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.: 043

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

FACTURA No.: F19328

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 marzo 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	
CADENAS PRODUCTIVAS	

DEPTO. DE TESORERÍA

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

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
17	5	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 marzo 2021.

FECHA DE RECEPCIÓN: marzo 2021

No. DE CONTRATO: 39/5/2017"B"
No. DE REQUISICIÓN: 043

No. DE FACTURA: F19328

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 19328

Folio Fiscal	7E590376-FACD-4B85-8D60-FC6882E06E4F
Fecha Emisión	2021-04-12T00:00:00
Fecha Certificación	2021-04-12T18:29:18
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	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 marzo 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

KLdVXXbA7tMlLQzlO68w5GGOeVyEqTsKuSluyqHIb5UskvqMwZ45n4iDYcN+6D2BrabThOxRJ1jsjH3EGYUnVTJzZ0ckqQ93d6/eGYiObFJQ/pUhvist/XL8sbsQ0+4KpTT7ekohbBF/2YyXYYHGHp7qdRQq0Y0Uekux1zBc6gDMv2uIIQFhBfM0ahdqYCTnpvzerff+JxXOjsPEnMWXvvROaAvM2MBRwy54QwwymRQJS3H84xUVbb96e+YI/8U7r/fDBTn8BGMrVLwLwiJvd8LfyYhdDvGnBB49rRjVblFDgW+VgKHgKJcohshyeBxEvHTB6axwg8p3BTb0b6ROSA==

Sello digital del SAT

Id7/HG8KlSfAGZDMgjunI/K8q3mU9uJu2JA8W+5MwyRHIJaJ5XJQKKbyuwVbfVadonXK4qNGbV2nMJsESXBEat9dZnHGh7GBW0JnnZP6CxeM67TTxq9cQsSqBQKTq8EwQoBQZPvq4/luM7Sy4qo8hFU3hmS28TCPAD+aQuEGxvYTioshVECAxnSw8fTGAmLvZmg1n2It2JCT6+hzVVXGNSdsGF+9LUZfLl8pMEA/bYQrfsboo8WazvLC9Ydyf13fYrQpDaCa2xQNicmh15xydxPgeneooAq53nFbx3yurLf4IuC7irM1DkM5fSPM+53WmfvhkiPMy62eRzyZsMnQnA==

Cadena original del complemento de certificación digital del SAT

||1.1|7E590376-FACD-4B85-8D60-FC6882E06E4F|2021-04-12T18:29:18|TLE011122SC2|KLdVXXbA7tMlLQzlO68w5GGOeVyEqTsKuSluyqHIb5UskvqMwZ45n4iDYcN+6D2BrabThOxRJ1jsjH3EGYUnVTJzZ0ckqQ93d6/eGYiObFJQ/pUhvist/XL8sbsQ0+4KpTT7ekohbBF/2YyXYYHGHp7qdRQq0Y0Uekux1zBc6gDMv2uIIQFhBfM0ahdqYCTnpvzerff+JxXOjsPEnMWXvvROaAvM2MBRwy54QwwymRQJS3H84xUVbb96e+YI/8U7r/fDBTn8BGMrVLwLwiJvd8LfyYhdDvGnBB49rRjVblFDgW+VgKHgKJcohshyeBxEvHTB6axwg8p3BTb0b6ROSA==|00001000000503270882||

Recepción de compra

Número recepción de compra: RECEP-21-0505
Fecha recepción de compra: 21/05/2021

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 06/01/2021
Id. proveedor P01001338

Confirmar a
Comprador
Número pedido C-PED-21-0513
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

No. CFACT-21-0505

Número factura compra: F19328
Fecha factura compra: 21/05/2021
Número de evento: EV1-21-000290

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 06/01/2021
Términos
Id. proveedor P01001338

Confirmar a
Comprador
Número pedido C-PED-21-0513
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	4,017.94	4,017.94
	013	31603	1	12	MATERIALES INDIRECTOS	SER	1	3,443.98	3,443.98
	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	18,367.85	18,367.85
	013	31603	1	23	MATERIALES INDIRECTOS	SER	1	9,183.93	9,183.93
	013	31603	1	24	MATERIALES INDIRECTOS	SER	1	9,183.94	9,183.94
	013	31603	1	31	GASTOS DE VENTA	SER	1	2,295.98	2,295.98
	013	31603	1	32	GASTOS DE VENTA	SER	1	4,017.96	4,017.96
	001	31603	1	41	GASTOS DE ADMINISTRACION	SER	1	2,869.98	2,869.98
	001	31603	1	42	GASTOS DE ADMINISTRACION	SER	1	29,273.75	29,273.75
	001	31603	1	43	GASTOS DE ADMINISTRACION	SER	1	14,349.87	14,349.87
	013	31603	1	51	MATERIALES INDIRECTOS	SER	1	6,313.95	6,313.95
	013	31603	1	52	MATERIALES INDIRECTOS	SER	1	16,071.87	16,071.87
	013	31603	1	53	MATERIALES INDIRECTOS	SER	1	22,959.81	22,959.81
	013	31603	1	54	GASTOS DE ADMINISTRACION	SER	1	6,313.94	6,313.94
	001	31603	1	61	GASTOS DE ADMINISTRACION	SER	1	6,313.94	6,313.94

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

Autorización de pago

RAUL YAU

SUBDIRECTOR GENERAL TECNICO
Y OPERATIVO

Presente:

No.: SP-21-00676

No. Autorización: SP-21-00676

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-21-00676

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 TE CNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN	
				Total:	193,091.96

Proceso:

Número:

Ticket: SP-21-00676

Folio:

Procesada: SP-21-00676

No. CLC: SP-21-00676

Observaciones: Servicio de Internet Dedicado, Seguridad Perimetral (UTM), Servicio de Seguridad para Servidores web y Servicio de Monitoreo Monitoreo y Reportes.
MARZO 2021.

Autorización de pago

Reporte de Acceso a Internet

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

MARZO 2021

Información General del Documento

Entregable

Clave	Servicio	Medio
TC-DUAI	Internet Dedicado	Electrónico

Elaboración

Puesto	Nombre	Firma
Responsable del Servicio	Lorena García García	PA

Revisión

Puesto	Nombre	Firma
Líder de proyecto	Victor 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		16/07/2021

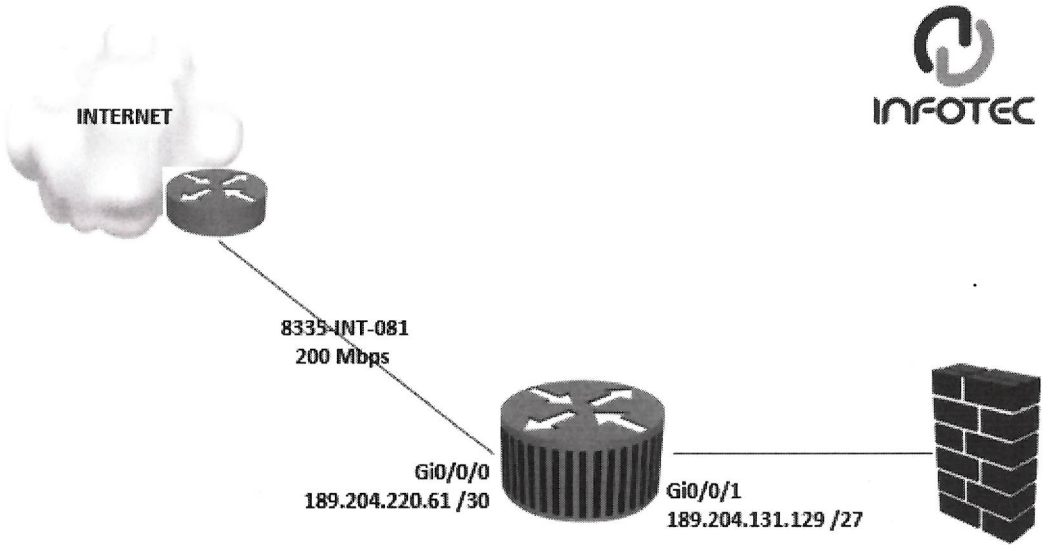
Aprobación Cliente

Puesto	Nombre	Firma	Fecha
Jefe de Unidad Departamental	Ing. Emilio René García Rodríguez		

Tabla de contenido

3. Diagrama de Topología de Acceso y Publicación a Internet

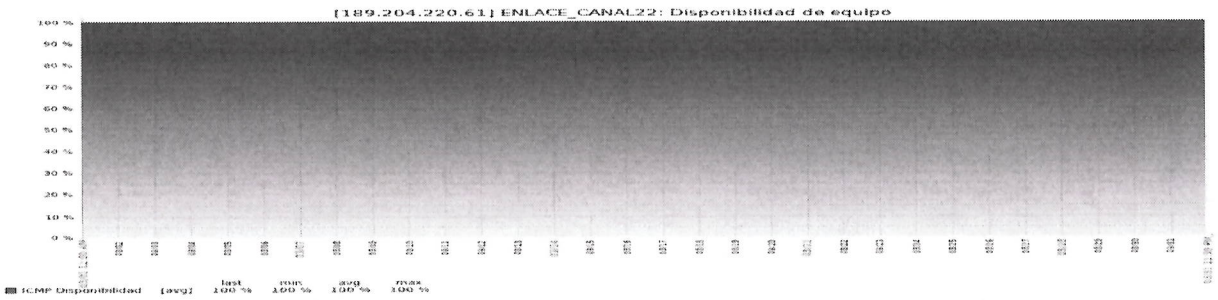
El siguiente diagrama muestra la topología de Acceso y publicación a Internet del cliente Canal 22.



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

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.

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

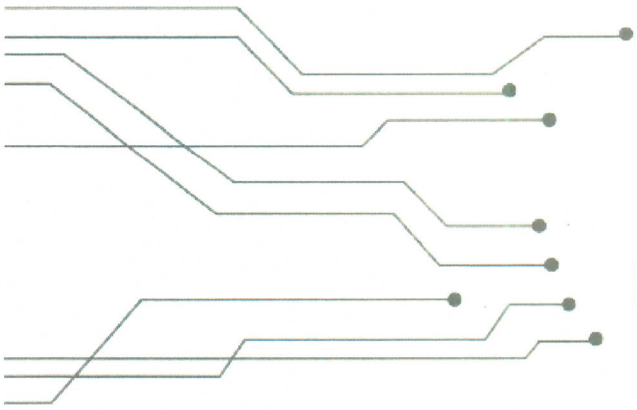
- Discard Exceptions (# de muestras)
- Discard Exceptions (% de muestras)

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)



INFOTEC

Reporte de Seguridad Perimetral UTM y Seguridad para Servidores Web

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

MARZO 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
Coordinador del SOC	Mtro. 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		16/04/2021

Aprobación Cliente

Puesto	Nombre	Firma	Fecha
Jefe de Unidad Departamental	Ing. Emilio René García Rodríguez		

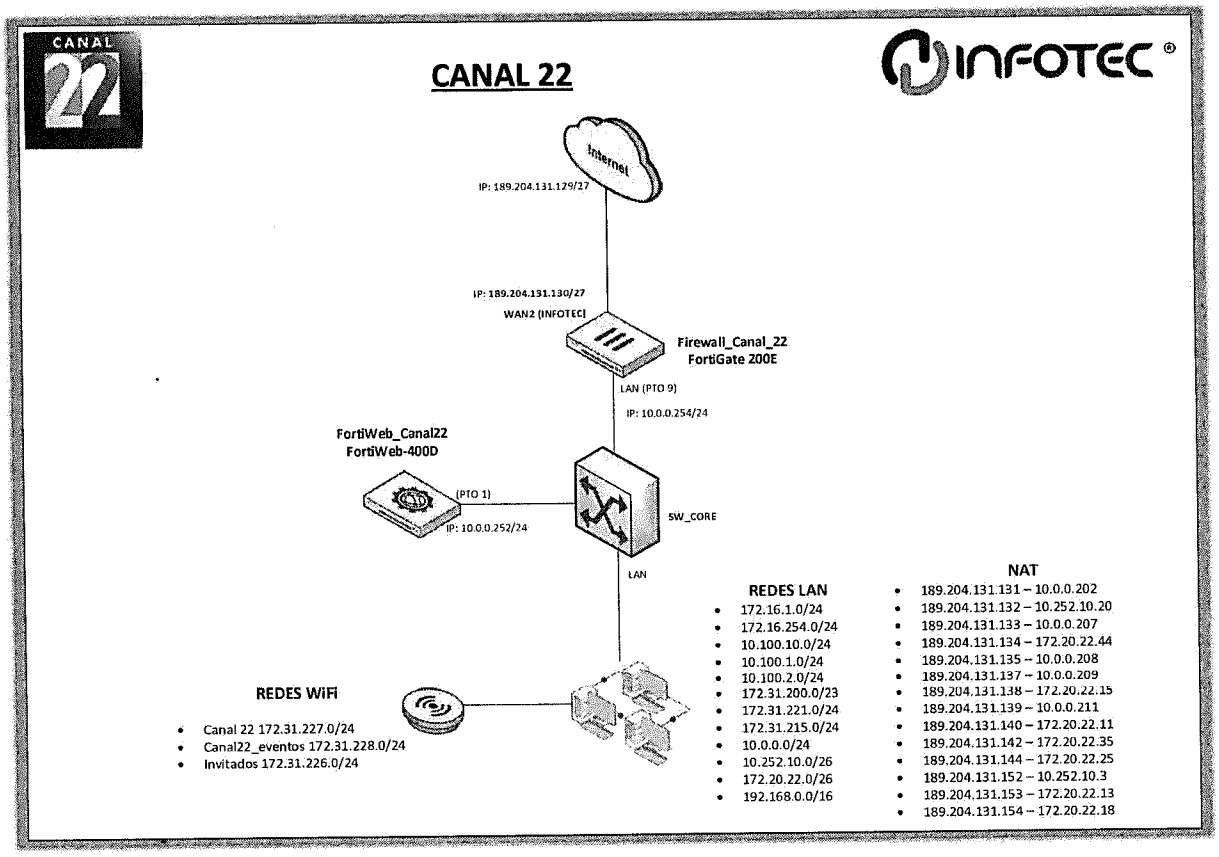
Tabla de contenido

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	Security Profiles	NAT	Action
Red_Local (port9)	sd-wan	172.31.220.1/32_Emilio	all	always	ALL		Enabled	ACCEPT
Red_Local (port9)	sd-wan	172.31.220.124/32 172.31.210.100/32	all	always	ALL		189.240.110.155_Niba	ACCEPT
Red_Local (port9)	sd-wan	172.16.1.0/24 10.100.10.0/24	all	always	ALL	AV WEB APP SSL	Enabled	ACCEPT
Red_Local (port9)	sd-wan	10.100.1.0/24 10.100.2.0/24	all	always	ALL	AV WEB APP SSL	Enabled	ACCEPT
Red_Local (port9)	sd-wan	172.31.220.241-172.31.220.248	all	always	ALL	WEB APP SSL	Enabled	ACCEPT
Red_Local (port9)	sd-wan	172.31.220.189/32 172.31.220.2/32 172.31.220.241-172.31.220.248 172.16.1.194-172.16.1.198 172.31.215.184-172.31.215.188	all	always	ALL	WEB APP SSL	Enabled	ACCEPT
Red_Local (port9)	sd-wan	172.31.210.33	all	always	ALL	WEB APP SSL	Enabled	ACCEPT
Red_Local (port9)	sd-wan	172.31.210.18/32 172.31.210.188/32	all	always	ALL	WEB APP SSL	Enabled	ACCEPT
Canal 22 (canal22)	sd-wan	172.31.227.0/24	all	always	ALL	WEB APP SSL	Enabled	ACCEPT
SSL-VPN tunnel interface (ssl.root)	Red_Local (port9)	SSLVPN_TUNNEL_ADDR1 SOC	10.0.0.252_WAF 10.0.0.254/32 10.0.0.0/24 172.20.22.0/26 10.0.0.1-10.0.0.251	always	ALL		Disabled	ACCEPT
SSL-VPN tunnel interface (ssl.root)	Red_Local (port9)	SSLVPN_TUNNEL_ADDR1 Sendra	172.16.1.179/32 172.20.22.13/32	always	ALL		Disabled	ACCEPT

From	To	Source	Destination	Schedule	Service	Security Profiles	NAT	Action
SSL-VPN tunnel interface (ssl.root)	Red_Local (port9)	SSLVPN_TUNNEL_ADDR1 alejandro.martinez	172.31.201.168/32 10.100.1.0/24 10.100.10.0/24 10.100.2.0/24	always	ALL		Disabled	ACCEPT
SSL-VPN tunnel interface (ssl.root)	Red_Local (port9)	SSLVPN_TUNNEL_ADDR1 osvaldo.alonso	172.31.201.169/32 10.100.1.0/24 10.100.10.0/24 10.100.2.0/24	always	ALL		Disabled	ACCEPT
SSL-VPN tunnel interface (ssl.root)	Red_Local (port9)	SSLVPN_TUNNEL_ADDR1 emmanuel.olguin	172.31.200.153/32 172.31.200.154/32 172.31.201.202/32	always	ALL		Disabled	ACCEPT
SSL-VPN tunnel interface (ssl.root)	Red_Local (port9)	SSLVPN_TUNNEL_ADDR1 luis.noquez	172.31.200.161/32 10.100.1.0/24 10.100.10.0/24 10.100.2.0/24	always	ALL		Disabled	ACCEPT
SSL-VPN tunnel interface (ssl.root)	Red_Local (port9)	SSLVPN_TUNNEL_ADDR1 javier.rosario	172.31.201.117/32 10.100.1.0/24 10.100.10.0/24 10.100.2.0/24	always	ALL		Disabled	ACCEPT
SSL-VPN tunnel interface (ssl.root)	Red_Local (port9)	SSLVPN_TUNNEL_ADDR1 alma	172.16.1.179/32 172.20.22.13/32	always	ALL		Disabled	ACCEPT
SSL-VPN tunnel interface (ssl.root)	Red_Local (port9)	SSLVPN_TUNNEL_ADDR1 navision	172.20.22.56/32 172.20.22.58/32	always	ALL		Disabled	ACCEPT
SSL-VPN tunnel interface (ssl.root)	Red_Local (port9)	SSLVPN_TUNNEL_ADDR1 Archivo	10.252.10.11/32 172.20.22.28/32_IMPR 172.20.22.27/32 172.31.220.145/32 172.20.22.16/32	always	ALL		Disabled	ACCEPT

From	To	Source	Destination	Schedule	Service	Security Profiles	NAT	Action
SSL-VPN tunnel interface (ssl.root)	Red_Local (port9)	SSLVPN_TUNNEL_ADDR1 Canal 22	172.20.22.0/26 192.168.0.0/24 10.0.0.0/24 10.100.10.0/24 10.252.10.0/24 172.16.1.0/24 172.31.200.0/23 172.31.215.0/24 172.31.221.0/24	always	ALL		Enabled	ACCEPT
SSL-VPN tunnel interface (ssl.root)	Red_Local (port9)	SSLVPN_TUNNEL_ADDR1 leticia.reyes grassvalley promexar1 promexar2	10.100.10.0/24	always	ALL		Disabled	ACCEPT
SSL-VPN tunnel interface (ssl.root)	Red_Local (port9)	SSLVPN_TUNNEL_ADDR1 alexis.lopez	10.100.10.0/24 10.100.1.0/24 10.100.2.0/24	always	ALL		Disabled	ACCEPT
SSL-VPN tunnel interface (ssl.root)	Red_Local (port9)	SSLVPN_TUNNEL_ADDR1 pedro.rodriguez	10.100.10.0/24 10.100.1.0/24	always	ALL		Disabled	ACCEPT
SSL-VPN tunnel interface (ssl.root)	Red_Local (port9)	SSLVPN_TUNNEL_ADDR1 jantonio.ruiz	10.100.1.0/24	always	ALL		Disabled	ACCEPT
SSL-VPN tunnel interface (ssl.root)	TVmetro_Invitados (invitados)	SSLVPN_TUNNEL_ADDR1 emilio_rene	172.31.226.0/24	always	ALL		Disabled	ACCEPT
SSL-VPN tunnel interface (ssl.root)	Canal 22 (canal22)	SSLVPN_TUNNEL_ADDR1 emilio_rene	172.31.227.0/24	always	ALL		Disabled	ACCEPT
SSL-VPN tunnel interface (ssl.root)	Eventos_Canal22 (canal22_eventos)	SSLVPN_TUNNEL_ADDR1 emilio_rene	172.31.228.0/24	always	ALL		Disabled	ACCEPT

From	To	Source	Destination	Schedule	Service	Security Profiles	NAT	Action
sd-wan Red_Local (port9)	Red_Local (port9)	china CHINA_	all	always	ALL			DENY
sd-wan	Red_Local (port9)	Ramsonware	all	always	ALL			DENY
sd-wan	Red_Local (port9)	all	Mail_server_list_POP3 Mail_server_list_SMTP	always	POP3 SMTP	AV WF	Disabled	ACCEPT
sd-wan	Red_Local (port9)	all	Desarrollo_443 Desarrollo Desarrollo_8080	always	8080,TCP HTTP HTTPS	AV WF	Enabled	ACCEPT
sd-wan	Red_Local (port9)	all	Portal Proyectos Portal Proyectos_443	always	ALL_ICMP HTTP HTTPS	AV WF	Disabled	ACCEPT
sd-wan	Red_Local (port9)	all	Noticias_php_443 Noticias_php_80	always	HTTP ALL_ICMP HTTPS	AV WF	Enabled	ACCEPT
sd-wan	Red_Local (port9)	all	MIP 189.204.131.154 - 172.20.22.18 189.204.131.142 172.20.22.35	always	HTTP HTTPS	AV WF	Enabled	ACCEPT
sd-wan	Red_Local (port9)	all	Publicacion_Canal22-80 Publicacion_Canal22_443	always	HTTP ALL_ICMP HTTPS TRACEROUTE	AV WF	Enabled	ACCEPT
sd-wan	Red_Local (port9)	all	Publicacion_Programa Portal_Clic_Clac Publicacion_minisitios1 Fireball Ituvatar Ituvatar 443	always	HTTP ALL_ICMP HTTPS	AV WF	Enabled	ACCEPT
Canal 22 (canal22)	sd-wan	172.31.227.0/24	www.centroculturadigital.mx	always	ALL	AV WF APP	Enabled	ACCEPT

From	To	Source	Destination	Schedule	Service	Security Profiles	NAT	Action
Eventos_Canal22 (canal22_eventos)	sd-wan	172.31.228.0/24	all	always	ALL	WEB APP DNS	Enabled	ACCEPT
Eventos_Canal22 (canal22_eventos)	sd-wan	172.31.228.0/24	www.centroculturadigital.mx	always	ALL	WEB APP DNS	Enabled	ACCEPT
TVinetro_Invitados (invitados)	sd-wan	172.31.226.0/24	all	always	ALL	WEB APP DNS	Enabled	ACCEPT
TVinetro_Invitados (invitados)	sd-wan	172.31.226.0/24	www.centroculturadigital.mx	always	ALL	WEB APP DNS	Enabled	ACCEPT
Red_Local (port9)	sd-wan	10.252.10.0/26 172.16.1.0/24 172.20.22.0/26 172.31.215.0/24 192.168.0.0/16 192.168.222.0/24 10.0.0.252_WAF	www.centroculturadigital.mx	always	ALL	WEB APP DNS	Enabled	ACCEPT
Red_Local (port9)	sd-wan	172.16.1.0/24	all	always	ALL	WEB APP DNS	Enabled	ACCEPT
Red_Local (port9)	sd-wan	172.31.215.0/24	all	always	ALL	WEB APP DNS	Enabled	ACCEPT
Red_Local (port9)	sd-wan	172.20.22.10/32	all	always	ALL	AV WEB DNS APP SSH	Enabled	ACCEPT
Red_Local (port9)	sd-wan	172.20.22.15 correo	all	always	ALL		Enabled	ACCEPT
Red_Local (port9)	sd-wan	172.20.22.0/26	all	always	ALL	WEB APP DNS	Enabled	ACCEPT
Red_Local (port9)	sd-wan	10.252.10.0/26	all	always	ALL	WEB APP DNS	Enabled	ACCEPT
Red_Local (port9)	sd-wan	172.16.1.0/24 172.20.22.0/26 172.31.215.0/24 192.168.0.0/16 192.168.222.0/24 10.0.0.252_WAF	all	always	ALL	WEB APP DNS	Enabled	ACCEPT
Red_Local (port9)	sd-wan	10.0.0.0/24	all	always	ALL	WEB APP DNS	Enabled	ACCEPT

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		Server	Linux
3Com.OfficeConnect.Utility.CGI.Remote.Command.Execution		Server	Linux
7-Zip.RAR.Solid.Compression.Remote.Code.Execution		Server, Client	Windows
74CMS.Config.Controller.Remote.Code.Execution		Server	Windows, Linux, BSD, Solaris, MacO
427BB.Cookie.Based.Authentication.Bypass		Server	Other
Aardvark.Topsites.PHP.Remote.Command.Execution		Server	Windows, Linux, BSD, Solaris, MacO
ABBS.Audio.Media.Player.LST.Buffer.Overflow		Server, Client	Windows
ACal.Calendar.Cookie.Based.Authentication.Bypass		Server	Windows, Linux, BSD, Solaris, MacO
Accellion.FTA.Cookie.Information.Disclosure		Server	Linux, BSD
Accellion.FTA.getStatus.verify_oauth_token.Command.Injection		Server	Linux, BSD
ACME.mini_httpd.Arbitrary.File.Read		Server	Linux
ActivePDF.Toolkit.Multiple.File.Memory.Corruption		Server, Client	Windows
ActivePerl.PerlIS.dll.Remote.Buffer.Overflow		Server	Windows
ActualAnalyzer.ANT.Cookie.Command.Injection		Server	Linux, BSD
Acunetix.Web.Vulnerability.Scanner		Server	All
AdMentor.Admin.SQL.Injection		Server	Windows
Admin.PHP.Upload.Invalid.Memory		Server	Windows, Linux, BSD, Solaris, MacO
Adobe.Acrobat.and.Reader.Triangle.Object.Memory.Corruption		Server, Client	Windows, Linux, MacOS
Adobe.Acrobat.BMP.Colors.Parsing.Memory.Corruption		Server, Client	Windows, MacOS

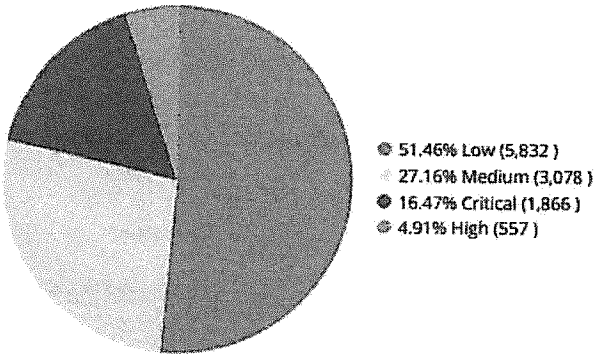
« ‹ 1 /56 › » [Total: 2761]

3.1. Ataques detectados y detenidos por el IPS

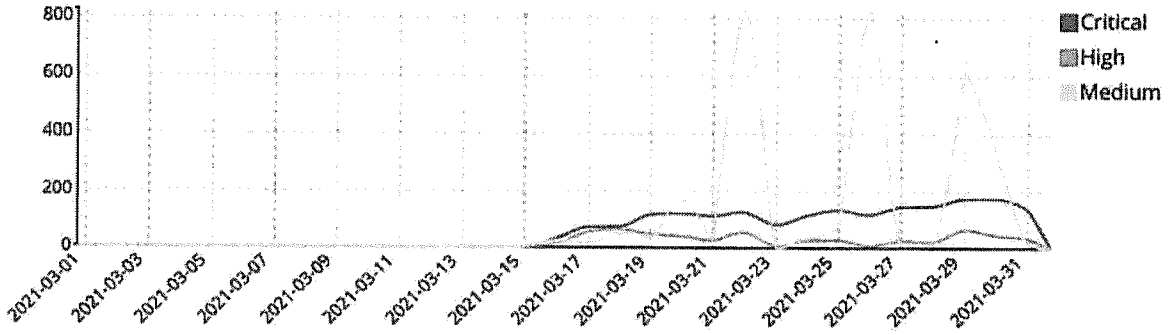
Las firmas que coincidieron con eventos de intrusión se muestran en las gráficas siguientes:

Summary

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	739
2	ThinkPHP.Controller.Parameter.Remote.Code.Execution	CVE-2019-9082,CVE-2018-20062	Code Injection	453
3	Dasan.GPON.Remote.Code.Execution	CVE-2018-10561,CVE-2018-10562	OS Command Injection	141
4	D-Link.Devices.HNAP.SOAPAction-Header.Command.Execution	CVE-2015-2051,CVE-2019-10891	OS Command Injection	124
5	WordPress.HTTP.Path.Traversal	CVE-2019-9618,CVE-2018-16283,CVE-2018-16299,CVE-2020-11738	Path Traversal	84
6	vBulletin.Routestring.widgetConfig.Remote.Code.Execution	CVE-2019-16759	Code Injection	73
7	Joomla!.Core.Session.Remote.Code.Execution	CVE-2015-8562	Code Injection	60
8	Drupal.Core.Form.Rendering.Component.Remote.Code.Execution	CVE-2018-7600	OS Command Injection	48
9	vBulletin.tabbedcontainer.Template.Remote.PHP.Code.Execution	CVE-2020-7373,CVE-2020-17496	Code Injection	41
10	Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execution	CVE-2017-5638	Code Injection	24
11	NETGEAR.DGN1000.CGI.Unauthenticated.Remote.Code.Execution		Code Injection	21
12	Telerik.Web.UI.RadAsyncUpload.Handling.Arbitrary.File.Upload	CVE-2017-11317,CVE-2017-11357,CVE-2019-18935	Improper Authentication	15
13	Shenzhen.TVT.DVR.Remote.Code.Execution		Permission/Priviledge/Access Control	14
14	HTTP.URI.Java.Code.Injection	CVE-2018-1273	Code Injection	10
15	Bladabindi.Botnet			4
16	GhOst.Rat.Botnet			4
17	Linux.Kernel.TCP.SACK.Panic.DoS	CVE-2019-11477,CVE-2019-11478,CVE-2019-11479	DoS	3
18	WordPress.Plugin.Userpro.Authentication.Bypass	CVE-2017-16562	Improper Authentication	3
19	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	2
20	MikroTik.RouterOS.Arbitrary.File.Read	CVE-2018-14847	Path Traversal	1

High Severity Intrusions

#	Attack Name	CVE-ID	Intrusion Type	Counts
1	PHP.URI.Code.Injection		Code Injection	86
2	Mirai.Botnet			84
3	HTTP.URI.SQL.Injection		SQL Injection	84
4	PHP.CGI.Argument.Injection	CVE-2012-1823,CVE-2012-2311	Code Injection	51
5	PhpStudy.Web.Server.Remote.Code.Execution		Code Injection	41
6	HTTP.Header.SQL.Injection		SQL Injection	40
7	PHP.Malicious.Shell		Malware	33
8	Axis.SSI.camnbr.Remote.Command.Execution		Code Injection	23
9	China.Chopper.Web.Shell.Client.Connection		Anomaly	20
10	Generic.XXE.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
11	Tomato.Router.Default.Credentials		Anomaly	13
12	Tongda.Office.Anywhere.Unauthorized.File.Upload		Improper Authentication	11
13	Tenda.AC15.AC1900.Authenticated.Remote.Command.Injection	CVE-2020-10987,CVE-2020-15916	OS Command Injection	10
14	ThinkPHP.HTTP.VARS.S.Remote.Code.Injection		Code Injection	10
15	Netlink.GPON.Router formPing.Remote.Command.Injection		OS Command Injection	9
16	ThinkPHP.Request.Method.Remote.Code.Execution		Code Injection	9
17	WordPress.Platform.Theme.Arbitrary.File.Upload		Permission/Priviledge/Access Control	6
18	Seeyon.Office.Anywhere.html officeservlet.Arbitrary.File.Upload		OS Command Injection	5
19	JAWS.DVR.CCTV.Shell.Unauthenticated.Command.Execution		OS Command Injection	3
20	VACRON.CCTV.Board.CGI.cmd.Parameter.Command.Execution		OS Command Injection	1

Medium Severity Intrusions

#	Attack Name	CVE-ID	Intrusion Type	Counts
1	WordPress.xmlrpc.php.system.multicall.Amplification.Attack		Anomaly	2,683
2	Web.Server.Password.Files.Access		Permission/Priviledge/Access Control	130
3	PHP.Diescan		Anomaly	104
4	FCKeditor.CurrentFolder.Arbitrary.File.Upload	CVE-2009-2265	Permission/Priviledge/Access Control	71
5	HTTP.Referer.Header.SQL.Injection	CVE-2007-1061	SQL Injection	36
6	WordPress.REST.API.Username.Enumeration.Information.Disclosure	CVE-2017-5487	Information Disclosure	31
7	Phpweb.CMS.appcode.Information.Disclosure		Information Disclosure	10
8	Apache.Axis2.Default.Password.Access	CVE-2010-0219	Other	7
9	WordPress.Plugin.Social.Warfare.XSS	CVE-2019-9978	XSS	3
10	WebUI.Mainfile.php.Arbitrary.Command.Injection		Code Injection	2
11	phpMyAdmin.scripts.setup.php.Insecure.Deserialization		Code 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	739
2	ThinkPHP.Controller.Parameter.Remote.Code.Execution	Critical	453
3	D-Link.Devices.HNAP.SOAPAction-Header.Command.Execution	Critical	124
4	Dasan.GPON.Remote.Code.Execution	Critical	109
5	WordPress.HTTP.Path.Traversal	Critical	84
6	vBulletin.Routestring.widgetConfig.Remote.Code.Execution	Critical	73
7	Joomla!.Core.Session.Remote.Code.Execution	Critical	60
8	Drupal.Core.Form.Rendering.Component.Remote.Code.Execution	Critical	48
9	vBulletin.tabbedcontainer.Template.Remote.PHP.Code.Execution	Critical	41
10	Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execution	Critical	23
11	Shenzhen.TVT.DVR.Remote.Code.Execution	Critical	14
12	NETGEAR.DGN1000.CGI.Unauthenticated.Remote.Code.Execution	Critical	14
13	Telerik.Web.UI.RadAsyncUpload.Handling.Arbitrary.File.Upload	Critical	14
14	Bladabindi.Botnet	Critical	4
15	Ghost.Rat.Botnet	Critical	4
16	WordPress.Plugin.Userpro.Authentication.Bypass	Critical	3
17	Linux.Kernel.TCP.SACK.Panic.DoS	Critical	3
18	Bash.Function.Definitions.Remote.Code.Execution	Critical	2
19	SonicWall.GMS.XMLRPC.set_time_zone.Remote.Code.Execution	Critical	1
20	PHP.URI.Code.Injection	High	86
21	HTTP.URI.SQL.Injection	High	84
22	Mirai.Botnet	High	82
23	PHP.CGI.Argument.Injection	High	51
24	PhpStudy.Web.Server.Remote.Code.Execution	High	41
25	HTTP.Header.SQL.Injection	High	40
26	PHP.Malicious.Shell	High	33
27	Axis.SSI.cumrsbr.Remote.Command.Execution	High	22
28	China.Chopper.Web.Shell.Client.Connection	High	20
29	Generic.XXE.Detection	High	16

#	Attack Name	Severity	Attack Counts
30	Tongda.Office.Anywhere.Unauthorized.File.Upload	High	11
31	ThinkPHP.HTTP.VARS.S.Remote.Code.Injection	High	10
32	Tenda.AC15.AC1900.Authenticated.Remote.Command.Injection	High	10
33	ThinkPHP.Request.Method.Remote.Code.Execution	High	9
34	Netlink.GPON.Router.formPing.Remote.Command.Injection	High	8
35	WordPress.Platform.Theme.Arbitrary.File.Upload	High	6
36	Seeyon.Office.Anywhere.htmloffices.servlet.Arbitrary.File.Upload	High	5
37	JAWS.DVR.CCTV.Shell.Unauthenticated.Command.Execution	High	3
38	WordPress.Web.API.Endpoint.Privilege.Escalation	High	1
39	WordPress.xmlrpc.php.system.multicall.Amplification.Attack	Medium	2,683
40	Web.Server.Password.Files.Access	Medium	130
41	PHP.Diescan	Medium	104
42	FCKeditor.CurrentFolder.Arbitrary.File.Upload	Medium	71
43	HTTP.Referer.Header.SQL.Injection	Medium	36
44	WordPress.REST.API.Username.Enumeration.Information.Disclosure	Medium	31
45	Phpweb.CMS.appcode.Information.Disclosure	Medium	10
46	Apache.Axis2.Default.Password.Access	Medium	7
47	WordPress.Plugin.Social.Warfare.XSS	Medium	3
48	WebUI.Mainfile.php.Arbitrary.Command.Injection	Medium	2
49	phpMyAdmin.scripts.setup.php.Insecure.Deserialization	Medium	1

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				2,873	52.23%
2	172.20.22.44				548	9.96%
3	172.20.22.35				304	5.53%
4	10.0.0.209				295	5.36%
5	10.0.0.207				277	5.04%
6	172.20.22.25				255	4.64%
7	10.0.0.202				250	4.54%
8	172.20.22.11				239	4.34%
9	10.0.0.211				197	3.58%
10	172.20.22.18				145	2.64%
11	10.252.10.20				118	2.15%

Intrusion Sources

#	Attack Source	Counts	Critical	High	Medium	Percent of Total Attacks
1	142.93.4.240				914	42.00%
2	45.146.165.157				370	17.00%
3	116.213.43.216				128	5.88%
4	116.213.43.238				73	3.35%
5	45.146.165.165				66	3.03%
6	139.199.65.226				53	2.44%
7	132.232.70.247				51	2.34%
8	134.175.166.254				50	2.30%
9	168.195.168.80				50	2.30%
10	210.212.250.39				49	2.25%
11	122.114.186.213				47	2.16%
12	185.175.35.179				44	2.02%
13	152.136.43.147				43	1.98%
14	212.64.98.122				38	1.75%
15	116.213.43.237				37	1.70%
16	160.251.4.88				33	1.52%
17	45.148.10.45				33	1.52%
18	45.43.18.3				33	1.52%
19	153.127.65.64				32	1.47%
20	173.249.45.197				32	1.47%

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	739
2	ThinkPHP.Controller.Parameter.Remote.Code.Execution	Code Injection	Critical	453
3	Dasan.GPON.Remote.Code.Execution	OS Command Injection	Critical	141
4	D-Link.Devices.HNAP.SOAPAction-Header.Command.Execution	OS Command Injection	Critical	124
5	WordPress.HTTP.Path.Traversal	Path Traversal	Critical	84
6	vBulletin.Routestring.widgetConfig.Remote.Code.Execution	Code Injection	Critical	73
7	Joomla!.Core.Session.Remote.Code.Execution	Code Injection	Critical	60
8	Drupal.Core.Form.Rendering.Component.Remote.Code.Execution	OS Command Injection	Critical	48
9	vBulletin.tabbedcontainer.Template.Remote.PHP.Code.Execution	Code Injection	Critical	41
10	Apache.Struts.2.Jakarta.Multipart.Parser.Code.Execution	Code Injection	Critical	24
11	NETGEAR.DGN1000.CGI.Unauthenticated.Remote.Code.Execution	Code Injection	Critical	21
12	Telerik.Web.UI.RadAsyncUpload.Handling.Arbitrary.File.Upload	Improper Authentication	Critical	15
13	Shenzhen.TVT.DVR.Remote.Code.Execution	Permission/Priviledge/Access Control	Critical	14
14	HTTP.URI.Java.Code.Injection	Code Injection	Critical	10
15	Bladabindi.Botnet		Critical	4
16	Gh0st.Rat.Botnet		Critical	4
17	Linux.Kernel.TCP.SACK.Panic.DoS	DoS	Critical	3
18	WordPress.Plugin.Userpro.Authentication.Bypass	Improper Authentication	Critical	3
19	Bash.Function.Definitions.Remote.Code.Execution	OS Command Injection	Critical	2
20	Red.Hat.JBoss.AS.doFilter.Insecure.Deserialization	OS Command Injection	Critical	1

3.4. Tipo y número de ataques detectados y detenidos

Intrusions By Types

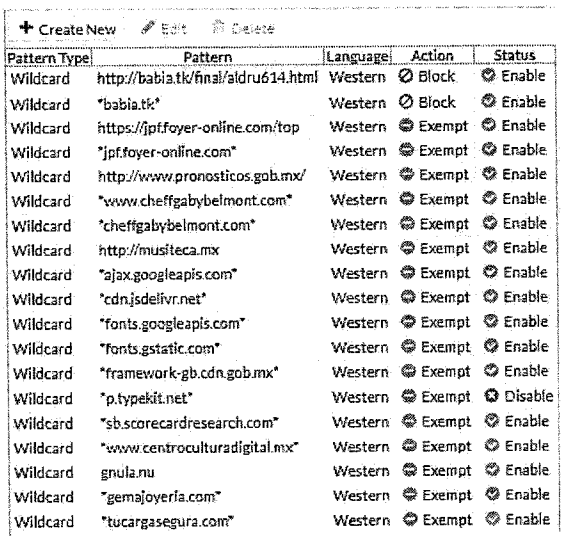
#	Intrusion Type	Counts
1	Anomaly	8,483
2	Code Injection	1,645
3	OS Command Injection	344
4	Permission/Priviledge/Access Control	223
5	Malware	202
6	SQL Injection	160
7	Path Traversal	85
8	Information Disclosure	41
9	Improper Authentication	29
10	Other	23
11	DoS	3
12	XSS	3

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:

+ Create | Edit | Delete | Search

URL	Type	Action	Status
babia.tk	Wildcard	Block	Enable
http://www.pronosticos.gob.mx/	Wildcard	Allow	Enable
loyorgroup.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
mardoniocarballo.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.typekkit.net	Wildcard	Allow	Enable
www.google-analytics.com	Wildcard	Allow	Enable
www.youtube.com	Wildcard	Allow	Enable
fonts.gstatic.com	Wildcard	Allow	Enable
i.ytimg.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.fotenal.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



+ Create New | Edit | Delete

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

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	22,713

5. Direcciones ip con mayor consumo de ancho de banda

Top 20 Bandwidth Users

#	User (or IP)	Bandwidth
1	172.31.215.168	76.87 GB
2	10.100.1.231	37.47 GB
3	172.31.226.18	28.67 GB
4	172.16.1.6	27.57 GB
5	172.16.1.108	25.10 GB
6	172.16.1.153	15.31 GB
7	172.16.1.185	15.26 GB
8	172.31.226.13	14.42 GB
9	172.16.1.1	13.94 GB
10	172.16.1.236	11.60 GB
11	172.16.1.241	11.15 GB
12	172.31.226.15	10.77 GB
13	172.16.1.245	10.04 GB
14	172.16.1.219	9.44 GB
15	172.31.226.3	9.16 GB
16	172.16.1.4	8.54 GB
17	172.16.1.39	7.20 GB
18	172.31.226.43	6.77 GB
19	172.31.226.107	6.38 GB
20	172.31.215.174	6.28 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 Applications by Bandwidth and Sessions

#	Application	Bandwidth	Sent	Received	Sessions
1	HTTPS		1.66 TB		3,197,905
2	HTTPS.BROWSER		324.01 GB		1,092,197
3	udp/443		293.31 GB		454,048
4	RTMP		269.53 GB		63
5	Facebook		219.39 GB		267,136
6	HTTP		211.22 GB		267,669
7	YouTube		139.35 GB		88,102
8	SSH		132.58 GB		4
9	SMTP		127.27 GB		42,388,923
10	Microsoft.SharePoint		85.91 GB		18,811
11	Microsoft.Outlook.Office.365		73.94 GB		332,044
12	Microsoft.Office.Update		65.08 GB		9,657
13	udp/8801		46.71 GB		674
14	Netflix		33.75 GB		15,459
15	Google.Services		32.37 GB		294,197
16	Zoom		30.66 GB		3,708
17	TeamViewer		20.83 GB		7,678
18	WhatsApp		20.50 GB		93,392
19	Apple.Software.Update		18.36 GB		47,799
20	TikTok		18.03 GB		32,205
21	udp/33001		17.08 GB		114
22	STUN		15.17 GB		8,064
23	Microsoft.Portal		14.86 GB		1,863,004
24	Skype		14.26 GB		6,357
25	Citrix.Services		13.73 GB		3,610
26	HTTP.BROWSER		12.98 GB		132,774
27	Spotify		12.23 GB		9,804
28	udp/6881		10.57 GB		2,537,094
29	Adobe.Web		9.78 GB		60,756
30	tcp/5001		7.69 GB		2,270

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	493.85 GB
2	Web.Client	336.99 GB
3	Social.Media	204.36 GB
4	Email	202.82 GB
5	Collaboration	201.33 GB
6	Update	86.70 GB
7	General.Interest	54.12 GB
8	Unknown	40.77 GB
9	Network.Service	31.60 GB
10	Remote.Access	27.94 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	Iluvatar	VS_Iluvatar	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	☑	

6.2. Resumen de tipo de ataque.

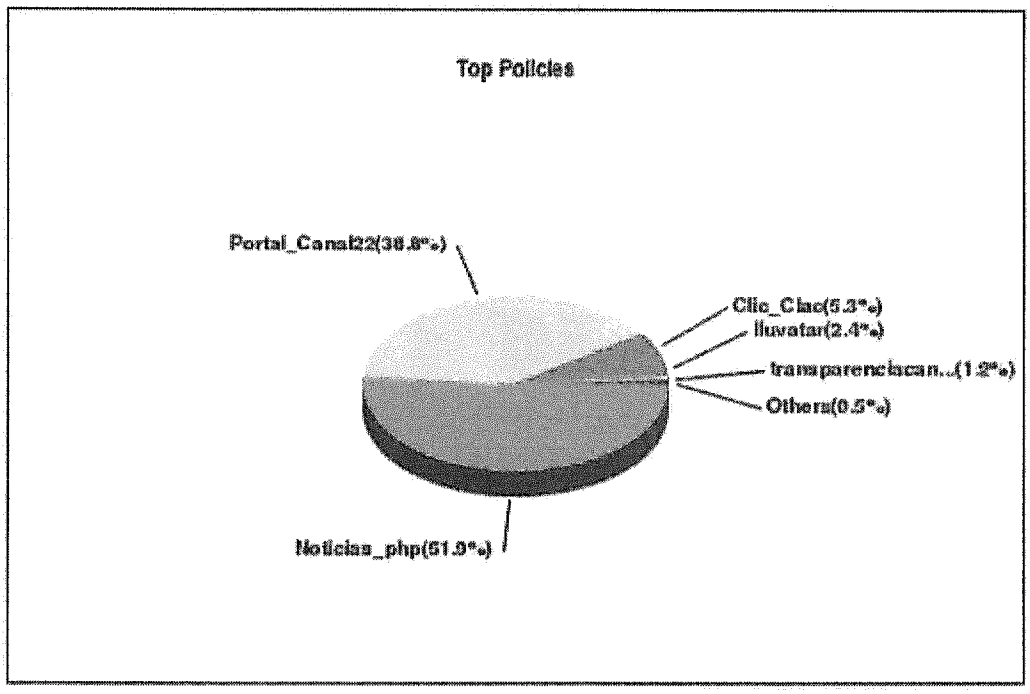
La tabla siguiente muestra un resumen de los ataques detectados y bloqueados por el WAF

Top Attack Types by Date

The daily breakdown of the most frequently detected attack types.

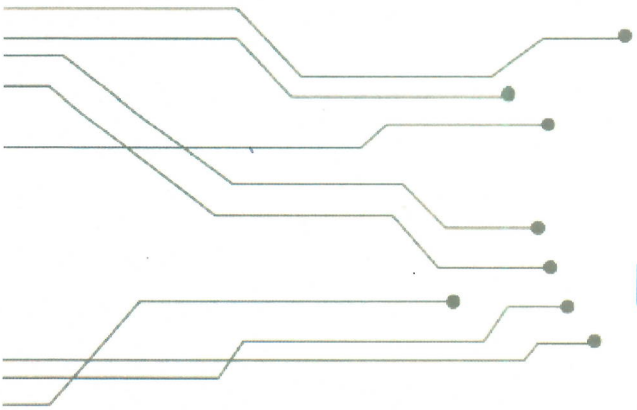
Top Attack Types by Date			
Date	Attack Type	Events	Percent
2021-02-28	Directory Listing	99	66.44
	HTTP Header Leakage	35	23.49
	Bad Robot	4	2.68
	Other(6)	11	7.38
	Subtotal(9)	149	0.11
2021-03-01	Directory Listing	3071	64.56
	HTTP Header Leakage	1354	28.46
	Application Availability/Errors	61	1.28
	Other(26)	271	5.70
	Subtotal(29)	4757	3.50
2021-03-02	HTTP Header Leakage	2741	54.42
	Directory Listing	1927	38.26
	Bad Robot	170	3.38
	Other(21)	199	3.95
	Subtotal(24)	5037	3.71
2021-03-03	Directory Listing	1402	47.82
	HTTP Header Leakage	1165	39.73
	Bad Robot	135	4.60
	Other(17)	230	7.84
	Subtotal(20)	2932	2.16
2021-03-04	Directory Listing	3235	72.94
	HTTP Header Leakage	782	17.63
	Bad Robot	118	2.66
	Other(17)	300	6.76
	Subtotal(20)	4435	3.27
2021-03-05	HTTP Header Leakage	3461	50.97
	Directory Listing	2832	41.71
	Malformed Request	165	2.43
	Other(19)	332	4.89
	Subtotal(22)	6790	5.00
Other(26)		111676	82.25
Total(32)		**135776**	**100.00**

6.3. Top de políticas por porcentaje.



6.4. Top de ataques por URL.

Top Attack URLs		
URL	Events	Percent
/xmlrpc.php	77450	57.04
/cartelera/backend/application.php	17645	13.00
/	17211	12.68
none	2719	2.00
/ap/uedata	1285	0.95
/programacion.php	1232	0.91
Other(6506)	18234	13.43
Total(6512)	**135776**	**100.00**



INFOTEC

Reporte de Incidentes y Solicitudes de Mesa de Servicio

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

MARZO 2021

Información general del documento

Entregable

Clave	Servicio	Medio
MCS-CANAL 22	Mesa de Servicio	Electrónico / Físico

Elaboración

Puesto	Nombre	Firma	Fecha
Coordinador de Mesa de Servicio	Alejandro Rubén de la Cruz		01/04/2021

Revisión

Puesto	Nombre	Firma	Fecha
Líder de Proyecto	Víctor Quiroz Barrientos		01/04/2021

Aprobación

Puesto	Nombre	Firma	Fecha
Subgerente de Centro de Datos y Mesa de Servicio	Lic. Lesli Neri Valderrama		01/04/2021

Recepción Cliente

Puesto	Nombre	Firma	Fecha
Gerente de Tecnologías de la Información	Ing. Juan Pablo Rosas Turanzas		16/04/2021

Aprobación Cliente

Puesto	Nombre	Firma	Fecha
Jefe de Unidad Departamental	Ing. Emilio René García Rodríguez		

Introducción al documento.

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

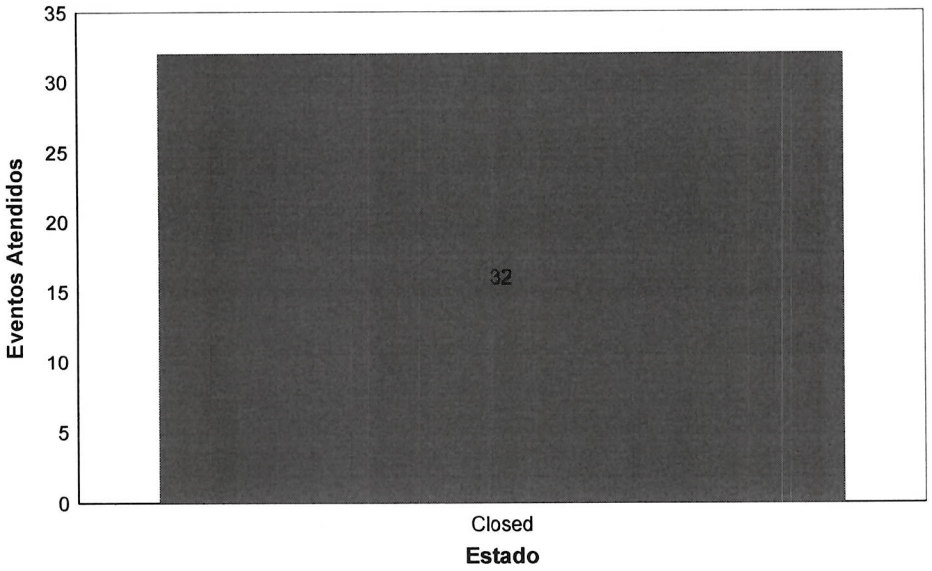
Atentamente.

Mesa Central de Servicios INFOTEC
Dirección Adjunta de Desarrollo Tecnológico.

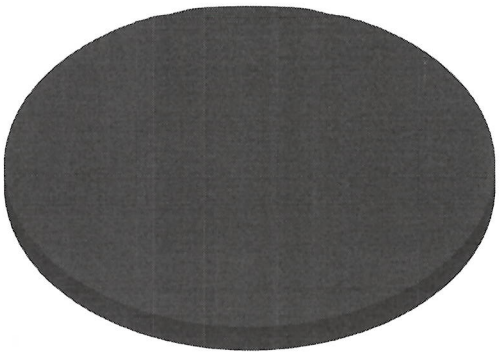
CANAL 22

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

Estado de Eventos



Tipo de Eventos

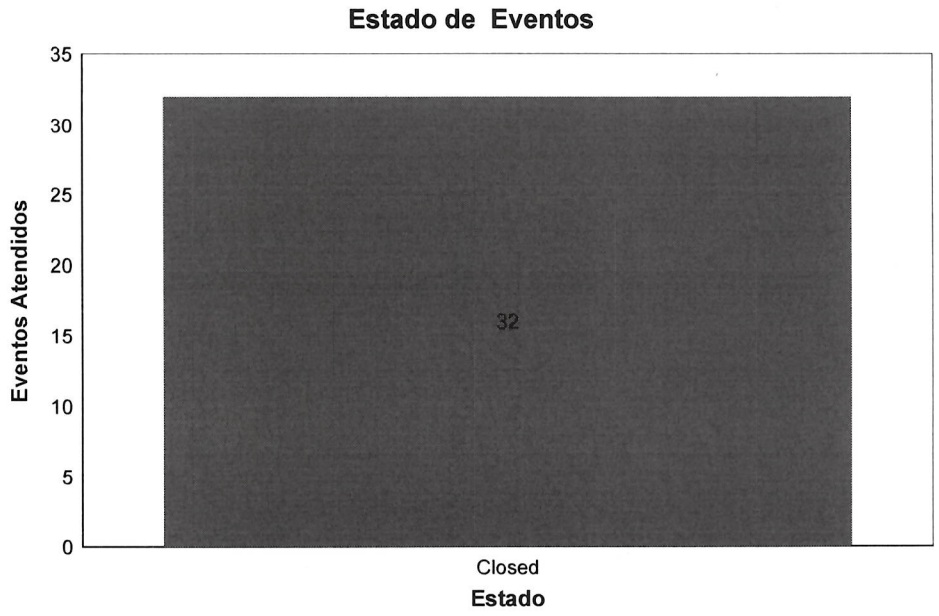


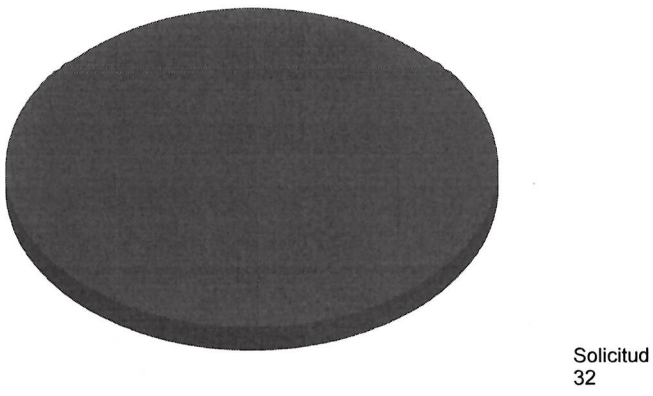
Solicitud
32

Nota:
Solicitud de Servicio se deberá entender como Requerimiento.

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:	Reporte de consumo de ancho de banda-2021-03-01-1000
Descripción: de banda del cliente CANAL 22.	Favor de levantar un TK al área del SOC para la generación del reporte de consumo de ancho
Atendido por:	SANTILLAN MANON, ABRAHAM
Usuario que abre evento:	GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura:	01/03/2021 10:06:18a.m.
Ticket asignado:	TK310156
Medio de contacto:	Correo electronico
Estado evento:	Cerrado
Solución: SOC:	01/03/2021 10:00 Hrs. En atención al evento se reciben comentarios por parte del Área del

Se adjunta el reporte.

Fecha y hora de cierre:	01/03/2021 07:04:12p.m.
Tiempo total del Ticket:	00 08:57:54

Título:	Reporte de consumo de ancho de banda-2021-03-02-1000_CANAL 22
Descripción: de banda del cliente CANAL 22.	Favor de levantar un TK al área del SOC para la generación del reporte de consumo de ancho
Atendido por:	SANTILLAN MANON, ABRAHAM
Usuario que abre evento:	GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura:	02/03/2021 10:11:52a.m.
Ticket asignado:	TK310245
Medio de contacto:	Correo electronico
Estado evento:	Cerrado
Solución: SOC:	02/03/2021 10:00 Hrs. En atención al evento se reciben comentarios por parte del área del

Se adjunta el reporte.

CANAL 22

Detalle de Eventos

Fecha y hora de cierre:	02/03/2021 08:08:47p.m.
Tiempo total del Ticket:	00 09:56:55

Título:	Reporte de consumo de ancho de banda-2021-03-03-1000 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:	03/03/2021 10:13:17a.m.
Ticket asignado:	TK310312
Medio de contacto:	Correo electronico
Estado evento:	Cerrado
Solución:	03/03/2021 10:00 Hrs. En atencion al evento se reciben comentarios por parte de SOC:

Se adjunta el reporte.

Fecha y hora de cierre:	03/03/2021 12:45:32p.m.
Tiempo total del Ticket:	00 02:32:15

CANAL 22

Detalle de Eventos

Título: Alta de Cliente VPN CANAL 22

Descripción:

Solicito su ayuda para dar de alta un cliente VPN con los siguientes datos:

Nombre

Usuario

Contraseña

Acceso IP's

Pedro O. Rodríguez

pedro.rodriguez

p3dr0Rodr1gu3z*

10.100.1.0/24
10.100.10.0/24

Quedo atento a 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:	03/03/2021 11:08:19a.m.
Ticket asignado:	TK310318
Medio de contacto:	Correo electronico
Estado evento:	Cerrado

CANAL 22

Detalle de Eventos

Solución: 03/03/2021 11:27 Hrs. En atención al evento se reciben comentarios del Ing. Efrain Nochebuena de SOC:

Se configuró la nueva cuenta de VPN. Y las políticas de comunicación de acuerdo a la solictud.

Fecha y hora de cierre: 03/03/2021 04:00:05p.m.

Tiempo total del Ticket: 00 04:51:46

Título: Certificado SSL noticias.canal22.org.mx_CANAL 22

Descripción: Solicito su ayuda para realizar el cambio del certificado SSL dentro del WAF para el portal de canal22.org.mx, con el siguiente NAT:

IP Publica

WAF

IP Interna

189.204.131.131

10.0.0.202

172.20.22.10

Adjunto los certificados y la contraseña es canal22*

Quedo al pendiente de cualquier duda o aclaración.

CANAL 22

Detalle de Eventos

Atendido por:	RODRIGUEZ VELAZQUEZ, YURIKA
Usuario que abre evento:	GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura:	03/03/2021 11:29:18a.m.
Ticket asignado:	TK310320
Medio de contacto:	Correo electronico
Estado evento:	Cerrado
Solución:	03/03/21 18:47 Hrs. En atención al evento, se reciben comentarios por parte del Ing. Carlos Lira del SOC: Se realizó la carga del certificado digital correspondiente al dominio www.canal22.org.mx. La carga fue realizada en el equipo WAF. Se enviaron las evidencias correspondientes a través de la mesa de servicio.
Fecha y hora de cierre:	04/03/2021 06:52:20a.m.
Tiempo total del Ticket:	00 19:23:02

Título:	Reporte de consumo de ancho de banda-2021-03-04-1000_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:	04/03/2021 10:09:31a.m.
Ticket asignado:	TK310367
Medio de contacto:	Correo electronico
Estado evento:	Cerrado
Solución:	04/03/2021 10:09 Hrs. En atencion al evento se reciben comentarios por parte de SOC: Se adjunta el reporte.
Fecha y hora de cierre:	04/03/2021 05:54:33p.m.
Tiempo total del Ticket:	00 07:45:02

CANAL 22

Detalle de Eventos

Título: Modificar IP publica para transparencia.canal22.org.mx

Descripción: Solicito de su ayuda para confirmar que la IP homologada 189.204.131.156 no este asignada a ningun servicio, de estar libre sustituir la IP publica del DNS transparencia.canal22.org.mx así mismo ajustar el NAT dentro del Firewall con la finalidad de realizar una modificación de IP Homologada al portal de transparenica.canal22.org.mx , actualmente configurado con el siguiente NAT:

DNS

IP Publica

WAF

IP Interna

transparencia.canal22.org.mx

189.204.131.153

10.0.0.215

172.20.22.13

La actualización en el Firewall, WAF y DNS deberá quedar de la siguiente forma:

DNS

IP Publica

WAF

IP Interna

transparencia.canal22.org.mx

189.204.131.156

CANAL 22

Detalle de Eventos

10.0.0.215

172.20.22.13

Adjunto el archivo para la modificación de DNS.

Atendido por:	SANTILLAN MANON, ABRAHAM
Usuario que abre evento:	GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura:	05/03/2021 10:59:52a.m.
Ticket asignado:	TK310428
Medio de contacto:	Correo electronico
Estado evento:	Cerrado

Solución: 05/03/2021 12:02 Hrs. En atención al evento se reciben comentarios por parte de la Ing. Anabel Jerónimo del SO Linux:

Se actualizo el registro transparencia IN A 189.204.131.153 por transparencia IN A 189.204.131.156

Fecha y hora de cierre:	07/03/2021 12:20:22p.m.
Tiempo total del Ticket:	02 01:20:30

Título:	Reporte de consumo de ancho de banda-2021-03-08-1000_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:	SANTILLAN MANON, ABRAHAM
Usuario que abre evento:	GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura:	08/03/2021 10:02:16a.m.
Ticket asignado:	TK310492
Medio de contacto:	Correo electronico
Estado evento:	Cerrado

CANAL 22

Detalle de Eventos

Solución: 08/03/2021 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: 09/03/2021 10:45:40a.m.
Tiempo total del Ticket: 01 00:43:24

Título: Reporte de consumo de ancho de banda-2021-03-09-1000 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: 09/03/2021 10:10:54a.m.
Ticket asignado: TK310574
Medio de contacto: Correo electronico
Estado evento: Cerrado

Solución: 09/03/2021 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: 09/03/2021 07:13:58p.m.
Tiempo total del Ticket: 00 09:03:04

CANAL 22

Detalle de Eventos

Título: Reporte de consumo de ancho de banda-2021-03-10-1000

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: GUEVARA MORALES, TERESA_.
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 10/03/2021 10:03:11a.m.
Ticket asignado: TK310622
Medio de contacto: Correo electronico
Estado evento: Cerrado

Solución: 10/03/2021 10:10 Hrs. En atención al evento se reciben comentarios por parte del área del SOC:

Se adjunta el reporte.

Fecha y hora de cierre: 11/03/2021 11:19:14p.m.
Tiempo total del Ticket: 01 13:16:03

Título: Reporte de consumo de ancho de banda-2021-03-11-1000

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: SANTILLAN MANON, ABRAHAM
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 11/03/2021 10:06:09a.m.
Ticket asignado: TK310685
Medio de contacto: Correo electronico
Estado evento: Cerrado

CANAL 22

Detalle de Eventos

Solución: 11/03/2021 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: 11/03/2021 11:19:06p.m.
Tiempo total del Ticket: 00 13:12:57

Título: Bloqueo web filter_CANAL 22
Descripción: Les informo que dentro del segmento 10.252.10.0/26 tenemos servidores con sistemas operativos Linux que al realizar actualizaciones arroja un error de bloqueo para las direcciones de los repositorios de actualización por tal motivo solicito su ayuda para agregar una excepción dentro del web filter que permita la conexión a dichos repositorios.

Atendido por: SANTILLAN MANON, ABRAHAM
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 11/03/2021 03:32:13p.m.
Ticket asignado: TK310713
Medio de contacto: Correo electronico
Estado evento: Cerrado

Solución: 12/03/21 09:53: Hrs En atención al evento se reciben comentarios por parte del Ing. Ramses Lopez de SOC:
Se realizo apoyo, se agrego dominio en el webfilter, se valida correcto acceso.

Fecha y hora de cierre: 12/03/2021 10:58:35a.m.
Tiempo total del Ticket: 00 19:26:22

Título: Reporte de consumo de ancho de banda-2021-03-12-1000_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.

CANAL 22

Detalle de Eventos

Atendido por:	SANTILLAN MANON, ABRAHAM
Usuario que abre evento:	GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura:	12/03/2021 10:02:01a.m.
Ticket asignado:	TK310758
Medio de contacto:	Correo electronico
Estado evento:	Cerrado
Solución:	12/03/2021 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:	12/03/2021 12:20:47p.m.
Tiempo total del Ticket:	00 02:18:46

Título:	Reporte de consumo de ancho de banda-2021-03-13-1000_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:	13/03/2021 10:15:51a.m.
Ticket asignado:	TK310814
Medio de contacto:	Correo electronico
Estado evento:	Cerrado
Solución:	13/03/2021 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:	16/03/2021 07:38:40p.m.
Tiempo total del Ticket:	03 09:22:49

CANAL 22

Detalle de Eventos

Título:	Reporte de consumo de ancho de banda-2021-03-14-1000_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:	VAZQUEZ FLORES, LUIS NOE
Usuario que abre evento:	GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura:	14/03/2021 10:07:48a.m.
Ticket asignado:	TK310839
Medio de contacto:	Correo electronico
Estado evento:	Cerrado
Solución:	14/03/2021 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:	16/03/2021 09:53:52p.m.
Tiempo total del Ticket:	02 11:46:04

Título:	Reporte de consumo de ancho de banda-2021-03-15-1000_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:	15/03/2021 10:05:09a.m.
Ticket asignado:	TK310848
Medio de contacto:	Correo electronico
Estado evento:	Cerrado

CANAL 22

Detalle de Eventos

Solución: 15/03/2021 10:06 Hrs. En atención al evento se reciben comentarios del los ingenieros de SOC :

Se adjunta el reporte.

Fecha y hora de cierre: 16/03/2021 07:41:07p.m.
Tiempo total del Ticket: 01 09:35:58

Título: Reporte de consumo de ancho de banda-2021-03-16-1000_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: SANTILLAN MANON, ABRAHAM
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 16/03/2021 10:07:20a.m.
Ticket asignado: TK310872
Medio de contacto: Correo electronico
Estado evento: Cerrado

Solución: 16/03/2021 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: 16/03/2021 07:42:00p.m.
Tiempo total del Ticket: 00 09:34:40

CANAL 22

Detalle de Eventos

Título:	Reporte de consumo de ancho de banda-2021-03-17-1000 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:	17/03/2021 10:24:31a.m.
Ticket asignado:	TK310939
Medio de contacto:	Correo electronico
Estado evento:	Cerrado
Solución:	17/03/2021 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:	17/03/2021 02:54:07p.m.
Tiempo total del Ticket:	00 04:29:36

Título:	Reporte de consumo de ancho de banda-2021-03-18-1000_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:	GONZALEZ CURENO, ROGELIO
Usuario que abre evento:	GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura:	18/03/2021 10:04:58a.m.
Ticket asignado:	TK310983
Medio de contacto:	Correo electronico
Estado evento:	Cerrado

CANAL 22

Detalle de Eventos

Solución: 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: 18/03/2021 10:37:47a.m.
Tiempo total del Ticket: 00 00:32:49

Título: Reporte de consumo de ancho de banda-2021-03-19-1000
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.

Atendido por: GUEVARA MORALES, TERESA_.
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 19/03/2021 10:02:01a.m.
Ticket asignado: TK311034
Medio de contacto: Correo electronico
Estado evento: Cerrado

Solución: 19/03/2021 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: 19/03/2021 02:33:26p.m.
Tiempo total del Ticket: 00 04:31:25

Título: Reporte de consumo de ancho de banda-2021-03-20-1000_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:	20/03/2021 10:02:22a.m.
Ticket asignado:	TK311095
Medio de contacto:	Correo electronico
Estado evento:	Cerrado
Solución:	20/03/2021 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:	21/03/2021 09:57:59p.m.
Tiempo total del Ticket:	01 11:55:37

Título:	Reporte de consumo de ancho de banda-2021-03-21-1000_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:	21/03/2021 10:04:26a.m.
Ticket asignado:	TK311123
Medio de contacto:	Correo electronico
Estado evento:	Cerrado
Solución:	21/03/2021 10:00 Hrs. En atención al evento se reciben comentarios por parte del Área del SOC:

Se adjunta el reporte.

Ingenieros, les informamos que se registró el TK311123, solicitando de su apreciable apoyo para brindar atención al evento que se describe en el correo que antecede.

Fecha y hora de cierre:	21/03/2021 09:59:29p.m.
Tiempo total del Ticket:	00 11:55:03

CANAL 22

Detalle de Eventos

Título:	Reporte de consumo de ancho de banda-2021-03-22-1000 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.

--
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:	22/03/2021 10:22:34a.m.
Ticket asignado:	TK311173
Medio de contacto:	Correo electronico
Estado evento:	Cerrado
Solución:	22/03/2021 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:	22/03/2021 10:39:13a.m.
Tiempo total del Ticket:	00 00:16:39

Título:	Reporte de consumo de ancho de banda-2021-03-23-1000_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.

Atendido por:	SANTILLAN MANON, ABRAHAM
Usuario que abre evento:	GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura:	23/03/2021 10:04:05a.m.
Ticket asignado:	TK311236
Medio de contacto:	Correo electronico
Estado evento:	Cerrado

CANAL 22

Detalle de Eventos

Solución: 23/03/2021 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: 23/03/2021 12:57:28p.m.
Tiempo total del Ticket: 00 02:53:23

Título: Reporte de consumo de ancho de banda-2021-03-24-1000_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: GUEVARA MORALES, TERESA_.
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 24/03/2021 10:03:10a.m.
Ticket asignado: TK311286
Medio de contacto: Correo electronico
Estado evento: Cerrado

Solución: 24/03/2021 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: 24/03/2021 03:08:55p.m.
Tiempo total del Ticket: 00 05:05:45

Título: Reporte de consumo de ancho de banda-2021-03-25-1000_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.

CANAL 22

Detalle de Eventos

Atendido por:	GONZALEZ CURENO, ROGELIO
Usuario que abre evento:	GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura:	25/03/2021 10:11:20a.m.
Ticket asignado:	TK311357
Medio de contacto:	Correo electronico
Estado evento:	Cerrado
Solución:	25/03/2021 10:10 Hrs. En atención al evento se reciben comentarios por parte del Área del SOC:

Se adjunta el reporte.

Fecha y hora de cierre:	25/03/2021 03:45:38p.m.
Tiempo total del Ticket:	00 05:34:18

Título:	Reporte de consumo de ancho de banda-2021-03-26-1000_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:	26/03/2021 10:02:54a.m.
Ticket asignado:	TK311401
Medio de contacto:	Correo electronico
Estado evento:	Cerrado
Solución:	26/03/2021 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:	26/03/2021 12:33:49p.m.
Tiempo total del Ticket:	00 02:30:55

CANAL 22

Detalle de Eventos

Título:	Reporte de consumo de ancho de banda-2021-03-27-1000_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.

Se adjunta el reporte.

Atendido por:	GUEVARA MORALES, TERESA_.
Usuario que abre evento:	GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura:	27/03/2021 10:02:45a.m.
Ticket asignado:	TK311442
Medio de contacto:	Correo electronico
Estado evento:	Cerrado
Solución:	27/03/2021 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:	28/03/2021 10:01:52p.m.
Tiempo total del Ticket:	01 11:59:07

Título:	Reporte de consumo de ancho de banda-2021-03-28-1000
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:	28/03/2021 10:11:03a.m.
Ticket asignado:	TK311460
Medio de contacto:	Correo electronico
Estado evento:	Cerrado

CANAL 22

Detalle de Eventos

Solución: 28/03/2021 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: 28/03/2021 10:19:58p.m.
Tiempo total del Ticket: 00 12:08:55

Título: Reporte de consumo de ancho de banda-2021-03-29-1000
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: 29/03/2021 10:13:56a.m.
Ticket asignado: TK311484
Medio de contacto: Correo electronico
Estado evento: Cerrado

Solución: 29/03/2021 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: 29/03/2021 07:00:20p.m.
Tiempo total del Ticket: 00 08:46:24

CANAL 22

Detalle de Eventos

Título: Reporte de consumo de ancho de banda-2021-03-30-1000_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.

Atendido por: SANTILLAN MANON, ABRAHAM
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 30/03/2021 10:09:12a.m.
Ticket asignado: TK311551
Medio de contacto: Correo electronico
Estado evento: Cerrado

Solución: 30/03/2021 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: 30/03/2021 10:46:06a.m.
Tiempo total del Ticket: 00 00:36:54

Título: Reporte de consumo de ancho de banda-2021-03-31-1000

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: GONZALEZ CURENO, ROGELIO
Usuario que abre evento: GARCIA RODRIGUEZ, EMILIO RENE
Fecha y hora de apertura: 31/03/2021 10:08:14a.m.
Ticket asignado: TK311605
Medio de contacto: Correo electronico
Estado evento: Cerrado

Solución: 31/03/2021 10:16 Hrs. Ingenieros de SOC, solicitamos de su apreciable apoyo para la documentación del Q156580 asignada a su grupo de trabajo, para proceder al cierre del TK

31/03/2021 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:	31/03/2021 12:02:27p.m.
Tiempo total del Ticket:	00 01:54:13

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.