

# Reporte Productivity Guru

Cidexsa-Aeropuerto FWF30D

Elaborado para: Daniel Gomez



Fecha: 2019-08-02

Periodo: 2019-07-02 - 2019-08-02

# Tabla de contenidos.

Introducción

Consumo de banda ancha

Bandwidth por usuario

Audio y video

Bandwidth Audio y video

Sitios web

Bloqueos

Virus

Conclusiones

## Introducción

Productivity Guru, es un sistema con el que apoyamos a las empresas a ser mas productivas, eficientes y a disminuir gastos operativos para aumentar la rentabilidad de la empresa.

Es en base a la experiencia que RealNet brinda en sus servicios de asesoramiento y soluciones por medio de recursos TI, asesorando y administrando las redes de sus clientes con tecnologías de vanguardia que resulten confiables, economicas y flexibles para enfrentarse a los retos del mercado actual.

El objetivo principal de este reporte es, mostrar el comportamiento de los usuarios en internet de la empresa .



(55) 5219 - 8656



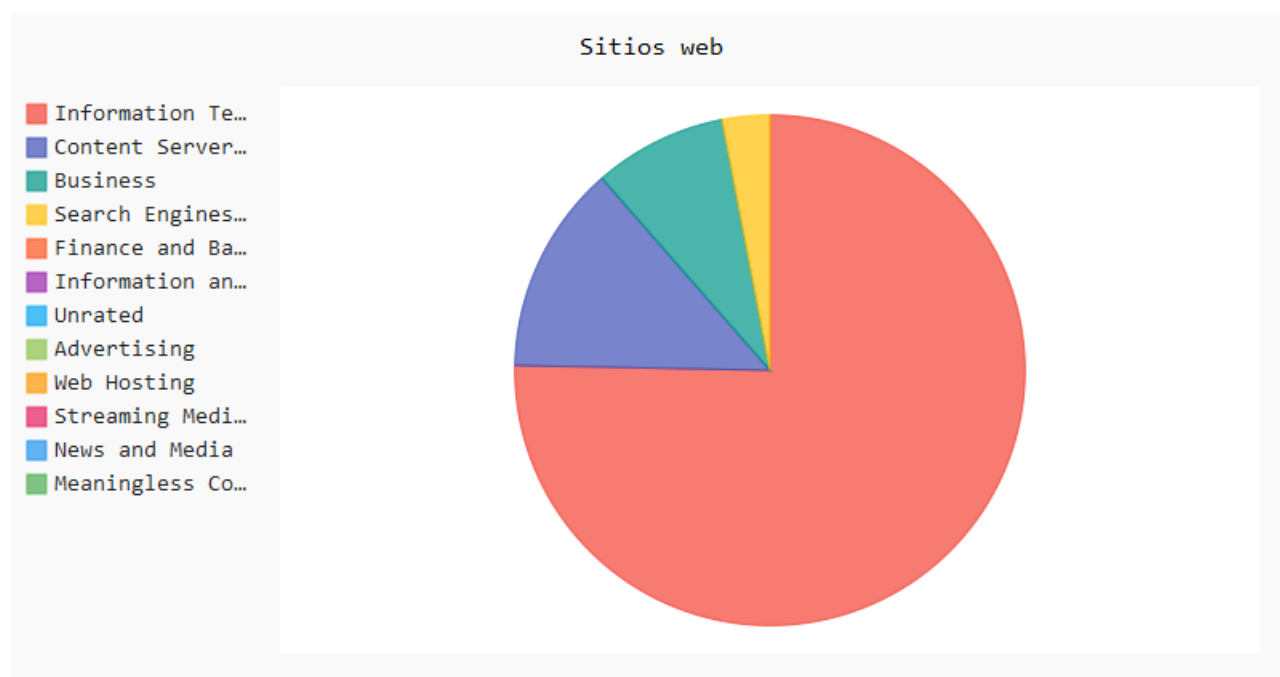
Tonalá 6 - 202. Col. Roma 06700,  
CDMX.



## Consumo de banda ancha

El ancho de banda es la cantidad de datos que los usuarios utilizan mientras se comunican a través de internet. Esto nos permite conocer el grado de utilización de la red en relación con cada usuario

En la siguiente grafica se muestra el consumo de ancho de banda por categoria de aplicaciones



Las categorias con mayor consumo de ancho de banda son de la categoria **Information Technology** con un consumo de 125.76MB, seguida de la categoria **Content Servers** , y **Business**

A continuación se da un mejor detalle de la información anterior

| #  | Categoría                         | Uso de datos |
|----|-----------------------------------|--------------|
| 1  | Information Technology            | 125.76MB     |
| 2  | Content Servers                   | 22.36MB      |
| 3  | Business                          | 14.04MB      |
| 4  | Search Engines and Portals        | 5.75MB       |
| 5  | Finance and Banking               | 0.23MB       |
| 6  | Information and Computer Security | 0.21MB       |
| 7  | Unrated                           | 0.21MB       |
| 8  | Advertising                       | 0.1MB        |
| 9  | Web Hosting                       | 0.04MB       |
| 10 | Streaming Media and Download      | 0.02MB       |

## Bandwidth por usuario

La siguiente tabla muestra a los usuarios que mas ancho de banda utilizaron, en primer lugar se encuentra la ip **192.168.0.51** y un total de **32.53MB**. Seguido por la ip **192.168.0.32** con un total de **30.35MB**, y la ip **192.168.0.35** con un total de **15.64MB**.

A continuacion se muestra la informacion mas detallada:

| #  | Usuario | IP            | Host                                      | Categoria              | Total           |
|----|---------|---------------|---|------------------------|-----------------|
| 1  |         | 192.168.0.51  | tlu.dl.delivery.mp.microsoft.com          | Information Technology | <b>32.53MB.</b> |
| 2  |         | 192.168.0.32  | 11.tlu.dl.delivery.mp.microsoft.com       | Information Technology | <b>30.35MB.</b> |
| 3  |         | 192.168.0.35  | eus-streaming-video-msn-com.akamaized.net | Content Servers        | <b>15.64MB.</b> |
| 4  |         | 192.168.0.51  | 11.tlu.dl.delivery.mp.microsoft.com       | Information Technology | <b>13.03MB.</b> |
| 5  |         | 192.168.0.34  | gomasa.ddns.net:8088                      | Business               | <b>11.44MB.</b> |
| 6  |         | 192.168.0.32  | 3.tlu.dl.delivery.mp.microsoft.com        | Information Technology | <b>9.51MB.</b>  |
| 7  |         | 192.168.0.32  | 2.tlu.dl.delivery.mp.microsoft.com        | Information Technology | <b>9.46MB.</b>  |
| 8  |         | 192.168.0.32  | 7.tlu.dl.delivery.mp.microsoft.com        | Information Technology | <b>6.37MB.</b>  |
| 9  |         | 192.168.0.104 | 38.90.226.39:80                           | Information Technology | <b>5.37MB.</b>  |
| 10 |         | 192.168.0.35  | dmd.metaservices.microsoft.com            | Information Technology | <b>5.25MB.</b>  |

## Bandwidth WIFI

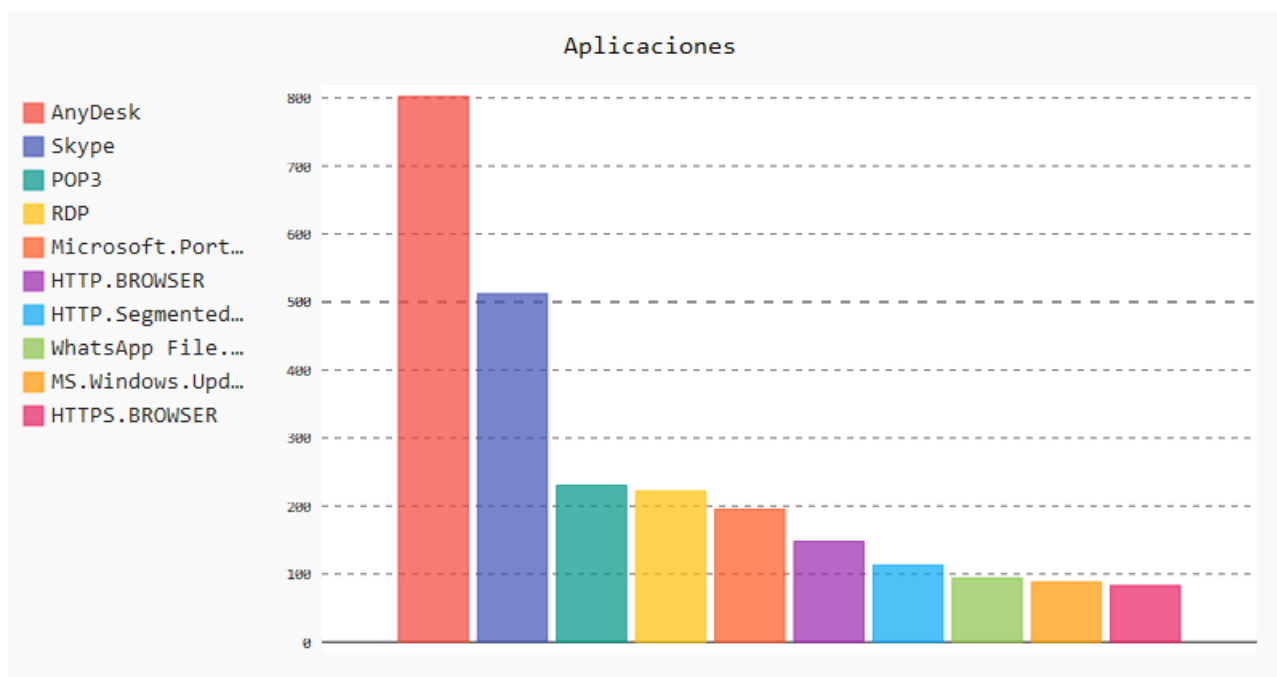
La siguiente tabla muestra a los usuarios que más ancho de banda utilizaron, siendo la ip **192.168.10.115** y un total de **88.94MB.** por medio de la red **Schott** Seguido por la ip **192.168.10.108** con un total de **55.95MB.** por medio de la red **Schott**, y la ip **192.168.10.102** con un total de **22.68MB.** por medio de la red **Schott**.

A continuacion se muestra la informacion mas detallada:

| #  | Usuario | IP             | SSID   | Total           |
|----|---------|----------------|--------|-----------------|
| 1  |         | 192.168.10.115 | Schott | <b>88.94MB.</b> |
| 2  |         | 192.168.10.108 | Schott | <b>55.95MB.</b> |
| 3  |         | 192.168.10.102 | Schott | <b>22.68MB.</b> |
| 4  |         | 192.168.10.117 | Schott | <b>21.84MB.</b> |
| 5  |         | 192.168.10.100 | Schott | <b>13.51MB.</b> |
| 6  |         | 192.168.10.113 | Schott | <b>8.92MB.</b>  |
| 7  |         | 192.168.10.103 | Schott | <b>7.66MB.</b>  |
| 8  |         | 192.168.10.104 | Schott | <b>4.07MB.</b>  |
| 9  |         | 192.168.10.112 | Schott | <b>3.03MB.</b>  |
| 10 |         | 192.168.10.105 | Schott | <b>2.28MB.</b>  |

## Aplicaciones más utilizadas

La siguiente gráfica muestra las aplicaciones más utilizadas y el ancho de banda consumido.



Las aplicaciones con mayor consumo de ancho de banda son **AnyDesk** con un consumo de **802.48MB**, seguida de la categoría **Skype**, y **POP3**



A continuación se da un mejor detalle de la información anterior

| #  | Aplicación              | Categoría       | Uso de datos |
|----|-------------------------|-----------------|--------------|
| 1  | AnyDesk                 | Remote.Access   | 802.48MB.    |
| 2  | Skype                   | Collaboration   | 512.05MB.    |
| 3  | POP3                    | Email           | 230.5MB.     |
| 4  | RDP                     | Remote.Access   | 222.1MB.     |
| 5  | Microsoft.Portal        | Collaboration   | 195.88MB.    |
| 6  | HTTP.BROWSER            | Web.Client      | 148.12MB.    |
| 7  | HTTP.Segmented.Download | Network.Service | 113.74MB.    |
| 8  | WhatsApp File.Transfer  | Collaboration   | 94.74MB.     |
| 9  | MS.Windows.Update       | Update          | 88.92MB.     |
| 10 | HTTPS.BROWSER           | Web.Client      | 83.7MB.      |

## Aplicaciones más utilizadas Video/Audio

El monitoreo de aplicaciones de Video o Audio tiene como intención aumentar la productividad, ya que el uso de aplicaciones de este tipo afecta en el rendimiento de los usuarios como de la red.



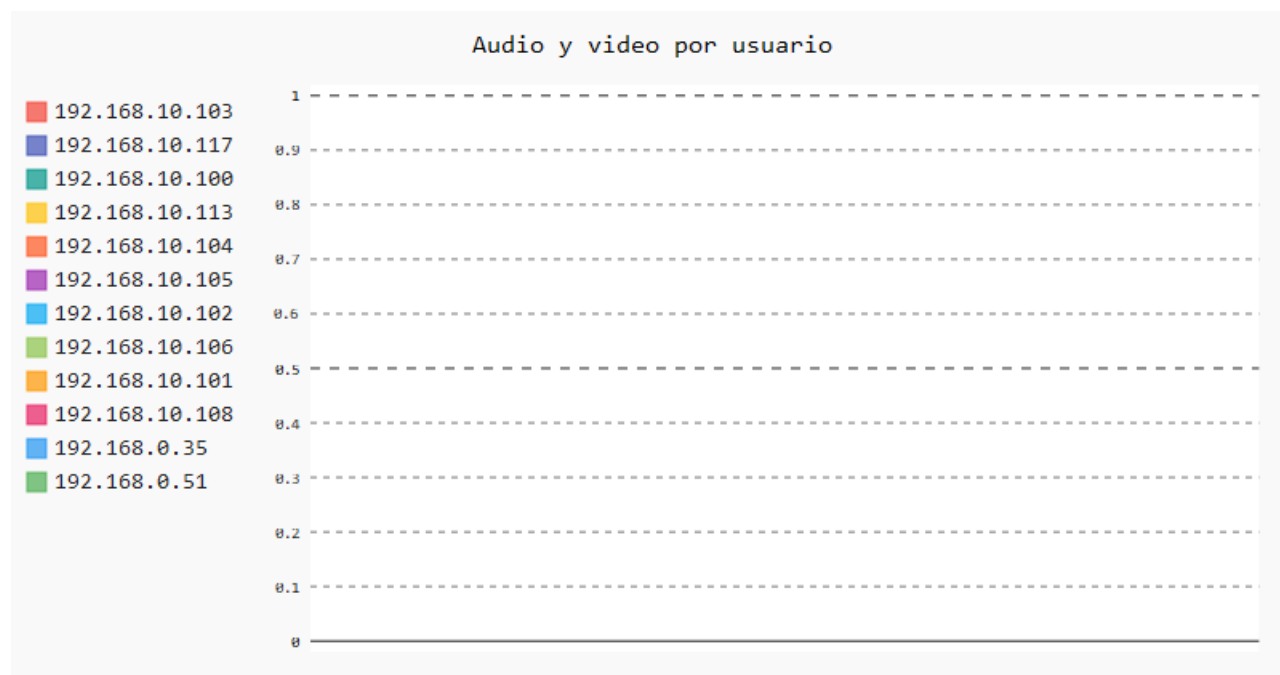
Las aplicaciones con mayor consumo de ancho de banda de la categoría **Video/Audio** siendo **YouTube** la primera con un consumo de **0.58MB**, seguida de la categoría **HTTP.Video**, y **Dailymotion**

A continuación se da un mejor detalle de la información anterior

| # | Aplicación  | Categoría   | Uso de datos |
|---|-------------|-------------|--------------|
| 1 | YouTube     | Video/Audio | 0.58MB.      |
| 2 | HTTP.Video  | Video/Audio | 0.01MB.      |
| 3 | Dailymotion | Video/Audio | 0.01MB.      |
| 4 | Spotify     | Video/Audio | 0.0MB.       |

## Aplicaciones más utilizadas Video/Audio usuario

En esta gráfica analizamos el tráfico de los usuarios del tipo Audio y video, esto nos ayuda a saber de forma clara cual de los usuarios esta haciendo uso de aplicaciones relacionadas a audio y video.



La siguiente tabla muestra a los usuarios que más ancho de banda utilizaron, siendo la ip **192.168.10.103** y un total de **0.12MB.** accediendo a **YouTube** Seguido por la ip **192.168.10.117** con un total de **0.12MB.** accediendo a **YouTube**, y la ip **192.168.10.100** con un total de **0.09MB.** accediendo a **YouTube**.

A continuación se da un mejor detalle de la información anterior

| #  | Usuario | IP | Aplicación  | Categoría   | Uso de datos |
|----|---------|----|-------------|-------------|--------------|
| 1  |         |    | YouTube     | Video/Audio | 0.12MB.      |
| 2  |         |    | YouTube     | Video/Audio | 0.12MB.      |
| 3  |         |    | YouTube     | Video/Audio | 0.09MB.      |
| 4  |         |    | YouTube     | Video/Audio | 0.07MB.      |
| 5  |         |    | YouTube     | Video/Audio | 0.06MB.      |
| 6  |         |    | YouTube     | Video/Audio | 0.03MB.      |
| 7  |         |    | YouTube     | Video/Audio | 0.03MB.      |
| 8  |         |    | YouTube     | Video/Audio | 0.03MB.      |
| 9  |         |    | YouTube     | Video/Audio | 0.01MB.      |
| 10 |         |    | YouTube     | Video/Audio | 0.01MB.      |
| 11 |         |    | HTTP.Video  | Video/Audio | 0.01MB.      |
| 12 |         |    | Dailymotion | Video/Audio | 0.01MB.      |

## Bandwidth WIFI Video/Audio

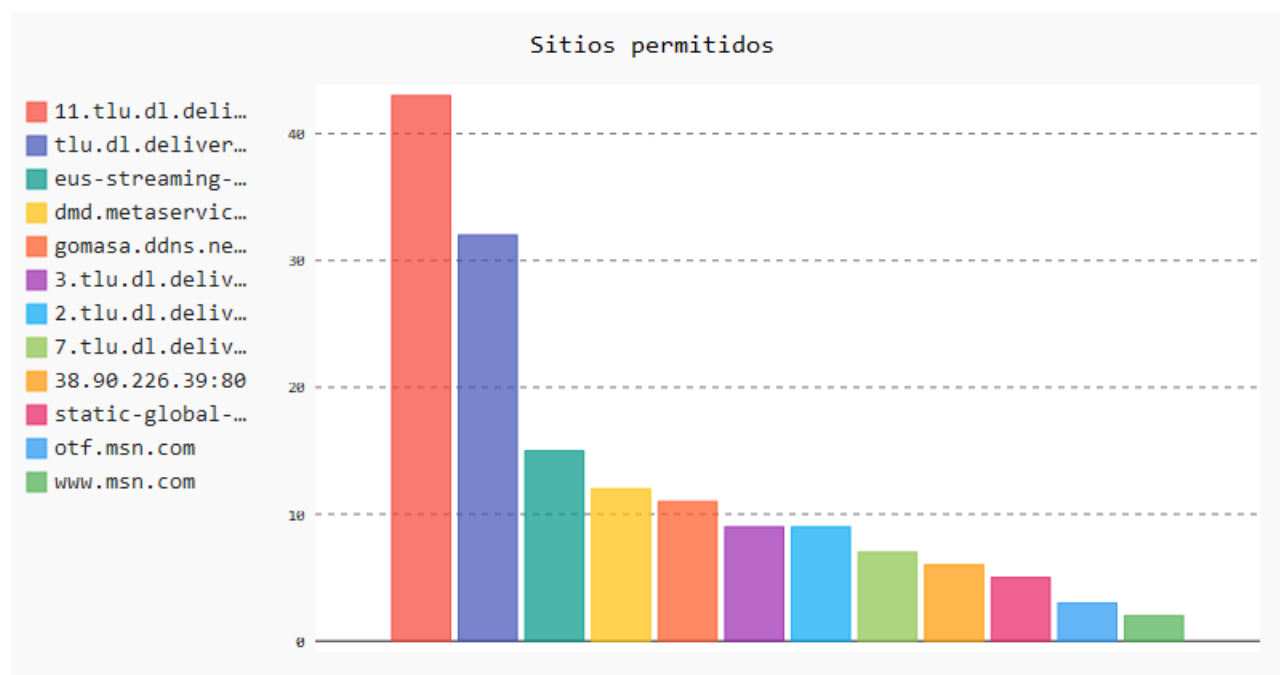
La siguiente tabla muestra a los Usuarios que más ancho de banda utilizaron por medio de WIFI y referente a categorías de **Video/Audio**, siendo la IP y un total de **0.12MB.** por medio de la red **Schott** Seguido por la IP con un total de **0.12MB.** por medio de la red **Schott**, y la IP con un total de **0.09MB.** por medio de la red **Schott**.

A continuacion se muestra la informacion mas detallada:

| #  | Usuario | IP             | SSID   | Total   |
|----|---------|----------------|--------|---------|
| 1  |         | 192.168.10.103 | Schott | 0.12MB. |
| 2  |         | 192.168.10.117 | Schott | 0.12MB. |
| 3  |         | 192.168.10.100 | Schott | 0.09MB. |
| 4  |         | 192.168.10.113 | Schott | 0.07MB. |
| 5  |         | 192.168.10.104 | Schott | 0.06MB. |
| 6  |         | 192.168.10.105 | Schott | 0.03MB. |
| 7  |         | 192.168.10.102 | Schott | 0.03MB. |
| 8  |         | 192.168.10.106 | Schott | 0.03MB. |
| 9  |         | 192.168.10.101 | Schott | 0.01MB. |
| 10 |         | 192.168.10.108 | Schott | 0.01MB. |
| 11 |         | 192.168.10.128 | Schott | 0.0MB.  |
| 12 |         | 192.168.10.115 | Schott | 0.0MB.  |

## Sitios web permitidos

La siguiente tabla muestra la distribución de las categorías web referentes a la navegación web del periodo. Se puede observar que, en el transcurso del periodo, los usuarios manejaron una tendencia principal hacia sitios catalogados de la siguiente manera:



El sitio web que más accesos tuvo fue **11.tlu.dl.delivery.mp.microsoft.com** con un consumo de 43.38MB, seguido de **tlu.dl.delivery.mp.microsoft.com**, y **eus-streaming-video-msn-com.akamaized.net**

A continuación se da un mejor detalle de la información anterior

| #  | Hostname                                  | Uso de datos |
|----|---|--------------|
| 1  | 11.tlu.dl.delivery.mp.microsoft.com       | 43.38MB      |
| 2  | tlu.dl.delivery.mp.microsoft.com          | 32.53MB      |
| 3  | eus-streaming-video-msn-com.akamaized.net | 15.64MB      |
| 4  | dmd.metaservices.microsoft.com            | 12.46MB      |
| 5  | gomasa.ddns.net:8088                      | 11.44MB      |
| 6  | 3.tlu.dl.delivery.mp.microsoft.com        | 9.52MB       |
| 7  | 2.tlu.dl.delivery.mp.microsoft.com        | 9.46MB       |
| 8  | 7.tlu.dl.delivery.mp.microsoft.com        | 7.38MB       |
| 9  | 38.90.226.39:80                           | 6.58MB       |
| 10 | static-global-s-msn-com.akamaized.net     | 5.04MB       |
| 11 | otf.msn.com                               | 3.29MB       |
| 12 | www.msn.com                               | 2.06MB       |



## Categorías bloqueadas

En la tabla se muestra las categorías web que fueron bloqueadas durante el periodo debido a intentos de acceso no autorizados.

A continuación se da un mejor detalle de la información anterior

| # | Hostname                     | Peticiones |
|---|------------------------------|------------|
| 1 | Advertising                  | 38         |
| 2 | Streaming Media and Download | 15         |
| 3 | Games                        | 2          |
| 4 | Social Networking            | 1          |

## Sitios web bloqueados

En la tabla se muestra los sitios web más bloqueados debido a intentos de acceso no autorizados

A continuación se da un mejor detalle de la información anterior

| #  | Hostname                | Categoría                    | Peticiones |
|----|-------------------------|------------------------------|------------|
| 1  | b.scorecardresearch.com | Advertising                  | 37910      |
| 2  | ib.adnxs.com            | Advertising                  | 34654      |
| 3  | acdn.adnxs.com          | Advertising                  | 27894      |
| 4  | api.snappea.com         | Streaming Media and Download | 14179      |
| 5  | sensors.snappea.com     | Streaming Media and Download | 4849       |
| 6  | widgets.outbrain.com    | Advertising                  | 4217       |
| 7  | analytics.snappea.com   | Streaming Media and Download | 1400       |
| 8  | contextual.media.net    | Advertising                  | 1374       |
| 9  | adm.fwmrm.net           | Streaming Media and Download | 929        |
| 10 | push.api.snappea.com    | Streaming Media and Download | 221        |
| 11 | c.whatsapp.net          | Social Networking            | 157        |
| 12 | cdf-anon.xboxlive.com   | Games                        | 138        |

## Usuarios bloqueados

En la tabla se muestra los usuarios que fueron bloqueados, la IP del equipo y el consumo de ancho de banda que utilizaron en datos enviados y recibidos.

**A continuación se da un mejor detalle de la información anterior**

| # | Usuario | IP             | Categorías                   | Uso de datos |
|---|---------|----------------|------------------------------|--------------|
| 1 |         | 192.168.0.35   | Advertising                  | 0.09MB       |
| 2 |         | 192.168.10.115 | Streaming Media and Download | 0.02MB       |
| 3 |         | 192.168.0.104  | Advertising                  | 0.01MB       |
| 4 |         | 192.168.0.35   | Streaming Media and Download | 0.0MB        |
| 5 |         | 192.168.10.117 | Social Networking            | 0.0MB        |
| 6 |         | 192.168.0.52   | Games                        | 0.0MB        |
| 7 |         | 192.168.0.32   | Games                        | 0.0MB        |

## Virus

Se han detectado equipos infectados con virus dentro de la red interna de Chiltepec la intrusión identificada es de tipo Virus, en las siguientes tablas se muestra información detallada

| #  | Virus                | Fecha      | Hora     | IP            | Usuario | Accion  | Incidencias |
|----|----------------------|------------|----------|---------------|---------|---------|-------------|
| 1  | W32/Injector.EGUR!tr | 2019-07-29 | 10:10:07 | 192.168.0.106 |         | blocked | 1           |
| 2  | W32/Injector.EGUR!tr | 2019-07-29 | 10:20:08 | 192.168.0.106 |         | blocked | 1           |
| 3  | W32/Injector.EGUR!tr | 2019-07-29 | 09:25:04 | 192.168.0.106 |         | blocked | 1           |
| 4  | W32/Injector.EGUR!tr | 2019-07-29 | 10:55:12 | 192.168.0.106 |         | blocked | 1           |
| 5  | W32/Injector.EGUR!tr | 2019-07-29 | 10:15:06 | 192.168.0.106 |         | blocked | 1           |
| 6  | W32/Injector.EGUR!tr | 2019-07-29 | 10:45:11 | 192.168.0.106 |         | blocked | 1           |
| 7  | W32/Injector.EGUR!tr | 2019-07-29 | 10:05:06 | 192.168.0.106 |         | blocked | 1           |
| 8  | W32/Injector.EGUR!tr | 2019-07-29 | 09:37:26 | 192.168.0.106 |         | blocked | 1           |
| 9  | W32/Injector.EGUR!tr | 2019-07-29 | 09:36:39 | 192.168.0.106 |         | blocked | 1           |
| 10 | W32/Injector.EGUR!tr | 2019-07-29 | 09:50:06 | 192.168.0.106 |         | blocked | 1           |
| 11 | W32/Injector.EGUR!tr | 2019-07-29 | 10:48:57 | 192.168.0.106 |         | blocked | 1           |
| 12 | W32/Injector.EGUR!tr | 2019-07-29 | 09:30:06 | 192.168.0.106 |         | blocked | 1           |
| 13 | W32/Injector.EGUR!tr | 2019-07-29 | 10:25:09 | 192.168.0.106 |         | blocked | 1           |
| 14 | W32/Injector.EGUR!tr | 2019-07-29 | 10:02:35 | 192.168.0.106 |         | blocked | 1           |
| 15 | W32/Injector.EGUR!tr | 2019-07-29 | 09:37:53 | 192.168.0.106 |         | blocked | 1           |
| 16 | W32/Injector.EGUR!tr | 2019-07-29 | 09:45:08 | 192.168.0.106 |         | blocked | 1           |
| 17 | W32/Injector.EGUR!tr | 2019-07-29 | 10:46:57 | 192.168.0.106 |         | blocked | 1           |
| 18 | W32/Injector.EGUR!tr | 2019-07-29 | 09:40:06 | 192.168.0.106 |         | blocked | 1           |
| 19 | W32/Injector.EGUR!tr | 2019-07-29 | 10:02:08 | 192.168.0.106 |         | blocked | 1           |
| 20 | W32/Injector.EGUR!tr | 2019-07-29 | 10:35:15 | 192.168.0.106 |         | blocked | 1           |

| #  | Virus                | Fecha      | Hora     | IP            | Usuario | Accion  | Incidencias |
|----|----------------------|------------|----------|---------------|---------|---------|-------------|
| 21 | W32/Injector.EGUR!tr | 2019-07-29 | 10:01:12 | 192.168.0.106 |         | blocked | 1           |
| 22 | W32/Injector.EGUR!tr | 2019-07-29 | 10:00:07 | 192.168.0.106 |         | blocked | 1           |
| 23 | W32/Injector.EGUR!tr | 2019-07-29 | 09:35:12 | 192.168.0.106 |         | blocked | 1           |
| 24 | W32/Injector.EGUR!tr | 2019-07-29 | 09:38:53 | 192.168.0.106 |         | blocked | 1           |
| 25 | W32/Injector.EGUR!tr | 2019-07-29 | 10:40:10 | 192.168.0.106 |         | blocked | 1           |
| 26 | W32/Injector.EGUR!tr | 2019-07-29 | 11:00:15 | 192.168.0.106 |         | blocked | 1           |
| 27 | W32/Injector.EGUR!tr | 2019-07-29 | 10:50:10 | 192.168.0.106 |         | blocked | 1           |
| 28 | W32/Injector.EGUR!tr | 2019-07-29 | 09:55:08 | 192.168.0.106 |         | blocked | 1           |
| 29 | W32/Injector.EGUR!tr | 2019-07-29 | 09:47:23 | 192.168.0.106 |         | blocked | 1           |
| 30 | W32/Injector.EGUR!tr | 2019-07-29 | 10:01:41 | 192.168.0.106 |         | blocked | 1           |
| 31 | W32/Injector.EGUR!tr | 2019-07-29 | 10:09:14 | 192.168.0.106 |         | blocked | 1           |

## Conclusiones

En el reporte de este mes las políticas establecidas con anterioridad están mejorando la productividad dentro de la empresa, así como la navegación segura en internet permitiendo que los usuarios entren a los sitios que tienen permisos

---

Se detectaron 31 virus. Tu red esta en un estado critico, contacta al equipo de Productivity Guru para hacer un analisis de tu red y evitar perdida de información

---

Se detectaron accesos a sitios con la categoria **Audio/Video**, contacta al equipo de Productivity Guru para solucionarlo.

---

Se estan bloqueando los sitios adecuadamente



(55) 5219 - 8656



Tonalá 6 - 202. Col. Roma 06700,  
CDMX.

