



TELEVISIÓN METROPOLITANA, S.A. DE C.V.
 SUBDIRECCIÓN GENERAL DE ADMINISTRACIÓN Y FINANZAS
 DIRECCIÓN DE FINANZAS

N° de Solicitud		
FECHA DE RECEPCIÓN		
DIA	MES	AÑO

SOLICITUD DE PAGO

ÁREA SOLICITANTE : _____
 CENTRO DE COSTO: _____ REQUISICIÓN No.: _____
 FORMA DE ADJUDICACIÓN: _____ CONTRATO No.: _____
 DIRECTA: _____ INVITACIÓN: _____ LICITACIÓN: _____ No. SICOP: _____
 EXCEPCIÓN ART.41

BENEFICIARIO: _____ **RFC:** _____
IMPORTE: _____ /100 MN)
DESCRIPCIÓN DEL BIEN O SERVICIO:

Transferencia Bancaria: _____ **CLABE:** _____
Banco: _____
Cuenta: _____

PARA USO EXCLUSIVO DE LA DIRECCIÓN DE FINANZAS

GERENCIA DE PRESUPUESTO		DEPTO. DE TESORERÍA	
PRE PROCESO:		No. PROCESO	
PRE SUF:		FOLIO	
COM. PROCESO		No.SOL	
COMPROMISO		No.PRO DOC.COMP	
		FOLIO	
		CLC	
CADENAS PRODUCTIVAS		FECHA DE PAGO	

CLAVE DE AFECTACIÓN PRESUPUESTAL RUBRICA
 PARTIDA: _____ C.C. _____ FF: _____ VISTO BUENO DE CONTABILIDAD RUBRICA
 NOMBRE: _____ NOMBRE: _____

ÁREA RESPONSABLE DEL GASTO: _____ **AUTORIZA:** _____



TELEVISIÓN METROPOLITANA, S.A. DE C.V.
SUBDIRECCIÓN GENERAL DE ADMINISTRACIÓN Y FINANZAS
DIRECCIÓN DE FINANZAS

FECHA		
DÍA	MES	AÑO

CONSTANCIA ACEPTACIÓN DEL BIEN O SERVICIO

EL QUE SUSCRIBE LA PRESENTE BAJO PROTESTA DE DECIR VERDAD, MANIFIESTO HABER RECIBIDO A MI ENTERA SATISFACCIÓN LOS:

BIENES: _____

SERVICIOS: _____

DESCRIPCIÓN:

FECHA DE RECEPCIÓN:

No. DE CONTRATO:
No. DE REQUISICIÓN:

No. DE FACTURA:

DEL PROVEEDOR Y/O PRESTADOR DE SERVICIOS:

POR LAS CARACTERÍSTICAS Y NATURALEZA DE LOS BIENES Y/O SERVICIOS RECIBIDOS, LOS MISMOS QUEDARÁN BAJO LA CUSTODIA DE:

POR LO ANTERIOR Y BAJO MI RESPONSABILIDAD, SOLICITO SEA CUBIERTO EL PAGO CORRESPONDIENTE.

ATENTAMENTE

NOMBRE:
CARGO:

Av. San Fernando No. 37
Toriello Guerra, Tlalpan
Ciudad de México, México, CP. 14050
FID741230A22
Tel: +52(55) 5624 2800, Fax: +52(55) 5624 2825
www.infotec.com.mx

Factura

F 19227

Folio Fiscal D9C30AC2-393F-4B1C-9277-DEA81C9D28C7
Fecha Emisión 2021-03-11T00:00:00
Fecha Certificación 2021-03-11T16:22:46
Lugar de 14050

FACTURAR A

TELEVISIÓN METROPOLITANA, S.A. DE C.V.
ATLETAS, NO. 2, COUNTRY CLUB,
C.P. 04210, COYOACAN, CIUDAD DE MÉXICO, MEX
TME901116GZ8

Clave Cliente TME901116GZ8
Programa 21421113/TME
Atención Ing. Juan Pablo Rosas Turanzas
Puesto Gerencia en Tecnologías de la Información

Cantidad	Clave	Descripción	Unidad	Precio Unitario	Importe	
1.00	81141902	Servicio de Internet Dedicado	E48	132,734.94	132,734.94	
		Impuesto	Tipo	Tasa	Base	Importe
		Traslado	002	Tasa	0.160000	132,734.94
1.00	81141902	Servicio de Seguridad Perimetral (UTM)	E48	5,081.51	5,081.51	
		Impuesto	Tipo	Tasa	Base	Importe
		Traslado	002	Tasa	0.160000	5,081.51
1.00	81141902	Servicio de Seguridad para Servidores Web	E48	15,755.25	15,755.25	
		Impuesto	Tipo	Tasa	Base	Importe
		Traslado	002	Tasa	0.160000	15,755.25
1.00	81141902	Servicio de Monitoreo y Reportes	E48	12,886.89	12,886.89	
		Impuesto	Tipo	Tasa	Base	Importe
		Traslado	002	Tasa	0.160000	12,886.89
		Impuesto	Tipo	Tasa	Base	Importe
		Traslado	002	Tasa	0.160000	12,886.89

Servicios correspondientes al mes de febrero de 2021

Tipo de Comprobante: I
Uso CFDI: P01
Forma de Pago: 99
Metodo de Pago: PPD
Regimen Fiscal: 603

Subtotal 166,458.59
IVA 16.00% 26,633.37
Total 193,091.96

Cantidad con Letra: (CIENTO NOVENTA Y TRES MIL NOVENTA Y UN PESOS 96/100 M.N.)



Sello digital del CFDI

JDX7eRa09MrzyqRUtVsT/8ImeloGfllBbXMRKizKdywW45pfgl2tz16SUn+Bw+/WXal0WOYrXhprjPI9L772AhX/0f68rEzXC8wY1QBFTXfLNn7LdLrjaVqo2ATyAtpWel3yEuAi5EOJTLzmbh
BvxQ00CR+mcTK+d2e2JLpd3wYA76jUt2QhJgKqdbm+tXovZglOQfX5mjXffAU/3edfzd4rSAq1L2Zwml+/eKRBLSEowl+3JGCB0DRv8T3nOYYxTVM2ZFIM5i+UnYqnkCoot04cDilcna1uC
0ImDGV91xZ7jjVyagZ44IjMkjX8lluGoCC7+kYTaPyyEqPGacFYQ==

Sello digital del SAT

TSjVFtn3VQaDemeg7nwMnPkPvpmhopcushIKV94WKXUN44dsrH0b3jI3u4QbdKJi32JwcPY1+6D+wBt/FeoUX35UWj4CnqsjE7/RyQiytAaoY9iFN7Um1RGKIRkXIIAovTqjyPd63MdUc
Ubfk+hkcnXzwq9DNysKOLef/r1aI40UkwSF7oTWODAnFZkCrX5B+hfhNhZrZqh4t8HzcTgdNtuWCUeyVsSsxiYWSLf99xEGWUKO0zrJHihbSrN9PDENcMuA7DoHZ3yngzirlcDPTtNPV
PL4Ze/pVIQYtbZNeaH5hKJoJNfBrVKX2/S3tGU9z0pquCJbh+dy95eiMA==

Cadena original del complemento de certificación digital del SAT

||1.1|D9C30AC2-393F-4B1C-9277-DEA81C9D28C7|2021-03-11T16:22:46|TLE011122SC2|JDX7eRa09MrzyqRUtVsT/8ImeloGfllBbXMRKizKdywW45pfgl2tz16SUn+Bw+/WXal0WOYrXhprjPI9L772AhX/0f68rEzXC8wY1QBFTXfLNn7LdLrjaVqo2ATyAtpWel3yEuAi5EOJTLzmbhBvxQ00CR+mcTK+d2e2JLpd3wYA76jUt2QhJgKqdbm+tXovZglOQfX5mjXffAU/3edfzd4rSAq1L2Zwml+/eKRBLSEowl+3JGCB0DRv8T3nOYYxTVM2ZFIM5i+UnYqnkCoot04cDilcna1uC0ImDGV91xZ7jjVyagZ44IjMkjX8lluGoCC7+kYTaPyyEqPGacFYQ==||00001000000503270882||

Recepción de compra

Pág.: 1

Número recepción de compra: RECEP-21-0502
Fecha recepción de compra: 21/05/2021

Compra

De: INFOTEC CENTRO DE INVESTIGACIÓN E INNOVACIÓN EN TECNOLOGÍAS DE LA
INFORMACIÓN Y COMUNICACIÓN
Fernanda Camacho
Av. San Fernando No.37
Toriello Guerra
Tlalpan, Distrito Federal 14050
México

Enviar
Para:

Envío a través de

Recibir por 06/01/2021
Id. proveedor P01001338

Confirmar a
Comprador
Número pedido C-PED-21-0511
Fecha pedido 21/05/2021

Nº producto	Descripción	Unidad	Recibido	Pedido	Pedido pendiente
	Nº licitación: PC-21-0172				
	MATERIALES INDIRECTOS	SER	1	1	
	MATERIALES INDIRECTOS	SER	1	1	
	MATERIALES INDIRECTOS	SER	1	1	
	MATERIALES INDIRECTOS	SER	1	1	
	MATERIALES INDIRECTOS	SER	1	1	
	MATERIALES INDIRECTOS	SER	1	1	
	MATERIALES INDIRECTOS	SER	1	1	
	GASTOS DE VENTA	SER	1	1	
	GASTOS DE VENTA	SER	1	1	
	GASTOS DE ADMINISTRACION	SER	1	1	
	GASTOS DE ADMINISTRACION	SER	1	1	
	GASTOS DE ADMINISTRACION	SER	1	1	
	MATERIALES INDIRECTOS	SER	1	1	
	MATERIALES INDIRECTOS	SER	1	1	
	MATERIALES INDIRECTOS	SER	1	1	
	GASTOS DE ADMINISTRACION	SER	1	1	
	GASTOS DE ADMINISTRACION	SER	1	1	

Factura compra

Pág.: 1

No. CFACT-21-0502
Número factura compra: F19227
Fecha factura compra: 21/05/2021
Número de evento: EV1-21-000290

Pagar
Para: INFOTEC CENTRO DE INVESTIGACIÓN E INNOVACIÓN EN TECNOLOGÍAS DE LA
INFORMACIÓN Y COMUNICACIÓN
Fernanda Camacho
Av. San Fernando No.37
Toriello Guerra
Tlalpan, Distrito Federal 14050
México

Enviar
Para:

Tipo de Persona Moral
Envío a través de
Recibir por 06/01/2021
Términos
Id. proveedor P01001338

Confirmar a
Comprador
Número pedido C-PED-21-0511
Fecha pedido 21/05/2021
Forma de pago

Nº producto	PP	PTDA ESP	FF	CECO	Descripción	Unidad	Cantidad	Precio	Precio total
					Nº licitación: PC-21-0172				
013	31603	1	11		MATERIALES INDIRECTOS	SER	1	4,017.98	4,017.98
013	31603	1	12		MATERIALES INDIRECTOS	SER	1	3,443.97	3,443.97
013	31603	1	13		MATERIALES INDIRECTOS	SER	1	6,887.94	6,887.94
013	31603	1	21		MATERIALES INDIRECTOS	SER	1	4,591.96	4,591.96
013	31603	1	22		MATERIALES INDIRECTOS	SER	1	18,367.84	18,367.84
013	31603	1	23		MATERIALES INDIRECTOS	SER	1	9,183.92	9,183.92
013	31603	1	24		MATERIALES INDIRECTOS	SER	1	9,183.92	9,183.92
013	31603	1	31		GASTOS DE VENTA	SER	1	2,295.98	2,295.98
013	31603	1	32		GASTOS DE VENTA	SER	1	4,017.97	4,017.97
001	31603	1	41		GASTOS DE ADMINISTRACION	SER	1	2,869.97	2,869.97
001	31603	1	42		GASTOS DE ADMINISTRACION	SER	1	29,273.75	29,273.75
001	31603	1	43		GASTOS DE ADMINISTRACION	SER	1	14,349.88	14,349.88
013	31603	1	51		MATERIALES INDIRECTOS	SER	1	6,313.95	6,313.95
013	31603	1	52		MATERIALES INDIRECTOS	SER	1	16,071.86	16,071.86
013	31603	1	53		MATERIALES INDIRECTOS	SER	1	22,959.80	22,959.80
013	31603	1	54		GASTOS DE ADMINISTRACION	SER	1	6,313.95	6,313.95
001	31603	1	61		GASTOS DE ADMINISTRACION	SER	1	6,313.95	6,313.95

Subtotal: 166,458.59
Descuento factura: 0.00
IVA: 26,633.37
Total de MXN: 193,091.96



Autorización de pago

RAUL YAU

No.: SP-21-00675

SUBDIRECTOR GENERAL TECNICO
Y OPERATIVO

No. Autorización: SP-21-
00675

Presente:

Sírvase efectuar pago a favor de: INFOTEC CENTRO DE INVESTIGACIÓN E INNOVACIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

Por un importe de: \$193,091.96 (CIENTO NOVENTA Y TRES MIL NOVENTA Y UN PESOS 96/100 M.N.)

Por el pago que se indica en la Solicitud de Pago número SP-21-00675

Recibida con fecha: viernes, 21 de mayo de 2021

Descripción	Importe	No. evento
Servicio de Internet Dedicado, Seguridad Perimetra	193,091.96	EV1-21-000290
Total:		
	193,091.96	

Cheque/Transferencia				Beneficiario	Importe
Número	Fecha	Cuenta	No. de póliza	INFOTEC CENTRO DE INVESTIGACIÓN E INNOVACIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN	
				Total:	193,091.96

Proceso:

Número:

Ticket: SP-21-00675

Folio:

Procesada: SP-21-00675

No. CLC: SP-21-00675

Observaciones: Servicio de Internet Dedicado, Seguridad Perimetral (UTM), Servicio de Seguridad para Servidores web y Servicio de Monitoreo Monitoreo y Reportes. FEBRERO2021.



Autorización de pago



Reporte de acceso a Internet

CANAL 22 – TELEVISIÓN METROPOLITANA S.A DE C.V.



FEBRERO 2021

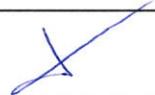
Información General del Documento

Entregable	Clave	Servicio	Medio
	TC-DUAI	Internet Dedicado	Electrónico / Físico

Elaboración	Puesto	Nombre	Firma
	Responsable del Servicio	Lorena García García	

Revisión	Puesto	Nombre	Firma
	Líder de proyecto	Víctor Quiroz Barrientos	

Aprobación	Puesto	Nombre	Firma
	Subgerente de Innovación Tecnológica	Lic. Adrián Moran Checa	

Recepción Cliente	Puesto	Nombre	Firma	Fecha
	Gerente de Tecnologías de la Información	Ing. Juan Pablo Rosas Turanzas		17/mar/2021

Aprobación Cliente	Puesto	Nombre	Firma	Fecha
	Jefe de Unidad Departamental	Ing. Emilio René García Rodríguez		17/mar/2021

Tabla de contenido

1. Introducción.....	4
2. Objetivo.....	4
3. Diagrama de Topología de Acceso y Publicación a Internet.....	5
4. Utilización de Enlaces de Salida a Internet.....	6
5. Glosario de Términos.....	7

1. Introducción

El presente documento muestra un resumen de las actividades realizadas como parte del Servicio de Telecomunicaciones que actualmente el **CANAL 22** tiene contratados con el **INFOTEC**, que consiste en administrar y dar soporte a los servicios Acceso y Publicación a Internet.

INFOTEC cuenta con la capacidad técnica para ejecutar y prestar servicios eficaz y eficientemente, garantizando que se apliquen las mejores prácticas en la industria, que cumplen con los requisitos y estándares que aplican en el Manual Administrativo de Aplicación General en Materia de Tecnologías de la Información y Comunicaciones y Seguridad de la Información (MAAGTICSI).

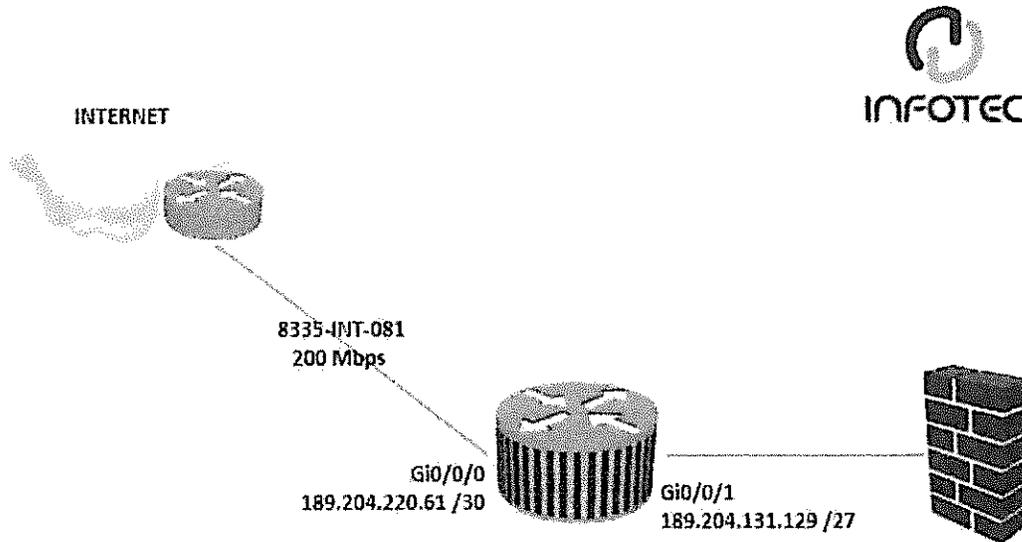
2. Objetivo

El presente documento tiene como objetivo reportar la disponibilidad de los enlaces contratados por el **CANAL 22**, el cual está integrado por un diagrama de topología de red y graficas que muestran la utilización de tráfico servicios de Acceso y Publicación a Internet, así como el intercambio de tráfico.

La comprobación de la prestación de los servicios que se informan en este documento corresponde a la operación del **01 de febrero de 2021 al 28 de febrero de 2021**.

3. Diagrama de Topología de Acceso y Publicación a Internet

El siguiente diagrama muestra la topología de Acceso y publicación a Internet del cliente Canal 22.



Segmentos de red que cuentan con el servicio de acceso y publicación a INTERNET.

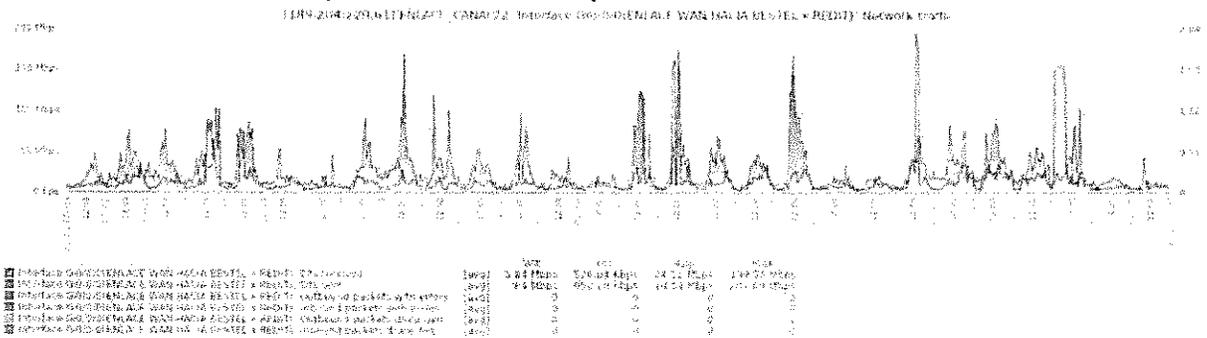
Red de Publicación a INTERNET		
VLAN	DIRECCIONAMIENTO IP	DESCRIPCIÓN
Por definir	189.204.131.128/27	Administración y Monitoreo

4. Utilización de Enlaces de Salida a Internet

Las siguientes gráficas muestran la utilización de ancho de banda (BW), del enlace para el acceso y publicación a Internet de Canal 22.

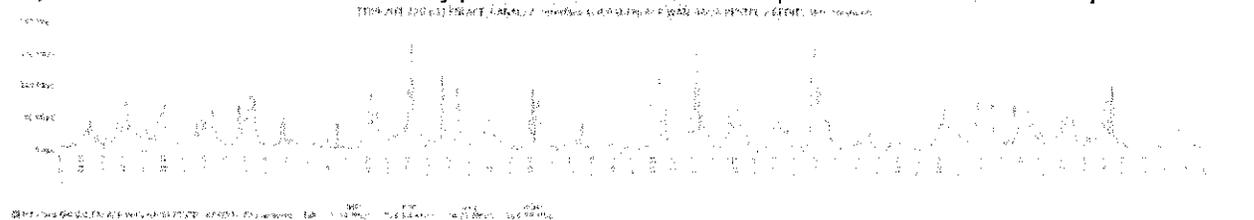
Durante el mes de febrero se presentaron los siguientes datos en la interface donde llega el enlace:

- Entradas de tráfico de un **promedio de 14.11 Mbps.**
- Salidas de tráfico de un **promedio de 14.54 Mbps.**



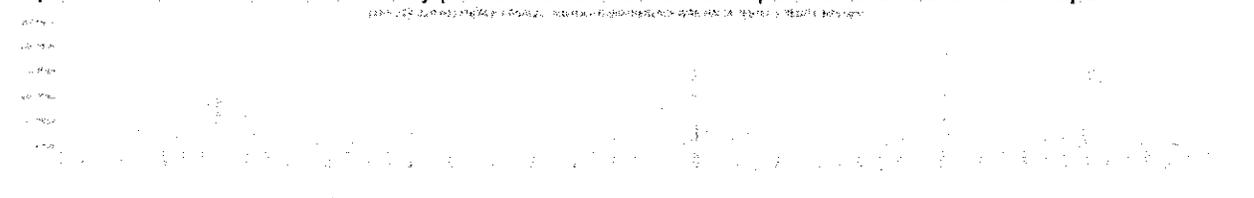
Trafico entrada

El **pico máximo de entrada** de acceso y publicación a internet correspondiente es de **199.55 Mbps.**

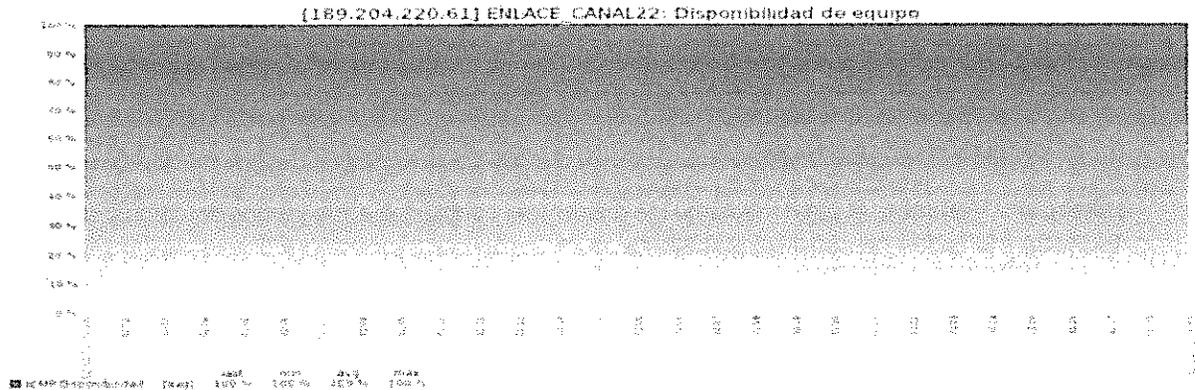


Trafico salida

El **pico máximo de salida** de acceso y publicación a internet correspondiente es de **203.69 Mbps.**



La disponibilidad del enlace para el servicio de acceso y publicación a internet es de: **100%**



5. Glosario de Términos

Ancho de Banda (BW). Es la cantidad de datos que se pueden transmitir en una unidad de tiempo.

Enlace E1. El formato de la señal E1 lleva datos en una tasa de 2,048 Mbps y puede llevar 32 canales de 64 Kbps cada uno, de los cuales treinta y uno son canales activos simultáneos para voz o datos en SS7 (Sistema de Señalización Número 7). En R2 el canal 16 se usa para señalización, por lo que están disponibles 30 canales para voz o datos.

Enlaces Ethernet. Son las redes de área local y dispositivos bajo el estándar IEEE 802.3 que define el protocolo CSMA/CD, ("Acceso Múltiple por Detección de Portadora con Detección de Colisiones"), actualmente se llama Ethernet a todas las redes cableadas que usan el formato, aunque no tenga CSMA/CD como método de acceso al medio.

LAN. Local Area Network (red de área local).

Segmento de Red. Suele ser definido mediante la configuración del hardware (comúnmente por Router o Switch) o una dirección de red específica.

Volume

- **Volume - Packets (suma):** total de paquetes de entrada contados, total de paquetes de salida contados.
- **Volume - Packets In (suma):** total de paquetes de entrada contados
- **Volume - Packets Out (suma):** total de paquetes de salida contados
- **Volumen - Bytes (suma) total de bytes de entrada contados. Total, de bytes de salida contados**963
- **Volume - Bytes In (suma):** total de bytes de entrada contados
- **Volume - Bytes Out (suma):** total de bytes de salida contados

Availability

Disponibilidad (prom%): la disponibilidad promedio para todas las muestras. Calculado con NNMI usando múltiples valores incluido, pero no limitado a: IfOperStatus, IfLastchange, ifDminstatus.

Utilization

Utilization - Avg%: consumo promedio de entrada, consumo promedio de salida

- **Utilization In (promedio)**
- **Utilization Out (promedio)**

Utilization- Max%: consumo máximo de entrada (valor más grande de cualquier muestra); consumo máximo de salida (el valor más grande de cualquier muestra)

- Utilization In (promedio)
- Utilization Out (promedio)

Utilization - Variance: el valor medio de las diferencias cuadradas entre puntos de datos y el promedio, la varianza es tabulada en unidades cuadradas.

- Utilization In (promedio)
- Utilization Out (promedio)

Errors:Número total de paquetes con errores, paquetes de entrada y salida combinados; número de paquetes de entrada con errores, número de paquetes de salida con errores.

- Errors - Packets (suma)
- Errors - Packets In(suma)
- Errors - Packets Out(suma)

Número total de paquetes con errores como un porcentaje del total de paquetes; seguido por el número de paquetes recibidos con errores, como un porcentaje del total de paquetes recibidos y el número de paquetes transmitidos con errores como un porcentaje del total de paquetes transmitidos.

- Error Rate (promedio)
- Error Rate (mínimo)
- Error Rate (máximo)
- Error Rate In(promedio)
- Error Rate In (mínimo)
- Error Rate In (máximo)
- Error Rate Out (promedio)
- Error Rate Out (mínimo)
- Error Rate Out (máximo)

Discard Rate

Número total de paquetes descartados como un porcentaje del total de paquetes(mínimo, máximo y promedio); seguido por el número de paquetes descartados de entrada, como un porcentaje del número total de paquetes de entrada (mínimo, máximo, promedio), y el número de paquetes descartados de salida, como un porcentaje del número total de paquetes de salida (mínimo, máximo, promedio).

- Discard Rate (promedio, mínimo y máximo)
- Discard Rate In(promedio, mínimo y máximo)
- Discard Rate Out(promedio, mínimo, máximo)

Exceptions

Utilization Exceptions: número de excepciones; porcentaje de muestras por encima o debajo del rango normal.

- Utilization Exceptions (# de muestras)
- Utilization Exceptions (% de muestras)

Discard Exceptions: número de excepciones de paquetes descartados, porcentaje de muestras sobre el umbral de la excepción de descarte.

- Discard Exceptions (# de muestras)
- Discard Exceptions (% de muestras)

Error Exceptions: número de excepciones de error de paquetes, porcentaje de muestras por encima del umbral de excepción de error.

- Error Exceptions (# de muestras)
- Error Exceptions (% de muestras)

Availability Exceptions: número de excepciones de disponibilidad; porcentaje de muestras que evidencian Ifoperstatus=down

- Availability Exceptions (# de muestras)
- Availability Exceptions (% de muestras)



Reporte de Incidentes y Solicitudes de Mesa de Servicio

CANAL 22



FEBRERO 2021

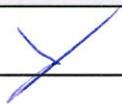
Firmas de revisión, aprobación y recepción del documento.

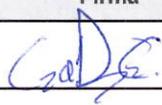
Entregable	Clave	Servicio	Medio
	MCS-CANAL 22	Mesa de Servicios	Electrónico

Elaboración	Puesto	Nombre	Firma	Fecha
	Coordinador de Mesa de Servicios	Alejandro Rubén de la Cruz Ornelas		01/03/2021

Revisión	Puesto	Nombre	Firma	Fecha
	Líder de Proyecto	Victor Quiroz Barrientos		01/03/2021

Aprobación	Puesto	Nombre	Firma	Fecha
	Subgerencia de Innovación Tecnológica	Lic. Adrian Morán Checa		01/03/2021

Recepción Cliente	Puesto	Nombre	Firma	Fecha
	Gerente de Tecnologías de la Información	Ing. Juan Pablo Rosas Turanzas		17/mar/2021

Aprobación Cliente	Puesto	Nombre	Firma	Fecha
	Jefe de Unidad Departamental	Ing. Emilio René García Rodríguez		17/mar/2021

Introducción al documento.

El presente documento muestra un concentrado de los eventos reportados a la Mesa Central de Servicios INFOTEC durante el mes FEBRERO 2021.

Se incluye el concentrado de eventos por categoría y las gráficas representativas de esta información; además de anexar el detalle de los incidentes en un archivo adjunto al presente, si es que aplica.

Al final, encontrará un glosario donde se definen los términos utilizados en este documento.

Esperamos que este documento le sea de utilidad para la toma de decisiones, con relación a los eventos reportados.

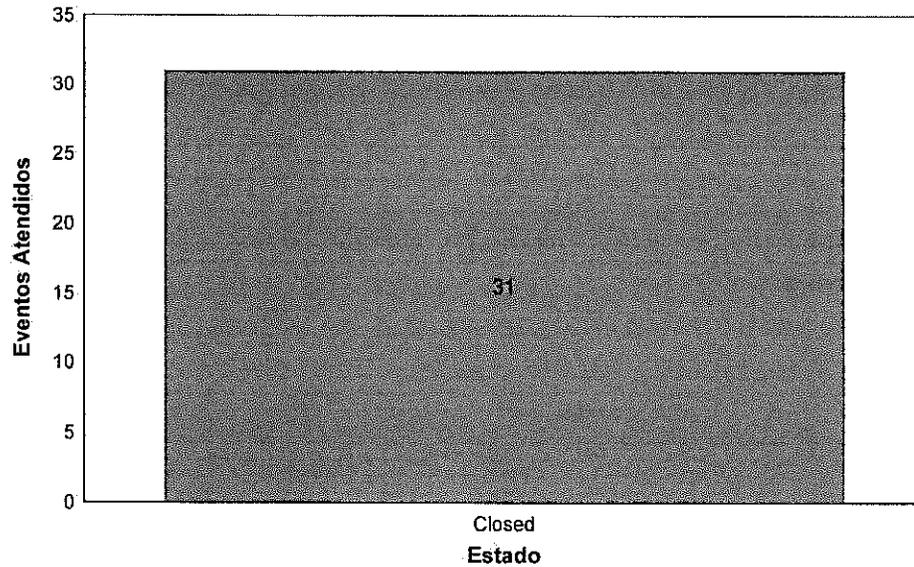
Atentamente.

Mesa Central de Servicios INFOTEC
Dirección Adjunta de Desarrollo Tecnológico.

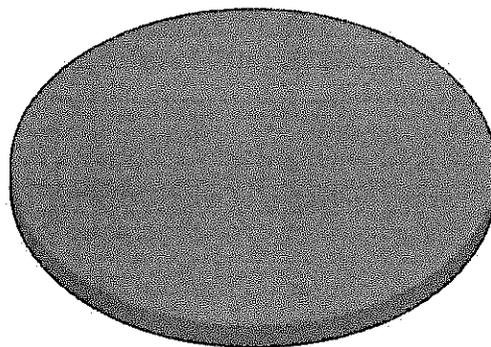
CANAL 22

Las siguientes gráficas muestran los eventos atendidos durante el periodo reportado, clasificados por tipo y estado.

Estado de Eventos



Tipo de Eventos



Solicitud
31

Nota:
Solicitud de Servicio se deberá entender como Requerimiento.

CANAL 22

Detalle de Eventos

Título: Reporte de consumo de ancho de banda-2021-02-01-1000
Descripción: Favor de levantar un TK al área del SOC para la generación del reporte de consumo de ancho de banda del cliente CANAL 22.

Se adjunta el reporte.

Atendido por: YEBRA MELENDEZ, MARCO ANTONIO
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 01/02/2021 10:14:12a.m.
Ticket asignado: TK308554
Medio de contacto: Correo electrónico
Estado evento: Cerrado
Solución: 01/02/2021 10:00 Hrs En atención al evento se reciben comentarios por parte de SOC:

Se adjunta el reporte.

Fecha y hora de cierre: 01/02/2021 01:20:45p.m.
Tiempo total del Ticket: 00 03:06:33

Título: Reporte de consumo de ancho de banda-2021-02-02-1000_Canal_22
Descripción: Favor de levantar un TK al área del SOC para la generación del reporte de consumo de ancho de banda del cliente CANAL 22.

Se adjunta el reporte.

Atendido por: GUEVARA MORALES, TERESA_
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 02/02/2021 10:03:01a.m.
Ticket asignado: TK308582
Medio de contacto: Correo electrónico
Estado evento: Cerrado

CANAL 22

Detalle de Eventos

Solución: 02/02/2021 10:03 Hrs. En atención al evento le hacemos llegar los comentarios del SOC.

Se adjunta el reporte.

Fecha y hora de cierre: 02/02/2021 11:10:18a.m.

Tiempo total del Ticket: 00 01:07:17

Título: Reporte de consumo de ancho de banda-2021-02-03-1000

Descripción: Buenos días,

Favor de levantar un TK al área del SOC para la generación del reporte de consumo de ancho de banda del cliente CANAL 22.

Se adjunta el reporte.

Saludos cordiales.

Atentamente
Centro de Operaciones de Seguridad
Dirección Adjunta de Desarrollo Tecnológico

Atendido por: SANCHEZ GARCIA, ARISTIDES DE JESUS

Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE

Fecha y hora de apertura: 03/02/2021 10:04:48a.m.

Ticket asignado: TK308659

Medio de contacto: Correo electronico

Estado evento: Cerrado

Solución: 03/02/21 10:04 Hrs En atencion al evento se reciben comentarios por parte del SOC:

Se adjunta el reporte.

Fecha y hora de cierre: 03/02/2021 02:06:46p.m.

Tiempo total del Ticket: 00 04:01:58

CANAL 22

Detalle de Eventos

Título: Reporte de consumo de ancho de banda-2021-02-04-1000_Canal_22
Descripción: Favor de levantar un TK al área del SOC para la generación del reporte de consumo de ancho de banda del cliente CANAL 22.

Se adjunta el reporte.

Atendido por: GUEVARA MORALES, TERESA_
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 04/02/2021 10:02:36a.m.
Ticket asignado: TK308762
Medio de contacto: Correo electronico
Estado evento: Cerrado
Solución: 04/02/2021 10:03 Hrs. En atención al evento le hacemos llegar los comentarios del SOC.

Se adjunta el reporte.

Fecha y hora de cierre: 04/02/2021 04:00:54p.m.
Tiempo total del Ticket: 00 05:58:18

Título: Alta de Redes - Acceso a Internet_CANAL 22

Descripción: A través del presente, solicito su apoyo para dar de alta las siguientes redes de datos en la solución de seguridad perimetral, con el fin de tener desde las mismas acceso a Internet y que conexiones VPN puedan llegar a estas redes.

Las redes que fueron habilitadas dentro de Canal 22 son las siguientes:

10.100.1.0/24
10.100.2.0/24

Sin más, quedo atento a sus comentarios, gracias.

Atendido por: CARLOS CRUZ, ELIDETH
Usuario que abre evento: AGUILAR RUIZ, ALFREDO
Fecha y hora de apertura: 04/02/2021 10:09:27p.m.
Ticket asignado: TK308826
Medio de contacto: Correo electronico
Estado evento: Cerrado

CANAL 22

Detalle de Eventos

Solución: 18/02/2021 11:55 Hrs. En atención al evento, se reciben comentarios por parte del especialista Efraín Nochebuena del SOC:

Se configuraron las políticas solicitadas. Se agrega evidencia:

Fecha y hora de cierre: 18/02/2021 05:05:56p.m.
Tiempo total del Ticket: 13 18:56:29

Título: Reporte de consumo de ancho de banda-2021-02-05-1000
Descripción: Favor de levantar un TK al área del SOC para la generación del reporte de consumo de ancho de banda del cliente CANAL 22.

Se adjunta el reporte.

--
Saludos cordiales.

Atentamente
Centro de Operaciones de Seguridad
Dirección Adjunta de Desarrollo Tecnológico

Atendido por: SANCHEZ GARCIA, ARISTIDES DE JESUS
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 05/02/2021 10:17:53a.m.
Ticket asignado: TK308849
Medio de contacto: Correo electrónico
Estado evento: Cerrado
Solución: 05/02/2021 10:21 Hrs En atención al evento se reciben comentarios pro parte de SOC:

Se adjunta el reporte

Fecha y hora de cierre: 05/02/2021 03:29:39p.m.
Tiempo total del Ticket: 00 05:11:46

CANAL 22

Detalle de Eventos

Título: Reporte de consumo de ancho de banda-2021-02-06-1000_CANAL 22
Descripción:
Favor de levantar un TK al área del SOC para la generación del reporte de consumo de ancho de banda del cliente CANAL 22.
Se adjunta el reporte.

Atendido por: SANTILLAN MANON, ABRAHAM
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 06/02/2021 10:07:02a.m.
Ticket asignado: TK308917
Medio de contacto: Correo electrónico
Estado evento: Cerrado

Solución: 06/02/2021 10:00 Hrs. En atención al evento se reciben comentarios por parte del SOC:
Favor de levantar un TK al área del SOC para la generación del reporte de consumo de ancho de banda del cliente CANAL 22.
Se adjunta el reporte.

Fecha y hora de cierre: 08/02/2021 11:24:51a.m.
Tiempo total del Ticket: 02 01:17:49

Título: Reporte de consumo de ancho de banda-2021-02-07-1000_CANAL 22
Descripción:
Favor de levantar un TK al área del SOC para la generación del reporte de consumo de ancho de banda del cliente CANAL 22.
Se adjunta el reporte.

Atendido por: YEBRA MELENDEZ, MARCO ANTONIO
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 07/02/2021 10:07:19a.m.
Ticket asignado: TK308955
Medio de contacto: Correo electrónico
Estado evento: Cerrado

CANAL 22

Detalle de Eventos

Solución: 07/02/2021 10:00 Hrs. Ingenieros, en atención al evento le hacemos llegar los comentarios del especialista:

Se adjunta el reporte

Fecha y hora de cierre: 08/02/2021 11:22:03a.m.
Tiempo total del Ticket: 01 01:14:44

Título: Reporte de consumo de ancho de banda-2021-02-08-1000_Canal_22
Descripción: Favor de levantar un TK al área del SOC para la generación del reporte de consumo de ancho de banda del cliente CANAL 22.

Se adjunta el reporte.

Atendido por: GUEVARA MORALES, TERESA_
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 08/02/2021 10:01:58a.m.
Ticket asignado: TK308998
Medio de contacto: Correo electronico
Estado evento: Cerrado

Solución: 08/02/2021 10:01 Hrs. En atención al evento le hacemos llegar los comentarios del SOC.

Se adjunta el reporte.

Fecha y hora de cierre: 08/02/2021 06:49:58p.m.
Tiempo total del Ticket: 00 08:48:00

CANAL 22

Detalle de Eventos

Título: Certificado SSL noticias.canal22.org.mx_CANAL 22
Descripción: Solicito su ayuda para instalar los certificados adjuntos al portal de noticias.canal22.org.mx con el siguiente NAT.

IP Publica

WAF

IP Interna

189.204.131.139

10.0.0.211

172.20.22.19

Quedo al pendiente de cualquier duda o aclaración.

Atendido por: VAZQUÉZ FLORES, LUIS NOE
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 08/02/2021 08:08:59p.m.
Ticket asignado: TK309054
Medio de contacto: Correo electronico
Estado evento: Cerrado
Solución: 08/02/2021 20:39 Hrs.En atención al evento se reciben comentarios del Ing. Carlos Lira del SOC:

Se realizó el cambio de certificado.

Favor de validar el servicio.

Fecha y hora de cierre: 09/02/2021 12:59:40a.m.
Tiempo total del Ticket: 00 04:50:41

CANAL 22

Detalle de Eventos

Título: Reporte de consumo de ancho de banda-2021-02-09-1000 CANAL 22
Descripción: Buenos días,

Favor de levantar un TK al área del SOC para la generación del reporte de consumo de ancho de banda del cliente CANAL 22.

Se adjunta el reporte.

--
Saludos cordiales.

Atentamente
Centro de Operaciones de Seguridad
Dirección Adjunta de Desarrollo Tecnológico

Atendido por: SANCHEZ GARCIA, ARISTIDES DE JESUS
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 09/02/2021 10:10:17a.m.
Ticket asignado: TK309091
Medio de contacto: Correo electronico
Estado evento: Cerrado

Solución: 09/02/2021 10:00 Hrs En atención al evento se reciben comentarios por parte de SOC:

Se adjunta el reporte.

Fecha y hora de cierre: 09/02/2021 12:03:55p.m.
Tiempo total del Ticket: 00 01:53:38

Título: Reporte de consumo de ancho de banda-2021-02-10-1000_CANAL_22
Descripción: Favor de levantar un TK al área del SOC para la generación del reporte de consumo de ancho de banda del cliente CANAL 22.

Se adjunta el reporte.

Atendido por: RODRIGUEZ VELAZQUEZ, YURIKA
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 10/02/2021 10:04:41a.m.
Ticket asignado: TK309172
Medio de contacto: Correo electronico
Estado evento: Cerrado

CANAL 22

Detalle de Eventos

Solución: 10/02/2021 10:00 Hrs En atencion al evento se reciben comentarios por parte de SOC:

Se adjunta el reporte.

Fecha y hora de cierre: 10/02/2021 12:31:30p.m.

Tiempo total del Ticket: 00 02:26:49

Título: Revisar portal de canal22
Descripción: Se comunica el Ing. Emilio Rene, solicitando se revise el portal de canal 22 ya que no esta respondiendo

Atendido por: HUERTA CLEMENTE, GERARDO DIEGO.

Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE

Fecha y hora de apertura: 10/02/2021 03:36:49p.m.

Ticket asignado: TK309204

Medio de contacto: Telefono

Estado evento: Cerrado

Solución: 10/02/2021 En atencion al evento se informa que los servicios se han reestablecido correctamente

Fecha y hora de cierre: 10/02/2021 10:09:13p.m.

Tiempo total del Ticket: 00 06:32:24

Título: Reporte de consumo de ancho de banda-2021-02-11-1000_CANAL_22
Descripción: Favor de levantar un TK al área del SOC para la generación del reporte de consumo de ancho de banda del cliente CANAL 22.

Se adjunta el reporte.

CANAL 22

Detalle de Eventos

Atendido por: RODRIGUEZ VELAZQUEZ, YURIKA
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 11/02/2021 10:10:03a.m.
Ticket asignado: TK309253
Medio de contacto: Correo electronico
Estado evento: Cerrado
Solución: 11/02/21 10:10 Hrs. En atención al evento, se reciben comentarios por parte del SOC:
Favor de levantar un TK al área del SOC para la generación del reporte de consumo de ancho de banda del cliente CANAL 22.

Se adjunta el reporte.

Fecha y hora de cierre: 11/02/2021 12:47:00p.m.
Tiempo total del Ticket: 00 02:36:57

Título: Reporte de consumo de ancho de banda-2021-02-12-1000_Canal_22
Descripción: Favor de levantar un TK al área del SOC para la generación del reporte de consumo de ancho de banda del cliente CANAL 22.

Se adjunta el reporte.

Atendido por: GUEVARA MORALES, TERESA_
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 12/02/2021 10:02:33a.m.
Ticket asignado: TK309311
Medio de contacto: Correo electronico
Estado evento: Cerrado
Solución: 12/02/2021 10:02 Hrs. En atención al evento le hacemos llegar los comentarios del SOC.

Se adjunta el reporte.

Fecha y hora de cierre: 12/02/2021 11:04:34a.m.
Tiempo total del Ticket: 00 01:02:01

CANAL 22

Detalle de Eventos

Título: Reporte de consumo de ancho de banda-2021-02-13-1000_CANAL 22
Descripción: Favor de levantar un TK al área del SOC para la generación del reporte de consumo de ancho de banda del cliente CANAL 22.

Se adjunta el reporte.

Atendido por: SANTILLAN MANON, ABRAHAM
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 13/02/2021 10:03:38a.m.
Ticket asignado: TK309379
Medio de contacto: Correo electronico
Estado evento: Cerrado
Solución: 13/02/2021 10:00 Hrs. En atención al evento se reciben comentarios por parte del especialista:

Se adjunta el reporte

Fecha y hora de cierre: 15/02/2021 09:46:24a.m.
Tiempo total del Ticket: 01 23:42:46

Título: Reporte de consumo de ancho de banda-2021-02-14-1000_CANAL 22
Descripción: Favor de levantar un TK al área del SOC para la generación del reporte de consumo de ancho de banda del cliente CANAL 22.

Se adjunta el reporte.

Atendido por: YEBRA MELENDEZ, MARCO ANTONIO
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 14/02/2021 10:06:44a.m.
Ticket asignado: TK309411
Medio de contacto: Correo electronico
Estado evento: Cerrado

CANAL 22

Detalle de Eventos

Solución: 14/02/2021 10:00 hrs. Ingenieros, en atención al evento le hacemos llegar los comentarios del especialista:

Se adjunta el reporte

Fecha y hora de cierre: 15/02/2021 09:44:44a.m.
Tiempo total del Ticket: 00 23:38:00

Título: Reporte de consumo de ancho de banda-2021-02-15-1000
Descripción: Buenos días,

Favor de levantar un TK al área del SOC para la generación del reporte de consumo de ancho de banda del cliente CANAL 22.

Se adjunta el reporte.

--
Saludos cordiales.

Atentamente
Centro de Operaciones de Seguridad
Dirección Adjunta de Desarrollo Tecnológico

Atendido por: SANCHEZ GARCIA, ARISTIDES DE JESUS
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 15/02/2021 10:06:42a.m.
Ticket asignado: TK309433
Medio de contacto: Correo electronico
Estado evento: Cerrado
Solución: 15/02/2021 10:10 Hrs En atencion al evento se reciben comentarios por parte de SOC:

Se adjunta el reporte.

Fecha y hora de cierre: 15/02/2021 06:05:55p.m.
Tiempo total del Ticket: 00 07:59:13

CANAL 22

Detalle de Eventos

Título: Reporte de consumo de ancho de banda-2021-02-16-1000_Canal_22
Descripción: Favor de levantar un TK al área del SOC para la generación del reporte de consumo de ancho de banda del cliente CANAL 22.

Se adjunta el reporte.

Atendido por: GUEVARA MORALES, TERESA_
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 16/02/2021 10:01:59a.m.
Ticket asignado: TK309510
Medio de contacto: Correo electronico
Estado evento: Cerrado
Solución: 15/02/2021 10:10 Hrs En atencion al evento se reciben comentarios por parte de SOC:

Se adjunta el reporte.

Fecha y hora de cierre: 16/02/2021 11:33:43a.m.
Tiempo total del Ticket: 00 01:31:44

Título: Reporte de consumo de ancho de banda-2021-02-17-1000_CANAL 22
Descripción: Favor de levantar un TK al área del SOC para la generación del reporte de consumo de ancho de banda del cliente CANAL 22.

Se adjunta el reporte.

Atendido por: YEBRA MELENDEZ, MARCO ANTONIO
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 17/02/2021 10:02:51a.m.
Ticket asignado: TK309582
Medio de contacto: Correo electronico
Estado evento: Cerrado

CANAL 22

Detalle de Eventos

Solución: 17/02/2021 10:00 hrs. En atención al evento, se reciben comentarios por parte del especialista del SOC:

Se adjunta el reporte

Fecha y hora de cierre: 17/02/2021 11:08:42a.m.

Tiempo total del Ticket: 00 01:05:51

Título: Reporte de consumo de ancho de banda-2021-02-18-1000_Canal_22

Descripción: Favor de levantar un TK al área del SOC para la generación del reporte de consumo de ancho de banda del cliente CANAL 22.

Se adjunta el reporte.

Atendido por: GUEVARA MORALES, TERESA_.

Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE.

Fecha y hora de apertura: 18/02/2021 10:03:18a.m.

Ticket asignado: TK309661

Medio de contacto: Correo electronico

Estado evento: Cerrado

Solución: 18/02/2021 10:02 Hrs. En atención al evento le hacemos llegar los comentarios del SOC.

Se adjunta el reporte.

Fecha y hora de cierre: 18/02/2021 12:39:51p.m.

Tiempo total del Ticket: 00 02:36:33

Título: Alta de VPN - Canal 22

Descripción: El presente correo es para solicitar su apoyo y generar la siguiente conexión VPN.

No.	Usuario	Usuario	Contraseña	Acceso IP's
1	José Antonio Ruiz Piña	jantonio.ruiz	p14aru1z.Internacional	10.100.1.0/24

CANAL 22

Detalle de Eventos

Atendido por: SANTILLAN MANON, ABRAHAM
Usuario que abre evento: AGUILAR RUIZ, ALFREDO
Fecha y hora de apertura: 18/02/2021 03:33:44p.m.
Ticket asignado: TK309682
Medio de contacto: Correo electronico
Estado evento: Cerrado
Solución: 18/02/2021 16:20 Hrs. atención al evento, se reciben comentarios por parte del Ing. Ramses Lopez del SOC:

Se realizo configuración solicitada, favor de validar el correcto acceso.

Fecha y hora de cierre: 18/02/2021 06:33:50p.m.
Tiempo total del Ticket: 00 03:00:06

Título: Reporte de consumo de ancho de banda-2021-02-19-1000_CANAL 22
Descripción: Favor de levantar un TK al área del SOC para la generación del reporte de consumo de ancho de banda del cliente CANAL 22.

Se adjunta el reporte.

Atendido por: SANTILLAN MANON, ABRAHAM
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 19/02/2021 10:07:26a.m.
Ticket asignado: TK309714
Medio de contacto: Correo electronico
Estado evento: Cerrado
Solución: 19/02/2021 10:00 Hrs. En atención al evento se reciben comentarios por parte del área del SOC:

Se adjunta el reporte.

Fecha y hora de cierre: 19/02/2021 12:44:48p.m.
Tiempo total del Ticket: 00 02:37:22

CANAL 22

Detalle de Eventos

Título: Reporte de consumo de ancho de banda-2021-02-20-1000_CANA L22
Descripción: Favor de levantar un TK al área del SOC para la generación del reporte de consumo de ancho de banda del cliente CANAL 22.

Se adjunta el reporte.

Atendido por: SANTILLAN MANON, ABRAHAM
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 20/02/2021 10:05:47a.m.
Ticket asignado: TK309773
Medio de contacto: Correo electrónico
Estado evento: Cerrado
Solución: 20/02/2021 10:00 Hrs. En atención al evento se reciben comentarios por parte del area del SOC.
Se adjunta el reporte.

Fecha y hora de cierre: 22/02/2021 11:35:03a.m.
Tiempo total del Ticket: 02 01:29:16

Título: Reporte de consumo de ancho de banda-2021-02-21-1000
Descripción: Buenos días,

Favor de levantar un TK al área del SOC para la generación del reporte de consumo de ancho de banda del cliente CANAL 22.

Se adjunta el reporte.

--
Saludos cordiales.

Atentamente
Centro de Operaciones de Seguridad
Dirección Adjunta de Desarrollo Tecnológico

Atendido por: SANCHEZ GARCIA, ARISTIDES DE JESUS
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 21/02/2021 10:25:08a.m.
Ticket asignado: TK309793
Medio de contacto: Correo electrónico
Estado evento: Cerrado

CANAL 22

Detalle de Eventos

Solución: 21/02/2021 10:31 Hrs En atencion al evento se reciben comentarios por parte de SOC:

Se adjunta el reporte.

Fecha y hora de cierre: 22/02/2021 11:34:33a.m.

Tiempo total del Ticket: 01 01:09:25

Título: Reporte de consumo de ancho de banda-2021-02-22-1000_Canal_22

Descripción: Favor de levantar un TK al área del SOC para la generación del reporte de consumo de ancho de banda del cliente CANAL 22.

Se adjunta el reporte.

Atendido por: GUEVARA MORALES, TERESA_

Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE

Fecha y hora de apertura: 22/02/2021 10:03:28a.m.

Ticket asignado: TK309809

Medio de contacto: Correo electronico

Estado evento: Cerrado

Solución: 21/02/2021 10:10 Hrs.En atencion al evento se reciben comentarios por parte de SOC:

Se adjunta el reporte.

Fecha y hora de cierre: 22/02/2021 11:38:51a.m.

Tiempo total del Ticket: 00 01:35:23

Título: Reporte de consumo de ancho de banda-2021-02-23-1000_Canal-22

Descripción: Favor de levantar un TK al área del SOC para la generación del reporte de consumo de ancho de banda del cliente CANAL 22.

Se adjunta el reporte.

CANAL 22

Detalle de Eventos

Atendido por: GUEVARA MORALES, TERESA_
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 23/02/2021 10:02:05a.m.
Ticket asignado: TK309873
Medio de contacto: Correo electronico
Estado evento: Cerrado
Solución: 22/02/2021 10:10 Hrs En atención al evento se reciben comentarios por parte de SOC:

Se adjunta el reporte.

Fecha y hora de cierre: 23/02/2021 12:43:21p.m.
Tiempo total del Ticket: 00 02:41:16

Título: Reporte de consumo de ancho de banda-2021-02-24-1000_CANAL_22
Descripción: Favor de levantar un TK al área del SOC para la generación del reporte de consumo de ancho de banda del cliente CANAL 22.

Se adjunta el reporte.

Atendido por: RODRIGUEZ VELAZQUEZ, YURIKA
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 24/02/2021 10:10:09a.m.
Ticket asignado: TK309959
Medio de contacto: Correo electronico
Estado evento: Cerrado
Solución: 24/02/21 10:10 Hrs. En atención al evento Ingenieros, les informamos que se registró el TK309959 solicitando de su apreciable apoyo para brindar atención al evento que se describe en el correo que antecede.

Fecha y hora de cierre: 26/02/2021 10:41:52a.m.
Tiempo total del Ticket: 02 00:31:43

CANAL 22

Detalle de Eventos

Título: Reporte de consumo de ancho de banda-2021-02-25-1000_Canal_22
Descripción: Favor de levantar un TK al área del SOC para la generación del reporte de consumo de ancho de banda del cliente CANAL 22.

Se adjunta el reporte.

Atendido por: GUEVARA MORALES, TERESA_
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 25/02/2021 10:04:02a.m.
Ticket asignado: TK310011
Medio de contacto: Correo electronico
Estado evento: Cerrado

Solución: 25/02/2021 10:10 Hrs En atencion al evento se reciben comentarios por parte de SOC:

Se adjunta el reporte.

Fecha y hora de cierre: 26/02/2021 10:40:33a.m.
Tiempo total del Ticket: 01 00:36:31

Título: Reporte de consumo de ancho de banda-2021-02-27-1000_CANAL 22
Descripción: Favor de levantar un TK al área del SOC para la generación del reporte de consumo de ancho de banda del cliente CANAL 22.

Atendido por: SANTILLAN MANON, ABRAHAM
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 27/02/2021 10:04:05a.m.
Ticket asignado: TK310125
Medio de contacto: Correo electronico
Estado evento: Cerrado

Solución: 27/02/2021 10:00 Hrs. En atención al evento se reciben comentarios por parte del Área del SOC:

Se adjunta el reporte.

CANAL 22

Detalle de Eventos

Fecha y hora de cierre: 01/03/2021 10:16:55a.m.
Tiempo total del Ticket: 02 00:12:50

Título: Reporte de consumo de ancho de banda-2021-02-28-1000_CANAL_22
Descripción: Favor de levantar un TK al área del SOC para la generación del reporte de consumo de ancho de banda del cliente CANAL 22.

Se adjunta el reporte.

Atendido por: YEBRA MELENDEZ, MARCO ANTONIO
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 28/02/2021 10:03:30a.m.
Ticket asignado: TK310139
Medio de contacto: Correo electronico
Estado evento: Cerrado
Solución: 28/02/2021 10:00 hrs. Ingenieros, en atención al evento le hacemos llegar los comentarios del especialista:

Se adjunta el reporte

Fecha y hora de cierre: 01/03/2021 10:15:37a.m.
Tiempo total del Ticket: 01 00:12:07

CANAL 22

Glosario

Atendido por:	Nombre completo del operador que registra el evento
Departamento:	En caso de estar registrado en la herramienta se presentará el "Departamento" al que pertenece el "Usuario que abre el evento".
Descripción:	Breve narrativa del evento reportado.
Evento:	Cambio de estado importante para: 1.- la gestión de un elemento de configuración, 2.- evaluación de impacto que pueda causar una desviación y/o 3.- de un servicio de TI.
Estado Evento:	Estado de la evento, en este caso es "Abierto", "Cerrado" o si se encuentra asociada a alguna otra actividad.
Fecha y hora de apertura:	Fecha y hora en que se realiza el registro del evento. El formato usado para este campo es dos dígitos para día, dos dígitos para mes, cuatro para año, dos para hora, dos para minutos y dos para segundo en formato de 12 horas indicando si es am o pm.
Fecha y hora de cierre:	Fecha y hora en que se cierra el evento. El formato usado para este campo es dos dígitos para día, dos dígitos para mes, cuatro para año, dos para hora, dos para minutos y dos para segundo en formato de 12 horas indicando si es am o pm.
Incidente:	Cualquier evento que no es parte de la operación estándar de un servicio de TI, y que causa, o puede causar, una interrupción de ese servicio o una disminución de la calidad del mismo.
Medio de contacto:	Medio por el cual se notifica el evento.
Solicitud de Servicio:	El título Solicitud de Servicio deberá ser entendido como Requerimiento que es como se define en el MAAGTIC.
Periodo:	Rango de fechas entre las que será obtenida la información, iniciando en la hora 00:00 del primer día del mes y concluyendo a las 24:00 hrs último día del mismo mes. El formato usado para este campo es dos dígitos para día, dos dígitos para mes y cuatro para año.
Requerimiento:	Solicitud de información, asesoría, un cambio de rutina o acceso a un servicio de TI por parte de un Usuario.
Solución:	Breve resumen de las actividades realizadas para la solución del evento.
Subclasificación1:	Tipo de evento subclasificado en nivel tres de conformidad con las tipificaciones establecidas para su registro.
Subclasificación2:	Detalle del tipo de evento subclasificado en nivel cuatro de conformidad con las tipificaciones establecidas para su registro.
Subtipo de evento:	Clasificación del evento, posterior a su categorización.
Ticket asignado:	Identificador alfanumérico que se le proporciona al "Usuario" para el seguimiento del evento reportado.
Tipo de evento:	Categoría con la cual se clasifica el evento.
Título:	Breve resumen que define el evento reportado.
Ubicación:	"Ubicación" a la cual esta asociado el "Usuario que abre el evento".
Usuario que abre evento:	Nombre completo del "Usuario que reporta el evento".

Notas:

En la gráfica Estado de Eventos las etiquetas de Estado aparecen en inglés pues es como están definidas en la herramienta, y dado que la gráfica se genera automáticamente no es posible cambiarlas. Sin embargo en los datos se generó una función que sustituye el texto en inglés por la correspondiente etiqueta en español.



**Reporte de Seguridad
Perimetral UTM y Seguridad
Para Servidores Web**

CANAL 22 – TELEVISIÓN METROPOLITANA S.A DE C.V.



FEBRERO 2021

Entregable	Clave	No. de contrato	Servicio	Medio
	OP-REP-IPS	A-DGAPEASTI-31602-009-16	Seguridad Perimetral UTM y Seguridad para Servidores Web	Electrónico / Físico

Elaboración	Puesto	Nombre	Firma
	Coordinador del SOC	Miguel Ángel Ávila Cruz	

Revisión	Puesto	Nombre	Firma
	Líder de Proyecto	Víctor Quiroz Barrientos	

Aprobación	Puesto	Nombre	Firma
	Subgerente de Innovación Tecnológica	Lic. Adrián Moran Checa	

Recepción Cliente	Puesto	Nombre	Firma	Fecha
	Gerente de Tecnologías de la Información	Ing. Juan Pablo Rosas Turanzas		17/mar/2021

Aprobación Cliente	Puesto	Nombre	Firma	Fecha
	Jefe de Unidad Departamental	Ing. Emilio René García Rodríguez		17/mar/2021

Tabla de contenido

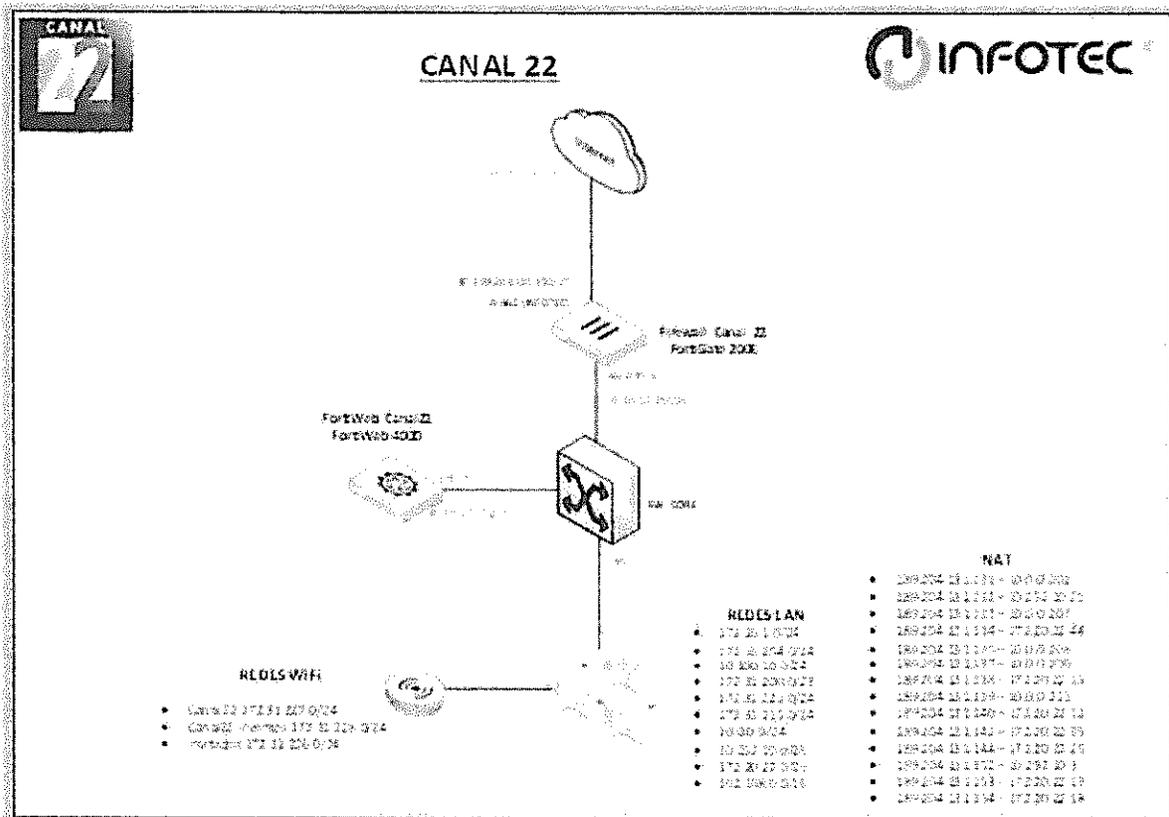
1. Introducción.....	4
2. Diagrama del Servicio.....	4
3. Servicio de Seguridad Perimetral UTM.....	5
3.1. Ataques detectados y detenidos por el IPS.....	9
3.2. Detalle de los ataques detectados y detenidos.....	10
3.3. Amenazas detectadas y bloqueadas.....	16
3.4. Tipo y número de ataques detectados y detenidos.....	17
4. Filtrado de contenido web.....	18
4.1. Bloqueo de usuarios por URL.....	19
5. Direcciones ip con mayor consumo de ancho de banda.....	20
5.1. Top de aplicaciones por consumo de ancho de banda.....	21
5.2. Top de aplicaciones con mayor tiempo de navegación en Internet.....	22
5.3. Consumo de ancho de banda por aplicaciones.....	23
6. Servicio de Seguridad para servidores WEB.....	24
6.1. Políticas aplicadas en WAF.....	24
6.2. Resumen de tipo de ataque.....	25
6.3. Top de políticas por porcentaje.....	26
6.4. Top de ataques por URL.....	26

1. Introducción

El presente documento muestra las políticas reportadas durante el mes, así como la información generada por el Firewall y sus servicios UTM como lo son el IPS y sus firmas activadas para prevenir la intrusión, Las URL's bloqueadas y los usuarios que las visitan, así como la seguridad en las aplicaciones y portales Web. Esto con la finalidad de contar con un reporte de la red de Canal 22.

2. Diagrama del Servicio

Se presenta el diagrama general de red para seguridad a la WAN y protección a la red perimetral:



Prevención de Intrusos

Durante el mes no se solicitaron políticas de IPS. La configuración del mes cuenta con la protección de las firmas indicadas a continuación (2761 Firmas activas):

Edit Filter ✕

Target: server
 OS: Other
 OS: Windows
 OS: Linux
 OS: Solaris
 Application: Other
 Application: IIS
 Application: Apache
 Application: Oracle
 Application: MSSQL
 Application: MySQL
 Application: IE
 Application: Mozilla
 Application: MS_Office
 Application: Adobe
 Application: PHP_app
 Application: ASP_app
 Application: IM
 Protocol: HTTP
 Add Filter

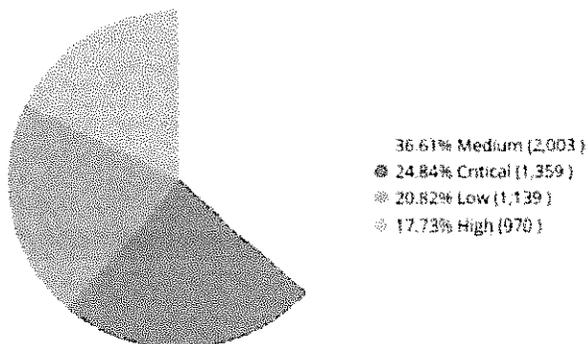
Name	Severity	Target	OS
3Com/OfficeConnect/ADSL Wireless/Firewall/Router/DOS	CRITICAL	Server	Linux
3Com/OfficeConnect/Unity/CDL/Remote/Command/Execution	CRITICAL	Server	Linux
7-Zip/RAR/Soft/Compression/Remote/Code/Execution	CRITICAL	Server/Client	Windows
4COM/Soft/Control/Remote/Code/Execution	CRITICAL	Server	Windows, Linux, BSD, Solaris, Mac OS
427B/Cookie/Based/Authentication/Bypass	CRITICAL	Server	Other
4ardark/Topolab/PHP/Remote/Command/Execution	CRITICAL	Server	Windows, Linux, BSD, Solaris, Mac OS
ABBS/Audio/Media/Player/IST/Buffer/Overflow	CRITICAL	Server/Client	Windows
ACat/Calendar/Cookie/Based/Authentication/Bypass	CRITICAL	Server	Windows, Linux, BSD, Solaris, Mac OS
Accellion/FTA/Content/Information/Disclosure	CRITICAL	Server	Linux, BSD
Accellion/FTA/getStatus/cookie_auth_token/Command/Injection	CRITICAL	Server	Linux, BSD
ACME/Unit/Httpd/Arbitrary/File/Read	CRITICAL	Server	Linux
ActivePDF/Tools/IL/Multiple/File/Memory/Corruption	CRITICAL	Server/Client	Windows
ActivePerl/Perl5/dl/Remote/Buffer/Overflow	CRITICAL	Server	Windows
ActualAnalyzer/ANT/Cookie/Command/Injection	CRITICAL	Server	Linux, BSD
Acunetix/Web/Vulnerability/Scanner	CRITICAL	Server	All
AdMendar/Amn/SQL/Injection	CRITICAL	Server	Windows
Admin/PHP/Upload/Inj/and/Memory	CRITICAL	Server	Windows, Linux, BSD, Solaris, Mac OS
Adobe/Action/and/Render/Triangle/Object/Memory/Corruption	CRITICAL	Server/Client	Windows, Linux, Mac OS
Adobe/Action/and/DMFC/Color/Par/ing/Memory/Corruption	CRITICAL	Server/Client	Windows, Mac OS

1 46 [Total: 2761]

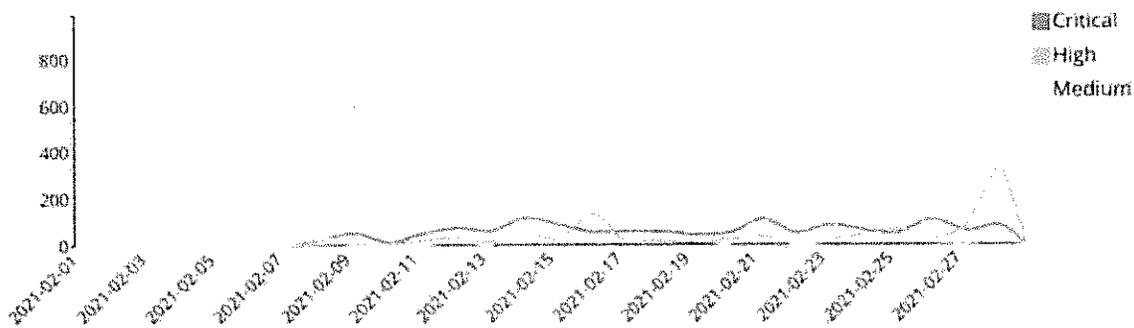
3.1. Ataques detectados y detenidos por el IPS

Las firmas que coincidieron con eventos de intrusión se muestran en las gráficas siguientes:

Intrusions By Severity



Critical High and Medium Intrusions Timeline



3.2. Detalle de los ataques detectados y detenidos

Critical Severity Intrusions

#	Attack Name	CVE-ID	Intrusion Type	Counts
1	PHPMailer Email Injection (PHPMailer) Critical Execution	CVE-2017-9841	Code Injection	488
2	WordPress HTTP Path Traversal	CVE-2019-9618,CVE-2018-16283,CVE-2018-16289,CVE-2020-11738	Path Traversal	120
3	Drupal Drupal.org Drupal Core Path Traversal Critical Execution	CVE-2015-2051,CVE-2019-10891	OS Command Injection	120
4	WordPress Authentication widget Critical Remote Code Execution	CVE-2019-16759	Code Injection	114
5	Drupal Drupal.org Drupal Core Drupal.org Critical Execution	CVE-2018-10561,CVE-2018-10562	OS Command Injection	110
6	WordPress Controller Parameter Remote Code Execution	CVE-2019-9082,CVE-2018-20062	Code Injection	108
7	WordPress Core Security Remote Code Execution	CVE-2015-8562	Code Injection	96
8	WordPress WordPress Core Template Remote PHP Code Execution	CVE-2020-7373,CVE-2020-17496	Code Injection	66
9	WordPress WordPress Core WordPress Core Security Remote Code Execution	CVE-2009-0545,CVE-2019-12725	Code Injection	55
10	WordPress WordPress Core WordPress Core Security Remote Code Execution		Code Injection	22
11	WordPress WordPress Core WordPress Core Security Remote Code Execution	CVE-2014-6271,CVE-2014-6277,CVE-2014-6278,CVE-2014-7169,CVE-2014-7186,CVE-2014-7187	OS Command Injection	16
12	WordPress WordPress Core WordPress Core Security Remote Code Execution	CVE-2017-11317,CVE-2017-11357,CVE-2019-18935	Improper Authentication	12
13	WordPress WordPress Core WordPress Core Security Remote Code Execution	CVE-2018-2600	OS Command Injection	11
14	WordPress WordPress Core WordPress Core Security Remote Code Execution	CVE-2018-1273	Code Injection	9
15	WordPress WordPress Core			4
16	WordPress WordPress Core WordPress Core Security Remote Code Execution	CVE-2019-19781	Path Traversal	3
17	WordPress WordPress Core			2
18	WordPress WordPress Core			2
19	WordPress WordPress Core WordPress Core Security Remote Code Execution	CVE-2016-4438,CVE-2017-12611	Code Injection	1

High Severity Intrusions

#	Attack Name	CVE-ID	Intrusion Type	Counts
1	 HTTP URI SQL Injection		SQL Injection	571
2	 PHP CGI Argument Injection	CVE-2012-1823,CVE-2012-2311	Code Injection	99
3	 Mirai Botnet			99
4	 PhpStudy Web Server Remote Code Execution		Code Injection	64
5	 ThinkPHP HTTP VARS S Remote Code Injection		Code Injection	18
6	 Tongda Office Anywhere Unauthorized File Upload		Improper Authentication	17
7	 General CVE Detection	CVE-2012-3363,CVE-2013-4295,CVE-2013-5015,CVE-2014-3490,CVE-2018-8527,CVE-2018-8532,CVE-2018-8533,CVE-2019-0537,CVE-2019-0948,CVE-2019-2647,CVE-2019-2648,CVE-2019-2649,CVE-2019-2650,CVE-2020-0765,CVE-2018-13415,CVE-2018-13416,CVE-2018-13417,CVE-2018-15444,CVE-2018-18471,CVE-2019-17554,CVE-2019-18227,CVE-2019-18227,CVE-2020-15418,CVE-2020-15419,CVE-2020-26981	Other	16
8	 JAWS DVR CCTV Shell Unauthorized Command Execution		OS Command Injection	15
9	 Geogon Office Anywhere Unauthorized Arbitrary File Upload		OS Command Injection	13
10	 ThinkPHP Request Method Remote Code Execution		Code Injection	11
11	 HTTP Header SQL Injection		SQL Injection	11
12	 Lifeay Portal SOWMS Insecure Deserialization	CVE-2020-7961	Permission/Privilege/Access Control	8
13	 Tongda Router Default Credentials		Anomaly	8
14	 PHP Malicious Shell		Malware	8
15	 Linksys Routers Administrative Console Authentication Bypass		Permission/Privilege/Access Control	6
16	 Netlink SPON Router Remote Command Injection		OS Command Injection	2
17	 U-Frame Connector Unauthorized Arbitrary File Upload	CVE-2020-25212	Permission/Privilege/Access Control	2
18	 Shenzhen TVI DVR Hardcode Credential Login		Permission/Privilege/Access Control	1
19	 Apache Tomcat Arbitrary File Upload	CVE-2017-12615,CVE-2017-12617	Code Injection	1

Medium Severity Intrusions

#	Attack Name	CVE-ID	Intrusion Type	Counts
1	Apache/2.4.18 (Ubuntu) /etc/crontab user agent compromise in /etc/crontab		Anomaly	1,659
2	PHP Disclosure		Anomaly	163
3	Web Server /etc/passwd Files Access		Permission/Privilege/Access Control	89
4	WordPress REST API Username Enumeration Information Disclosure	CVE-2017-5487	Information Disclosure	44
5	Phpseclib 2.0.15 upgrade information disclosure		Information Disclosure	17
6	Apache/2.4.12 (Ubuntu) /etc/passwd Access	CVE-2010-0219	Other	14
7	HTTP Request Injection SQL Injection	CVE-2007-1061	SQL Injection	11
8	PHP/Script /etc/passwd/Arbitrary File Upload	CVE-2009-2265	Permission/Privilege/Access Control	3
9	Drupal 7.30.0 /etc/passwd Arbitrary File Upload	CVE-2018-14773	Permission/Privilege/Access Control	3

En otra categoría también se observaron intentos de ataques sobre HTTP y HTTPS, los cuales fueron bloqueados.

Attacks Over HTTP/HTTPS

#	Attack Name	Severity	Attack Counts	
1	PHP-FPM Localhost RFI Remote Code Execution	Critical	498	498
2	WordPress HTTP Path Traversal	Critical	120	120
3	WordPress WP_Filesystem::copy_dir() Command Execution	Critical	120	120
4	WordPress Router.php widgetConfig Remote Code Execution	Critical	114	114
5	WordPress wp-admin Parameter Remote Code Execution	Critical	108	108
6	WordPress WP_Cache Remote Code Execution	Critical	100	100
7	WordPress wp-admin Remote Code Execution	Critical	96	96
8	WordPress wp-admin Template Remote File Upload	Critical	66	66
9	WordPress wp-admin Type Parameter Remote Command Execution	Critical	55	55
10	WordPress wp-admin Remote Code Execution	Critical	16	16
11	WordPress wp-admin Router.php Remote Code Execution	Critical	11	11
12	WordPress wp-admin wp-admin Arbitrary File Upload	Critical	11	11
13	WordPress wp-admin wp-admin Remote Code Execution	Critical	10	10
14	WordPress wp-admin	Critical	4	4
15	WordPress wp-admin wp-admin Arbitrary File Upload	Critical	3	3
16	WordPress wp-admin	Critical	2	2
17	WordPress wp-admin	Critical	2	2
18	WordPress wp-admin wp-admin Remote Code Execution	Critical	1	1
19	HTTP GET/POST Injection	High	571	571
20	HTTP GET/POST Injection	High	99	99
21	HTTP GET/POST Injection	High	96	96
22	WordPress Web Server Remote Code Execution	High	64	64
23	WordPress wp-admin wp-admin Remote Code Execution	High	18	18
24	WordPress wp-admin wp-admin Arbitrary File Upload	High	17	17
25	WordPress wp-admin	High	16	16
26	WordPress wp-admin wp-admin Remote Code Execution	High	15	15
27	WordPress wp-admin wp-admin	High	11	11
28	WordPress wp-admin wp-admin Arbitrary File Upload	High	11	11

#	Attack Name	Severity	Attack Counts
29	Thin Client Request Method Remote Code Execution	High	11
30	Library Patch(JSANWS) Insecure Deserialization	High	8
31	PHP Mailer Injection	High	8
32	SQL Server Connector Arbitrary File Upload	High	2
33	WordPress Core Update Fingerprinting Remote Code Execution	High	2
34	WordPress TVT DWR Wordpress Core Patch Logic	High	1
35	Apache Remote Access by FTP Method	High	1
36	WordPress Remote php system results via AmptHttpbin Attack	Medium	1,659
37	PHP CRLF	Medium	163
38	Web Server Password Info Access	Medium	89
39	WordPress REST API Usernames Enumeration Attack via Enumeration	Medium	44
40	WordPress Core update information disclosure	Medium	17
41	Apache Remote Access Passwords Access	Medium	12
42	HTTP Method includes SQL Injection	Medium	11
43	WordPress Core update Arbitrary File Upload	Medium	3
44	Symlinky HTTP request header Security Bypass	Medium	3

Direcciones IP de víctimas y direcciones IP orígenes de intentos de intrusión bloqueados por el IPS.

Intrusion Victims

#	Attack Victim	Counts	Critical	High	Medium	Percent of Total Attacks
1	10.0.0.208	1805	0	0	1805	41.67%
2	172.20.22.44	519	0	0	519	18.91%
3	172.20.22.35	300	0	0	300	6.93%
4	10.0.0.211	227	0	0	227	5.24%
5	10.0.0.202	218	0	0	218	5.03%
6	172.20.22.11	205	0	0	205	4.73%
7	172.20.22.25	190	0	0	190	4.39%
8	10.252.10.20	181	0	0	181	4.18%
9	10.0.0.207	178	0	0	178	4.11%
10	10.0.0.209	108	0	0	108	2.49%
11	172.20.22.18	101	0	0	101	2.33%

Intrusion Sources

#	Attack Source	Counts	Critical	High	Medium	Percent of Total Attacks
1	20.52.25.231	1654	0	0	1654	51.43%
2	45.155.205.108	447	0	0	447	13.90%
3	45.155.205.225	144	0	0	144	4.48%
4	68.106.234.65	123	0	0	123	3.82%
5	119.28.222.106	103	0	0	103	3.20%
6	192.96.203.71	86	0	0	86	2.67%
7	112.213.98.9	77	0	0	77	2.39%
8	80.250.82.41	72	0	0	72	2.24%
9	36.112.130.101	52	0	0	52	1.62%
10	36.83.184.231	51	0	0	51	1.59%
11	59.10.151.102	51	0	0	51	1.59%
12	58.47.177.161	49	0	0	49	1.52%
13	106.12.54.16	48	0	0	48	1.49%
14	106.13.120.112	48	0	0	48	1.49%
15	129.204.77.236	45	0	0	45	1.40%
16	77.247.127.87	39	0	0	39	1.21%
17	194.246.92.210	36	0	0	36	1.12%
18	148.101.34.58	31	0	0	31	0.96%
19	194.246.92.250	30	0	0	30	0.93%
20	194.246.92.220	30	0	0	30	0.93%

3.3. Amenazas detectadas y bloqueadas

A continuación, se muestra la gráfica de las principales amenazas descartadas por el IPS.

Intrusions Blocked

#	Intrusion Name	Intrusion Type	Severity	Counts	
1	Denial of Service (DoS) - Flood (Flood) - Denial of Service (DoS) - Flood (Flood) - Denial of Service (DoS) - Flood (Flood)	Code Injection	Critical	488	
2	Denial of Service (DoS) - Flood (Flood) - Denial of Service (DoS) - Flood (Flood) - Denial of Service (DoS) - Flood (Flood)	OS Command Injection	Critical	120	
3	Denial of Service (DoS) - Flood (Flood) - Denial of Service (DoS) - Flood (Flood) - Denial of Service (DoS) - Flood (Flood)	Path Traversal	Critical	120	
4	Denial of Service (DoS) - Flood (Flood) - Denial of Service (DoS) - Flood (Flood) - Denial of Service (DoS) - Flood (Flood)	Code Injection	Critical	114	
5	Denial of Service (DoS) - Flood (Flood) - Denial of Service (DoS) - Flood (Flood) - Denial of Service (DoS) - Flood (Flood)	OS Command Injection	Critical	110	
6	Denial of Service (DoS) - Flood (Flood) - Denial of Service (DoS) - Flood (Flood) - Denial of Service (DoS) - Flood (Flood)	Code Injection	Critical	108	
7	Denial of Service (DoS) - Flood (Flood) - Denial of Service (DoS) - Flood (Flood) - Denial of Service (DoS) - Flood (Flood)	Code Injection	Critical	96	
8	Denial of Service (DoS) - Flood (Flood) - Denial of Service (DoS) - Flood (Flood) - Denial of Service (DoS) - Flood (Flood)	Code Injection	Critical	66	
9	Denial of Service (DoS) - Flood (Flood) - Denial of Service (DoS) - Flood (Flood) - Denial of Service (DoS) - Flood (Flood)	Code Injection	Critical	55	
10	Denial of Service (DoS) - Flood (Flood) - Denial of Service (DoS) - Flood (Flood) - Denial of Service (DoS) - Flood (Flood)	Code Injection	Critical	22	
11	Denial of Service (DoS) - Flood (Flood) - Denial of Service (DoS) - Flood (Flood) - Denial of Service (DoS) - Flood (Flood)	OS Command Injection	Critical	16	
12	Denial of Service (DoS) - Flood (Flood) - Denial of Service (DoS) - Flood (Flood) - Denial of Service (DoS) - Flood (Flood)	Improper Authentication	Critical	12	
13	Denial of Service (DoS) - Flood (Flood) - Denial of Service (DoS) - Flood (Flood) - Denial of Service (DoS) - Flood (Flood)	OS Command Injection	Critical	11	
14	Denial of Service (DoS) - Flood (Flood) - Denial of Service (DoS) - Flood (Flood) - Denial of Service (DoS) - Flood (Flood)	Code Injection	Critical	9	
15	Denial of Service (DoS) - Flood (Flood) - Denial of Service (DoS) - Flood (Flood) - Denial of Service (DoS) - Flood (Flood)		Critical	4	
16	Denial of Service (DoS) - Flood (Flood) - Denial of Service (DoS) - Flood (Flood) - Denial of Service (DoS) - Flood (Flood)	Path Traversal	Critical	3	
17	Denial of Service (DoS) - Flood (Flood) - Denial of Service (DoS) - Flood (Flood) - Denial of Service (DoS) - Flood (Flood)		Critical	2	
18	Denial of Service (DoS) - Flood (Flood) - Denial of Service (DoS) - Flood (Flood) - Denial of Service (DoS) - Flood (Flood)		Critical	2	
19	Denial of Service (DoS) - Flood (Flood) - Denial of Service (DoS) - Flood (Flood) - Denial of Service (DoS) - Flood (Flood)	Code Injection	Critical	1	
20	Denial of Service (DoS) - Flood (Flood) - Denial of Service (DoS) - Flood (Flood) - Denial of Service (DoS) - Flood (Flood)	SQL Injection	High	571	

3.4. Tipo y número de ataques detectados y detenidos

Intrusions By Types

#	Intrusion Type	Counts
1	Anomaly	2,934
2	Code Injection	1,152
3	SQL Injection	593
4	OS Command Injection	287
5	Path Traversal	123
6	Permission/Privilege/Access Control	112
7	Information Disclosure	61
8	Malware	43
9	Other	30
10	Improper Authentication	29

4. Filtrado de contenido web

El filtrado de contenido permite bloquear el acceso a sitios de Internet de acuerdo una clasificación por categorías. El perfil activo en las políticas es el siguiente:

URL	Type	Action	Status	Pattern Type	Pattern	Language	Action	Status
bablatk	Wildcard			Wildcard	http://bablatk.fincalidru214.html	Western		
http://www.pronovations.gob.mx/lovegroup.gal	Wildcard			Wildcard	*bablatk*	Western		
http://bablatk.fincalidru214.html	Wildcard			Wildcard	http://jeffloveronline.com/top	Western		
http://jeffloveronline.com/top	Wildcard			Wildcard	*jeffloveronline.com*	Western		
jeffloveronline.com	Wildcard			Wildcard	http://www.pronovations.gob.mx/lovegroup.gal	Western		
relistadantail.com	Wildcard			Wildcard	*www.cheffgabibeimont.com*	Western		
mandorlacarbali.com	Wildcard			Wildcard	*cheffgabibeimont.com*	Western		
centrocientocatron.com	Wildcard			Wildcard	http://musiteca.mx	Western		
www.relistadantail.com/festival/ficha.php	Simple			Wildcard	*tala-google.es/*	Western		
www.cheffgabibeimont.com	Wildcard			Wildcard	*tala-jodelin.net*	Western		
cheffgabibeimont.com	Wildcard			Wildcard	*font-google.es/*	Western		
http://musiteca.mx	Wildcard			Wildcard	*font-google.com*	Western		
musiteca.mx	Wildcard			Wildcard	*framework-gb.cdn.godims*	Western		
tala-google.es/	Wildcard			Wildcard	*p-typek1.net*	Western		
tala-jodelin.net	Wildcard			Wildcard	*ob-scorecardresearch.com*	Western		
font-google.es/	Wildcard			Wildcard	*www.centrosculturadigital.mx	Western		
font-google.com	Wildcard			Wildcard	gnula-4-	Western		
framework-gb.cdn.godims	Wildcard			Wildcard	*gamajoveria.com*	Western		
p-typek1.net	Wildcard			Wildcard	*tucorgapegula.com*	Western		
ob-scorecardresearch.com	Wildcard							
*www.centrosculturadigital.mx	Wildcard							
gnula-4-	Wildcard							
gamajoveria.com	Wildcard							
tucorgapegula.com	Wildcard							

4.1. Bloqueo de usuarios por URL

A continuación, se muestran las direcciones ip más bloqueadas, así como los destinos a los que se denegó la conexión.

Top 20 Most Blocked Users

#	User (or IP)	Requests	
1	 10.252.10.1		672,703
2	 172.20.22.10		27,833
3	 10.252.10.11		23,724
4	 10.252.10.8		14,076
5	 10.252.10.7		12,110
6	 10.252.10.20		460
7	 10.252.10.44		320
8	 10.252.10.4		153
9	 10.252.10.40		129
10	 10.252.10.41		114
11	 10.252.10.43		114
12	 10.252.10.42		114
13	 10.252.10.9		10

5. Direcciones ip con mayor consumo de ancho de banda

Top 20 Bandwidth Users

#	User (or IP)	Bandwidth
1	172.31.227.12	70.24 GB
2	172.31.226.16	55.95 GB
3	172.16.1.153	33.13 GB
4	172.16.1.6	23.98 GB
5	172.16.1.1	18.31 GB
6	172.31.226.6	17.20 GB
7	172.16.1.241	17.01 GB
8	172.31.226.12	16.89 GB
9	172.31.226.14	16.84 GB
10	172.16.1.236	16.27 GB
11	172.31.215.168	14.78 GB
12	172.31.226.5	14.04 GB
13	10.100.1.19	12.76 GB
14	172.31.226.7	12.25 GB
15	172.16.1.108	11.78 GB
16	172.31.226.10	11.43 GB
17	172.16.1.185	11.29 GB
18	172.31.227.4	11.25 GB
19	172.31.215.174	11.08 GB
20	172.31.228.3	10.30 GB

5.1. Top de aplicaciones por consumo de ancho de banda

La siguiente gráfica muestra la información de las aplicaciones que cuentan con mayor consumo de ancho de banda durante el mes.

Application Categories by Bandwidth

#	Application Category	Bandwidth
1	Web.Client	14.76 GB
2	Social.Media	7.58 GB
3	Email	4.91 GB
4	Video/Audio	3.11 GB
5	Update	2.41 GB
6	Collaboration	782.20 MB
7	Network.Service	497.54 MB
8	General.Interest	291.07 MB
9	Unknown	105.33 MB
10	Remote.Access	75.21 MB

5.2. Top de aplicaciones con mayor tiempo de navegación en Internet

La siguiente gráfica muestra la información de las aplicaciones que cuentan con mayor consumo de ancho de banda durante el mes.

Top 30 Applications by Bandwidth and Sessions

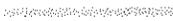
#	Application	Bandwidth	Sent	Received	Sessions
1	HTTP5	60.30 GB			143,297
2	HTTP	18.52 GB			80,176
3	udp/443	10.62 GB			9,103
4	HTTP.BROWSER	7.84 GB			49,993
5	Facebook	7.60 GB			4,296
6	HTTPS.BROWSER	6.91 GB			16,863
7	SMTP	4.36 GB			2,635,680
8	YouTube	2.13 GB			1,454
9	Microsoft.Office.Update	2.02 GB			388
10	udp/3408	2.01 GB			2
11	Netflix	955.98 MB			69
12	VNC	768.20 MB			53
13	Microsoft.Outlook.Office.365	643.39 MB			12,212
14	Microsoft.Portal	567.31 MB			76,002
15	DNS	314.34 MB			1,196,438
16	Apple.Software.Update	306.26 MB			1,781
17	udp/51517	303.22 MB			2
18	Google.Services	217.72 MB			3,977
19	STUN	178.11 MB			227
20	udp/3389	162.79 MB			6
21	udp/55489	106.61 MB			2
22	MS.Windows.Update	74.67 MB			34,604
23	Microsoft.Teams	73.51 MB			3,095
24	TeamViewer	72.86 MB			182
25	tcp/28386	58.78 MB			1
26	tcp/30147	58.40 MB			1
27	tcp/27357	58.36 MB			1
28	Microsofts.Office.365.Portal	46.47 MB			2,821
29	Adobe.Web	35.64 MB			694
30	Microsoft.Authentication	33.10 MB			2,341

5.3. Consumo de ancho de banda por aplicaciones

Un factor importante para el control de servicios es el consumo, ya que permite identificar si alguno de los servicios requiere prioridad alta o si se requiere asignar un mayor número de recursos a un servicio específico.

A continuación, se muestran los consumos por categoría de aplicaciones:

Application Categories by Bandwidth

#	Application Category	Bandwidth	
1	Web.Client		14.76 GB
2	Social.Media		7.58 GB
3	Email		4.91 GB
4	Video/Audio		3.11 GB
5	Update		2.41 GB
6	Collaboration		782.20 MB
7	Network.Service		497.54 MB
8	General.Interest		291.07 MB
9	Unknown		105.33 MB
10	Remote.Access		75.21 MB

6. Servicio de Seguridad para servidores WEB.

6.1. Políticas aplicadas en WAF.

La imagen siguiente muestra las políticas aplicadas en el equipo.

ID	Policy Name	Virtual Server	HTTP Service	HTTPS Service	Deployment Mode	Web Protection Profile	Monitor Mode	Enable	Status
1	Wafgs	Wafgs	HTTP		Single Server/Server Pool	Canal22 Alert Only	Disable	<input checked="" type="checkbox"/>	
2	Informacion	informacion	HTTP		Single Server/Server Pool	Canal22 Alert Only	Disable	<input checked="" type="checkbox"/>	
3	Aplicaciones	Aplicaciones	HTTP		Single Server/Server Pool	Intrusion Alert Only	Disable	<input checked="" type="checkbox"/>	
4	Portal_Canal22	VS_Portal_Canal22	HTTP	HTTPS	Single Server/Server Pool	cc22-portal	Disable	<input checked="" type="checkbox"/>	
5	Informacion_Canal22	VS_Informacion_Canal22	HTTP		Single Server/Server Pool	cc22-portal	Disable	<input checked="" type="checkbox"/>	
6	Canal22ac	VS_Canal22ac	HTTP	HTTPS	Single Server/Server Pool	Intrusion Alert Only	Disable	<input checked="" type="checkbox"/>	
7	Programas	VS_Programas	HTTP		Single Server/Server Pool	Intrusion Alert Only	Disable	<input checked="" type="checkbox"/>	
8	Futbol	VS_Futbol	HTTP		Single Server/Server Pool	Intrusion Alert Only	Disable	<input checked="" type="checkbox"/>	
9	Programas	VS_Programas	HTTP		Single Server/Server Pool	Intrusion Alert Only	Disable	<input checked="" type="checkbox"/>	
10	Historico	VS_Historico	HTTP		HTTP Content Routing	Intrusion Alert Only	Disable	<input checked="" type="checkbox"/>	
11	Analisis de Datos	analisis de datos	HTTP	HTTPS	Single Server/Server Pool	cc22-portal	Disable	<input checked="" type="checkbox"/>	
12	epi_canal22	epi_canal22.gru.mx	HTTP	HTTPS	Single Server/Server Pool	cc22-portal	Disable	<input checked="" type="checkbox"/>	
13	Informacion_php	Informacion_php	HTTP	HTTPS	Single Server/Server Pool	cc22-portal	Disable	<input checked="" type="checkbox"/>	
14	huevo_de_pavito	huevo de pavito	HTTP	HTTPS	Single Server/Server Pool	High Level Security	Enable	<input checked="" type="checkbox"/>	
15	manipareto canal22	manipareto canal22	HTTP	HTTPS	Single Server/Server Pool	cc22-portal	Disable	<input checked="" type="checkbox"/>	

6.2. Resumen de tipo de ataque.

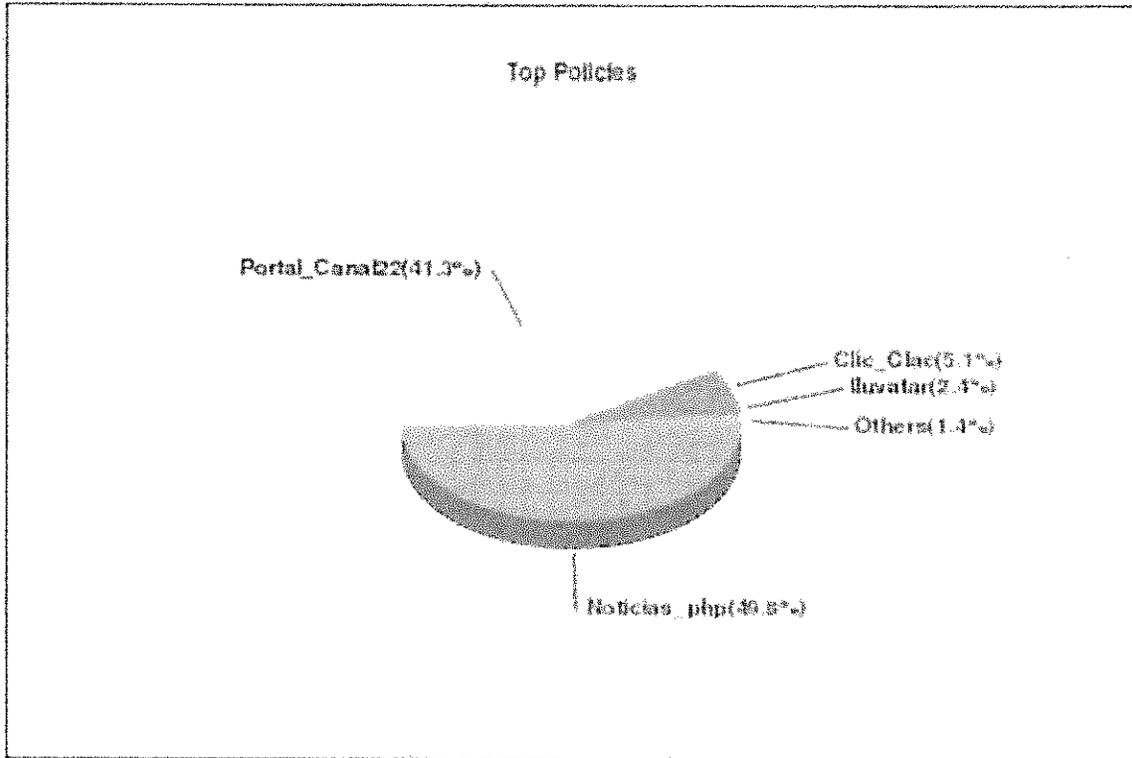
La tabla siguiente muestra un resumen de los ataques detectados y bloqueados por el WAF

Top Attack Types by Date

The daily breakdown of the most frequently detected attack types.

Top Attack Types by Date			
Date	Attack Type	Events	Percent
2021-02-01	HTTP Header Leakage	1390	46.58
	Directory Listing	1196	40.08
	Bad Robot	153	5.13
	Other(16)	245	8.21
	Subtotal(19)	2984	2.90
2021-02-02	Directory Listing	2351	67.83
	HTTP Header Leakage	703	20.28
	Bad Robot	132	3.81
	Other(18)	280	8.08
	Subtotal(21)	3466	3.37
2021-02-03	HTTP Header Leakage	1670	45.94
	Directory Listing	1459	40.14
	Malformed Request	193	5.31
	Other(20)	313	8.61
	Subtotal(23)	3635	3.53
2021-02-04	Directory Listing	2863	70.24
	HTTP Header Leakage	698	17.12
	Malformed Request	281	6.89
	Other(17)	234	5.74
	Subtotal(20)	4076	3.96
2021-02-05	HTTP Header Leakage	1476	47.84
	Directory Listing	1228	39.81
	Malformed Request	123	3.99
	Other(19)	258	8.36
	Subtotal(22)	3085	3.00
2021-02-06	Directory Listing	1747	64.99
	HTTP Header Leakage	699	26.00
	Bad Robot	70	2.60
	Other(16)	172	6.40
	Subtotal(19)	2688	2.61
Other(22)		83050	80.64
Total(28)		102984	100.00

6.3. Top de políticas por porcentaje.



6.4. Top de ataques por URL.

Top Attack URLs		
URL	Events	Percent
/xmlrpc.php	50953	49.48
/cartelera/backend/application.php	17694	17.18
/	16329	15.86
none	2612	2.54
/wp-comments-post.php	1782	1.73
/ap/uedata	1230	1.19
Other(1106)	12384	12.03
Total(1112)	102984	100.00