6.4)	51192	SSL Certificate Cannot Be Trusted
Medium (5.0)	35291	SSL Certificate Signed Using Weak Hashing Algorithm
Medium (5.0)	42873	SSL Medium Strength Cipher Suites Supported
Info	10107	HTTP Server Type and Version
Info	10287	Traceroute Information
Info	10863	SSL Certificate Information
Info	11219	Nessus SYN scanner
Info	19506	Nessus Scan Information
Info	21643	SSL Cipher Suites Supported
Info	22964	Service Detection
Info	24260	HyperText Transfer Protocol (HTTP) Information
Info	46180	Additional DNS Hostnames

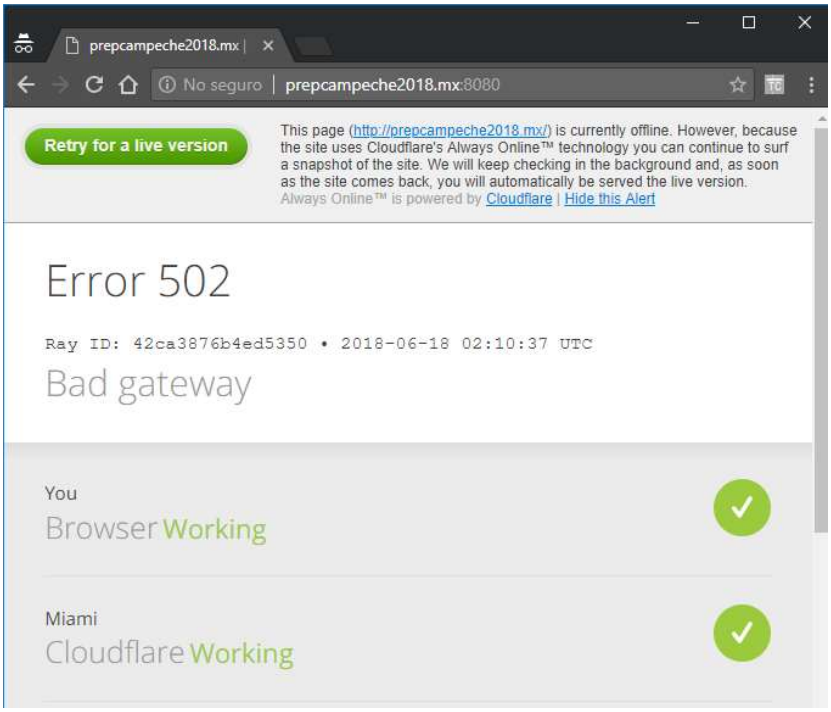
Servicios Expuestos

Servicios Vulnerables – Sin Riesgo

Puertos y Servicios Abiertos desde internet:

80/tcp open http Cloudflare nginx
443/tcp open ssl/https cloudflare
2052/tcp open http Cloudflare nginx
2053/tcp open ssl/http nginx
2082/tcp open http Cloudflare nginx
2086/tcp open http Cloudflare nginx
2087/tcp open ssl/http nginx
2095/tcp open http Cloudflare nginx
2096/tcp open ssl/http nginx
8080/tcp open http Cloudflare nginx
8443/tcp open ssl/https-alt cloudflare
8880/tcp open http Cloudflare nginx

```
2086/tcp open  http          Cloudflare nginx
|_http-server-header: cloudflare-nginx
2087/tcp open  ssl/http      nginx
|_http-server-header: cloudflare
|_http-title: 400 The plain HTTP request was sent to HTTPS port
| ssl-cert: Subject: commonName=ssl877068.cloudflaressl.com
| Subject Alternative Name: DNS:ssl877068.cloudflaressl.com, DNS:*.
| Issuer: commonName=COMODO ECC Domain Validation Secure Server CA
| Public Key type: unknown
| Public Key bits: 256
| Signature Algorithm: ecdsa-with-SHA256
| Not valid before: 2018-06-13T00:00:00
| Not valid after:  2019-03-10T23:59:59
| MD5:   83b4 b81a 49d4 f8fd 8127 098a 6832 5920
|_SHA-1: 2a22 79a6 8c34 3d04 b96f 464c 8a2b 6bc4 1cef 2ce1
|_ssl-date: 2018-06-18T03:35:44+00:00; +10s from scanner time.
| tls-nextprotoneg:
|   h2
|_  http/1.1
2095/tcp open  http          Cloudflare nginx
|_http-server-header: cloudflare-nginx
2096/tcp open  ssl/http      nginx
|_http-server-header: cloudflare
|_http-title: 400 The plain HTTP request was sent to HTTPS port
| ssl-cert: Subject: commonName=ssl877068.cloudflaressl.com
| Subject Alternative Name: DNS:ssl877068.cloudflaressl.com, DNS:*.
| Issuer: commonName=COMODO ECC Domain Validation Secure Server CA
| Public Key type: unknown
| Public Key bits: 256
| Signature Algorithm: ecdsa-with-SHA256
| Not valid before: 2018-06-13T00:00:00
```

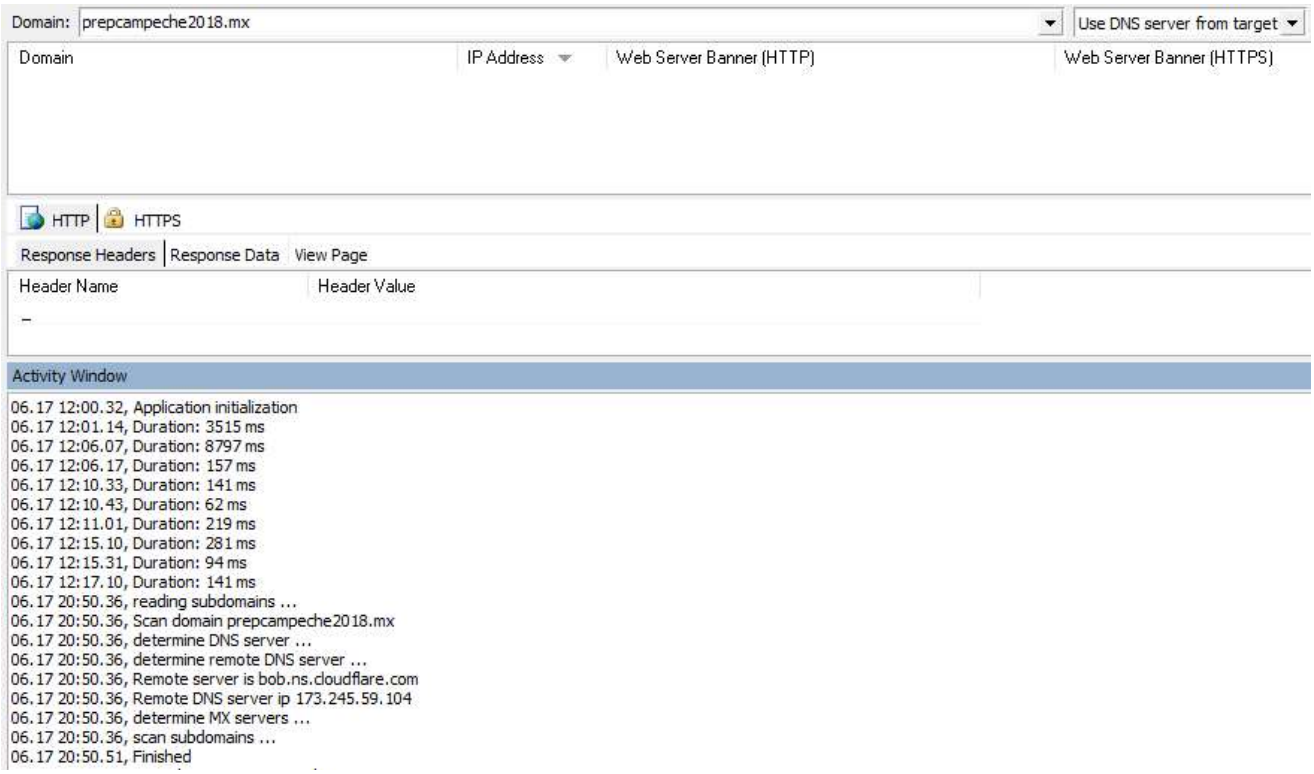


Servicios en Incumplimiento – Sin Riesgo

Cabe resultar que los servicios expuestos a internet no suponen ningún riesgo para el sitio web o el servidor en él.

Información Expuesta

Enumeración de dominios – Sin Riesgo



Detección de servidor Web – Sin Riesgo

Mapa de Aplicación – Sin Riesgo

Método	URI
GET	http://prepcampeche2018.mx
GET	http://prepcampeche2018.mx/robots.txt
GET	http://prepcampeche2018.mx/sitemap.xml
GET	https://www.facebook.com/sharer/sharer.php?quote=%7B%7Btitle%7D%7D&u=...
GET	https://twitter.com/intent/tweet?source=%7B%7Burl%7D%7D&text=%7B%7Btitle...
GET	http://prepcampeche2018.mx/cdn-cgi/l/email-protection
GET	http://prepcampeche2018.mx/%7B%7Bople_link%7D%7D
GET	http://prepcampeche2018.mx/
GET	http://prepcampeche2018.mx/ayuda/lista_nominal
GET	http://prepcampeche2018.mx/src/favicon.png
GET	http://prepcampeche2018.mx/bower_components/bootstrap/dist/css/bootstrap....
GET	http://prepcampeche2018.mx/css/styles.min.css
GET	http://prepcampeche2018.mx/css/responsive.min.css
GET	http://prepcampeche2018.mx/js/highcharts/css/highcharts.css
GET	http://prepcampeche2018.mx/config.js
GET	http://prepcampeche2018.mx/cdn-cgi/scripts/f2bf09f8/cloudflare-static/email-dec...
GET	http://prepcampeche2018.mx/bower_components/moment/min/moment-with-lo...
GET	http://prepcampeche2018.mx/bower_components/jquery/dist/jquery.min.js
GET	http://prepcampeche2018.mx/bower_components/angular/angular.min.js
GET	http://prepcampeche2018.mx/bower_components/angular-cookies/angular-cook...
GET	http://prepcampeche2018.mx/bower_components/angular-route/angular-route.js

Registro del dominio – Sin Riesgo

Domain Name: prepcampeche2018.mx

Created On: 2018-03-05
Expiration Date: 2019-03-05
Last Updated On: 2018-06-11
Registrar: Akky (Una division de NIC Mexico)
URL: http://www.akky.mx
Whois TCP URI: whois.akky.mx
Whois Web URL: http://www.akky.mx/jsf/whois/whois.jsf

Registrant:
Name: Grupo Proisi, SA de CV
City: Saltillo
State: Coahuila
Country: Mexico

Administrative Contact:
Name: Guillermo Dewey Guerra
City: Santa Catarina
State: Nuevo Leon
Country: Mexico

Technical Contact:
Name: Guillermo Dewey Guerra
City: Santa Catarina
State: Nuevo Leon
Country: Mexico

Billing Contact:
Name: Guillermo Dewey Guerra
City: Santa Catarina
State: Nuevo Leon
Country: Mexico

Name Servers:
DNS: bob.ns.cloudflare.com
DNS: dina.ns.cloudflare.com

DNSSEC DS Records:

Análisis de Cifrados

Protocolos de Cifrado – Sin Riesgo

SERVER PREFERRED CIPHER SUITES

Preferred cipher suite for each protocol supported (except SSLv2). Expected configuration are ciphers allowed by PCI DSS and enabling PFS:

TLSv1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLSv1.1	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
TLSv1.2	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 - TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256

```
Other addresses for prepcampeche2018.mx (not scanned): 2400:cb00:2048:1::6814:5ca8 2400:cb00:2048:1::6814:5da8 104.20.92.168
Not shown: 996 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
443/tcp  open  https
| ssl-enum-ciphers:
|   TLSv1.0:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_3DES_EDE_CBC_SHA (rsa 2048) - C
|     compressors:
|       NULL
|     cipher preference: server
|     warnings:
|       64-bit block cipher 3DES vulnerable to SWEET32 attack
|   TLSv1.1:
|     ciphers:
|       TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_128_CBC_SHA (rsa 2048) - A
|       TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|       TLS_RSA_WITH_AES_256_CBC_SHA (rsa 2048) - A
|     compressors:
|       NULL
|     cipher preference: server
|   TLSv1.2:
|     ciphers:
|       TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 - unknown
|       TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 - unknown
|       TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256-draft - unknown
|       TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 - unknown
|       TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 - unknown
|       TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 - unknown
|       TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (rsa 2048) - A
|       TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (rsa 2048) - A
|       TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256-draft (rsa 2048) - A
```

Algoritmos de Cifrado – Sin Riesgo

TLSV1.0

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_RSA_WITH_AES_128_CBC_SHA	Good configuration
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_RSA_WITH_AES_256_CBC_SHA	Good configuration
TLS_RSA_WITH_3DES_EDE_CBC_SHA	Non-compliant with HIPAA guidance

Los cifrados DES y 3DES son algoritmos de cifrados débiles susceptibles a ataques como SWEET32.

RECOMENDACIONES

- ✓ Contar con una página personalizada de errores mandando redireccionamiento al sitio de inicio.
- ✓ Deshabilitar el protocolo de cifrado TLS 1.0.
- ✓ Deshabilitar los algoritmos de cifrados DES y 3DES.
- ✓ Hacer uso de una comunicación cifrada (HTTPS) el sitio tiene problemas al conectarse con la base de datos origen. Es posible que la Base de Datos deba actualizarse e instalar el .Net Framework a la última versión (4.7).