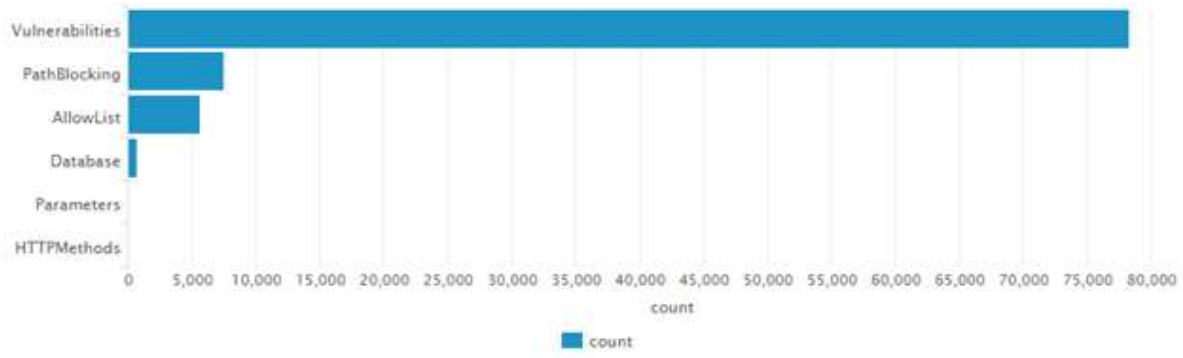
REPORTE DE INCIDENCIA DE GLESEC

TLP-AMBAR

Organización	Metrobank, S.A
Fecha	18/12/2018
Servicio	MSS-VM
Nivel de Severidad	Alto
Nivel de Impacto	Alto
Nivel de Vulnerabilidad	Alto

La información que se presenta a continuación representa los ataques detenidos, sin embargo, GLESEC como su proveedor de ciberseguridad, sentimos la necesidad de informarle el aumento de ataques a nivel aplicativo y de un posible ataque dirigido como se muestra en la página 4 de este documento.

Nuestro Centro de Operaciones ha detectado que durante los últimos 7 días hubo un incremento importante en la cantidad de ataques críticos reportados, se muestran 91,964 ataques.



Values	Count	%
190.34.183.138	91,964	100%

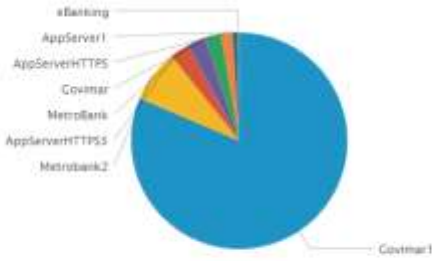
Gráfica 1 – Cantidad de ataques por categoría
En esta gráfica se muestra la cantidad de ataques registrados por categoría.

REPORTE DE INCIDENCIA DE GLESEC

TLP-AMBAR

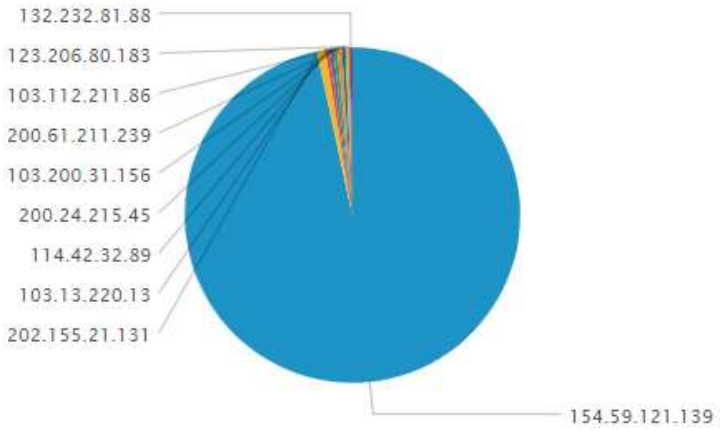
Todos estos ataques a nivel aplicativos van dirigidos a las siguientes webApp.

Gráfica 2.



WebApp	count
Covimar1	74879
Metrobank2	7204
AppServerHTTPS3	3684
MetroBank	3468
Covimar	2308
AppServerHTTPS	1568
AppServer1	792
eBanking	163

En la siguiente grafica puede visualizar las fuentes de ataques más persistentes



REPORTE DE INCIDENCIA DE GLESEC

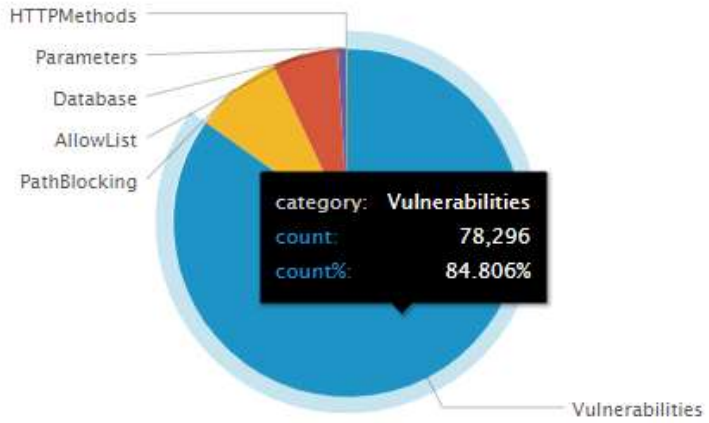
TLP-AMBAR

Este aumento de ataques críticos se enmarca, considerablemente, en la categoría ***Vulnerabilities*** de *Radware*, donde sólo esta categoría representa el 84.8%.

Nota: ***La categoría Vulnerabilidades del dispositivo AppWall se describe como "la comprobación, en las solicitudes, de patrones de vulnerabilidad conocidos basados en un conjunto determinista de reglas que generan un evento cuando se detecta un patrón de vulnerabilidad", según Radware.***

El total de categorías registradas se muestran a continuación:

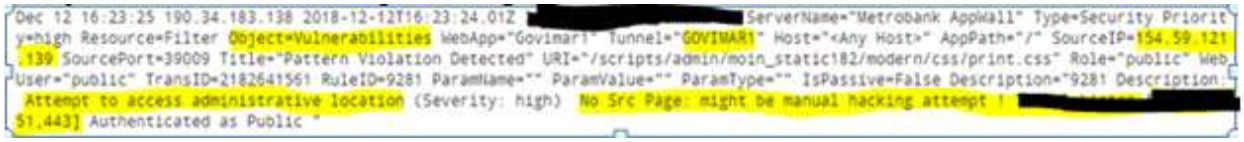
Gráfica 3 – Categorías de vulnerabilidades
En esta gráfica se muestran las categorías de los ataques críticos recibidos.



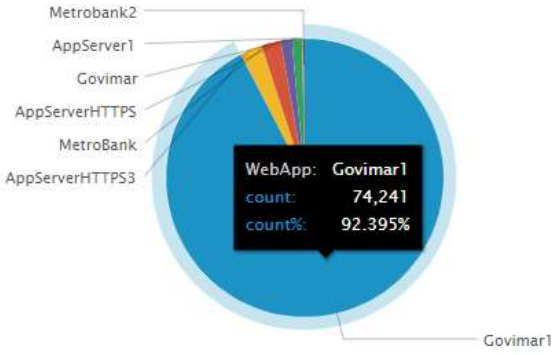
REPORTE DE INCIDENCIA DE GLESEC

TLP-AMBAR

Gráfica 4 – Evento registrado raw data
La gran mayoría de todos estos ataques (87%) proviene de la dirección IP 154.59.121.139 la cual está identificada como una amenaza para su organización



Gráfica 5 – Proporción de ataques con respecto a túneles o webapps.



La gran mayoría de todos estos ataques (87%) provienen de la dirección IP 154.59.121.139, la cual está identificada como una amenaza para su organización.

De los ataques provenientes de la dirección IP mencionada anteriormente, la mayoría fueron dirigidos a las siguientes WebApps: Govimar1 (92%), AppServerHTTPS3 (3%) y MetroBank (2%).

El día 12 de diciembre se reportó la mayor cantidad de ataques críticos detenidos por el dispositivo AppWall (85,980).

REPORTE DE INCIDENCIA DE GLESEC

TLP-AMBAR

A continuación, se presenta una tabla de los sistemas críticos de su organización, tal y como fue provisto por ustedes. Esto con el motivo de recalcar que estos sistemas presentan vulnerabilidades.

Server or App	Type of System	IP address	Comments
SERVER	WINDOWS	190.34.183.131	WEB GOVIMAR
SERVER	WINDOWS	190.34.183.152	WEB METROBANK
SERVER	WINDOWS	190.34.183.139	APP SERVER
SERVER	WINDOWS	190.34.183.148	MAIL – DISPOSITIVO DE SEGURIDAD
SERVER	WINDOWS	190.34.183.149	EXCHANGE
SERVER	WINDOWS	190.34.183.154	EBANKING IBM

Vulnerabilidades de severidad alta, las cuales están relacionadas con el hecho de que el sistema objetivo permite conexiones débiles a través de SSLv2, SSLv3 y TLS 1.0 con suites de cifrados medios y/o débiles. La versión de protocolo conocido como seguro (hasta el momento) es TLS 1.2 en adelante. Existen diferentes tipos de *exploits* publicados en Internet para realizar ataques a estas versiones antiguas y obsoletas de este protocolo lo cual representa un alto riesgo.

De las vulnerabilidades de severidad alta encontradas en los sistemas que se muestran anteriormente podemos resaltar:

EXCHANGE

SSL 2.0, SSL 3.0 y TLS 1.0 con suites de cifrados débiles y medios permitidos. No soporta conexiones a través de TLS 1.2 en algunos casos

REPORTE DE INCIDENCIA DE GLESEC

TLP-AMBAR

.

A continuación se muestran los resultados de lo mencionado anteriormente.
Lo resaltado en amarillo representa los protocolos y las suites de cifrados que son permitidos y vulnerables en el servidor. Entre los resultados se puede observar que hay llaves de cifrado de una longitud corta (por ejemplo 40 y 56 bits), se ha demostrado que el uso de llaves cortas le facilita al atacante poder explotar las vulnerabilidades presentes en los protocolos.

Es conocido que SSL V2 y 3 son protocolos vulnerables. Desde abril 2015 está recomendado su deshabilitarlo.
Referencia: ***https://www.pcisecuritystandards.org/documents/Migrating-from-SSL-Early-TLS-Info-Supp-v1_1.pdf?hsCtaTracking=1e14979b-2625-4998-8bd9-ffc64b1e8639%7Cc1f68dab-de90-4f48-befb-3c15d520a19a%20Hace%202%20minutos***

En esta página de referencia, en la sección “What is the risk” de la página 2, se detallan los riesgos de utilizar protocolos no seguros como SSLv2 y v3.

```
Connected to 190.34.183.149

Testing SSL server 190.34.183.149 on port 443 using SNI name 190.34.183.149

  TLS Fallback SCSV:
Server only supports TLSv1.0

  TLS renegotiation:
Secure session renegotiation supported

  TLS Compression:
Compression disabled

  Heartbleed:
TLS 1.2 not vulnerable to heartbleed
TLS 1.1 not vulnerable to heartbleed
TLS 1.0 not vulnerable to heartbleed

  Supported Server Cipher(s):
Preferred TLSv1.0  256 bits  ECDHE-RSA-AES256-SHA          Curve P-256 DHE 256
Accepted  TLSv1.0  128 bits  ECDHE-RSA-AES128-SHA          Curve P-256 DHE 256
Accepted  TLSv1.0  256 bits  AES256-SHA
Accepted  TLSv1.0  128 bits  AES128-SHA
Accepted  TLSv1.0  112 bits  DES-CBC3-SHA
Accepted  TLSv1.0  128 bits  RC4-SHA
Accepted  TLSv1.0  128 bits  RC4-MD5
Preferred SSLv3    112 bits  DES-CBC3-SHA
Accepted  SSLv3    128 bits  RC4-SHA
Accepted  SSLv3    128 bits  RC4-MD5
Preferred SSLv2    128 bits  RC4-MD5
Accepted  SSLv2    112 bits  DES-CBC3-MD5

  SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength:    2048

Subject:  mail.metrobanksa.com
Altnames: DNS:mail.metrobanksa.com
Issuer:   GlobalSign Organization Validation CA - SHA256 - G2

Not valid before: Feb 19 22:16:01 2018 GMT
Not valid after:  Feb 20 22:16:01 2019 GMT
```

EBANKING IBM

SSL 3.0, TLS 1.0 y TLS 1.1 con suites de cifrados débiles y medios permitidos.

REPORTE DE INCIDENCIA DE GLESEC

TLP-AMBAR

```
Connected to 190.34.183.154

Testing SSL server 190.34.183.154 on port 443 using SNI name 190.34.183.154

  TLS Fallback SCSV:
Server does not support TLS Fallback SCSV

  TLS renegotiation:
Secure session renegotiation supported

  TLS Compression:
Compression disabled

  Heartbleed:
TLS 1.2 not vulnerable to heartbleed
TLS 1.1 not vulnerable to heartbleed
TLS 1.0 not vulnerable to heartbleed

  Supported Server Cipher(s):
```

Accepted	TLSv1.2	128 bits	ECDHE-RSA-RC4-SHA	Curve P-256 DHE 256
Accepted	TLSv1.2	128 bits	AECDH-RC4-SHA	Curve P-256 DHE 256
Accepted	TLSv1.2	128 bits	RC4-SHA	
Accepted	TLSv1.2	128 bits	RC4-MD5	
Accepted	TLSv1.2	112 bits	ECDHE-RSA-DES-CBC3-SHA	Curve P-256 DHE 256
Accepted	TLSv1.2	112 bits	EDH-RSA-DES-CBC3-SHA	DHE 1024 bits
Accepted	TLSv1.2	112 bits	AECDH-DES-CBC3-SHA	Curve P-256 DHE 256
Accepted	TLSv1.2	112 bits	DES-CBC3-SHA	
Accepted	TLSv1.2	56 bits	EDH-RSA-DES-CBC-SHA	DHE 1024 bits
Accepted	TLSv1.2	56 bits	DES-CBC-SHA	
Accepted	TLSv1.2	40 bits	EXP-EDH-RSA-DES-CBC-SHA	DHE 512 bits
Accepted	TLSv1.2	40 bits	EXP-DES-CBC-SHA	RSA 512 bits
Accepted	TLSv1.2	40 bits	EXP-RC2-CBC-MD5	RSA 512 bits
Accepted	TLSv1.2	40 bits	EXP-RC4-MD5	RSA 512 bits
Preferred	TLSv1.1	256 bits	ECDHE-RSA-AES256-SHA	Curve P-256 DHE 256
Accepted	TLSv1.1	256 bits	DHE-RSA-AES256-SHA	DHE 1024 bits
Accepted	TLSv1.1	256 bits	DHE-RSA-CAMELLIA256-SHA	DHE 1024 bits
Accepted	TLSv1.1	256 bits	AECDH-AES256-SHA	Curve P-256 DHE 256
Accepted	TLSv1.1	256 bits	AES256-SHA	
Accepted	TLSv1.1	256 bits	CAMELLIA256-SHA	
Accepted	TLSv1.1	128 bits	ECDHE-RSA-AES128-SHA	Curve P-256 DHE 256
Accepted	TLSv1.1	128 bits	DHE-RSA-AES128-SHA	DHE 1024 bits
Accepted	TLSv1.1	128 bits	DHE-RSA-SEED-SHA	DHE 1024 bits
Accepted	TLSv1.1	128 bits	DHE-RSA-CAMELLIA128-SHA	DHE 1024 bits
Accepted	TLSv1.1	128 bits	AECDH-AES128-SHA	Curve P-256 DHE 256
Accepted	TLSv1.1	128 bits	AES128-SHA	
Accepted	TLSv1.1	128 bits	SEED-SHA	
Accepted	TLSv1.1	128 bits	CAMELLIA128-SHA	
Accepted	TLSv1.1	128 bits	IDEA-CBC-SHA	
Accepted	TLSv1.1	128 bits	ECDHE-RSA-RC4-SHA	Curve P-256 DHE 256
Accepted	TLSv1.1	128 bits	AECDH-RC4-SHA	Curve P-256 DHE 256
Accepted	TLSv1.1	128 bits	RC4-SHA	
Accepted	TLSv1.1	128 bits	RC4-MD5	
Accepted	TLSv1.1	112 bits	ECDHE-RSA-DES-CBC3-SHA	Curve P-256 DHE 256
Accepted	TLSv1.1	112 bits	EDH-RSA-DES-CBC3-SHA	DHE 1024 bits
Accepted	TLSv1.1	112 bits	AECDH-DES-CBC3-SHA	Curve P-256 DHE 256
Accepted	TLSv1.1	112 bits	DES-CBC3-SHA	
Accepted	TLSv1.1	56 bits	EDH-RSA-DES-CBC-SHA	DHE 1024 bits
Accepted	TLSv1.1	56 bits	DES-CBC-SHA	

REPORTE DE INCIDENCIA DE GLESEC

TLP-AMBAR

```
Accepted  TLSv1.0  128 bits  RC4-SHA
Accepted  TLSv1.0  128 bits  RC4-MD5
Accepted  TLSv1.0  112 bits  ECDHE-RSA-DES-CBC3-SHA          Curve P-256 DHE 256
Accepted  TLSv1.0  112 bits  EDH-RSA-DES-CBC3-SHA           DHE 1024 bits
Accepted  TLSv1.0  112 bits  AECDH-DES-CBC3-SHA             Curve P-256 DHE 256
Accepted  TLSv1.0  112 bits  DES-CBC3-SHA
Accepted  TLSv1.0  56 bits   EDH-RSA-DES-CBC-SHA            DHE 1024 bits
Accepted  TLSv1.0  56 bits   DES-CBC-SHA
Accepted  TLSv1.0  40 bits   EXP-EDH-RSA-DES-CBC-SHA        DHE 512 bits
Accepted  TLSv1.0  40 bits   EXP-DES-CBC-SHA                RSA 512 bits
Accepted  TLSv1.0  40 bits   EXP-RC2-CBC-MD5                RSA 512 bits
Accepted  TLSv1.0  40 bits   EXP-RC4-MD5                    RSA 512 bits
Preferred SSLv3    256 bits  ECDHE-RSA-AES256-SHA           Curve P-256 DHE 256
Accepted  SSLv3    256 bits  DHE-RSA-AES256-SHA             DHE 1024 bits
Accepted  SSLv3    256 bits  DHE-RSA-CAMELLIA256-SHA        DHE 1024 bits
Accepted  SSLv3    256 bits  AECDH-AES256-SHA               Curve P-256 DHE 256
Accepted  SSLv3    256 bits  AES256-SHA
Accepted  SSLv3    256 bits  CAMELLIA256-SHA
Accepted  SSLv3    128 bits  ECDHE-RSA-AES128-SHA           Curve P-256 DHE 256
Accepted  SSLv3    128 bits  DHE-RSA-AES128-SHA             DHE 1024 bits
Accepted  SSLv3    128 bits  DHE-RSA-SEED-SHA               DHE 1024 bits
Accepted  SSLv3    128 bits  DHE-RSA-CAMELLIA128-SHA        DHE 1024 bits
Accepted  SSLv3    128 bits  AECDH-AES128-SHA               Curve P-256 DHE 256
Accepted  SSLv3    128 bits  AES128-SHA
Accepted  SSLv3    128 bits  SEED-SHA
Accepted  SSLv3    128 bits  CAMELLIA128-SHA
Accepted  SSLv3    128 bits  IDEA-CBC-SHA
Accepted  SSLv3    128 bits  ECDHE-RSA-RC4-SHA              Curve P-256 DHE 256
Accepted  SSLv3    128 bits  AECDH-RC4-SHA                  Curve P-256 DHE 256
Accepted  SSLv3    128 bits  RC4-SHA
Accepted  SSLv3    128 bits  RC4-MD5
Accepted  SSLv3    112 bits  ECDHE-RSA-DES-CBC3-SHA         Curve P-256 DHE 256
Accepted  SSLv3    112 bits  EDH-RSA-DES-CBC3-SHA           DHE 1024 bits
Accepted  SSLv3    112 bits  AECDH-DES-CBC3-SHA             Curve P-256 DHE 256
Accepted  SSLv3    112 bits  DES-CBC3-SHA
Accepted  SSLv3    56 bits   EDH-RSA-DES-CBC-SHA            DHE 1024 bits
Accepted  SSLv3    56 bits   DES-CBC-SHA
Accepted  SSLv3    40 bits   EXP-EDH-RSA-DES-CBC-SHA        DHE 512 bits
Accepted  SSLv3    40 bits   EXP-DES-CBC-SHA                RSA 512 bits
Accepted  SSLv3    40 bits   EXP-RC2-CBC-MD5                RSA 512 bits
Accepted  SSLv3    40 bits   EXP-RC4-MD5                    RSA 512 bits

  SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength:    2048

Subject:  metronet.metrobanksa.com
Altnames: DNS:metronet.metrobanksa.com, DNS:www.metronet.metrobanksa.com
Issuer:   COMODO RSA Domain Validation Secure Server CA

Not valid before: Jan 10 00:00:00 2018 GMT
Not valid after:  Jan 10 23:59:59 2019 GMT
```

APPSERVER

SSL 2.0, SSL 3.0, TLS 1.0 y TLS 1.1 con suites de cifrados débiles y medios permitidos.

```
Connected to 190.34.183.139

Testing SSL server 190.34.183.139 on port 443 using SNI name 190.34.183.139

  TLS Fallback SCSV:
Server does not support TLS Fallback SCSV

  TLS renegotiation:
Secure session renegotiation supported

  TLS Compression:
Compression disabled
```

REPORTE DE INCIDENCIA DE GLESEC

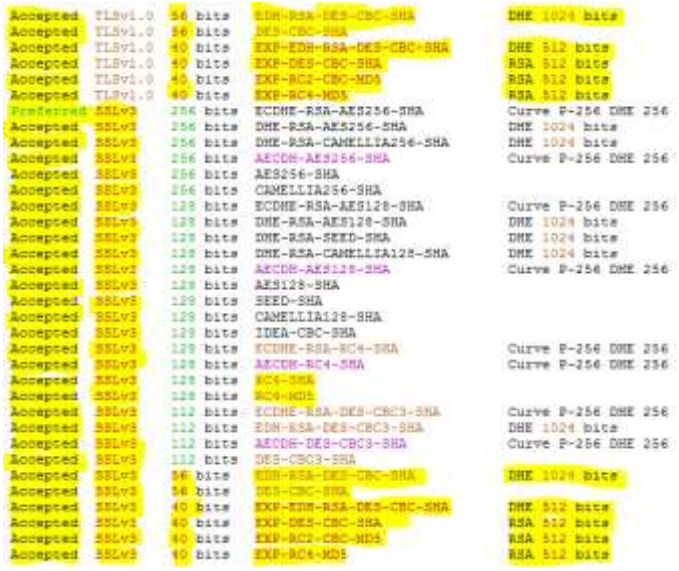
TLP-AMBAR

```
  Supported Server Cipher(s):
Preferred TLSv1.2  256 bits  ECDHE-RSA-AES256-GCM-SHA384   Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA384       Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  ECDHE-RSA-AES256-SHA          Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  DHE-RSA-AES256-GCM-SHA384     DHE 1024 bits
Accepted  TLSv1.2  256 bits  DHE-RSA-AES256-SHA256         DHE 1024 bits
Accepted  TLSv1.2  256 bits  DHE-RSA-AES256-SHA            DHE 1024 bits
Accepted  TLSv1.2  256 bits  DHE-RSA-CAMELLIA256-SHA       DHE 1024 bits
Accepted  TLSv1.2  256 bits  AECDH-AES256-SHA              Curve P-256 DHE 256
Accepted  TLSv1.2  256 bits  AES256-GCM-SHA384
Accepted  TLSv1.2  256 bits  AES256-SHA256
Accepted  TLSv1.2  256 bits  AES256-SHA
Accepted  TLSv1.2  256 bits  CAMELLIA256-SHA
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-GCM-SHA256   Curve P-256 DHE 256
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-SHA256       Curve P-256 DHE 256
Accepted  TLSv1.2  128 bits  ECDHE-RSA-AES128-SHA          Curve P-256 DHE 256
Accepted  TLSv1.2  128 bits  DHE-RSA-AES128-GCM-SHA256     DHE 1024 bits
Accepted  TLSv1.2  128 bits  DHE-RSA-AES128-SHA256         DHE 1024 bits
Accepted  TLSv1.2  128 bits  DHE-RSA-AES128-SHA            DHE 1024 bits
Accepted  TLSv1.2  128 bits  DHE-RSA-SEED-SHA             DHE 1024 bits
Accepted  TLSv1.2  128 bits  DHE-RSA-CAMELLIA128-SHA       DHE 1024 bits
Accepted  TLSv1.2  128 bits  AECDH-AES128-SHA              Curve P-256 DHE 256
Accepted  TLSv1.2  128 bits  AES128-GCM-SHA256
Accepted  TLSv1.2  128 bits  AES128-SHA256
Accepted  TLSv1.2  128 bits  AES128-SHA
Accepted  TLSv1.2  128 bits  SEED-SHA
Accepted  TLSv1.2  128 bits  CAMELLIA128-SHA
Accepted  TLSv1.2  128 bits  IDEA-CBC-SHA
Accepted  TLSv1.2  128 bits  ECDHE-RSA-RC4-SHA            Curve P-256 DHE 256
Accepted  TLSv1.2  128 bits  AECDH-RC4-SHA                Curve P-256 DHE 256
Accepted  TLSv1.2  128 bits  RC4-SHA
Accepted  TLSv1.2  128 bits  RC4-MD5
Accepted  TLSv1.2  112 bits  ECDHE-RSA-DES-CBC3-SHA       Curve P-256 DHE 256
Accepted  TLSv1.2  112 bits  EDH-RSA-DES-CBC3-SHA         DHE 1024 bits
Accepted  TLSv1.2  112 bits  AECDH-DES-CBC3-SHA           Curve P-256 DHE 256
Accepted  TLSv1.2  112 bits  DES-CBC3-SHA

Accepted  TLSv1.2  56 bits   EDH-RSA-DES-CBC-SHA          DHE 1024 bits
Accepted  TLSv1.2  56 bits   DES-CBC-SHA
Accepted  TLSv1.2  40 bits   EXP-EDH-RSA-DES-CBC-SHA      DHE 512 bits
Accepted  TLSv1.2  40 bits   EXP-DES-CBC-SHA              RSA 512 bits
Accepted  TLSv1.2  40 bits   EXP-RC2-CBC-MD5              RSA 512 bits
Accepted  TLSv1.2  40 bits   EXP-RC4-MD5                  RSA 512 bits
Preferred TLSv1.1  256 bits  ECDHE-RSA-AES256-SHA         Curve P-256 DHE 256
Accepted  TLSv1.1  256 bits  DHE-RSA-AES256-SHA           DHE 1024 bits
Accepted  TLSv1.1  256 bits  DHE-RSA-CAMELLIA256-SHA      DHE 1024 bits
Accepted  TLSv1.1  256 bits  AECDH-AES256-SHA             Curve P-256 DHE 256
Accepted  TLSv1.1  256 bits  AES256-SHA
Accepted  TLSv1.1  256 bits  CAMELLIA256-SHA
Accepted  TLSv1.1  128 bits  ECDHE-RSA-AES128-SHA         Curve P-256 DHE 256
Accepted  TLSv1.1  128 bits  DHE-RSA-AES128-SHA           DHE 1024 bits
Accepted  TLSv1.1  128 bits  DHE-RSA-SEED-SHA            DHE 1024 bits
Accepted  TLSv1.1  128 bits  DHE-RSA-CAMELLIA128-SHA      DHE 1024 bits
Accepted  TLSv1.1  128 bits  AECDH-AES128-SHA             Curve P-256 DHE 256
Accepted  TLSv1.1  128 bits  AES128-SHA
Accepted  TLSv1.1  128 bits  SEED-SHA
Accepted  TLSv1.1  128 bits  CAMELLIA128-SHA
Accepted  TLSv1.1  128 bits  IDEA-CBC-SHA
Accepted  TLSv1.1  128 bits  ECDHE-RSA-RC4-SHA           Curve P-256 DHE 256
Accepted  TLSv1.1  128 bits  AECDH-RC4-SHA               Curve P-256 DHE 256
Accepted  TLSv1.1  128 bits  RC4-SHA
Accepted  TLSv1.1  128 bits  RC4-MD5
Accepted  TLSv1.1  112 bits  ECDHE-RSA-DES-CBC3-SHA      Curve P-256 DHE 256
Accepted  TLSv1.1  112 bits  EDH-RSA-DES-CBC3-SHA        DHE 1024 bits
Accepted  TLSv1.1  112 bits  AECDH-DES-CBC3-SHA          Curve P-256 DHE 256
Accepted  TLSv1.1  112 bits  DES-CBC3-SHA
Accepted  TLSv1.1  56 bits   EDH-RSA-DES-CBC-SHA         DHE 1024 bits
Accepted  TLSv1.1  56 bits   DES-CBC-SHA
Accepted  TLSv1.1  40 bits   EXP-EDH-RSA-DES-CBC-SHA     DHE 512 bits
Accepted  TLSv1.1  40 bits   EXP-DES-CBC-SHA             RSA 512 bits
Accepted  TLSv1.1  40 bits   EXP-RC2-CBC-MD5             RSA 512 bits
Accepted  TLSv1.1  40 bits   EXP-RC4-MD5                 RSA 512 bits
Preferred TLSv1.0  256 bits  ECDHE-RSA-AES256-SHA         Curve P-256 DHE 256
Accepted  TLSv1.0  256 bits  DHE-RSA-AES256-SHA           DHE 1024 bits
Accepted  TLSv1.0  256 bits  DHE-RSA-CAMELLIA256-SHA      DHE 1024 bits
Accepted  TLSv1.0  256 bits  AECDH-AES256-SHA             Curve P-256 DHE 256
Accepted  TLSv1.0  256 bits  AES256-SHA
Accepted  TLSv1.0  256 bits  CAMELLIA256-SHA
```

REPORTE DE INCIDENCIA DE GLESEC

TLP-AMBAR



```
Accepted  TLSv1.0  56 bits  EDH-RSA-DES-CBC-SHA          DHE 1024 bits
Accepted  TLSv1.0  56 bits  DES-CBC-SHA
Accepted  TLSv1.0  40 bits  EXP-EDH-RSA-DES-CBC-SHA     DHE 512 bits
Accepted  TLSv1.0  40 bits  EXP-DES-CBC-SHA             RSA 512 bits
Accepted  TLSv1.0  40 bits  EXP-RC2-CBC-MD5             RSA 512 bits
Accepted  TLSv1.0  40 bits  EXP-RC4-MD5                 RSA 512 bits
Preferred SSLv3    256 bits ECDHE-RSA-AES256-SHA        Curve P-256 DHE 256
Accepted  SSLv3    256 bits DHE-RSA-AES256-SHA          DHE 1024 bits
Accepted  SSLv3    256 bits DHE-RSA-CAMELLIA256-SHA     DHE 1024 bits
Accepted  SSLv3    256 bits AECDH-AES256-SHA            Curve P-256 DHE 256
Accepted  SSLv3    256 bits AES256-SHA
Accepted  SSLv3    256 bits CAMELLIA256-SHA
Accepted  SSLv3    128 bits ECDHE-RSA-AES128-SHA        Curve P-256 DHE 256
Accepted  SSLv3    128 bits DHE-RSA-AES128-SHA          DHE 1024 bits
Accepted  SSLv3    128 bits DHE-RSA-SEED-SHA            DHE 1024 bits
Accepted  SSLv3    128 bits DHE-RSA-CAMELLIA128-SHA     DHE 1024 bits
Accepted  SSLv3    128 bits AECDH-AES128-SHA            Curve P-256 DHE 256
Accepted  SSLv3    128 bits AES128-SHA
Accepted  SSLv3    128 bits SEED-SHA
Accepted  SSLv3    128 bits CAMELLIA128-SHA
Accepted  SSLv3    128 bits IDEA-CBC-SHA
Accepted  SSLv3    128 bits ECDHE-RSA-RC4-SHA           Curve P-256 DHE 256
Accepted  SSLv3    128 bits AECDH-RC4-SHA               Curve P-256 DHE 256
Accepted  SSLv3    128 bits RC4-SHA
Accepted  SSLv3    128 bits RC4-MD5
Accepted  SSLv3    112 bits ECDHE-RSA-DES-CBC3-SHA      Curve P-256 DHE 256
Accepted  SSLv3    112 bits EDH-RSA-DES-CBC3-SHA        DHE 1024 bits
Accepted  SSLv3    112 bits AECDH-DES-CBC3-SHA          Curve P-256 DHE 256
Accepted  SSLv3    112 bits DES-CBC3-SHA
Accepted  SSLv3    56 bits  EDH-RSA-DES-CBC-SHA         DHE 1024 bits
Accepted  SSLv3    56 bits  DES-CBC-SHA
Accepted  SSLv3    40 bits  EXP-EDH-RSA-DES-CBC-SHA     DHE 512 bits
Accepted  SSLv3    40 bits  EXP-DES-CBC-SHA             RSA 512 bits
Accepted  SSLv3    40 bits  EXP-RC2-CBC-MD5             RSA 512 bits
Accepted  SSLv3    40 bits  EXP-RC4-MD5                 RSA 512 bits
```

```
  SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength:    2048

Subject:  appserver.metrobanksa.com
Altnames: DNS:appserver.metrobanksa.com
Issuer:   GlobalSign Organization Validation CA - SHA256 - G2

Not valid before: Feb 19 22:16:05 2018 GMT
Not valid after:  Feb 20 22:16:05 2019 GMT
```

WEB METROBANK

SSL 2.0, SSL 3.0, TLS 1.0 y TLS 1.1 con suites de cifrados débiles y medios permitidos.

```
Connected to 190.34.183.152

Testing SSL server 190.34.183.152 on port 443 using SNI name 190.34.183.152

  TLS Fallback SCSV:
Server does not support TLS Fallback SCSV

  TLS renegotiation:
Secure session renegotiation supported

  TLS Compression:
Compression disabled
```

REPORTE DE INCIDENCIA DE GLESEC

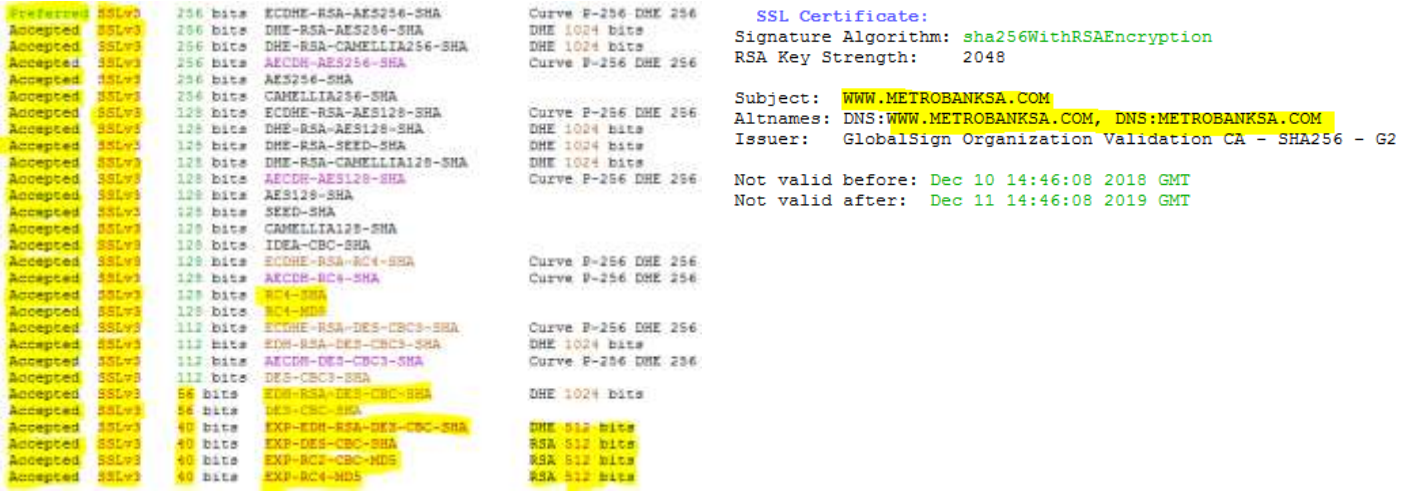
TLP-AMBAR

Supported Server Cipher(s):

Accepted	TLSv1.2	128 bits	RC4-SHA	
Accepted	TLSv1.2	128 bits	RC4-MD5	
Accepted	TLSv1.2	112 bits	ECDHE-RSA-DES-CBC3-SHA	Curve P-256 DHE 256
Accepted	TLSv1.2	112 bits	EDH-RSA-DES-CBC3-SHA	DHE 1024 bits
Accepted	TLSv1.2	112 bits	AECDH-DES-CBC3-SHA	Curve P-256 DHE 256
Accepted	TLSv1.2	112 bits	DES-CBC3-SHA	
Accepted	TLSv1.2	56 bits	EDH-RSA-DES-CBC-SHA	DHE 1024 bits
Accepted	TLSv1.2	56 bits	DES-CBC-SHA	
Accepted	TLSv1.2	40 bits	EXP-EDH-RSA-DES-CBC-SHA	DHE 512 bits
Accepted	TLSv1.2	40 bits	EXP-DES-CBC-SHA	RSA 512 bits
Accepted	TLSv1.2	40 bits	EXP-RC2-CBC-MD5	RSA 512 bits
Accepted	TLSv1.2	40 bits	EXP-RC4-MD5	RSA 512 bits
Preferred	TLSv1.1	256 bits	ECDHE-RSA-AES256-SHA	Curve P-256 DHE 256
Accepted	TLSv1.1	256 bits	DHE-RSA-AES256-SHA	DHE 1024 bits
Accepted	TLSv1.1	256 bits	DHE-RSA-CAMELLIA256-SHA	DHE 1024 bits
Accepted	TLSv1.1	256 bits	AECDH-AES256-SHA	Curve P-256 DHE 256
Accepted	TLSv1.1	256 bits	AES256-SHA	
Accepted	TLSv1.1	256 bits	CAMELLIA256-SHA	
Accepted	TLSv1.1	128 bits	ECDHE-RSA-AES128-SHA	Curve P-256 DHE 256
Accepted	TLSv1.1	128 bits	DHE-RSA-AES128-SHA	DHE 1024 bits
Accepted	TLSv1.1	128 bits	DHE-RSA-SEED-SHA	DHE 1024 bits
Accepted	TLSv1.1	128 bits	DHE-RSA-CAMELLIA128-SHA	DHE 1024 bits
Accepted	TLSv1.1	128 bits	AECDH-AES128-SHA	Curve P-256 DHE 256
Accepted	TLSv1.1	128 bits	AES128-SHA	
Accepted	TLSv1.1	128 bits	SEED-SHA	
Accepted	TLSv1.1	128 bits	CAMELLIA128-SHA	
Accepted	TLSv1.1	128 bits	IDEA-CBC-SHA	
Accepted	TLSv1.1	128 bits	ECDHE-RSA-RC4-SHA	Curve P-256 DHE 256
Accepted	TLSv1.1	128 bits	AECDH-RC4-SHA	Curve P-256 DHE 256
Accepted	TLSv1.1	128 bits	RC4-SHA	
Accepted	TLSv1.1	128 bits	RC4-MD5	
Accepted	TLSv1.1	112 bits	ECDHE-RSA-DES-CBC3-SHA	Curve P-256 DHE 256
Accepted	TLSv1.1	112 bits	EDH-RSA-DES-CBC3-SHA	DHE 1024 bits
Accepted	TLSv1.1	112 bits	AECDH-DES-CBC3-SHA	Curve P-256 DHE 256
Accepted	TLSv1.1	112 bits	DES-CBC3-SHA	
Accepted	TLSv1.1	56 bits	EDH-RSA-DES-CBC-SHA	DHE 1024 bits
Accepted	TLSv1.1	56 bits	DES-CBC-SHA	
Accepted	TLSv1.1	40 bits	EXP-EDH-RSA-DES-CBC-SHA	DHE 512 bits
Accepted	TLSv1.1	40 bits	EXP-DES-CBC-SHA	RSA 512 bits
Accepted	TLSv1.1	40 bits	EXP-RC2-CBC-MD5	RSA 512 bits
Accepted	TLSv1.1	40 bits	EXP-RC4-MD5	RSA 512 bits
Preferred	TLSv1.0	256 bits	ECDHE-RSA-AES256-SHA	Curve P-256 DHE 256
Accepted	TLSv1.0	256 bits	DHE-RSA-AES256-SHA	DHE 1024 bits
Accepted	TLSv1.0	256 bits	DHE-RSA-CAMELLIA256-SHA	DHE 1024 bits
Accepted	TLSv1.0	256 bits	AECDH-AES256-SHA	Curve P-256 DHE 256
Accepted	TLSv1.0	256 bits	AES256-SHA	
Accepted	TLSv1.0	256 bits	CAMELLIA256-SHA	
Accepted	TLSv1.0	128 bits	ECDHE-RSA-AES128-SHA	Curve P-256 DHE 256
Accepted	TLSv1.0	128 bits	DHE-RSA-AES128-SHA	DHE 1024 bits
Accepted	TLSv1.0	128 bits	DHE-RSA-SEED-SHA	DHE 1024 bits
Accepted	TLSv1.0	128 bits	DHE-RSA-CAMELLIA128-SHA	DHE 1024 bits
Accepted	TLSv1.0	128 bits	AECDH-AES128-SHA	Curve P-256 DHE 256
Accepted	TLSv1.0	128 bits	AES128-SHA	
Accepted	TLSv1.0	128 bits	SEED-SHA	
Accepted	TLSv1.0	128 bits	CAMELLIA128-SHA	
Accepted	TLSv1.0	128 bits	IDEA-CBC-SHA	
Accepted	TLSv1.0	128 bits	ECDHE-RSA-RC4-SHA	Curve P-256 DHE 256
Accepted	TLSv1.0	128 bits	AECDH-RC4-SHA	Curve P-256 DHE 256
Accepted	TLSv1.0	128 bits	RC4-SHA	
Accepted	TLSv1.0	128 bits	RC4-MD5	
Accepted	TLSv1.0	112 bits	ECDHE-RSA-DES-CBC3-SHA	Curve P-256 DHE 256
Accepted	TLSv1.0	112 bits	EDH-RSA-DES-CBC3-SHA	DHE 1024 bits
Accepted	TLSv1.0	112 bits	AECDH-DES-CBC3-SHA	Curve P-256 DHE 256
Accepted	TLSv1.0	112 bits	DES-CBC3-SHA	
Accepted	TLSv1.0	56 bits	EDH-RSA-DES-CBC-SHA	DHE 1024 bits
Accepted	TLSv1.0	56 bits	DES-CBC-SHA	
Accepted	TLSv1.0	40 bits	EXP-EDH-RSA-DES-CBC-SHA	DHE 512 bits
Accepted	TLSv1.0	40 bits	EXP-DES-CBC-SHA	RSA 512 bits
Accepted	TLSv1.0	40 bits	EXP-RC2-CBC-MD5	RSA 512 bits
Accepted	TLSv1.0	40 bits	EXP-RC4-MD5	RSA 512 bits

REPORTE DE INCIDENCIA DE GLESEC

TLP-AMBAR



Preferred	SSLv3	256 bits	ECDHE-RSA-AES256-SHA	Curve P-256 DHE 256
Accepted	SSLv3	256 bits	DHE-RSA-AES256-SHA	DHE 1024 bits
Accepted	SSLv3	256 bits	DHE-RSA-CAMELLIA256-SHA	DHE 1024 bits
Accepted	SSLv3	256 bits	AECDH-AES256-SHA	Curve P-256 DHE 256
Accepted	SSLv3	256 bits	AES256-SHA	
Accepted	SSLv3	256 bits	CAMELLIA256-SHA	
Accepted	SSLv3	128 bits	ECDHE-RSA-AES128-SHA	Curve P-256 DHE 256
Accepted	SSLv3	128 bits	DHE-RSA-AES128-SHA	DHE 1024 bits
Accepted	SSLv3	128 bits	DHE-RSA-SEED-SHA	DHE 1024 bits
Accepted	SSLv3	128 bits	DHE-RSA-CAMELLIA128-SHA	DHE 1024 bits
Accepted	SSLv3	128 bits	AECDH-AES128-SHA	Curve P-256 DHE 256
Accepted	SSLv3	128 bits	AES128-SHA	
Accepted	SSLv3	128 bits	SEED-SHA	
Accepted	SSLv3	128 bits	CAMELLIA128-SHA	
Accepted	SSLv3	128 bits	IDEA-CBC-SHA	
Accepted	SSLv3	128 bits	ECDHE-RSA-RC4-SHA	Curve P-256 DHE 256
Accepted	SSLv3	128 bits	AECDH-RC4-SHA	Curve P-256 DHE 256
Accepted	SSLv3	128 bits	RC4-SHA	
Accepted	SSLv3	128 bits	RC4-MD5	
Accepted	SSLv3	112 bits	ECDHE-RSA-DES-CBC3-SHA	Curve P-256 DHE 256
Accepted	SSLv3	112 bits	EDH-RSA-DES-CBC3-SHA	DHE 1024 bits
Accepted	SSLv3	112 bits	AECDH-DES-CBC3-SHA	Curve P-256 DHE 256
Accepted	SSLv3	112 bits	DES-CBC3-SHA	
Accepted	SSLv3	56 bits	EDH-RSA-DES-CBC-SHA	DHE 1024 bits
Accepted	SSLv3	56 bits	DES-CBC-SHA	
Accepted	SSLv3	40 bits	EXP-EDH-RSA-DES-CBC-SHA	DHE 512 bits
Accepted	SSLv3	40 bits	EXP-DES-CBC-SHA	RSA 512 bits
Accepted	SSLv3	40 bits	EXP-RC2-CBC-MD5	RSA 512 bits
Accepted	SSLv3	40 bits	EXP-RC4-MD5	RSA 512 bits

```
  SSL Certificate:
Signature Algorithm: sha256WithRSAEncryption
RSA Key Strength:    2048

Subject:  WWW.METROBANKSA.COM
Altnames: DNS:WWW.METROBANKSA.COM, DNS:METROBANKSA.COM
Issuer:   GlobalSign Organization Validation CA - SHA256 - G2

Not valid before: Dec 10 14:46:08 2018 GMT
Not valid after:  Dec 11 14:46:08 2019 GMT
```

PROTOCOLO DE COMPARTICION DE INFORMACION DE GLESEC

LOS REPORTES DE INCIDENCIAS DE CYBERSEGURIDAD DE GLESEC están en cumplimento con el protocolo de Semáforo (TLP) del Departamento de Seguridad de Estado de Estados Unidos (DHS): TLP -Blanco (Divulgación no limitada), TLP-Verde (Divulgación Limitada, Restringida, solo para la comunidad), TLP-Ámbar (Divulgación Limitada, Restringida, Para los participantes de la Organización) y TLP-Rojo (No Divulgación, Restringida/Confidencial – Solo compartida con el US DHS).