TELEVISIÓN METROPOLITANA, S.A. DE C.V.

SUBDIRECCIÓN GENERAL DE ADMINISTRACIÓN Y FINANZAS

DIRECCIÓN DE FINANZAS

Nº de Solicitud		
FECHA DE RECEPCIÓN		
DIA	MES	AÑO

SOLICITUD DE PAGO

ÁREA SOLICITANTE : GERENCIA DE TECNOLOGÍAS DE LA INFORMACIÓN

CENTRO DE COSTO: VARIOS

REQUISICIÓN No.: 217

CONTRATO No.: 39/5/2017"C"

FACTURA No.: F19675

No. SICOP: 016674

FORMA DE ADJUDICACIÓN:

DIRECTA: [✓] INVITACIÓN: [ ] LICITACIÓN: [ ] EXCEPCIÓN ART.41 [ ]

BENEFICIARIO: INFOTEC CENTRO DE INVESTIGACIÓN E INNOVACIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN **RFC:** FID741230A22

IMPORTE: $193,091.96

CIENTO NOVENTA Y TRES MIL NOVENTA Y UN PESOS 96 */100 MN)*

DESCRIPCIÓN DEL BIEN O SERVICIO: Servicio de Internet Dedicado, Servicio de Seguridad Perimetral UTM, Servicio de Seguridad para Servidores WEB y Servicio de Monitoreo y Reportes.

Correspondiente al mes de junio 2021.

Transferencia Bancaria: ***CLABE:*** 012180001540457774

Banco: BBVA Bancomer, S.A.

Cuenta: 0154045777

PARA USO EXCLUSIVO DE LA DIRECCIÓN DE FINANZAS

GERENCIA DE PRESUPUESTO

PRE PROCESO:	
PRE SUF:	
COM. PROCESO	
COMPROMISO	

DEPTO. DE TESORERÍA

No. PROCESO	
FOLIO	
No.SOL	
No.PRO DOC.COMP	
FOLIO	
CLC	
FECHA DE PAGO	

CADENAS PRODUCTIVAS	

CLAVE DE AFECTACIÓN PRESUPUESTAL RUBRICA

PARTIDA:_____ **C.C.**_____ **FF:**_____

NOMBRE:

VISTO BUENO DE CONTABILIDAD RUBRICA

NOMBRE:

ÁREA RESPONSABLE DEL GASTO:

ING. JUAN PABLO ROSAS TURANZAS

GERENTE DE TECNOLOGÍAS DE LA INFORMACIÓN

AUTORIZA:

ING. RAÚL YAU MENDOZA

SUBDIRECTOR GENERAL TÉCNICO Y OPERATIVO

TELEVISIÓN METROPOLITANA, S.A. DE C.V.

SUBDIRECCIÓN GENERAL DE ADMINISTRACIÓN Y FINANZAS

DIRECCIÓN DE FINANZAS

FECHA		
DÍA	MES	AÑO
10	9	2021

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: Servicio de Internet Dedicado, Servicio de Seguridad Perimetral UTM, Servicio de Seguridad para Servidores WEB y Servicio de Monitoreo y Reportes. Correspondiente al mes de junio 2021.

FECHA DE RECEPCIÓN: junio 2021

No. DE CONTRATO: 39/5/2017"C"
No. DE REQUISICIÓN: 217

No. DE FACTURA: F19675

DEL PROVEEDOR Y/O PRESTADOR DE SERVICIOS: INFOTEC CENTRO DE INVESTIGACIÓN E INNOVACIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN.

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

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

ATENTAMENTE

NOMBRE: ING. JUAN PABLO ROSAS TURANZAS
CARGO: GERENTE DE TECNOLOGÍAS DE LA INFORMACIÓN

INFOTEC CENTRO DE INVESTIGACIÓN E INNOVACIÓN EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

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 19675

Folio Fiscal	F1920DE2-3673-4B8A-ADFF-CFB597914E73
Fecha Emisión	2021-07-26T00:00:00
Fecha Certificación	2021-07-26T17:54:15
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	
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	21,237.59

Cantidad	Clave	Descripción	Unidad	Precio Unitario	Importe
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	813.04

Cantidad	Clave	Descripción	Unidad	Precio Unitario	Importe
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	2,520.84

Cantidad	Clave	Descripción	Unidad	Precio Unitario	Importe
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	2,061.90

Servicios correspondientes al mes de junio de 2021

Tipo de Comprobante: I
Uso CFDI: G03
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

dh8Urke1rUnQLkkofvtNPst42OKG7RQBdkPHUwci5DFmffdynWKQIPYTwUXN4sPPL45vEM1PNY2l9ZC0vUnhOZl5Va7//K6XSjjjYRZzjoKiC0lY8sx+10Yn/Gento4XjsQiYb5fmeBwmey5HtdFMAb873fpGDHv93KeoRoWdfbpV8lrDX2KSAzF0APU0+hP3d+z13lnPJETtT18vlzhhlOpzOWimgVX8aoxNk1c6ewdzDvi4U+J/Dl8N7Vt6eTXfgTA/rhesH59eZJsFnX4c8pcjslUODuTUfis9uv1lCCQhvRdSvlv/sVPxdiWsl3m9pciYGOHbPyRVL7Gc2ypgw==

Sello digital del SAT

eE7vE64OqpudZHaS/y8kEMtphUCMdheTaoPM4AlbOqPBoN/dmZmNoZEa747kUSLvSfb2N0dKaFsjMalGg5LmlfmKsvexLIbtEz5rVXM/ZKBYnJWQb7ZC4+ZfftY4GKrlEGXXQ9y3PSOwRlZcOrZ3YriLAvAj9FrJ5lTWM1kFBcXkv7aeQSkhFuHsv1bt63Lx/ggvOKQk96lIfwi0ZaMJ22dzgMxGk8AJLOlhTaN3ATOqUZ42HkobV4pKXSE7wA+sHcKrNjFCggO0YbKgm60nqa6WsEgu8hY1hIloXgCQH3+4KdXS69cEJ6+2LTkR0pc8Y+u5SttZ9wScZ+DSfXthlQ==

Cadena original del complemento de certificación digital del SAT

||1.1|F1920DE2-3673-4B8A-ADFF-CFB597914E73|2021-07-26T17:54:15|TLE011122SC2|dh8Urke1rUnQLkkofvtNPst42OKG7RQBdkPHUwci5DFmffdynWKQIPYTwUXN4sPPL45vEM1PNY2l9ZC0vUnhOZl5Va7//K6XSjjjYRZzjoKiC0lY8sx+10Yn/Gento4XjsQiYb5fmeBwmey5HtdFMAb873fpGDHv93KeoRoWdfbpV8lrDX2KSAzF0APU0+hP3d+z13lnPJETtT18vlzhhlOpzOWimgVX8aoxNk1c6ewdzDvi4U+J/Dl8N7Vt6eTXfgTA/rhesH59eZJsFnX4c8pcjslUODuTUfis9uv1lCCQhvRdSvlv/sVPxdiWsl3m9pciYGOHbPyRVL7Gc2ypgw==|00001000000503270882||

Recepción de compra

Número recepción de compra: RECEP-21-1084
Fecha recepción de compra: 20/09/2021

Compra
De: INFOTEC CENTRO DE INVESTIGACIÓN E INNOVACIÓN EN TE CNOLOGÍAS 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 17/09/2021
Id. proveedor P01001338

Confirmar a
Comprador
Número pedido C-PED-21-1128
Fecha pedido 20/09/2021

Nº producto	Descripción	Unidad	Recibido	Pedido	Pedido pendiente
	Nº licitación: PC-21-0279				
	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

No. CFACT-21-1084

Número factura compra: F19675
Fecha factura compra: 20/09/2021
Número de evento: EV1-21-000970

Pagar
Para: INFOTEC CENTRO DE INVESTIGACIÓN E INNOVACIÓN EN TE CNOLOGÍAS 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 17/09/2021
Términos
Id. proveedor P01001338

Confirmar a
Comprador
Número pedido C-PED-21-1128
Fecha pedido 20/09/2021
Forma de pago

Nº producto	PP	PTDA ESP	FF	CECO	Descripción	Unidad	Cantidad	Precio	Precio total
					Nº licitación: PC-21-0279				
	013	31603	1	11	MATERIALES INDIRECTOS	SER	1	4,920.00	4,920.00
	013	31603	1	12	MATERIALES INDIRECTOS	SER	1	2,008.97	2,008.97
	013	31603	1	13	MATERIALES INDIRECTOS	SER	1	5,206.94	5,206.94
	013	31603	1	21	MATERIALES INDIRECTOS	SER	1	11,397.90	11,397.90
	013	31603	1	22	MATERIALES INDIRECTOS	SER	1	21,811.81	21,811.81
	013	31603	1	23	MATERIALES INDIRECTOS	SER	1	7,338.94	7,338.94
	013	31603	1	24	MATERIALES INDIRECTOS	SER	1	15,661.87	15,661.87
	013	31603	1	31	GASTOS DE VENTA	SER	1	4,509.96	4,509.96
	013	31603	1	32	GASTOS DE VENTA	SER	1	1,352.98	1,352.98
	001	31603	1	41	GASTOS DE ADMINISTRACION	SER	1	5,042.95	5,042.95
	001	31603	1	42	GASTOS DE ADMINISTRACION	SER	1	6,969.91	6,969.91
	001	31603	1	43	GASTOS DE ADMINISTRACION	SER	1	10,946.90	10,946.90
	013	31603	1	51	MATERIALES INDIRECTOS	SER	1	4,673.96	4,673.96
	013	31603	1	52	MATERIALES INDIRECTOS	SER	1	16,112.85	16,112.85
	013	31603	1	53	MATERIALES INDIRECTOS	SER	1	28,453.75	28,453.75
	013	31603	1	54	GASTOS DE ADMINISTRACION	SER	1	12,996.98	12,996.98
	001	31603	1	61	GASTOS DE ADMINISTRACION	SER	1	7,051.94	7,051.94

Subtotal:	**166,458.61**
Descuento factura:	0.00
IVA:	26,633.38
Total de MXN:	**193,091.99**

Autorización de pago

RAUL YAU

SUBDIRECTOR GENERAL TECNICO
Y OPERATIVO

Presente:

No.: SP-21-01494

No. Autorización: SP-21-01494

Sirvase efectuar pago a favor de: INFOTEC CENTRO DE INVESTIGACIÓN E INNOVACIÓN EN TE CNOLOGÍAS 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.)

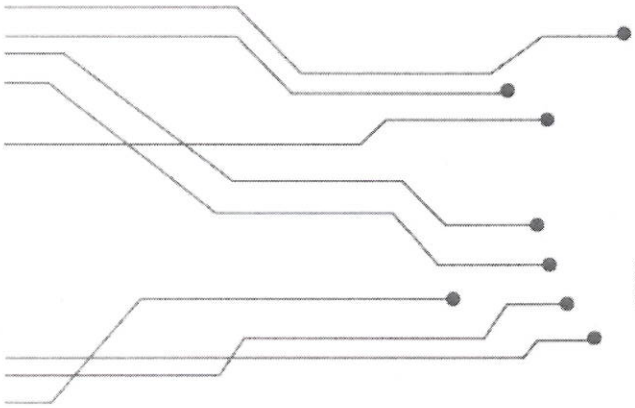
Por el pago que se indica en la Solicitud de Pago número SP-21-01494

Recibida con fecha: lunes, 20 de septiembre de 2021

Descripción	Importe	No. evento
Servicio de internet dedicado, Seguridad perimetra	193,091.96	EV1-21-000970
Total:	193,091.96	

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

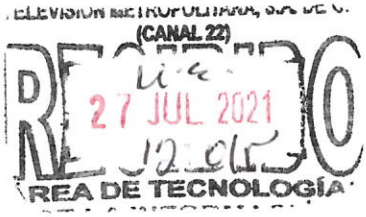
Observaciones: Servicio de Internet Dedicado, Servicio de Seguridad Perimetral UTM, Servicio de Seguridad para Servidores WEB y Servicio de Monitoreo y Reportes.
Correspondiente al mes de junio 2021.



INFOTEC

Reporte de acceso a Internet

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



JUNIO 2021

Información General del Documento

Entregable

Clave	Servicio	Medio
TC-DUAI	Internet Dedicado	Electrónico / Físico

Elaboración

Puesto	Nombre	Firma
Responsable del Servicio	Leones Rodríguez Edgar Abraham	

Revisión

Puesto	Nombre	Firma
Líder de proyecto	Victor Quiroz Barrientos	

Aprobación

Puesto	Nombre	Firma
Encargado del Centro de Operaciones de Seguridad	Lic. Alejandro Camargo Montaño	

Recepción Cliente

Puesto	Nombre	Firma	Fecha
Gerente de Tecnologías de la Información	Ing. Juan Pablo Rosas Turanzas		27/07/2021

Aprobación Cliente

Puesto	Nombre	Firma	Fecha
Jefe de Unidad Departamental	Ing. Emilio René García Rodríguez		27/07/2021

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 Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación (**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).

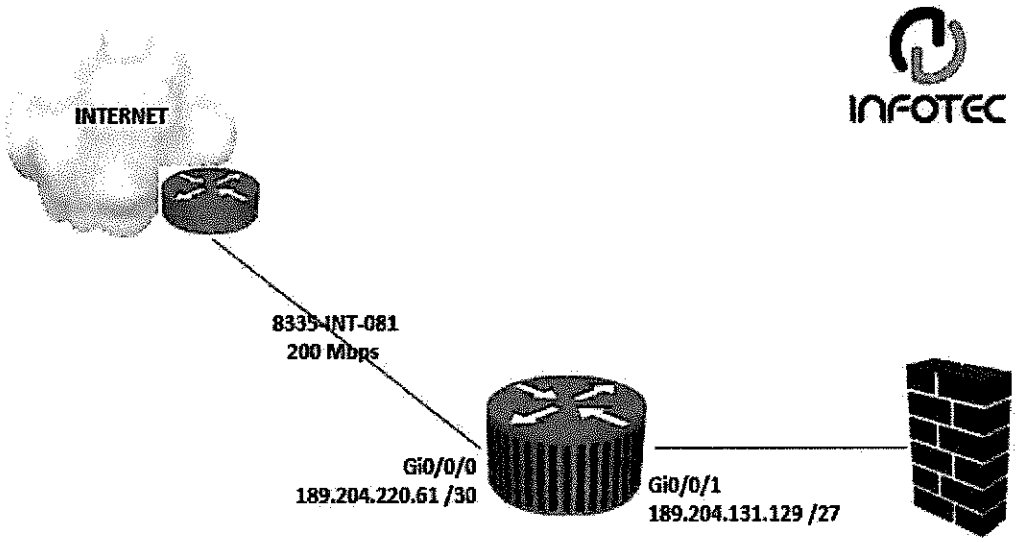
2. Objetivo

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 junio de 2021 al 30 de junio 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.

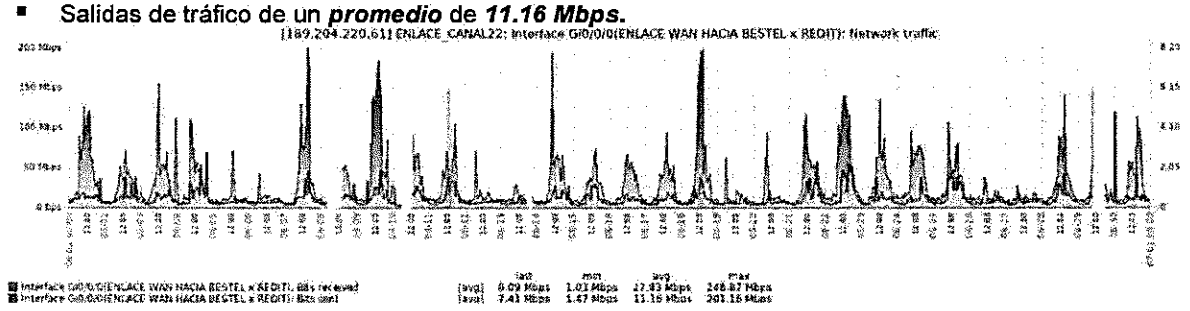
Red de Publicación a INTERNET		
VLAN	**DIRECCIONAMIENTO IP**	**DESCRIPCIÓN**
Por definir	189.204.131.128/27	Administración y Monitoreo

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.

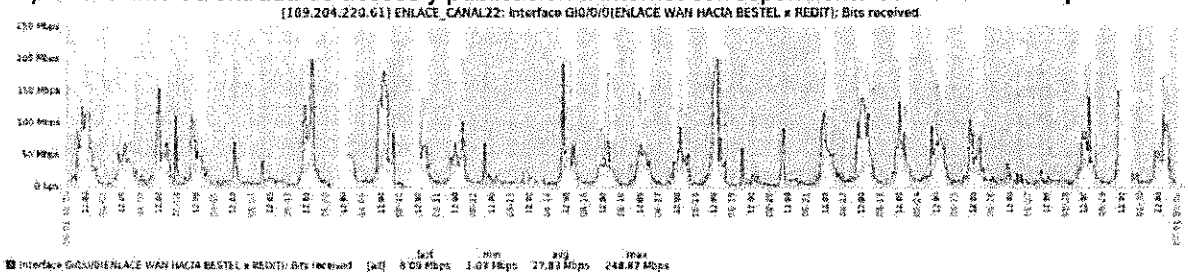
Durante el mes de junio se presentaron los siguientes datos en la interface donde llega el enlace:

- Entradas de tráfico de un ***promedio*** de ***27.83 Mbps.***
- Salidas de tráfico de un ***promedio*** de ***11.16 Mbps.***



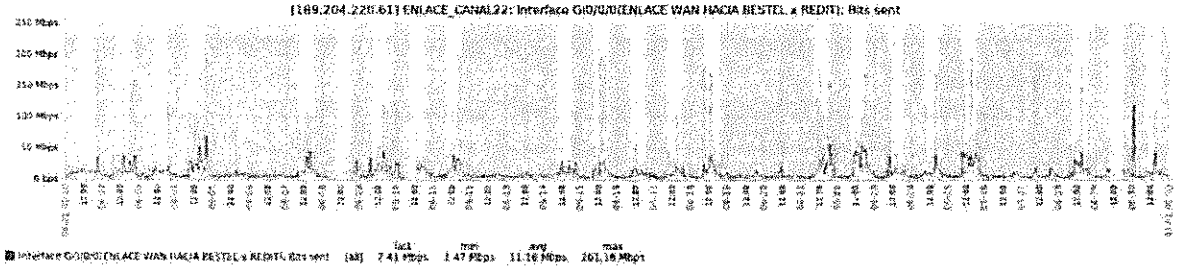
Trafico entrada

El *pico máximo de entrada* de acceso y publicación a internet correspondiente es de **248.87 Mbps.**

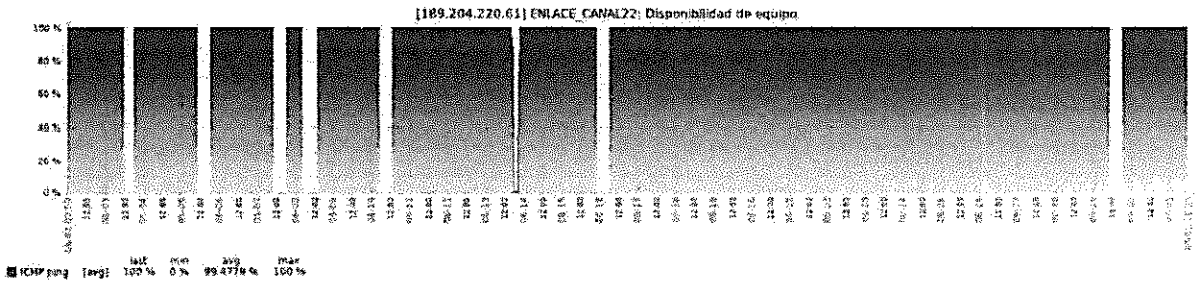


Trafico salida

El *pico máximo de salida* de acceso y publicación a internet correspondiente es de **201.16 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 contados963
- 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

JUNIO 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
Supervior de Mesa de Servicios	Gerardo Diego Huerta Clemente		5/7/2021

Revisión

Puesto	Nombre	Firma	Fecha
Coordinador de Mesa de Servicios	Alejandro Rubén de la Cruz Ornelas		5/7/2021

Aprobación

Puesto	Nombre	Firma	Fecha
Líder de Proyecto	Victor Quiroz Barrientos		5/7/2021

Recepción Cliente

Puesto	Nombre	Firma	Fecha
Gerente de Tecnologías de la Información	Ing. Juan Pablo Rosas Turanzas		27/07/2021

Aprobación Cliente

Puesto	Nombre	Firma	Fecha
Jefe de Unidad Departamental	Ing. Emilio René García Rodríguez		27/07/2021

Introducción al documento.

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

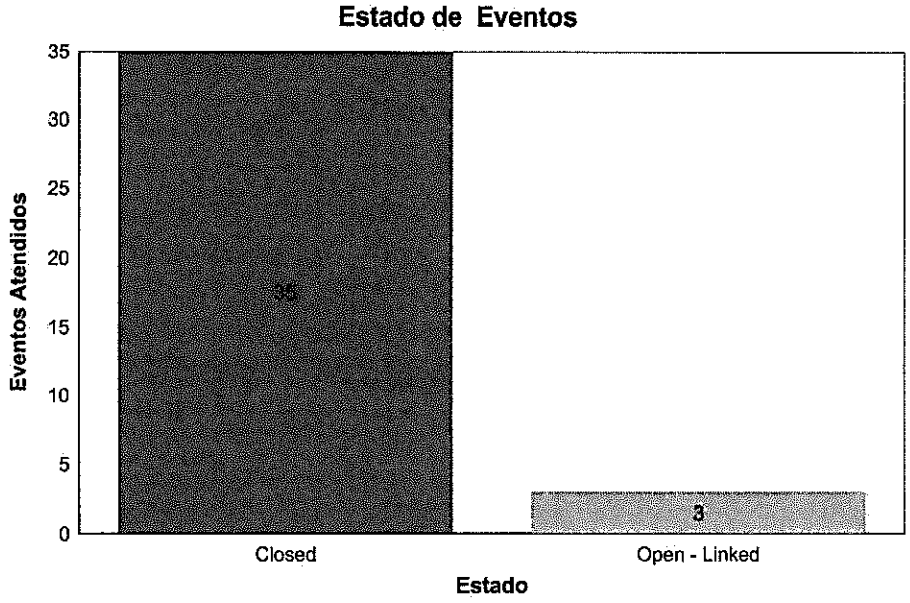
Esperamos que este documento le sea de utilidad para la toma de decisiones, con relación a los eventos reportados.

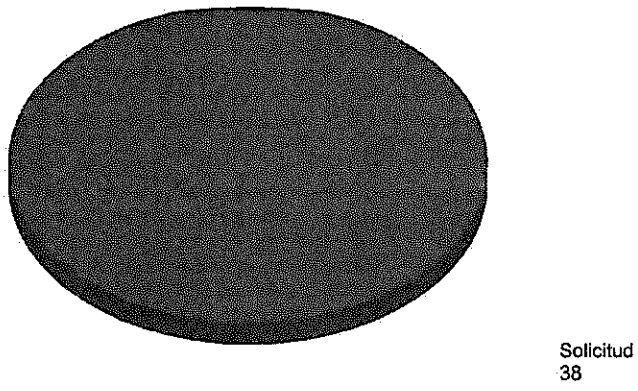
Atentamente.

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.





Nota:
Solicitud de Servicio se deberá entender como Requerimiento.

CANAL 22

Detalle de Eventos

Título:	Solicitud de Actualizar Certificado_CANAL 22
Descripción:	Solicitud de Actualizar Certificado
Atendido por:	YEBRA MELENDEZ, MARCO ANTONIO
Usuario que abre evento:	GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura:	01/06/2021 08:44:06p.m.
Ticket asignado:	TK314404
Medio de contacto:	Telefono
Estado evento:	Cerrado

Solución: 01/06/2021 23:47 Hrs. En atención al evento, se realiza conferencia entre la Ing. Beatriz Escoto el Ing. Víctor Quiroz, el Ing. Kevin Vázquez, el Ing Fermín Sánchez y el Ing. Emilio García de Canal 22, en conferencia se realiza la solicita y se valida por parte del cliente indicando que ya se puede dar por atendido el evento pues las validaciones han sido exitosas.

Fecha y hora de cierre:	02/06/2021 02:01:44a.m.
Tiempo total del Ticket:	00 05:17:38

Título:	Reporte de consumo de ancho de banda-2021-06-02-1000_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.
Atendido por:	SANTILLAN MANON, ABRAHAM
Usuario que abre evento:	GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura:	02/06/2021 10:05:32a.m.
Ticket asignado:	TK314430
Medio de contacto:	Correo electronico
Estado evento:	Cerrado

Solución: 02/06/2021 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:	07/06/2021 08:24:41p.m.
Tiempo total del Ticket:	05 10:19:09

CANAL 22

Detalle de Eventos

Título: Certificado SSL www.canal22.org.mx

Descripción: Solicito su ayuda para realizar el cambio del certificado SSL adjunto para el sitio www.canal22.org.mx con el siguiente direccionamiento:

IP Publica

WAF

IP Interna

Puertos

Descripcion

189.204.131.131

10.0.0.202

172.20.22.10

TCP: 80 -- 443

https://canal22.org.mx

Quedo al pendiente de cualquier duda o aclaración.

Atendido por: SANTILLAN MANON, ABRAHAM
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 02/06/2021 12:21:09p.m.
Ticket asignado: TK314441
Medio de contacto: Correo electronico
Estado evento: Cerrado

CANAL 22

Detalle de Eventos

Solución: 10/06/21 16:29 Hrs. En atención al evento, se reciben comentarios por parte del Ing. Efrain Nochebuena del SOC:

Ya se actualizo el certificado

Fecha y hora de cierre: 10/06/2021 11:51:35p.m.
Tiempo total del Ticket: 08 11:30:26

Título: Estado AP_CANAL 22
Descripción: Solicito su ayuda para verificar el estado del AP con No. de serie: FAP21B3U10004414

Atendido por: SANTILLAN MANON, ABRAHAM
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 02/06/2021 12:55:34p.m.
Ticket asignado: TK314442
Medio de contacto: Correo electronico
Estado evento: Cerrado

Solución: 17/06/2021 00:09 Hrs. En atencion al evento se reciben comentarios del Ing. Kevin Vazquez del SOC:

El estado del AP con No. de serie: FAP21B3U10004414 es :
Autorizado; Desconectado (Sin conexión).

Fecha y hora de cierre: 17/06/2021 05:06:50a.m.
Tiempo total del Ticket: 14 16:11:16

Título: Reporte de consumo de ancho de banda-2021-06-04-1000
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.

CANAL 22

Detalle de Eventos

Atendido por:	GONZALEZ CURENO, ROGELIO
Usuario que abre evento:	GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura:	04/06/2021 10:13:21a.m.
Ticket asignado:	TK314566
Medio de contacto:	Correo electronico
Estado evento:	Cerrado
Solución:	04/06/2021 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:	07/06/2021 08:26:38p.m.
Tiempo total del Ticket:	03 10:13:17

Título:	Reporte de consumo de ancho de banda-2021-06-05-1000
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.

Atendido por:	RODRIGUEZ VELAZQUEZ, YURIKA
Usuario que abre evento:	GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura:	05/06/2021 10:09:53a.m.
Ticket asignado:	TK314630
Medio de contacto:	Correo electronico
Estado evento:	Cerrado
Solución:	04/06/2021 10:00 Hrs. En atención al evento se reciben comentarios por parte del área del SOC:

Se adjunta el reporte.

Ingenieros, les informamos TK314630, solicitando de su apreciable apoyo para brindar atención al evento que se describe en el correo que antecede.

Fecha y hora de cierre:	07/06/2021 08:27:52p.m.
Tiempo total del Ticket:	02 10:17:59

CANAL 22

Detalle de Eventos

Título:	Reporte de consumo de ancho de banda-2021-06-06-1000_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:	GUEVARA MORALES, TERESA_.
Usuario que abre evento:	GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura:	06/06/2021 10:01:59a.m.
Ticket asignado:	TK314647
Medio de contacto:	Correo electronico
Estado evento:	Cerrado
Solución:	06/06/2021 10:05 Hrs. En atención al evento se reciben comentarios por parte del área del SOC:

Se adjunta el reporte.

Fecha y hora de cierre:	07/06/2021 08:24:03p.m.
Tiempo total del Ticket:	01 10:22:04

Título:	Reporte de consumo de ancho de banda-2021-06-07-1000_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.

Atendido por:	SANTILLAN MANON, ABRAHAM
Usuario que abre evento:	GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura:	07/06/2021 10:13:35a.m.
Ticket asignado:	TK314664
Medio de contacto:	Correo electronico
Estado evento:	Cerrado
Solución:	07/06/2021 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:	07/06/2021 08:26:34p.m.
Tiempo total del Ticket:	00 10:12:59

CANAL 22

Detalle de Eventos

Título:	Certificado SSL clicclac.mx CANAL 22
Descripción:	Estimados

Buen día

Solicito su ayuda para instalar el certificado SSL para el sitio https://www.clicclac.mx son el siguiente direccionamiento:

IP Publica

WAF

IP Interna

Puertos

Descripcion

189.204.131.133

10.0.0.207

172.20.22.46

TCP: 80 --> 443

http://clicclac.mx

Quedo al pendiente de cualquier duda o aclaración.

Saludos.

CANAL 22

Detalle de Eventos

Atendido por:	SANCHEZ GARCIA, ARISTIDES DE JESUS
Usuario que abre evento:	GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura:	07/06/2021 11:00:01a.m.
Ticket asignado:	TK314667
Medio de contacto:	Correo electronico
Estado evento:	Cerrado
Solución: del SOC:	21/06/2021 21:44 Hrs. En atencion al evento se reciben comentarios del Ing. Kevin Vazquez

Se ha realizado el cambio de certificado por el proporcionado por el cliente. Además se valido su correcta funcionalidad.

Fecha y hora de cierre:	09/06/2021 04:47:17a.m.
Tiempo total del Ticket:	01 17:47:16

CANAL 22

Detalle de Eventos

Título: Alta clientes VPN CANAL 22

Descripción: Estimados

Buenos dias

Solicito su ayuda para dar de alta los siguientes clientes VPN:

Nombre

Usuario

Contraseña

Acceso IP's

Eva Patricia Arellano

ev4.arellano

3v44r3ll4n0*

10.100.10.20

Rodrigo Moctezuma

rodrigo.moctezuma

m0ct3zum4C22

10.100.10.20

Angélica Aguirre

angelica.aguirre

4ng3l1c4C22*

CANAL 22

Detalle de Eventos

10.100.10.20

Quedo al pendiente de cualquier duda o aclaración.

Saludos.

Atendido por:	SANCHEZ GARCIA, ARISTIDES DE JESUS
Usuario que abre evento:	GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura:	07/06/2021 11:53:46a.m.
Ticket asignado:	TK314673
Medio de contacto:	Correo electronico
Estado evento:	Cerrado
Solución:	08/06/2021 11:02Hrs. en atencion al evento se reciben comentarios del ing. efrain Nochebuena de SOC: Se dieron de alta las VPN ssl. Favor de validar la conexión.

Fecha y hora de cierre:	08/06/2021 05:18:21p.m.
Tiempo total del Ticket:	01 05:24:35

Título:	Monitoreo IP_CANAL 22
Descripción:	Nos están reportando que la IP 172.31.215.168 tiene intermitencia en la red ya que al cargar videos a YouTube en ocasiones se suben y en otras corta la transferencia, por este motivo solicito su ayuda para monitorear la IP durante el día de hoy y hasta el viernes con la finalidad de descartar problemas en la red, cabe mencionar que ya se realizaron pruebas internas para verificar el estado del cableado, switch, plugs, etc.

Quedo al pendiente de cualquier duda o aclaración.

CANAL 22

Detalle de Eventos

Atendido por:	SANTILLAN MANON, ABRAHAM
Usuario que abre evento:	GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura:	07/06/2021 02:09:40p.m.
Ticket asignado:	TK314686
Medio de contacto:	Correo electronico
Estado evento:	Cerrado
Solución:	14/06/2021 22:33 Hrs. En atención al evento se reciben comentarios por parte del Ing. Efrain Nochebuena de SOC:

No se observaron problemas en la navegación en internet ni alto consumo de AB.

Fecha y hora de cierre:	15/06/2021 12:14:03a.m.
Tiempo total del Ticket:	07 10:04:23

Título:	Reporte de consumo de ancho de banda-2021-06-08-1000
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:	RODRIGUEZ VELAZQUEZ, YURIKA
Usuario que abre evento:	GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura:	08/06/2021 10:04:11a.m.
Ticket asignado:	TK314709
Medio de contacto:	Correo electronico
Estado evento:	Cerrado
Solución:	08/06/2021 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:	08/06/2021 11:59:25a.m.
Tiempo total del Ticket:	00 01:55:14

CANAL 22

Detalle de Eventos

Título:	Reporte de consumo de ancho de banda-2021-06-09-1000_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:	09/06/2021 10:14:28a.m.
Ticket asignado:	TK314763
Medio de contacto:	Correo electronico
Estado evento:	Cerrado
Solución:	09/06/2021 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:	10/06/2021 03:49:11a.m.
Tiempo total del Ticket:	00 17:34:43

Título:	Reporte de consumo de ancho de banda-2021-06-10-1000_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.
Atendido por:	SANTILLAN MANON, ABRAHAM
Usuario que abre evento:	GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura:	10/06/2021 10:05:43a.m.
Ticket asignado:	TK314813
Medio de contacto:	Correo electronico
Estado evento:	Cerrado
Solución:	10/06/2021 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:	10/06/2021 07:15:31p.m.
Tiempo total del Ticket:	00 09:09:48

CANAL 22

Detalle de Eventos

Título:	Reporte de consumo de ancho de banda-2021-06-11-1000 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:	11/06/2021 10:17:39a.m.
Ticket asignado:	TK314842
Medio de contacto:	Correo electronico
Estado evento:	Cerrado

Solución:
11/06/2021 10:23 Hrs En atencion al evento se reciben comentarios por parte de SOC:
Se adjunta el reporte.

Fecha y hora de cierre:	11/06/2021 11:42:01a.m.
Tiempo total del Ticket:	00 01:24:22

Título:	Reporte de consumo de ancho de banda-2021-06-12-1000_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.
Atendido por:	SANTILLAN MANON, ABRAHAM
Usuario que abre evento:	GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura:	12/06/2021 10:01:56a.m.
Ticket asignado:	TK314888
Medio de contacto:	Correo electronico
Estado evento:	Cerrado

CANAL 22

Detalle de Eventos

Solución: 12/06/2021 10:00 Htrs. En atención al evento se reciben comentarios por parte del área del SOC:

Se adjunta el reporte.

Fecha y hora de cierre: 14/06/2021 11:11:23p.m.
Tiempo total del Ticket: 02 13:09:27

Título: Reporte de consumo de ancho de banda-2021-06-13-1000_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: GUEVARA MORALES, TERESA_.
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 13/06/2021 10:02:43a.m.
Ticket asignado: TK314909
Medio de contacto: Correo electronico
Estado evento: Cerrado

Solución: 13/06/2021 10:05 Hrs. En atención al evento se reciben comentarios por parte del área del SOC:

Se adjunta el reporte.

Fecha y hora de cierre: 14/06/2021 06:09:25a.m.
Tiempo total del Ticket: 00 20:06:42

CANAL 22

Detalle de Eventos

Título:	Reporte de consumo de ancho de banda-2021-06-14-1000_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:	14/06/2021 10:04:19a.m.
Ticket asignado:	TK314933
Medio de contacto:	Correo electronico
Estado evento:	Cerrado
Solución:	14/06/2021 10:07 Hrs En atencion al evento se reciben comentarios por parte de SOC:

Se adjunta el reporte.

Fecha y hora de cierre:	14/06/2021 10:39:18p.m.
Tiempo total del Ticket:	00 12:34:59

Título:	Reporte de consumo de ancho de banda-2021-06-15-1000

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:	RODRIGUEZ VELAZQUEZ, YURIKA
Usuario que abre evento:	GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura:	15/06/2021 10:07:46a.m.
Ticket asignado:	TK314977
Medio de contacto:	Correo electronico
Estado evento:	Cerrado

CANAL 22

Detalle de Eventos

Solución: 15/06/2021 10:07 Hrs En atencion al evento se reciben comentarios por parte de SOC:

Se adjunta el reporte.

Fecha y hora de cierre: 15/06/2021 07:58:22p.m.
Tiempo total del Ticket: 00 09:50:36

Título: Reporte de consumo de ancho de banda-2021-06-16-1000_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: GONZALEZ CURENO, ROGELIO
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 16/06/2021 10:06:34a.m.
Ticket asignado: TK315032
Medio de contacto: Correo electronico
Estado evento: Cerrado

Solución: 16/06/2021 10:05 Hrs En atención al evento se reciben comentarios por parte de SOC:

Se adjunta el reporte.

Fecha y hora de cierre: 17/06/2021 12:10:14a.m.
Tiempo total del Ticket: 00 14:03:40

Título: Reporte de consumo de ancho de banda-2021-06-17-1000_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.

CANAL 22

Detalle de Eventos

Atendido por:	SANTILLAN MANON, ABRAHAM
Usuario que abre evento:	GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura:	17/06/2021 10:04:32a.m.
Ticket asignado:	TK315063
Medio de contacto:	Correo electronico
Estado evento:	Cerrado
Solución:	17/06/2021 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:	17/06/2021 10:23:21p.m.
Tiempo total del Ticket:	00 12:18:49

Título:	Reporte de consumo de ancho de banda-2021-06-18-1000
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:	18/06/2021 10:08:40a.m.
Ticket asignado:	TK315102
Medio de contacto:	Correo electronico
Estado evento:	Cerrado

CANAL 22

Detalle de Eventos

Solución: 17/06/2021 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: 19/06/2021 01:43:19a.m.
Tiempo total del Ticket: 00 15:34:39

Título: Alta DNS contenidos.canal22.org.mx
Descripción: Solicito su ayuda para dar de alta el dominio "contenidos.canal22.org.mx", para esto primero tenemos que validar que no este en uso la IP homologada 189.204.131.136. Si esta ocupada, solicitaría de su ayuda para que me proporcionen una IP libre, de lo contrario adjunto el formato para dar de alta el dominio.

Atendido por: SANTILLAN MANON, ABRAHAM
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 18/06/2021 01:07:20p.m.
Ticket asignado: TK315107
Medio de contacto: Correo electronico
Estado evento: Cerrado

Solución: 18/06/2021 20:48 Hrs. En atención al evento, se reciben comentarios por parte de la Ing. Anabel Jeronimo:
Les informo que se dio de alta el registro solicitado y ya se encuentra disponible como se muestra a continuación:

Fecha y hora de cierre: 22/06/2021 08:26:51p.m.
Tiempo total del Ticket: 04 07:19:31

Título: Reporte de consumo de ancho de banda-2021-06-19-1000
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.

CANAL 22

Detalle de Eventos

Atendido por:	RODRIGUEZ VELAZQUEZ, YURIKA
Usuario que abre evento:	GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura:	19/06/2021 10:10:54a.m.
Ticket asignado:	TK315149
Medio de contacto:	Correo electronico
Estado evento:	Cerrado
Solución:	19/06/2021 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:	20/06/2021 10:20:43p.m.
Tiempo total del Ticket:	01 12:09:49

Título:	Reporte de consumo de ancho de banda-2021-06-20-1000 CANAL 22
Descripción:	Buenos dias,

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:	20/06/2021 10:04:21a.m.
Ticket asignado:	TK315160
Medio de contacto:	Correo electronico
Estado evento:	Cerrado

CANAL 22

Detalle de Eventos

Solución: 20/06/2021 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: 20/06/2021 10:22:53p.m.
Tiempo total del Ticket: 00 12:18:32

Título: Reporte de consumo de ancho de banda-2021-06-21-1000
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: 21/06/2021 10:23:14a.m.
Ticket asignado: TK315175
Medio de contacto: Correo electronico
Estado evento: Cerrado

Solución: 21/06/2021 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: 23/06/2021 01:05:08a.m.
Tiempo total del Ticket: 01 14:41:54

CANAL 22

Detalle de Eventos

Título:	NAT Subdominio contenidos22.canal22.org.mx
Descripción:	Solicito su ayuda para realizar la publicación del sitio web "contenidos22.canal22.org.mx" con el siguiente NAT

Nombre Publicado Firewall

IP Publica

WAF

IP Interna

Puertos

Contenidos22

189.204.131.136

10.0.0.0/24

172.20.22.12

TCP: 80 --> 443

Quedo al pendiente de cualquier duda o aclaración.

Atendido por:	GONZALEZ CURENO, ROGELIO
Usuario que abre evento:	GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura:	22/06/2021 08:31:18a.m.
Ticket asignado:	TK315222
Medio de contacto:	Correo electronico
Estado evento:	Cerrado

CANAL 22

Detalle de Eventos

Solución: 23/06/21 01:02 Hrs. En atención al evento, se reciben comentarios por parte del Ing. Kevin Vazquez del SOC:

Se ha realizado la configuración solicitada. Favor de validar

Fecha y hora de cierre: 24/06/2021 12:24:29a.m.
Tiempo total del Ticket: 01 15:53:11

Título: Reporte de consumo de ancho de banda-2021-06-22-1000
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: RODRIGUEZ VELAZQUEZ, YURIKA
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 22/06/2021 10:09:08a.m.
Ticket asignado: TK315227
Medio de contacto: Correo electronico
Estado evento: Cerrado

Solución: 22/06/2021 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: 23/06/2021 12:58:42a.m.
Tiempo total del Ticket: 00 14:49:34

Título: Reporte de consumo de ancho de banda-2021-06-23-1000
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.

CANAL 22

Detalle de Eventos

Atendido por:	GUEVARA MORALES, TERESA_.
Usuario que abre evento:	GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura:	23/06/2021 10:15:32a.m.
Ticket asignado:	TK315267
Medio de contacto:	Correo electronico
Estado evento:	Cerrado
Solución:	23/06/2021 10:18 Hrs. En atención al evento se reciben comentarios por parte del área del SOC:

Se adjunta el reporte.

Fecha y hora de cierre:	23/06/2021 09:52:56p.m.
Tiempo total del Ticket:	00 11:37:24

CANAL 22

Detalle de Eventos

Título: Certificados SSL_CANAL 22

Descripción: Solicito su ayuda para agregar el certificado SSL adjunto al WAF para el sitio: http://contenidos22.canal22.org.mx con el siguiente direccionamiento:

Nombre Publicado Firewall

IP Publica

WAF

IP Interna

Puertos

Descripcion

contenidos22

189.204.131.136

10.0.0.217

172.20.22.12

TCP: 80 --> 443

https://contenidos22.canal22.org.mx

Una vez cargado el certificado pido su apoyo para redireccionar las peticiones del pueto 80 al 443.

CANAL 22

Detalle de Eventos

Atendido por:	SANTILLAN MANON, ABRAHAM
Usuario que abre evento:	GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura:	23/06/2021 11:54:00a.m.
Ticket asignado:	TK315276
Medio de contacto:	Correo electronico
Estado evento:	Cerrado

Solución: 24/06/2021 01:04 Hrs. En conferencia realizada entre el Ing. Emilio Garcia de Canal 22 y el especialista Kevin Vazquez del SOC, en conferencia comentan que el evento a quedado resuelto por lo que se envia como atendido_

Fecha y hora de cierre:	24/06/2021 03:39:19a.m.
Tiempo total del Ticket:	00 15:45:19

Título:	Reporte de consumo de ancho de banda-2021-06-24-1000
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:	24/06/2021 10:16:55a.m.
Ticket asignado:	TK315319
Medio de contacto:	Correo electronico
Estado evento:	Cerrado

CANAL 22

Detalle de Eventos

Solución: 24/06/2021 10:10 Hrs En atencion al evento se reciben comentarios por parte de soc:

Se adjunta el reporte.

Fecha y hora de cierre: 25/06/2021 02:01:23p.m.
Tiempo total del Ticket: 01 03:44:28

Título: Reporte de consumo de ancho de banda-2021-06-25-1000_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: 25/06/2021 10:02:26a.m.
Ticket asignado: TK315359
Medio de contacto: Correo electronico
Estado evento: Cerrado

Solución: 23/06/2021 10:05 Hrs. En atención al evento se reciben comentarios por parte del área del SOC:

Se adjunta el reporte.

Fecha y hora de cierre: 25/06/2021 11:51:27p.m.
Tiempo total del Ticket: 00 13:49:01

Título: Reporte de consumo de ancho de banda-2021-06-26-1000
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.

CANAL 22

Detalle de Eventos

Atendido por:	RODRIGUEZ VELAZQUEZ, YURIKA
Usuario que abre evento:	GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura:	26/06/2021 10:09:32a.m.
Ticket asignado:	TK315411
Medio de contacto:	Correo electronico
Estado evento:	Cerrado
Solución:	26/06/2021 10:05 Hrs. En atención al evento se reciben comentarios por parte del área del SOC:

Se adjunta el reporte.

Fecha y hora de cierre:	28/06/2021 01:57:17a.m.
Tiempo total del Ticket:	01 15:47:45

Título:	Reporte de consumo de ancho de banda-2021-06-27-1000
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.
Atendido por:	MORALES FAJARDO, LUIS ALBERTO
Usuario que abre evento:	GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura:	27/06/2021 10:09:50a.m.
Ticket asignado:	TK315433
Medio de contacto:	Correo electronico
Estado evento:	Cerrado
Solución:	27/06/2021 10:05 Hrs. En atención al evento se reciben comentarios por parte del área del SOC:

Se adjunta el reporte.

Fecha y hora de cierre:	28/06/2021 01:58:46a.m.
Tiempo total del Ticket:	00 15:48:56

CANAL 22

Detalle de Eventos

Título:	Reporte de consumo de ancho de banda-2021-06-28-1000
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:	28/06/2021 10:13:41a.m.
Ticket asignado:	TK315441
Medio de contacto:	Correo electronico
Estado evento:	Cerrado
Solución:	28/06/2021 10:15 Hrs. En atención al evento se reciben comentarios por parte del área del SOC:

Se adjunta el reporte.

Fecha y hora de cierre:	29/06/2021 12:13:22a.m.
Tiempo total del Ticket:	00 13:59:41

Título:	Revisión de enlace IP´s_CANAL 22
Descripción:	Solicito su ayuda para revisar el enlace ya que esta presentando mucha intermitencia en especifico en las siguientes IPs 172.31.200.41 y 172.31.227.21

Quedo al pendiente de cualquier duda o aclaración.

CANAL 22

Detalle de Eventos

Atendido por:	GONZALEZ CURENO, ROGELIO
Usuario que abre evento:	GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura:	28/06/2021 05:17:39p.m.
Ticket asignado:	TK315462
Medio de contacto:	Correo electronico
Estado evento:	Abierto con Registro Relacionado

Título:	Reporte de consumo de ancho de banda-2021-06-29-1000 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:	29/06/2021 10:09:08a.m.
Ticket asignado:	TK315478
Medio de contacto:	Correo electronico
Estado evento:	Abierto con Registro Relacionado
Solución:	29/06/2021 10:17 Hrs. En atención al evento se reciben comentarios por parte del área del SOC:

Se adjunta el reporte.

Título:	Reporte de consumo de ancho de banda-2021-06-30-1000_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.

CANAL 22

Detalle de Eventos

Atendido por:	SANTILLAN MANON, ABRAHAM
Usuario que abre evento:	GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura:	30/06/2021 10:05:28a.m.
Ticket asignado:	TK315518
Medio de contacto:	Correo electronico
Estado evento:	Abierto con Registro Relacionado
Solución:	30/06/2021 10:00 Hrs. En atención al evento se reciben comentarios por parte del área del SOC:

Se adjunta el reporte.

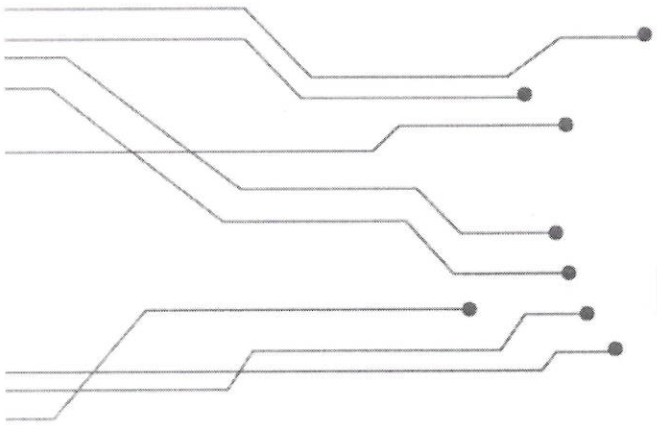
CANAL 22

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 estan 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.



INFOTEC

Reporte de Seguridad Perimetral UTM y Seguridad para Servidores Web

Televisión Metropolitana S.A. de C.V.
Canal 22

JUNIO 2021

Información general del documento

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
Responsable del Servicio	Eduardo Flores Calderón	

Revisión

Puesto	Nombre	Firma
Líder de Proyecto	Víctor Quiroz Barrientos	

Aprobación

Puesto	Nombre	Firma
Encargado del Centro de Operaciones de Seguridad	Lic. Alejandro Camargo Montaño	

Recepción Cliente

Puesto	Nombre	Firma	Fecha
Gerente de Tecnologías de la Información	Ing. Juan Pablo Rosas Turanzas		27/07/2021

Aprobación Cliente

Puesto	Nombre	Firma	Fecha
Jefe de Unidad Departamental	Ing. Emilio René García Rodríguez		27/07/2021

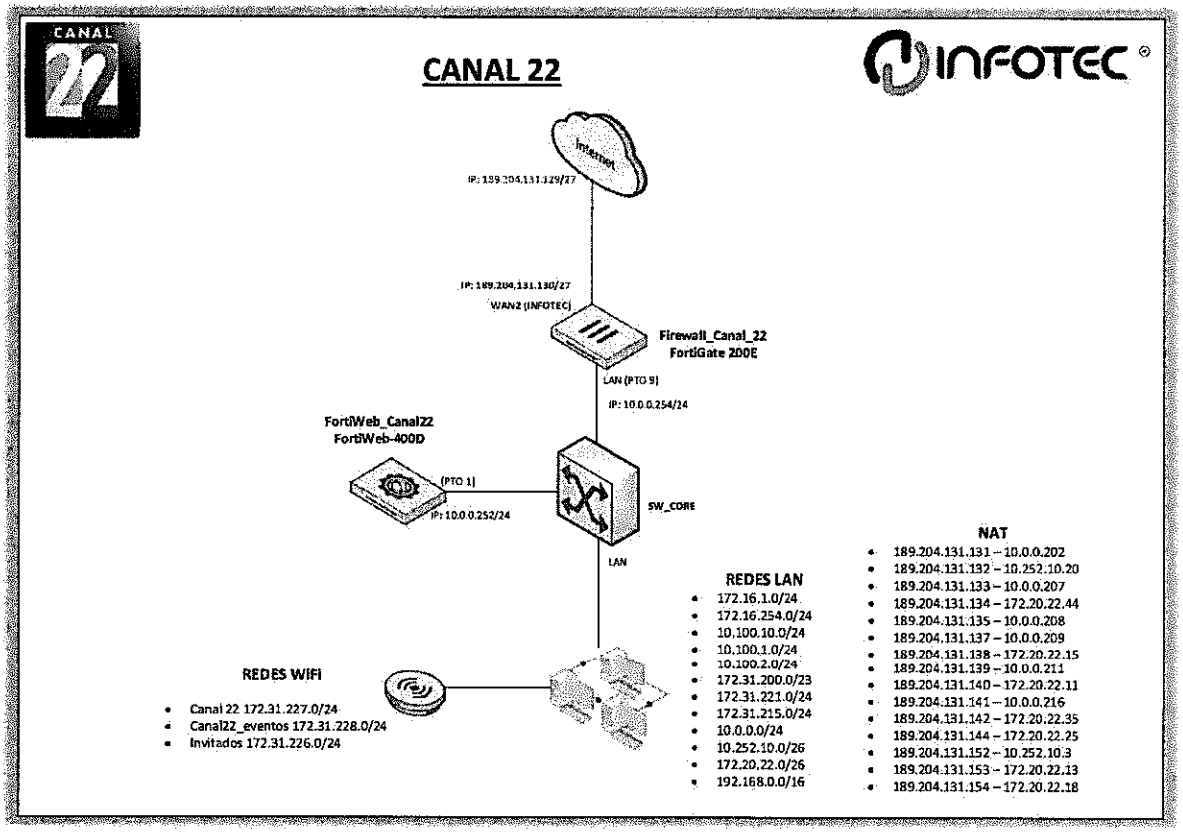
Tabla de contenido

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.

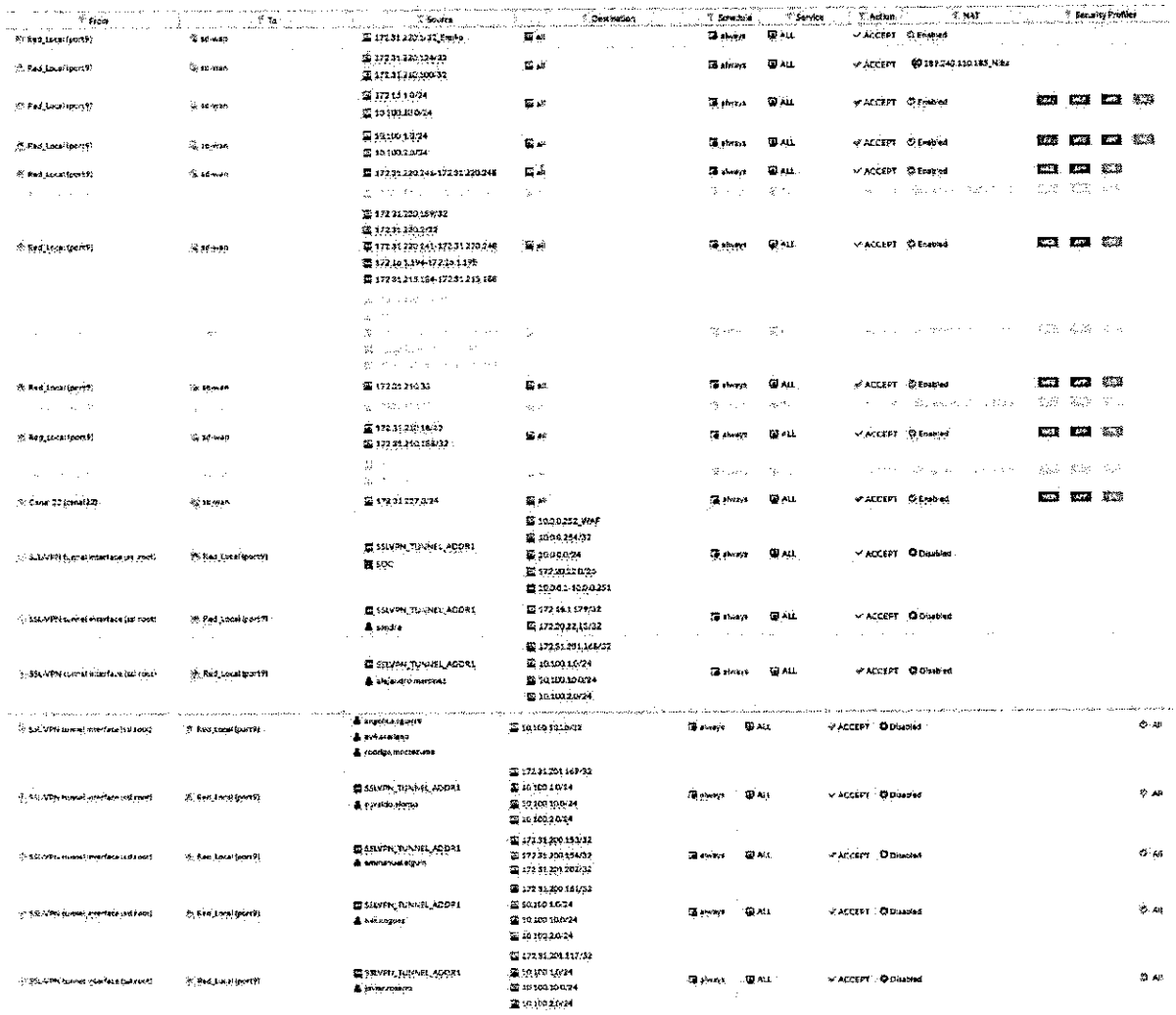
2. Diagrama del Servicio

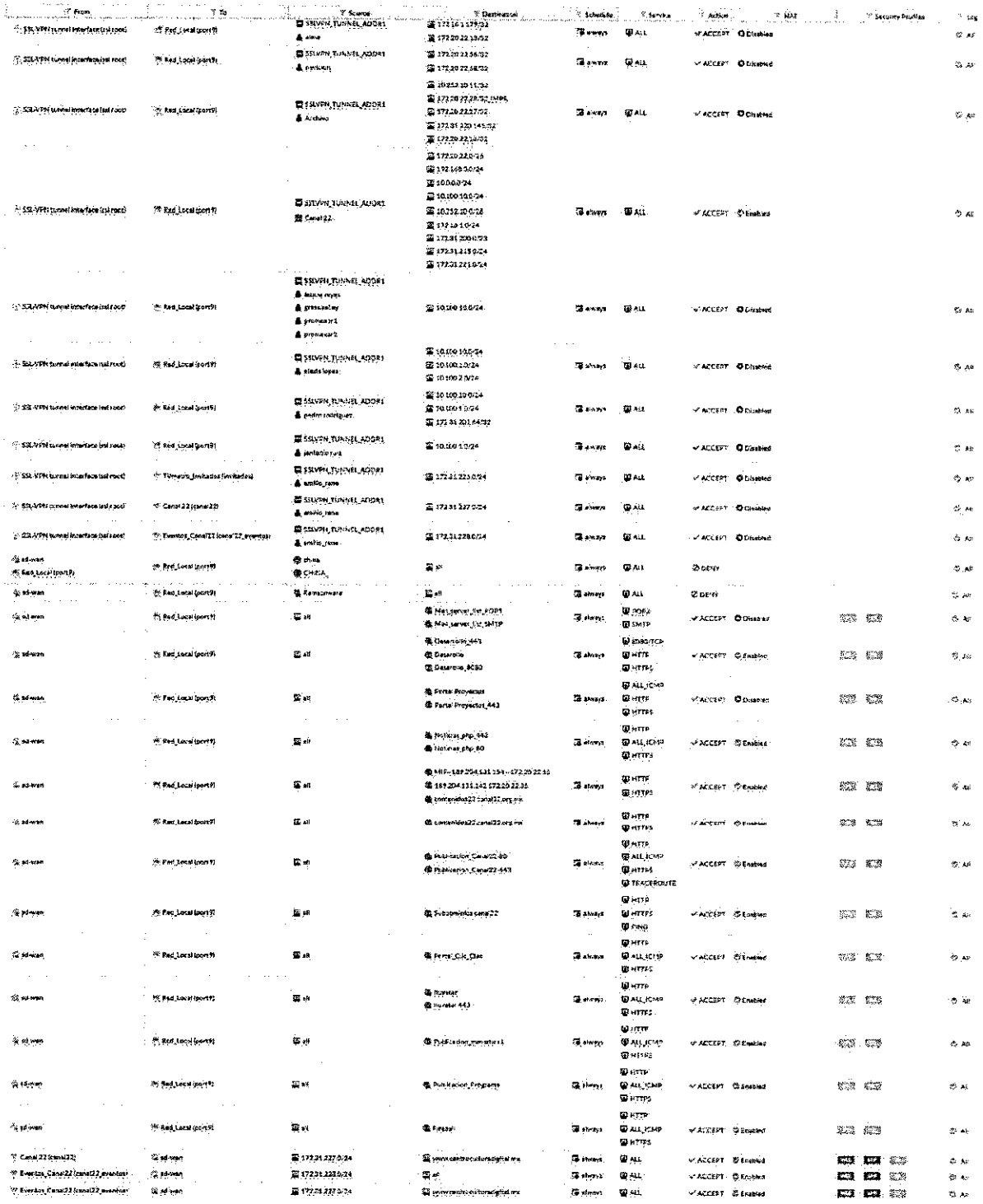
Se presenta el diagrama general de red para seguridad a la WAN y protección a la red perimetral:



3. Servicio de Seguridad Perimetral UTM

En el mes se solicitaron cambios en las políticas, a continuación, se enuncia el inventario de políticas aplicadas para cada uno de los servidores o servicios de la red de Canal 22.




From
To
Source
Destination
Schedule
Service
Action
NAT
Security Profiles
Log
SSLVPN tunnel interface (ssl.root)
Red_Local (port9)
SSLVPN_TUNNEL_ADDR1
always
ALL
ACCEPT
Disabled
All
SSLVPN_TUNNEL_ADDR1
always
ALL
ACCEPT
Disabled
All
SSLVPN_TUNNEL_ADDR1
always
ALL
ACCEPT
Disabled
All
SSLVPN_TUNNEL_ADDR1
Canal 22
always
ALL
ACCEPT
Enabled
All
SSLVPN_TUNNEL_ADDR1
always
ALL
ACCEPT
Disabled
All
SSLVPN_TUNNEL_ADDR1
always
ALL
ACCEPT
Disabled
All
SSLVPN_TUNNEL_ADDR1
always
ALL
ACCEPT
Disabled
All
SSLVPN_TUNNEL_ADDR1
always
ALL
ACCEPT
Disabled
All
SSLVPN_TUNNEL_ADDR1
always
ALL
ACCEPT
Disabled
All
SSLVPN_TUNNEL_ADDR1
always
ALL
ACCEPT
Disabled
All
sd-wan
Red_Local (port9)
always
ALL
DENY
All
sd-wan
Red_Local (port9)
Ransomware
all
always
ALL
DENY
All
sd-wan
Red_Local (port9)
all
always
ALL
ACCEPT
Disabled
All
sd-wan
Red_Local (port9)
all
always
ACCEPT
Enabled
All
sd-wan
Red_Local (port9)
all
always
ACCEPT
Disabled
All
sd-wan
Red_Local (port9)
all
always
ACCEPT
Enabled
All
sd-wan
Red_Local (port9)
all
always
ACCEPT
Enabled
All
sd-wan
Red_Local (port9)
all
always
ACCEPT
Enabled
All
sd-wan
Red_Local (port9)
all
always
ACCEPT
Enabled
All
sd-wan
Red_Local (port9)
all
always
ACCEPT
Enabled
All
sd-wan
Red_Local (port9)
all
always
ACCEPT
Enabled
All
sd-wan
Red_Local (port9)
all
always
ACCEPT
Enabled
All
sd-wan
Red_Local (port9)
all
always
ACCEPT
Enabled
All
sd-wan
Red_Local (port9)
all
always
ACCEPT
Enabled
All
Canal 22 (canal22)
sd-wan
always
ALL
ACCEPT
Enabled
All
sd-wan
always
ALL
ACCEPT
Enabled
All
sd-wan
always
ALL
ACCEPT
Enabled
All

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 (3010 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		Server	Linux	TCP, HTT
3Com.OfficeConnect.Utility.CGI.Remote.Command.Execution		Server	Linux	TCP, HTT
7-Zip.RAR.Solid.Compression.Remote.Code.Execution		Server, Client	Windows	TCP, HTT
427BB.Cookie.Based.Authentication.Bypass		Server	Other	TCP, HTT
Aardvark.Topsites.PHP.Remote.Command.Execution		Server	Windows, Linux, BSD, Solaris, MacOS	TCP, HTT
ABBS.Audio.Media.Player.LST.Buffer.Overflow		Server, Client	Windows	TCP, SM
ACal.Calendar.Cookie.Based.Authentication.Bypass		Server	Windows, Linux, BSD, Solaris, MacOS	TCP, HTT
Accellion.FTA.auth_params.CRLF.Injection		Server	Linux, BSD	TCP, HTT
Accellion.FTA.Cookie.Information.Disclosure		Server	Linux, BSD	TCP, HTT
Accellion.FTA.display_parameter.CRLF.Injection		Server	Linux, BSD	TCP, HTT
Accellion.FTA.getStatus.verify_oauth_token.Command.Injection		Server	Linux, BSD	TCP, HTT
Accellion.FTA.LDAP.Injection		Server	Linux, BSD	TCP, HTT
Accellion.FTA.wmProgressval.SSRF		Server	Linux, BSD	TCP, HTT
ACME.mini_httpd.Arbitrary.File.Read		Server	Linux	TCP, HTT
Acrobat.Acrobat.Reader.CVE-2020-24434.Out.of.Bounds.Read		Server, Client	Windows, MacOS	TCP, HTT
Acrobat.Reader.Acrobat.CVE-2020-24433.Arbitrary.File.Creation		Server, Client	Windows, MacOS	TCP, HTT
ActivePDFToolkit.Multiple.File.Memory.Corruption		Server, Client	Windows	TCP, HTT
ActivePerl.PerlIS.dll.Remote.Buffer.Overflow		Server	Windows	TCP, HTT
ActualAnalyzer.ANT.Cookie.Command.Injection		Server	Linux, BSD	TCP, HTT
Acunetix.Web.Vulnerability.Scanner		Server	All	TCP, HTT
AdMentor.Admin.SQL.Injection		Server	Windows	TCP, HTT
Admin.PHP.Upload.Invalid.Memory		Server	Windows, Linux, BSD, Solaris, MacOS	TCP, HTT
Adobe.Acrobat.and.Reader.JS.Field.Name.Out.of.Bounds.Read		Server, Client	Windows, MacOS	TCP, HTT

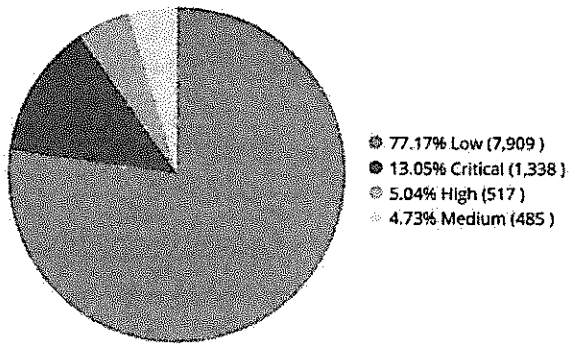
« ‹ 1 /61 › » [Total: 3010]

Save Filters Cancel

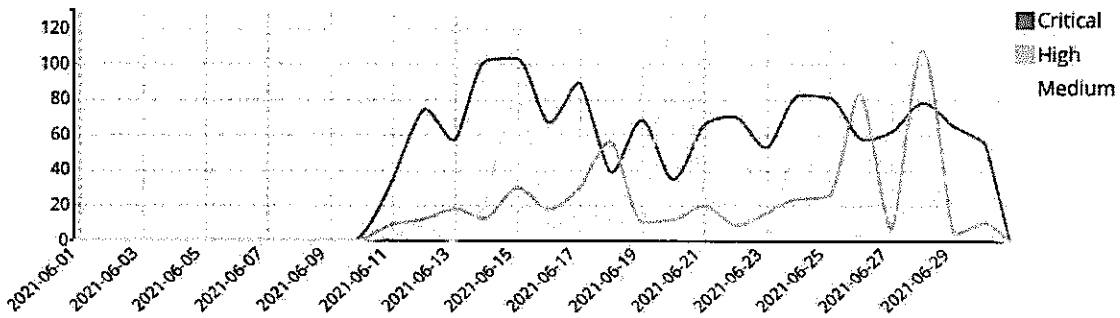
3.1. Ataques detectados y detenidos por el IPS

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	PHPUnit.Eval-stdin.PHP.Remote.Code.Execution	CVE-2017-9841	Code Injection	620
2	Dasan.GPON.Remote.Code.Execution	CVE-2018-10561,CVE-2018-10562	OS Command Injection	157
3	D-Link.Devices.HNAP.SOAPAction-Header.Command.Execution	CVE-2015-2051,CVE-2019-10891	OS Command Injection	148
4	ThinkPHP.Controller.Parameter.Remote.Code.Execution	CVE-2019-9082,CVE-2018-20062	Code Injection	140
5	Gozi.Botnet			75
6	Trojan.TrickBot			42
7	Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execution	CVE-2017-5638	Code Injection	31
8	Telerik.Web.UI.RadAsyncUpload.Handling.Arbitrary.File.Upload	CVE-2017-11317,CVE-2017-11357, CVE-2019-18935	Improper Authentication	26
9	NETGEAR.DGN1000.CGI.Unauthenticated.Remote.Code.Execution		Code Injection	16
10	vBulletin.Routestring.widgetConfig.Remote.Code.Execution	CVE-2019-16759	Code Injection	13
11	Bash.Function.Definitions.Remote.Code.Execution	CVE-2014-6271,CVE-2014-6277,CVE-2014-6278,CVE-2014-7169,CVE-2014-7186,CVE-2014-7187	OS Command Injection	10
12	Joomla!.Core.Session.Remote.Code.Execution	CVE-2015-8562	Code Injection	9
13	WordPress.HTTP.Path.Traversal	CVE-2019-9618,CVE-2018-16283,CVE-2018-16299,CVE-2020-11738	Path Traversal	9
14	vBulletin.tabbedcontainer.Template.Remote.PHP.Code.Execution	CVE-2020-7373,CVE-2020-17496	Code Injection	7
15	HTTP.URI.Java.Code.Injection	CVE-2018-1273	Code Injection	6
16	GhOst.Rat.Botnet			6
17	Bladabindi.Botnet			5
18	Joomla!.list.select.Parameter.SQL.Injection	CVE-2015-7297,CVE-2015-7857,CVE-2015-7858,CVE-2015-7859	Permission/Priviledge/Access Control	4
19	Linux.Kernel.TCP.SACK.Panic.DoS	CVE-2019-11477,CVE-2019-11478, CVE-2019-11479	DoS	4
20	Pushdo.Botnet			3

High Severity Intrusions

#	Attack Name	CVE-ID	Intrusion Type	Counts
1	Mirai.Botnet			155
2	HTTP.URI.SQL.Injection		SQL Injection	123
3	PHP.Malicious.Shell		Malware	50
4	ELFinder.Connector.Minimal.php.Arbitrary.File.Upload	CVE-2020-25213	Permission/Priviledge/Access Control	45
5	PHP.CGI.Argument.Injection	CVE-2012-1823,CVE-2012-2311	Code Injection	34
6	China.Chopper.Web.Shell.Client.Connection		Anomaly	32
7	D-Link.DSL.2640B.Unauthenticated.DNS.Change.Policy.Bypass		Improper Authentication	18
8	Generic.XXE.Detection	CVE-2012-3363,CVE-2013-4295,CVE-2013-5015,CVE-2014-3490,CVE-2016-9563,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,CVE-2021-21658,CVE-2021-21659,CVE-2021-29447	Other	18
9	JAWS.DVR.CCTV.Shell.Unauthenticated.Command.Execution		OS Command Injection	12
10	PhpStudy.Web.Server.Remote.Code.Execution		Code Injection	9
11	D-Link.DSL.2740R.Unauthenticated.DNS.Change.Policy.Bypass		Improper Authentication	6
12	FortiOS.SSL.VPN.Web.Portal.Pathname.Information.Disclosure	CVE-2018-13379	Information Disclosure	5
13	Tongda.Office.Anywhere.Unauthorized.File.Upload		Improper Authentication	2
14	ThinkPHP.HTTP.VARS.S.Remote.Code.Injection		Code Injection	2
15	VACRON.CCTV.Board.CGI.cmd.Parameter.Command.Execution		OS Command Injection	1
16	Linksys.Routers.Administrative.Console.Authentication.Bypass		Permission/Priviledge/Access Control	1
17	ThinkPHP.Request.Method.Remote.Code.Execution		Code Injection	1
18	HTTP.Header.SQL.Injection		SQL Injection	1
19	Seeyon.Office.Anywhere.html officeservlet.Arbitrary.File.Upload		OS Command Injection	1
20	Mitel.Audio.Web.Conferencing.Command.Injection		Code Injection	1

Medium Severity Intrusions

#	Attack Name	CVE-ID	Intrusion Type	Counts
1	WordPress.xmlrpc.php.system.multicall.Amplification.Attack		Anomaly	213
2	Web.Server.Password.Files.Access		Permission/Priviledge/Access Control	178
3	PHP.Diescan		Anomaly	57
4	WordPress.REST.API.Username.Enumeration.Information.Disclosure	CVE-2017-5487	Information Disclosure	28
5	Apache.Axis2.Default.Password.Access	CVE-2010-0219	Other	2
6	FCKeditor.CurrentFolder.Arbitrary.File.Upload	CVE-2009-2265	Permission/Priviledge/Access Control	2
7	Phpweb.CMS.appcode.Information.Disclosure		Information Disclosure	2
8	WordPress.Plugin.Social.Warfare.XSS	CVE-2019-9978	XSS	2
9	HTTP.Referer.Header.SQL.Injection	CVE-2007-1061	SQL Injection	1

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	PHPUnit.Eval-stdin.PHP.Remote.Code.Execution	Critical	620
2	D-Link.Devices.HNAP.SOAPAction-Header.Command.Execution	Critical	148
3	ThinkPHP.Controller.Parameter.Remote.Code.Execution	Critical	140
4	Dasan.GPON.Remote.Code.Execution	Critical	138
5	Gozi.Botnet	Critical	75
6	Trojan.TrickBot	Critical	42
7	Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execution	Critical	27
8	Telerik.Web.UI.RadAsyncUpload.Handling.Arbitrary.File.Upload	Critical	24
9	vBulletin.Routestring.widgetConfig.Remote.Code.Execution	Critical	13
10	Bash.Function.Definitions.Remote.Code.Execution	Critical	10
11	NETGEAR.DGN1000.CGI.Unauthenticated.Remote.Code.Execution	Critical	9
12	Joomla!.Core.Session.Remote.Code.Execution	Critical	9
13	WordPress.HTTP.Path.Traversal	Critical	9
14	vBulletin.tabbedcontainer.Template.Remote.PHP.Code.Execution	Critical	7
15	Gh0st.Rat.Botnet	Critical	6
16	Bladabindi.Botnet	Critical	5
17	Joomla!.list.select.Parameter.SQL.Injection	Critical	4
18	Linux.Kernel.TCP.SACK.Panic.DoS	Critical	4
19	Pushdo.Botnet	Critical	3
20	Red.Hat.JBoss.AS.doFilter.Insecure.Deserialization	Critical	2
21	WordPress.Plugin.Userpro.Authentication.Bypass	Critical	2
22	Drupal.Core.Form.Rendering.Component.Remote.Code.Execution	Critical	1
23	BuilderEngine.elFinder.Arbitrary.File.Upload	Critical	1
24	Mirai.Botnet	High	155
25	HTTP.URI.SQL.Injection	High	123
26	PHP.Malicious.Shell	High	50
27	ELFinder.Connector.Minimal.php.Arbitrary.File.Upload	High	45
28	PHP.CGI.Argument.Injection	High	34
29	China.Chopper.Web.Shell.Client.Connection	High	32
30	Generic.XXE.Detection	High	18

Direcciones IP de victimas 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	172.20.22.44				396	16.92%
2	10.0.0.208				327	13.97%
3	10.0.0.202				316	13.50%
4	172.20.22.11				181	7.74%
5	172.20.22.35				180	7.69%
6	10.0.0.211				166	7.09%
7	10.0.0.216				149	6.37%
8	172.20.22.25				138	5.90%
9	10.0.0.207				122	5.21%
10	10.0.0.209				119	5.09%
11	172.20.22.18				107	4.57%
12	10.252.10.20				95	4.06%
13	172.20.22.12				44	1.88%

Intrusion Sources

#	Attack Source	Counts	Critical	High	Medium	Percent of Total Attacks
1	45.146.165.123				640	54.42%
2	45.227.253.206				93	7.91%
3	154.22.119.141				84	7.14%
4	112.53.100.233				75	6.38%
5	189.203.227.36				45	3.83%
6	52.255.238.49				31	2.64%
7	138.68.24.187				24	2.04%
8	20.102.70.120				24	2.04%
9	185.19.29.163				24	2.04%
10	8.133.179.231				14	1.19%
11	195.15.229.173				13	1.11%
12	40.76.244.110				13	1.11%
13	142.93.77.108				12	1.02%
14	194.182.181.178				12	1.02%
15	134.122.11.62				12	1.02%
16	165.232.178.112				12	1.02%
17	206.81.23.215				12	1.02%
18	209.141.33.74				12	1.02%
19	167.71.21.202				12	1.02%
20	143.198.148.182				12	1.02%

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	PHPUnit.Eval-stdin.PHP.Remote.Code.Execution	Code Injection	Critical		620
2	Dasan.GPON.Remote.Code.Execution	OS Command Injection	Critical		157
3	D-Link.Devices.HNAP.SOAPAction-Header.Command.Execution	OS Command Injection	Critical		148
4	ThinkPHP.Controller.Parameter.Remote.Code.Execution	Code Injection	Critical		140
5	Gozi.Botnet		Critical		75
6	Trojan.TrickBot		Critical		42
7	Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execution	Code Injection	Critical		31
8	Telerik.Web.UI.RadAsyncUpload.Handling.Arbitrary.File.Upload	Improper Authentication	Critical		26
9	NETGEAR.DGN1000.CGI.Unauthenticated.Remote.Code.Execution	Code Injection	Critical		16
10	vBulletin.Routestring.widgetConfig.Remote.Code.Execution	Code Injection	Critical		13
11	Bash.Function.Definitions.Remote.Code.Execution	OS Command Injection	Critical		10
12	Joomla!.Core.Session.Remote.Code.Execution	Code Injection	Critical		9
13	WordPress.HTTP.Path.Traversal	Path Traversal	Critical		9
14	vBulletin.tabbedcontainer.Template.Remote.PHP.Code.Execution	Code Injection	Critical		7
15	HTTP.URI.Java.Code.Injection	Code Injection	Critical		6
16	Gh0st.Rat.Botnet		Critical		6
17	Bladabindi.Botnet		Critical		5
18	Joomla!.list.select.Parameter.SQL.Injection	Permission/Privilege/Access Control	Critical		4
19	Linux.Kernel.TCP.SACK.Panic.DoS	DoS	Critical		4
20	Red.Hat.JBoss.AS.doFilter.Insecure.Deserialization	OS Command Injection	Critical		3

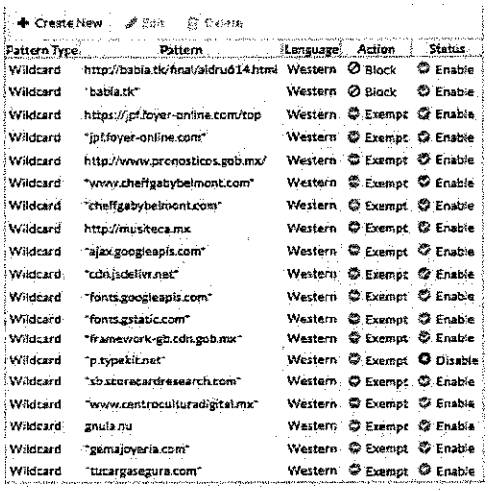
3.4. Tipo y número de ataques detectados y detenidos

Intrusions By Types

#	Intrusion Type	Counts
1	Anomaly	8,084
2	Code Injection	889
3	OS Command Injection	333
4	Permission/Priviledge/Access Control	231
5	Malware	177
6	SQL Injection	125
7	Improper Authentication	54
8	Information Disclosure	35
9	Other	20
10	Path Traversal	9
11	DoS	4
12	XSS	2

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:



Pattern Type	Pattern	Language	Action	Status
Wildcard	http://babia.tk/final/aldru614.html	Western	Block	Enable
Wildcard	"babia.tk"	Western	Block	Enable
Wildcard	https://jpf.foyer-online.com/top	Western	Exempt	Enable
Wildcard	"jpf.foyer-online.com"	Western	Exempt	Enable
Wildcard	http://www.pronosticos.gob.mx/	Western	Exempt	Enable
Wildcard	"www.cheffgabybelmont.com"	Western	Exempt	Enable
Wildcard	"cheffgabybelmont.com"	Western	Exempt	Enable
Wildcard	http://musiteca.mx	Western	Exempt	Enable
Wildcard	"ajax.googleapis.com"	Western	Exempt	Enable
Wildcard	"cdn.jsdelivr.net"	Western	Exempt	Enable
Wildcard	"fonts.googleapis.com"	Western	Exempt	Enable
Wildcard	"fonts.gstatic.com"	Western	Exempt	Enable
Wildcard	"framework-gb.cdn.gob.mx"	Western	Exempt	Enable
Wildcard	"p.typekit.net"	Western	Exempt	Disable
Wildcard	"sb.scorecardresearch.com"	Western	Exempt	Enable
Wildcard	"www.centroculturadigital.mx"	Western	Exempt	Enable
Wildcard	gnula.nu	Western	Exempt	Enable
Wildcard	"gemajoyeria.com"	Western	Exempt	Enable
Wildcard	"tucargasegura.com"	Western	Exempt	Enable

URL	Type	Action	Status
"babia.tk"	Wildcard	Block	Enable
http://www.pronosticos.gob.mx/	Wildcard	Allow	Enable
"foyergroup.ga"	Wildcard	Block	Enable
http://babia.tk/final/aldru614.html	Wildcard	Block	Enable
https://jpf.foyer-online.com/top	Wildcard	Allow	Enable
"jpf.foyer-online.com"	Wildcard	Allow	Enable
"revistapantalla.com/"	Wildcard	Allow	Enable
"mardenlocarballo.com"	Wildcard	Allow	Enable
"centrodemicorazon.com"	Wildcard	Allow	Enable
www.revistapantalla.com/festival/ficha.php	Simple	Allow	Enable
"www.cheffgabybelmont.com"	Wildcard	Allow	Enable
"cheffgabybelmont.com"	Wildcard	Allow	Enable
http://musiteca.mx	Wildcard	Allow	Enable
"musiteca.mx"	Wildcard	Allow	Enable
"ajax.googleapis.com"	Wildcard	Allow	Enable
"cdn.jsdelivr.net"	Wildcard	Allow	Enable
"fonts.googleapis.com"	Wildcard	Allow	Enable
"fonts.gstatic.com"	Wildcard	Allow	Enable
"framework-gb.cdn.gob.mx"	Wildcard	Allow	Enable
"p.typekit.net"	Wildcard	Allow	Enable
"sb.scorecardresearch.com"	Wildcard	Allow	Enable
"static.tumblr.com"	Wildcard	Allow	Enable
"use.typekit.net"	Wildcard	Allow	Enable
"www.google-analytics.com"	Wildcard	Allow	Enable
"www.youtube.com"	Wildcard	Allow	Enable
"fonts.gstatic.com"	Wildcard	Allow	Enable
"lytiing.com"	Wildcard	Allow	Enable
"yt3.ggpht.com"	Wildcard	Allow	Enable
"static.doubleclick.net"	Wildcard	Allow	Enable
"centroculturadigital"	Wildcard	Allow	Enable
http://www.centroculturadigital.mx	Wildcard	Allow	Enable
"centroculturadigital.mx	Wildcard	Allow	Enable
https://www.mitelcel.com/	Wildcard	Allow	Enable
http://www.iotenal.gob.mx	Wildcard	Allow	Enable
jpf.foyer-online.com/	Simple	Allow	Enable
"jpf.foyer-online.com"	Wildcard	Allow	Enable
https://jpf.foyer-online.com/	Wildcard	Allow	Enable
"salpimientacatering.com/"	Wildcard	Allow	Enable
"gnula.nu"	Wildcard	Allow	Enable
"gemajoyeria.com"	Wildcard	Allow	Enable
tucargasegura.com"	Wildcard	Allow	Enable

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	172.20.22.10	29,109

5. Direcciones ip con mayor consumo de ancho de banda

Top 20 Bandwidth Users

#	User (or IP)	Bandwidth
1	172.16.1.185	71.51 GB
2	172.31.215.168	44.17 GB
3	172.16.1.6	29.85 GB
4	172.16.1.61	22.10 GB
5	172.16.1.108	18.40 GB
6	172.16.1.1	17.44 GB
7	172.31.226.9	15.23 GB
8	172.16.1.153	13.95 GB
9	172.16.1.219	13.89 GB
10	172.31.226.15	12.19 GB
11	172.31.226.10	11.72 GB
12	172.31.226.7	10.93 GB
13	172.16.1.136	10.77 GB
14	172.31.226.6	9.93 GB
15	172.31.226.13	9.06 GB
16	10.100.10.38	8.98 GB
17	172.16.1.236	8.91 GB
18	172.31.226.11	8.75 GB
19	172.31.226.93	8.49 GB
20	172.31.226.16	8.26 GB

5.1. 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 Users by Bandwidth and Sessions

#	User(or IP)	Bandwidth	Sent	Received	Sessions
1	172.31.201.127		441.27 GB		46,674
2	172.31.201.17		312.94 GB		29,659
3	172.31.201.64		309.71 GB		1,210,235
4	172.31.201.205		297.49 GB		301,941
5	172.31.200.90		236.52 GB		55,620
6	10.252.10.8		216.79 GB		574
7	172.31.200.72		191.05 GB		32,864
8	10.252.10.7		179.18 GB		625
9	172.31.200.154		162.88 GB		201,294
10	172.31.200.101		146.08 GB		25,164
11	172.31.201.235		125.99 GB		228,624
12	172.31.200.79		117.61 GB		25,615
13	172.31.201.248		103.51 GB		313,684
14	172.31.215.168		89.64 GB		152,744
15	172.20.22.19		82.64 GB		64,876,360
16	172.31.201.88		80.95 GB		173,295
17	172.31.200.139		77.88 GB		438,427
18	172.16.1.185		75.89 GB		259,512
19	172.31.200.104		69.10 GB		67,356
20	172.31.201.246		57.59 GB		48,076
21	172.31.200.250		52.77 GB		297,655
22	172.31.200.123		51.92 GB		64,644
23	172.31.201.120		48.81 GB		15,334
24	172.31.200.185		46.59 GB		33,032
25	172.31.200.218		42.74 GB		93,008
26	172.31.226.10		40.14 GB		390,832
27	172.31.200.56		37.65 GB		20,246
28	172.31.201.25		36.85 GB		2,490
29	172.31.201.31		35.83 GB		102,715
30	172.31.226.7		35.28 GB		58,748

5.2. 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	Video/Audio	636.55 GB
2	Web.Client	559.11 GB
3	Social.Media	249.62 GB
4	Email	215.64 GB
5	Collaboration	177.08 GB
6	Network.Service	85.26 GB
7	General.Interest	78.12 GB
8	Update	64.33 GB
9	Storage.Backup	44.35 GB
10	Unknown	39.00 GB

6. Servicio de Seguridad para servidores WEB.

6.1. Políticas aplicadas en WAF.

La imagen siguiente muestra las políticas aplicadas en el equipo.

#	Policy Name	Virtual Server	HTTP Service	HTTPS Service	Deployment Mode	Web Protection Profile	Monitor Mode	Enable	Status
1	Blogs	blogs	HTTP		Single Server/Server Pool	Canal22 Alert Only	Disable	☑	
2	Informacion	informacion	HTTP		Single Server/Server Pool	Canal22 Alert Only	Disable	☑	
3	Aplicaciones	aplicaciones	HTTP		Single Server/Server Pool	Inline Alert Only	Disable	☑	
4	Portal_Canal22	VS_Portal_Canal22	HTTP	HTTPS	Single Server/Server Pool	c22-portal	Disable	☑	
5	Intranet_Canal22	VS_Intranet_Canal22	HTTP		Single Server/Server Pool	c22-portal	Disable	☑	
6	Clic_Clac	VS_Clic_Clac	HTTP	HTTPS	Single Server/Server Pool	Inline Alert Only	Disable	☑	
7	Ilovatar	VS_Ilovatar	HTTP		Single Server/Server Pool	Inline Alert Only	Disable	☑	
8	Fireball	VS_Fireball	HTTP		Single Server/Server Pool	Inline Alert Only	Disable	☑	
9	Programa	VS_Programa	HTTP		Single Server/Server Pool	Inline Alert Only	Disable	☑	
10	Minisitio	VS_Minisitios	HTTP		HTTP Content Routing	Inline Alert Only	Disable	☑	
11	analisisnoticias	analisisnoticias	HTTP	HTTPS	Single Server/Server Pool	c22-portal	Disable	☑	
12	pp_canal22	pp.canal22.org.mx	HTTP	HTTPS	Single Server/Server Pool	c22-portal	Disable	☑	
13	Noticias_php	Noticias_PHP	HTTP	HTTPS	Single Server/Server Pool	c22-portal	Disable	☑	
14	nuevo_corporativo	nuevocorporativo	HTTP	HTTPS	Single Server/Server Pool	Inline High Level Security	Enable	☑	
15	transparenciacanal22	transparencia canal22	HTTP	HTTPS	Single Server/Server Pool	transparenciacanal22	Disable	☑	
16	Subdominios	Subdominios canal22	HTTP	HTTPS	Single Server/Server Pool	Inline Alert Only	Disable	☑	
17	Contenidos_22	Contenidos22	HTTP	HTTPS	Single Server/Server Pool	Inline Alert Only	Disable	☑	

6.2. Resumen de tipo de ataque.

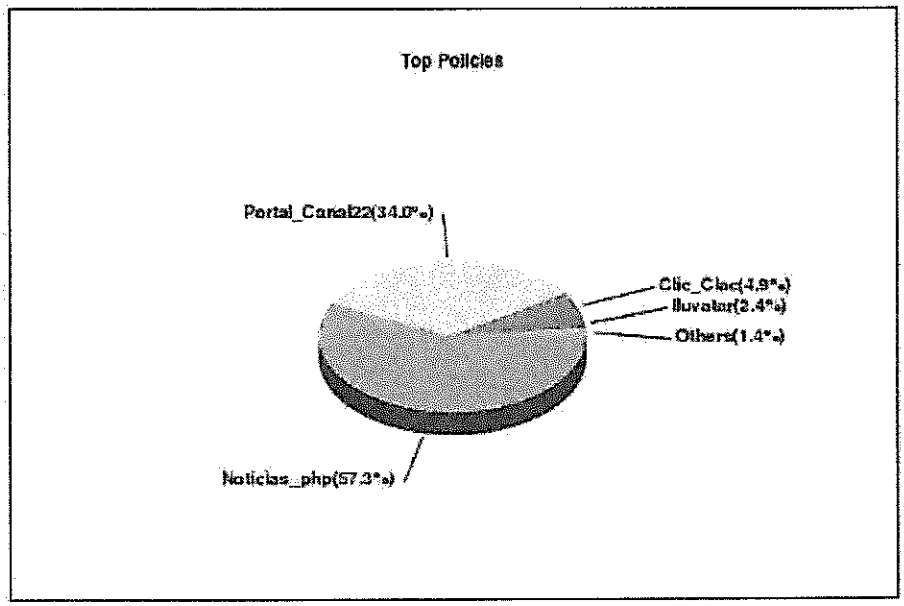
La tabla siguiente muestra un resumen de los ataques detectados y bloqueados por el WAF

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
2021-05-31	Directory Listing	172	86.43
	HTTP Header Leakage	17	8.54
	Malformed Request	3	1.51
	Other(5)	7	3.52
	Subtotal(8)	199	0.12
2021-06-01	Directory Listing	2531	47.33
	HTTP Header Leakage	2359	44.12
	Bad Robot	118	2.21
	Other(21)	339	6.34
	Subtotal(24)	5347	3.35
2021-06-02	Directory Listing	3303	64.76
	HTTP Header Leakage	1433	28.10
	Bad Robot	101	1.98
	Other(20)	263	5.16
	Subtotal(23)	5100	3.19
2021-06-03	Directory Listing	1716	53.14
	HTTP Header Leakage	1120	34.69
	Bad Robot	128	3.96
	Other(16)	265	8.21
	Subtotal(19)	3229	2.02
2021-06-04	Directory Listing	2072	59.15
	HTTP Header Leakage	1032	29.46
	Bad Robot	169	4.82
	Other(18)	230	6.57
	Subtotal(21)	3503	2.19
2021-06-05	Directory Listing	2665	60.34
	HTTP Header Leakage	1384	31.33
	Bad Robot	71	1.61
	Other(19)	297	6.72
	Subtotal(22)	4417	2.76
Other(25)		137989	86.36
Total(31)		159784	100.00

6.3. Top de políticas por porcentaje.



6.4. Top de ataques por URL.

Top Attack URLs

The most frequently detected attack URLs over the reporting period.

Top Attack URLs		
URL	Events	Percent
/xmlrpc.php	80412	50.33
/	16531	10.35
/cartelera/backend/application.php	16318	10.21
/wp-login.php	5857	3.67
none	2409	1.51
/ap/uedata	1634	1.02
Other(12853)	36623	22.92
Total(12859)	**159784**	**100.00**